



Andreas Folkers

# **DAS SICHERHEITSDISPOSITIV DER RESILIENZ**

*Katastrophische Risiken und die  
Biopolitik vitaler Systeme*

**campus**

## Das Sicherheitsdispositiv der Resilienz

*Andreas Folkers*, Dr. phil., ist wissenschaftlicher Mitarbeiter am Institut für Soziologie der Universität Frankfurt am Main.

Andreas Folkers

# Das Sicherheitsdispositiv der Resilienz

Katastrophische Risiken und die Biopolitik  
vitaler Systeme

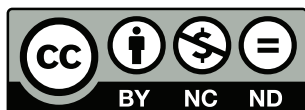
Campus Verlag  
Frankfurt/New York

Die Publikation wurde von der Deutschen Forschungsgemeinschaft gefördert.



Dissertation, Johann Wolfgang Goethe-Universität Frankfurt am Main, 2017, D.30

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Der Text dieser Publikation wird unter der Lizenz Namensnennung-Nicht kommerziell-Keine Bearbeitungen 4.0 International (CC BY-NC-ND 4.0) veröffentlicht. Den vollständigen Lizenztext finden Sie unter: <https://creativecommons.org/licenses/by-nd/4.0/legalcode.de>



Verwertung, die den Rahmen der CC BY-NC-ND 4.0 Lizenz überschreitet ist ohne Zustimmung des Verlags unzulässig. Das gilt insbesondere für die Bearbeitung und Übersetzungen des Werkes. Die in diesem Werk enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Quellenangabe/Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen.

ISBN 978-3-593-50879-5 Print

ISBN 978-3-593-43850-4 E-Book (PDF)

DOI 10.12907/978-3-593-43850-4

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung ist ohne Zustimmung des Verlags unzulässig. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen. Trotz sorgfältiger inhaltlicher Kontrolle übernehmen wir keine Haftung für die Inhalte externer Links. Für den Inhalt der verlinkten Seiten sind ausschließlich deren Betreiber verantwortlich.

Copyright © 2018 Campus Verlag GmbH, Frankfurt am Main

Umschlaggestaltung: Campus Verlag GmbH, Frankfurt am Main

Umschlagmotiv: © Flo Maak, ohne Titel, aus der Serie DANGER, 2015.

Gesetzt aus: Garamond

Druck und Bindung:

Printed in Germany

[www.campus.de](http://www.campus.de)

# Inhalt

Vorwort.....	9
Einleitung.....	15
1. Analytik des Sicherheitsdispositivs.....	29
1.1. Von der Risikosoziologie zur Analytik der Sicherheit.....	30
1.2. Die Achsen der Dispositivanalyse.....	42
1.2.1. Problematisierung: Jenseits von Konstruktivismus und Realismus.....	44
1.2.2. Von der Institution zur Technologie.....	48
1.2.3. Von der Funktion zur Strategie.....	53
1.3. Genealogie der Sicherheitsdispositive.....	57
1.4. Thematische Fokussierung und Forschungsdesign.....	72
1.4.1. Thematische Fokussierung.....	72
1.4.2. Materialauswahl.....	79
1.4.3. Auswertung des Materials.....	87
2. Die Regierung der Katastrophe.....	96
2.1. <i>Problematisierung</i> : Neuerhandlung des Katastrophen- und Zivilschutzes.....	99
2.1.1. Das Ereignis des 11. September.....	100
2.1.2. »Katastrophen kennen keine Grenzen«: Kritik des deutschen Katastrophenföderalismus.....	104
2.1.3. Vom »Gießkannenprinzip« zur Risikozone.....	109
2.2. <i>Institutionalisierung</i> : Bevölkerungsschutz als »Neue Sicherheitsstrategie«.....	116

2.2.1. Die »Neue Strategie zum Schutz der Bevölkerung in Deutschland« .....	117
2.2.2. Das BBK als »Zentralstelle und Netzknoten«.....	119
2.2.3. Ereignisorientierung und ambulante Gouvernamentalität.....	124
2.2.4. »Vernetzte Sicherheit« oder Sicherheitsdispositiv?.....	128
2.3. <i>Zeit und Raum</i> : Die Analyse katastrophischer Risiken.....	133
2.3.1. Die »bundesrelevante Katastrophe« .....	135
2.3.2. Die Risiko-Matrix: Zeit und Nichtwissen in der Risikoanalyse ...	138
2.3.3. Verwundbarkeitskartierung: Der Raum der Katastrophe .....	146
2.4. <i>Gegenstand</i> : Das »System« als Schutzobjekt und Gefährdungszusammenhang.....	154
2.4.1. Der Aufstieg des systemischen Risikos .....	156
2.4.2. Das »system of systems« als Horizont des Sicherheitsdispositivs	161
2.4.3. Sektorspezifische Systemrisiken .....	165
2.4.4. Systemische Finanzmarktrisiken.....	170
2.4.5. Problemtransfer im Sicherheitsdispositiv .....	175
2.5. <i>Norm</i> : Resilienz als Antwort auf systemische Gefährdung.....	179
2.5.1. Von der Normalität zur Normativität: Resilienz bei Holling.....	181
2.5.2. Reserven, Puffer, Redundanzen: Resilienz durch Vorratshaltung	186
2.5.3. Resilienz durch Gestaltung der Systemarchitektur.....	197
2.5.4. Evolutionäre Resilienz und die Kritik der Sicherheit.....	201
2.5.5. Das Sicherheitsdispositiv der Resilienz .....	209
Exkurs zur Gesellschaft: Selbstgefährdung und Selbstbeschreibung..	214
3. Der Schutz vitaler (Öko)systeme.....	222
3.1. Von der Daseinsvorsorge zum Schutz Kritischer Infrastruktur .	226
3.1.1. Die Vorsorgemaschine in der Vitalsphäre: Daseinsvorsorge bei Ernst Forsthoff.....	229
3.1.2. Von der Daseinsvorsorge zum Gewährleistungsstaat.....	243
3.1.3. Kritische Infrastruktur: Versorgungssicherheit im Gewährleistungsstaat .....	249
3.2. Von der großen zur grünen Infrastruktur? .....	260
3.2.1. Ausweitung der Vorsorgezone: Die Genese des <i>precautionary principle</i> .....	263

3.2.2. Deichgrafendämmung: Kritik hydraulischer Gouvernementalität .....	273
3.2.3. Zwischen Vorbeugung und Vorbereitung: Anpassungen an die neue Klimanormalität .....	281
3.2.4. Ökologische <i>life support systems</i> : Grüne Infrastruktur und das Erdsystem .....	290
3.3. Energiesicherheit: Vom Atomstaat zur Energiewende .....	300
3.3.1. Der nukleare Notstand: Der Atomstaat als Sicherheitsrisiko .....	303
3.3.2. Atommacht oder <i>Brittle Power</i> ? Widerstandskräfte im Energiesystem .....	311
3.3.3. Vom GAU zum Problem Versorgungssicherheit .....	319
3.3.4. Der <i>blackout</i> als »Verbundkatastrophe« .....	329
3.3.5. Technologie der Resilienz und Resilienz der Technologie .....	333
Exkurs zur Biopolitik: Politik des Lebens jenseits seiner selbst .....	343
4. Kontinuitätsmanagement: Betriebliche Katastrophenvorsorge .....	353
4.1. Geschichte und Gegenwart des Kontinuitätsmanagements .....	356
4.1.1. Der Aufstieg des Kontinuitätsmanagements im Kalten Krieg .....	357
4.1.2. Protokollarische Souveränität .....	364
4.1.3. Vom IT disaster recovery zum Business Continuity Management .....	369
4.2. Krisenroutine: Die Organisation des Notfalls im BCM .....	372
4.2.1. Standardisierung und Globalisierung des BCM .....	373
4.2.2. Die Vordringlichkeit des Zeitkritischen .....	377
4.2.3. Krise der Entscheidung, Krise der Hierarchie .....	381
4.2.4. Betriebswirtschaftliche Kalküle im Kontinuitätsmanagement .....	384
4.2.5. Autopoiesis jenseits gewohnter (Infra)Strukturen .....	389
4.3. Kontinuitätsmanagement im Finanzsektor .....	395
4.3.1. Operationelles Risiko als Grenzobjekt .....	397
4.3.2. BCM als globales Sicherheitsgefüge .....	401
4.3.3. Sicherung der Finanzinfrastrukturen .....	408
4.4. Management der Kontinuität, Politik des Ereignisses .....	416
4.4.1. Krise, Kritik und Kontinuität: Ereignisse im Raster des BCM .....	417
4.4.2. Ein Sturm im Finanzdistrikt: Hurricane Sandy in New York .....	421



4.4.3. Disruptive Demokratie: Blockupy in Frankfurt .....	428
Exkurs zur Zeit: »dass es so weitergeht...« .....	438
Fazit .....	448
Abkürzungen .....	469
Interviews .....	472
Literatur .....	473

# Vorwort

Sicherheit wird immer mehr zur zentralen Wertvorstellung westlicher Gesellschaften. Darin mag man ein Zeichen dafür sehen, dass wir in Zeiten politischer Resignation leben. Gewerkschaften und linke Parteien kämpfen nicht mehr gegen Ausbeutung und für die Aneignung der Produktionsmittel, sondern gegen Prekarisierung und für sichere Renten. Die Solidarität mit revolutionären Befreiungsbewegungen in Ländern des globalen Südens ist der Angst vor islamistischem Terrorismus gewichen. Die Beschwörung einer »Revolte der Natur« (Horkheimer 1967, 63–92) ist dem Eintreten für Klimaschutz zur Erhaltung des »safe operating space for humanity« (Rockström et al. 2009) gewichen. Wo die Aussicht auf globale Gerechtigkeit in weite Ferne gerückt ist, erscheint lediglich die humanitäre Forderung nach Sicherheit und Schutz für Geflüchtete halbwegs realistisch. Wenn sich die Glaubensgänger\_innen des Christentums damit abgefunden haben, dass die Erlösung in ein fernes Jenseits abgeschoben wurde, weil sich die fürsorgliche *caritas* zumindest der ärgsten irdischen Nöte annimmt, so scheinen wir uns damit arrangiert zu haben, auf allzu jenseitige Werte wie Freiheit und Gerechtigkeit zu verzichten, solange man uns nur mit ausreichend politischen, rechtlichen und ökonomischen Sicherungen versieht. Selbst die Kritik an den Auswüchsen der Sicherheit in Form staatlicher und privatwirtschaftlicher Überwachung kommt meist als Einklagung und Verteidigung der Datensicherheit oder des Schutzes der Privatsphäre, also ihrerseits als Ruf nach Sicherheit daher. Das Begehren nach Sicherheit, so scheint es, macht einen bestenfalls zur Merkelwählerin, schlimmstenfalls zum »besorgten Bürger«.

Es liegt deshalb aus kritischer sozialwissenschaftlicher Perspektive nahe, Sicherheit als Zielvorstellung per se abzulehnen, um wieder einen genuin politischen Möglichkeitshorizont zu eröffnen (Neocleous 2008). Es soll wieder um Demokratie und Gleichheit gehen und nicht nur um die Sicherung des Lebens. Dieses Buch setzt allerdings einen anderen Akzent. Es

versucht nicht, das Politische gegen das Streben nach Sicherheit auszuspielen, sondern will vielmehr die Politik der Sicherheit selbst beleuchten und zeigen, was bei dieser Politik auf dem Spiel steht. Sicherheit ist nicht nur eine Ablenkungsstrategie von Regierenden, nicht nur ein Trostpreis für politisch Resignierte, sondern fundamentaler Anspruch eines Lebens, dessen grundlegende Eigenschaft darin liegt, verwundbar und deshalb schutzbedürftig zu sein (Butler 2004). Wer das nicht wahrhaben will und stattdessen auf hochtrabenden politischen Programmatiken beharrt, reproduziert damit nur eine fatale Vorstellung politischer Subjektivität, die vollkommen bedürfnislos und autonom die politische Sphäre betritt, und lässt zudem die Ansprüche und Motivlagen faktisch handelnder politischer Subjekte außer Acht. Aber gerade weil Sicherheit ein so grundlegendes Bedürfnis des prekären Lebens ist, ist sie auch gefährlich. Das Verlangen nach Sicherheit lässt sich nämlich auf vielfältige Weise missbrauchen und ausbeuten. Nicht selten gehen Sicherheitsmaßnahmen deswegen mit neuen Formen sozialer Kontrolle und maßloser politischer Macht einher.

Dieses Buch untersucht diese Ambivalenz der Sicherheit zwischen sozialer Kontrolle und lebenswichtigem Anspruch am Fall der Sicherheitsmaßnahmen gegen katastrophische Risiken. Nirgendwo sonst wird die Verwundbarkeit des Lebens so sichtbar wie etwa nach Naturkatastrophen, die einer Vielzahl von Menschen auf einen Schlag ihr Leben, ihre Gesundheit oder ihre mühsam errichtete Lebensgrundlage nehmen. Nichts nutzt die Verwundbarkeit der Bevölkerung so schamlos und brutal aus wie Terroranschläge. Und nichts lässt sich so gut von Politiker\_innen nutzen wie ebendiese Anschläge, um ihren Ruf nach immer neuen Verschärfungen von Sicherheitsgesetzen Gehör zu verschaffen. Das Buch beschäftigt sich aber nicht nur mit diesen offensichtlichen Fällen des Katastrophischen, die regelmäßig viel Medienaufmerksamkeit auf sich ziehen und politische Debatten generieren. Es konzentriert sich zudem auf eine tiefe Schicht von Sicherungsmaßnahmen, die nicht nur gegen äußere Gefahren schützen, sondern das Leben, wie wir es kennen, überhaupt erst ermöglichen. Unter dem Überbegriff der »Biopolitik vitaler Systeme« beleuchtet das Buch eine Reihe von uns mittlerweile so selbstverständlich gewordenen Formen der Versorgungssicherheit und der technischen Sicherung wie fließendes Wasser, Strom- und Gesundheitsversorgung etc., die uns zumeist überhaupt erst dann ins Bewusstsein treten, wenn sie – ausgelöst durch externe katastrophische Ereignisse oder interne systemische Risiken – gestört oder nicht mehr verfügbar sind. Und weil in diesen Momenten offensichtlich

wird, wie abhängig Gesellschaften von den vielfältigen lebenserhaltenden Systemen geworden sind, ist der Systemzusammenbruch in jüngerer Zeit zur zentralen Figur des Katastrophischen aufgestiegen.

Katastrophische Risiken wie Terroranschläge und Naturgefahren ebenso wie systemische Risiken wie der Ausfall lebenswichtiger Infrastrukturen oder der Zusammenbruch des Finanzmarktes stellen das politische Versprechen der Sicherheit dabei immer wieder in Frage. Der in den letzten Jahren verstärkte Bezug auf das Konzept der Resilienz reagiert auf diese Verunsicherung und begleitet das zum Mantra gewordene Eingeständnis, dass es »keine hundertprozentige Sicherheit« gibt. Resilienz ist ein verändertes Leitbild der Sicherheit, bei dem weniger die vollkommene Abwesenheit von Gefahren angestrebt wird, sondern der erfolgreiche Umgang mit Risiken im Vordergrund steht. Auch dieses Leitbild der Sicherheit ist ambivalent, weil es einerseits reflexiven Abstand von überzogenen Ansprüchen und fatalen Paradoxien der Sicherheit nimmt, andererseits aber auch droht, die Abweisung von Schutzansprüchen der verwundbarsten Teile der Bevölkerung vorzubereiten.

Dieses Buch ist in den vergangenen sowohl persönlich wie politisch durchaus unsicheren Zeiten entstanden. Dass es schließlich doch in den sicheren Hafen dieser Publikation eingefahren ist, habe ich einer Reihe von Personen und Institutionen zu verdanken. Zuerst möchte ich der Studienstiftung des deutschen Volkes für die finanzielle und ideelle Förderung des Promotionsprojekts sowie meines Auslandsaufenthaltes in New York danken. Ebenso möchte ich der Deutschen Forschungsgemeinschaft danken, die diese Veröffentlichung mit einer großzügigen Publikationsbeihilfe unterstützt hat. Meinen nunmehr ehemaligen Mitbewohnern Bernhard, Boris, David und Flo danke ich für den nicht minder wichtigen häuslichen *support*. Flo Maak danke ich besonders dafür, dass er eine Fotografie seiner Serie »danger« als Titelbild für dieses Buch zur Verfügung gestellt hat. Isabell Trommer vom Campus-Verlag danke ich für ihre geduldige und aufmerksame Betreuung der Veröffentlichung.

Ich danke natürlich meinem Betreuer Thomas Lemke für die Betreuung des Projekts. Ebenso danke ich Peter Wehling, der mich als Zweitgutachter substantiell beraten und mit seinen kritischen Kommentaren wesentlich zur Schärfung der Argumentation der Arbeit beigetragen hat. Dem Drittgutachter Sven Opitz danke ich dafür, dass er mich stets als Wissenschaftler auf Augenhöhe ernstgenommen und gefördert hat. Ich danke meinen

Kolleg\_innen vom Arbeitsbereich in Frankfurt für die vielen produktiven Diskussionen der vergangenen Jahre: Sarah Dionisius, Torsten Heine- mann, Katharina Hoppe, Ulrike Manz, Tino Plümecke, Malaika Rödel, Jonas Rüppel und Susanne Schultz. Besonders bedanken möchte ich mich bei Renate Uhrig, die mir aus dem Sekretariat immer wieder dabei geholfen hat, den Alltag in der Uni zu meistern. Neben dem Arbeitsbereich haben besonders die *STS discussion group*, die Abteilung Wissen, Technik, Umwelt und meine Mitstreiter\_innen der Graduiertenkonferenzen »Emerging Forms of Sociality« und »Critical Matter« dazu beigetragen, dass ich in Frankfurt so viele spannende Diskussionen führen konnte, die auf die eine oder andere Weise Niederschlag in der Arbeit gefunden haben.

Als ich angefangen habe diese Dissertation zu schreiben, war das Institut für Vergleichende Irrelevanz noch im Kettenhofweg be(un)heimatet. Das *ivi* hat mir immer das Gefühl gegeben, dass meine Arbeit auch jenseits der Akademie eine Bedeutung hat. Das gilt auch für meine Tätigkeit in der Redaktion des *diskus*, wo ich erste Überlegungen zur Regierung der Katastrophe veröffentlicht und mit den Genoss\_innen der Redaktion debattiert habe. Ich hoffe, dem kritischen Ethos dieser fabelhaften Frankfurter Subkultur, der vom vollkommen unzeitgemäßen Glauben lebt, dass sich denkend die Welt wenn schon nicht verbessern, so doch zumindest besser ertragen lässt, in meiner Arbeit zumindest ein Stück weit gerecht geworden zu sein. Etwas von diesem Ethos habe ich auch bei vielen meiner Studierenden wiedergefunden. Ich habe in unseren Seminaren viel von ihnen gelernt und bin ihnen dafür sehr dankbar.

In der frühen Phase der Bewerbung um Förderung für das Projekt hatte ich das Glück, hilfreiche Hinweise von Urs Stäheli und Jörg Strübing als Gutachter der Studienstiftung, von Ilona Ostner als Vertrauensdozentin der Heinrich-Böll-Stiftung sowie von Andreas Reckwitz vom Graduiertenkolleg »Lebensformen und Lebenswissen« zu erhalten. Besonderer Dank gilt Stephen Collier, der so großzügig war mich als *visiting scholar* an die New School University einzuladen, ohne dass ich zum damaligen Zeitpunkt nennenswerte wissenschaftliche *credentials* hätte vorweisen können. In zahllosen Diskussionen in Frankfurt und New York habe ich mit ihm über sachliche Aspekte der Arbeit, methodische Zugänge und kritische Perspektiven diskutieren können. Während meines Aufenthalts in New York haben zudem Gespräche mit Nicholas Langlitz, Onur Ozgöde, Timothy Mitchell, Antina von Schnitzler und Ann Stoler für viele Impulse und Inspirationen gesorgt, von denen die Arbeit entscheidend profitiert

hat. Beim PhD-Workshop »Foucault, Governmentality, Biopolitics – Analytical strategies for critique of power« an der Copenhagen Business School konnte ich mit den Leitern Jeffrey Bussolini, Mitchell Dean, Thomas Dumm, Marius Gudmand-Høye und Kaspar Villadsen sowie mit den anderen PhD-Kandidat\_innen über ihre Promotionsprojekte und mein eigenes Projekt diskutieren und dabei wichtige Ideen für die Arbeit entwickeln.

Außer meinen Betreuern haben folgende Personen Teile der Arbeit gelesen und kommentiert: Endre Dányi, Torsten Heinemann, Katharina Hoppe, Martina Kolanoski, Il-Tschung Lim, Peter Lindner, Sven Opitz, Julian Stenmanns und Matthias Thiemann. Sie haben mich durch ihre intensive und kritische Lektüre vor Fehlern bewahrt, zu Klarstellungen und zur Schärfung der Argumentation gezwungen, mich aber auch in entscheidenden Punkten ermutigt und bestärkt. Das gesamte Manuskript hat Nadine Marquardt gelesen, kommentiert, korrigiert und kritisiert. Ihr gilt mein größter Dank – wenn sich das denn skalieren ließe. Kein Gedanke dieser Arbeit, der nicht ihr kluges Ohr und waches Urteil passiert hat. Danke für die Sorge und Sorgfalt um die Arbeit und ihren Autor. Meinen Eltern Gernot und Sabine Folkers danke ich dafür, das gesamte Manuskript Korrektur gelesen zu haben.

Gewidmet ist die Arbeit Sabine, die um den Wert der Sicherheit weiß, sich aber nie ihren Mut, ihren Verstand und ihre Herzlichkeit hat nehmen lassen, und Gernot, dem ich nicht erklären muss, dass Politik, Natur und Technik zusammengehören.



# Einleitung

Eine Vielzahl humanitärer, ökologischer, sozialer und ökonomischer Krisen und Katastrophen hat das noch junge 21. Jahrhundert heimgesucht. Der 11. September 2001 eröffnete eine Serie verheerender Terroranschläge in allen Teilen der Welt. Die globalen Finanzkrisen seit 2007, die ursprünglich von den US-amerikanischen Immobilienmärkten ausgegangen waren, haben wesentlich zur längst noch nicht überwundenen Staatsschuldenkrise in der Eurozone beigetragen. Die Explosion der BP-Ölplattform *deepwater horizon* im Jahr 2010 und die darauffolgende Ölpest im Golf von Mexiko ist eine der schwersten Umweltkatastrophen der Geschichte. Ein Jahr später, im März 2011, hat die Dreifachkatastrophe aus Erdbeben, Tsunami und GAU im Atomkraftwerk von Fukushima auf fatale Weise die Verwundbarkeit sozio-technischer Strukturen gegenüber Naturereignissen unterstrichen. Die Ebola-Epidemie im Jahr 2014 in Westafrika hat gezeigt, wie intensiver Personenverkehr und schlechte Gesundheitsinfrastrukturen zu einer bedrohlich-schnellen Ausbreitung von tödlichen ansteckenden Krankheiten beitragen können. In den letzten fünfzehn Jahren haben sich in allen Teilen der Welt und nicht zuletzt in Deutschland derartig viele als »Jahrhundertereignisse« klassifizierte Hochwasser- und Flutkatastrophen ereignet, dass sich immer stärker der Verdacht aufdrängt, dass wir es hier bereits mit den Auswirkungen des Klimawandels, der ultimativen planetarischen Katastrophe, zu tun haben. Mit geradezu imperativer Gewalt haben diese und andere Katastrophen und Krisenereignisse das politische Handeln bestimmt. Regierungen sind von immer neuen Krisenfällen bisweilen buchstäblich überschwemmt worden, so dass sie aus den Gehäusen ihrer bürokratischen Routinen heraustreten mussten. Szenarien über mögliche, teilweise weit entfernte katastrophische Zukünfte bestimmten immer häufiger politische Entscheidungen in der Gegenwart. Gleichzeitig forderten tatsächlich eintretende Ereignisse eine augenblickliche, unmittelbare Reaktion. Langfristige Planung weicht hier kurzfristigem Krisenmanagement,



das in nicht enden wollenden Krisen wiederum zum Dauermodus der Politik zu werden scheint.

Über die Zeit haben sich jedoch Handlungsmuster und Strategien der Krisenpolitik herauskristallisiert, in denen mehr gesehen werden muss als blinde Reaktionen auf immer neue Unglücksereignisse. Die Krisen der Routine haben zum Entstehen neuer Routinen der Krise geführt.<sup>1</sup> Die Regierung von Katastrophen hat sich als Politikstil und Tätigkeitsfeld mit eigenen Rationalitäten, Interventionsmustern und Legitimationsstrategien herausgebildet. Es reicht daher nicht, das Regieren der Krise lediglich als Abweichung von einer Normalversion politischen Handelns zu beschreiben, um mit Max Weber (2006, 610) weiterhin darauf zu beharren, dass Politik doch eigentlich im »langsamen Bohren von harten Brettern mit Leidenschaft und Augenmaß« bestehe. Als Regierungsstil eigenen Rechts erheischt die Regierung von Krisen und Katastrophen eine eigenständige soziologische Aufmerksamkeit, die ihr in dieser Arbeit zuteilwerden soll.

Ulrich Beck hatte bekanntlich schon in den 1980er Jahren darauf aufmerksam gemacht, dass das Auftauchen neuer und katastrophischer Risiken Politikformen Raum gegeben hat, die sich nicht mehr unter Rückgriff auf die klassischen Annahmen der politischen Soziologie begreifen lassen (Beck 1986). Sub-Politik ergänzt die professionelle Politik in bürokratischen Apparaten, Reflexivität tritt an die Stelle von Technokratie (Beck 1993), perennierendes Nichtwissen düpiert wissenschaftliche Experten (Beck und Wehling 2012), Weltpolitik drängt den Nationalstaat als Raum des Politischen zurück (Beck 2008, Beck und Grande 2010). Unbeirrt hat Beck an diesen Diagnosen auch im 21. Jahrhundert festgehalten. Das Auftauchen von Weltrisiken – vom internationalen Terrorismus über den Klimawandel bis hin zur Finanzkrise – eröffnet die Möglichkeit für einen anderen Umgang mit Risiken und neue Formen der Kosmopolitik. Diese Kosmopolitik schwört der bloßen Verwaltung von Risiken ab, während sie zugleich zu neuen, transnationalen und reflexiven Formen der Sozialität findet (Beck 2008).

Der faktische Umgang mit exzeptionellen, katastrophischen Ereignissen insbesondere seit dem 11. September 2001 wies allerdings allzu oft ein ganz anderes politisches Handlungsmuster auf, das eher Analyseansätzen recht zu geben schien, die auf ganz und gar nicht reflexiv-kosmopolitische Tendenzen kontemporären Regierens im Krisenmodus hingewiesen haben.

---

1 So der glückliche Titel des Soziologiekongresses 2014 in Trier.

Die sozialwissenschaftlichen *Security Studies* zeigen, dass die Politik im Angesicht von »existential threats« (Buzan, Wæver und De Wilde 1998, 24) zwar tatsächlich klassische Modi des Risikomanagements hinter sich lässt, an deren Stelle jedoch nicht Kosmopolitik, sondern drastische Maßnahmen der *securitization* setzt (zur Unterscheidung von *risk management* und *securitization* siehe: Munster 2005). Mit exzeptionellen Maßnahmen, die nicht selten die Regeln des Rechtsstaats und des Völkerrechts strapazieren, soll ebenso exzeptionellen und existenziellen Bedrohungen wie kriegerischen Konflikten oder Terrorismus begegnet werden. Gerade die Maßnahmen des sogenannten »Kriegs gegen den Terror« haben in diesem Zusammenhang viel sozial- und kulturwissenschaftliche Aufmerksamkeit auf sich gezogen: präventive Kriegsführung (Massumi 2007), umfassende Überwachung der Bevölkerung (Amoore und de Goede 2005), Politik der Ausnahmezustände (Agamben 2004), extraterritoriale Gefangenenlager (Aradau 2007) oder das *targeted killing* von Terroristen (Krasmann 2012) sind zu bevorzugten Gegenständen kritischer Analysen und Theorien geworden. Nicht reflexive Kosmopolitik, sondern eine »illiberale Gouvernamentalität« (Opitz 2008) sei typisch für die Reaktionen auf katastrophische Bedrohungen: eine Art der Regierung in liberalen Staaten, die versucht, die politische und ökonomische Verfassung offener Gesellschaften durch Maßnahmen zu sichern, die dieser Verfassung eigentlich widersprechen (siehe dazu auch: Bigo und Tsoukala 2008).

Die Krise des Nationalstaats eröffnet, anders als in Becks Vision der Kosmopolitik, also nicht die Bühne für eine demokratische Weltinnenpolitik, sondern verräumlicht sich in extra-territorialen Zonen (Opitz und Tellmann 2012) und Lagern (Agamben 2002, Hailey 2009), in denen Menschen- und Bürgerrechte eingeschränkt oder ausgesetzt werden. Während Beck die optimistische Auffassung vertreten hatte, dass mit den neuen globalen Risiken auch neuen demokratischen Politikformen der Weg geebnet wird, haben die Theoretiker\_innen des Ausnahmezustands, allen voran Giorgio Agamben (2004, 7–41), ein düsteres Szenario entworfen, in dem die Politik der Ausnahmezustände zum neuen »Paradigma des Regierens« wird.<sup>2</sup>

Jenseits von illiberaler Versicherheitlichung oder reflexiver Kosmopolitik, für die sich gewiss jeweils eine Reihe von empirischen Anhaltspunkten finden lassen, hat sich aber noch ein dritter Modus der Regierung von

---

<sup>2</sup>Für einen Versuch, beide Debattenstränge aufeinander zu beziehen, siehe: Holzinger, May und Pohler (2010).

Katastrophen herausgebildet, der weder ins Schema der düsteren Kritik des Ausnahmezustands noch der hoffnungsvollen Beschwörungen einer zweiten Moderne passt.<sup>3</sup> So wurden in einer Reihe westlicher Staaten Kapazitäten und Institutionen aufgebaut, die nicht primär darauf zielen, Katastrophen zu vermeiden, sondern vor allem darauf, sie besser zu bewältigen. Nicht die Vorbeugung von Ereignissen – entweder durch reflexive Vorsicht und Handlungsverzicht (*precaution*) (Sunstein 2007) oder durch immer drastischere Sicherheitsmaßnahmen, die proaktiv Gefahrenquellen ausschalten (*preemption*) (Massumi 2007) –, sondern die Vorbereitung (*preparedness*) (Lakoff 2007) auf Ereignisse steht hier im Vordergrund (zur Unterscheidung von *precaution*, *preemption* und *preparedness* siehe: Anderson 2010). Potenziell katastrophische Schadensereignisse, die niemals gänzlich abzuwenden sind, sollen nicht durch Ursachenbekämpfung, sondern durch Folgenkontrolle gemindert und dadurch regiert werden. Der vorsorgliche Aufbau von Strukturen soll dazu dienen, die Widerstandskraft und Krisenfestigkeit der Gesellschaft zu erhöhen, nicht dazu, sie von allen Gefahren abzuschirmen. Um eine Politik zu plausibilisieren, die sich vom Streben nach hundertprozentiger Sicherheit verabschiedet hat, wird immer wieder das schillernde Konzept der Resilienz angeführt,<sup>4</sup> verstanden als die Fähigkeit eines Systems, erfolgreich auf Störungen zu reagieren. Die Regierung der Katastrophe durch Vorbereitung ist weniger spektakulär als die Politik der Ausnahmezustände und Militäreinsätze und zumeist weniger öffentlich als Weltklimagipfel und UNO-Vollversammlungen. Hier geht es um Ersthelfer\_innen und Hilfskapazitäten, um Übungen des Katastrophenfalls, um den Aufbau von redundanten Infrastrukturen und Ressourcen, die Katastrophen abfedern können. Es geht um technische Fragen, robuste Architekturen und widerstandsfähiges Systemdesign. Nichtsdestotrotz geht es auch hier um die Vorbereitung auf *existential threats*, die ebenso bedrohlich wie ungewiss sind. Es geht um Katastro-

---

3 Ein weiterer Forschungsstrang, der sich der Verschränkung von militärischen und humanitären Interventionen gewidmet hat, lässt sich weniger jenseits, sondern vielmehr zwischen den Polen Kosmopolitik vs. Ausnahmezustand verorten. Siehe dazu: Fassin und Pandolfi (2010), Fassin (2012), Redfield (2013).

4 Auch jenseits der Regierung der Katastrophe ist Resilienz zu einem zentralen Konzept geworden (siehe: Endreß und Maurer 2014). Gerade in der klinischen Medizin und der Psychologie erfreut sich das Resilienzdenken großer Beliebtheit. Diese Arbeit konzentriert sich allerdings vor allem auf Konzepte und Praktiken der Steigerung systemischer Resilienz im Kontext der Regierung der Katastrophe und lässt den Themenbereich subjektiver Resilienz (siehe dazu etwa: O'Malley 2010, Leanza 2015) außen vor.

phenlagen, die sich über institutionelle, territoriale und geographische Grenzen hinaus ausbreiten und damit zugleich die Grenzen von innerer und äußerer Sicherheit verschwimmen lassen.

Hier setzt dieses Buch ein. Es untersucht die Formen der Regierung der Katastrophe jenseits von Ausnahmezustand und Kosmopolitik, die mit Konzepten wie Resilienz und Katastrophenvorbereitung in Verbindung stehen. Es geht hier also weniger um die schrillen Grenzphänomene der Krisenpolitik, sondern um historische Veränderungen von Wahrnehmungs-, Denk- und Handlungsweisen bei der Reaktion und Vorbereitung auf Katastropheneignisse. Damit schließt die Arbeit an eine jüngere interdisziplinäre und internationale Debatte um die Regierung der Katastrophe und Resilienz an (Lakoff 2007, Collier 2008, Lentzos und Rose 2009, Cooper und Walker 2011, Adey und Anderson 2012, Kaufmann 2012, Bröckling 2012, Corry 2014, Braun 2014, Collier und Lakoff 2015). In der bisherigen Debatte um Resilienz und *preparedness* wurde bereits das Aufkommen neuer und neu ausgerichteter Institutionen etwa seit der Jahrtausendwende nachgezeichnet, die sich auf die Bekämpfung von Katastrophen mit beliebigen Quellen – menschliche Handlungen, technisches Versagen, Naturgefahren – spezialisiert haben: etwa das Departement of Homeland Security in den USA, das Civil Contingencies Secretariat in Großbritannien oder das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe in Deutschland. Innerhalb dieser Institutionen haben sich neue Antizipations- und Interventionstechniken ausgebildet, die Katastrophen wenn auch nicht unbedingt beherrschbar, so doch in einer bestimmten Weise regierbar machen sollen. Allerdings konzentriert sich die Forschung bisher zumeist auf Entwicklungen in Großbritannien und den USA und ist zudem vor allem von den Politikwissenschaften, der Anthropologie und der Geographie geprägt. Die neuen Rationalitäten der Regierung von Katastrophen in Deutschland sind bisher nur ansatzweise analysiert worden (Kaufmann 2011), genauso wie eine soziologische Analyse neuer Praktiken der Sicherheit im Angesicht von Katastrophen noch in den Kinderschuhen steckt. An dieser doppelten Leerstelle setzt die vorliegende Arbeit an: Sie analysiert die Regierung der Katastrophe schwerpunktmäßig – wenngleich nicht ausschließlich – in Deutschland und entwickelt eine Analytik des Sicherheitsdispositivs, die in der Lage ist, bereits etablierte Ansätze der Soziologie des Risikos zu einer Soziologie der Sicherheit zu erweitern.

Empirisch untersucht die Arbeit Katastrophenvorbereitungsmaßnahmen in öffentlichen, aber auch privaten Institutionen. Sie untersucht dafür etwa neu geschaffene Institutionen wie das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das in der Folge des 11. September 2001 etabliert wurde, als sichtbarste Ausdrücke institutioneller und strategischer Verschiebungen deutscher Sicherheits- und Katastrophenvorsorgepolitik. Die Arbeit ist gleichwohl keine Institutionenanalyse, sondern eine Dispositivanalyse. Dieser analytische Zugang im Anschluss an Michel Foucault (1978, 119f.) bietet sich an, weil die Regierung der Katastrophe in Deutschland nicht von einer einzelnen Institution ausgeht, sondern von einer Vielzahl privater und öffentlicher Institutionen und Akteuren geleistet wird. Diese stehen bisweilen im regen Austausch, stimmen ihre Maßnahmen aufeinander ab, oder arbeiten gezielt miteinander. Und auch jenseits expliziter Koordinierung des Umgangs mit Katastropheneignissen gibt es eine Reihe von Gemeinsamkeiten zwischen Bereichen, die auf den ersten Blick ganz unterschiedliche Ziele verfolgen: etwa im Feld der inneren Sicherheit und im Finanzsektor, in der Umweltpolitik und im Schutz großtechnischer Systeme. In allen diesen Bereichen werden nämlich Gefahren befürchtet, die in einer noch ungewissen Zukunft lauern und die drohen, jenseits des unmittelbaren Schadens das fortgesetzte Funktionieren komplexer (gesellschaftlicher, technischer oder natürlicher) Systeme nachhaltig zu kompromittieren. Jeweils geht es deshalb darum, sich auf ebenso unwahrscheinliche wie unvermeidliche Risiken vorzubereiten, um die Resilienz der potentiell betroffenen Systeme zu erhöhen. Diese Gemeinsamkeiten liegen dabei weniger in gezielten Absprachen, sondern auf der Ebene von analogen Wissensformen und Interventionstechniken, die die jeweiligen Akteure informieren und die ihre Vorbereitungen und Reaktionen auf katastrophische Ereignisse strukturieren. Das lose über eine Vielzahl von Institutionen, Bereichen und Akteursgruppen verstreute Netzwerk analoger Antizipations- und Reaktionstechniken zur Regierung der Katastrophe wird in dieser Arbeit als »Dispositiv« bezeichnet und analysiert. Die Arbeit verfolgt die Hypothese, dass sich die Rationalitäten und Maßnahmen zur »Vorbereitung auf die Katastrophe« zu einem neuen Sicherheitsdispositiv, dem Sicherheitsdispositiv der Resilienz, versammelt haben. Das Sicherheitsdispositiv der Resilienz unterscheidet sich systematisch von anderen historisch konstituierten Sicherheitsdispositiven wie dem Dispositiv der souveränen Staatssicherheit und dem der Bevölkerungssicherheit.

Ein Dispositiv antwortet auf einen »Notstand« (Foucault 1978, 120). Tatsächlich sind weltweit viele der neuen Institutionen des Katastrophenschutzes als Konsequenz aus den Terroranschlägen des 11. September entstanden. Und auch die Finanzkrise hat zu neuen und neuausgerichteten Regulationsbemühungen des Finanzmarktes angeregt. Krisenereignisse sind Katalysatoren für sozio-politische Innovationen und dürfen von der Soziologie, die sich so gerne auf Strukturen und Routinen konzentriert, nicht marginalisiert werden (Folkers und Lim 2014). Es hieße gleichwohl, einer allzu linearen Chronologie und einem reichlich suggestiven Funktionalismus auf den Leim zu gehen, wollte man ein Dispositiv bloß als quasi notwendige Folge auf objektive Gefahrensituationen beschreiben. Die scheinbar unzweifelhafte Evidenz der Krise muss erst mühsam aus den Trümmern, die das Ereignis hinterlassen hat, geborgen und rekonstruiert werden. In Bezug auf Risiko ist die Situation, die immer wieder beschworene »Lage«, mindestens ebenso sehr von Erwartungen an die Zukunft wie von Ereignissen in der Vergangenheit abhängig. Zudem werde ich aber zeigen, inwiefern das Dispositiv der Resilienz nicht nur auf neue Sicherheitsprobleme, sondern ebenso auf ein Problematisch-Werden der Sicherheit selbst reagiert. Dass Sicherheitspolitik selbst riskant ist, weil sie bisweilen dazu neigt, Recht zu beugen, die Freiheit und die Privatsphäre der Bevölkerung einzuschränken oder unbeabsichtigt Gefahren heraufzubeschwören, hat sich nach einem Jahrzehnt der Verschärfung von Sicherheitsgesetzen, der staatlichen Überwachung, der nicht-intendierten Nebeneffekte des Risikomanagements auf den Finanzmärkten (Arnoldi 2009) und nicht zuletzt durch den katastrophal gescheiterten Krieg gegen den Terror (Massumi 2007) auch im Alltagsbewusstsein verankert. Gerade im Feld der Katastrophenvorsorge sind Phänomene der Verschränkung von Sicherheit und Gefahr besonders präsent. Katastrophen entstehen erst durch die Verflechtung von (falschen, unzureichenden, missglückten) Sicherheitsvorkehrungen und Schadensereignissen und nicht als von außen hereinbrechender *act of god* (Felgentreff und Dombrowsky 2008). Nicht selten begünstigen Maßnahmen, die für gewöhnlich sichernde Funktion haben, das Entstehen von Katastrophen: das Risikomanagement auf dem Finanzmarkt, Deiche, die bei Hochwasser bersten und das ungeschützte Land hinter sich verwüsten, Sicherheitsautomatiken in Atomkraftwerken, Antibiotika, die das Entstehen von resistenten Keimen bewirken etc. Die Sicherheitsrationalität der *Resilienz* wird daher häufig als Alternative zu einer verfehlten Sicherheitskultur ins Feld geführt, die vollkommenen

Schutz vor Gefahren verspricht und dabei die von Sicherheitsmaßnahmen selbst erzeugten Risiken übersieht.

Die Sozial- und Kulturwissenschaften, traditionell skeptisch gegenüber den Versprechen der Sicherheit eingestellt, haben schon früh auf die Paradoxien von Sicherheitsmaßnahmen hingewiesen und sie als »safety risks« (Wildavsky 1988, 48ff.), »Risiken zweiter Ordnung« (Bonß 1995) oder »Autoimmunität« (Derrida und Habermas 2004, Esposito 2004) beschrieben und kritisiert. Die systemtheoretische Risikosoziologie (Luhmann 2003) ist gar mit der Grundhypothese angetreten, dass jedes Entscheidungshandeln »riskant« ist, weil »Gefahren« als »Risiken« den Entscheidern zugerechnet werden können. Wenn aber Sicherheitsapparate unter Rekurs auf den Leitbegriff der Resilienz auf das Scheitern von Sicherheit reagieren und den Glauben an hundertprozentige Sicherheit aufgeben, droht diese Kritikstrategie ins Leere zu laufen. Anstatt Sicherheitsparadoxien extern zu beobachten und auf tiefere Strukturen – die Moderne, die Aufklärung, die Rationalisierung – zurückzuführen, soll in der vorliegenden Arbeit analysiert werden, wie Paradoxien der Sicherheit im untersuchten Feld selbst zur Sprache gebracht, kritisiert und zum Problem gemacht werden. Nicht die in der kritischen Sozialtheorie so beliebten Tropen wie Pathologie und Paradoxie (Honneth und Sutterlüty 2011) werden diagnostiziert, sondern faktisch auftretende Problematisierungen analysiert, die nicht nur Sicherheitsprobleme, sondern auch Probleme der Sicherheit artikulieren und kritisieren.

Mit ihrer analytischen Fokussierung auf Denk- und Verfahrensweisen der Sicherheit geht die Arbeit über die mittlerweile klassisch gewordene Soziologie des Risikos (Beck 1986, Luhmann 2003) hinaus. Sie verfolgt vielmehr eine Soziologie der Sicherheit. Die Arbeit untersucht die Regierung von Katastrophen, ist aber keine Katastrophensoziologie (Dombrowsky 1989, Clausen, Geenen und Macamo 2003) im klassischen Sinne. Ihr geht es nicht um Katastrophen *per se*, nicht darum, wie Katastrophen entstehen oder vermieden werden können, sondern darum, wie sie zum Problem der Regierung werden. Gegenstand der Arbeit sind Techniken der Sicherheit, die sich auf Katastrophen richten. »Sicherheit« wird in der Arbeit nicht als »heiler Zustand« verstanden, sondern als eine Aktivität von Techniken und Rationalitäten des Schutzes vor Gefahren, die mehr oder weniger erfolgreich sein und mehr oder weniger spektakulär scheitern können. Sicherheit bezeichnet nicht die Abwesenheit von Gefahren, sondern die Sorge um mögliche Gefahren. Sicherheit ist also gerade

nicht der paradiesische Zustand unhinterfragter Gewissheiten, sondern reagiert immer auf bereits eingetretene Verunsicherungen und sorgt sich um das noch Ungewisse und bedrohlich Kommende. Und gerade weil die Sicherheit nicht nichts ist – nicht die Abwesenheit von Gefahren, kein unerreichbares Ideal oder eine trügerische Ideologie –, sondern die Institutionalisierung und Materialisierung der Sorge um Gefahren, kann Sicherheit als Set von Handlungs- und Wahrnehmungsweisen, von Technologien und Problematisierungen untersucht werden.

Durch diese analytische Umstellung von der Soziologie des Risikos zur Soziologie der Sicherheit wird es möglich zu sehen, dass ein Sicherheitsdispositiv nicht einfach auf gegebene, äußerliche Gefahren reagiert, sondern spezifische Versionen dessen, worauf es sich richtet, selbst erstellt. Das heißt nicht, dass es keine Gefahren oder Katastrophen, keine großen Schadensereignisse mit schwerwiegenden Folgen gäbe, oder dass diese »nur konstruiert« seien. Die Analytik der Sicherheit untersucht Katastrophen jedoch nicht unabhängig von, sondern stets korrelativ zu den Sicherheitsapparaten, die sich mit ihnen beschäftigen. Sie untersucht Katastrophen als historisch, politisch, sozial, kulturell und materiell situiert. So steht im Sicherheitsdispositiv der Resilienz eine spezifische Version der Katastrophe im Zentrum der Aufmerksamkeit, die keineswegs eine zu allen Zeiten gleichermaßen mögliche und bedrohliche Heimsuchung darstellt, sondern erst in der Gegenwart zum zentralen Gegenstand der Sicherheitsbesorgnis werden konnte:<sup>5</sup> die Katastrophe als Unterbrechung von substantziellen Versorgungsströmen – Energie, Wasser, Geld, Mobilität, Waren, Informationen und Systemzusammenbruch etc. Der Schutz von Menschenleben und die Sicherung der Bevölkerung ist zwar weiterhin ein zentrales Anliegen der Regierung der Katastrophe. Mit seiner Fokussierung auf die Katastrophe als Unterbrechung sozio-technischer Zirkulationen zielt das Sicherheitsdispositiv aber auf eine entschieden kontemporäre Problemkonstellation. Es sorgt sich um eine Gesellschaft, die für ihr Funktionieren auf das ununterbrochene Operieren von technischen Systemen und Infrastrukturen angewiesen ist, die ihrerseits so komplex und inter-

---

5 Deswegen werde ich in dieser Arbeit auch keine generelle Definition der »Katastrophe« liefern, sondern vielmehr untersuchen, was durch unterschiedliche Konfigurationen der Sicherheit als Katastrophe definiert und inszeniert wird. Insofern die Arbeit also untersucht, welche Arten von Ereignis auf den Radar des Sicherheitsdispositivs geraten, und nicht selber »ihre Katastrophen« auswählt, ist ihr thematischer Fokus notwendig selektiv. Diese Selektivität reflektiert dabei zum Teil auch die des Feldes selbst (zu sozialen Mechanismen der Risikoselektion siehe: Douglas und Wildavsky 1982, 29–48).



dependent sind, dass sich Störungen schnell fortsetzen können. Genau diese eskalierende Fortsetzung von Störungen in komplexen sozialen und technischen Systemen wird von Sicherheitsexpert\_innen häufig als »systemisches Risiko« gefasst und als charakteristische Form der Katastrophe in der Gegenwart gefürchtet: der Zusammenbruch des Finanzmarkts, der Stromausfall, das gefährliche Umkippen von Ökosystemen und die Überschreitung von planetarischen Leitplanken.<sup>6</sup> Die Sorge um sogenannte Kritische Infrastrukturen, systemwichtige Institutionen, Lebenserhaltungssysteme und komplexe Katastrophenlagen fokussiert nicht nur auf externe Gefahrenquellen, sondern ebenso auf die interne Anfälligkeit und Verwundbarkeit der Gegenwartsgesellschaft. Die eigenen sozialen und technischen Strukturen werden als gefährlich erlebt – und zwar nicht nur, weil der technische Fortschritt als Nebenfolgen Risiken erzeugt (Beck 1986), sondern weil technische Netze und komplexe Systeme ebenso überlebenswichtig wie verwundbar geworden sind. Es sind kritische Systeme in einem doppelten Sinne: krisenanfällig, aber auch »vital« für das Funktionieren der Gesellschaft. Deswegen sind derartige »vitale Systeme« nicht nur Schutzobjekt, sondern selbst Gefährdungszusammenhang, weil sie Resonanzkörper für die Übertragung, Ausweitung und Fortsetzung von katastrophischen Risiken darstellen. Die Abhängigkeit von vitalen Systemen macht die Strategie des vorsorglichen Ausstiegs zumeist unmöglich und lässt stattdessen die Steigerung systemischer Resilienz zur Sicherheitsstrategie der Wahl werden. Insofern steht die Regierung katastrophischer Risiken mit einer umfassenden *Biopolitik vitaler Systeme* in Verbindung. Beide verweisen auf und erhellen einander. Während katastrophische Risiken erst die Abhängigkeit und damit die Bedeutung vitaler Systemen sichtbar werden lassen – erst der Stromausfall lässt uns die Bedeutung der Elektrizitätsinfrastruktur bewusst werden –, wird erst über den Rekurs auf die Biopolitik vitaler Systeme die spezifisch kontemporäre Figur der Katastrophe als Systemzusammenbruch verständlich. Das Sicherheitsdispositiv der Resilienz verklammert beide Aspekte, indem es versucht katastrophische Risiken abzuwenden, um vitale Systeme wie kritische Versorgungsdienstleistungen, systemwichtige Finanznetzwerke und lebenswichtige Ökosysteme zu schützen.

Die Arbeit trägt in zweifacher Hinsicht zu einer Diagnose der Gegenwartsgesellschaft bei. Sie untersucht erstens das Sicherheitsdispositiv der

---

<sup>6</sup> Auch in die Soziologie hat die Debatte um systemisches Risiko Einzug gehalten. Siehe dazu: Renn und Keil (2008), Willke, Becker und Rostásy (2013).

Resilienz als kontemporäre sozio-politische Konstellation, die quer durch die Gesellschaft wirksam ist. Das Resilienzdispositiv findet sich nämlich in ganz unterschiedlichen sozialen Bereichen wie der Politik, der Ökonomie und der Wissenschaft und hat Effekte in einer ganzen Reihe politischer Institutionen und Handlungsfeldern wie der nationalen Sicherheit, dem Umweltschutz und der Finanzmarktregulation. Zweitens legt sie durch die Rekonstruktion veränderter Wahrnehmungsweisen von Risiken und Handlungsrationitäten der Sicherheit eine für die Soziologie durchaus ungewöhnliche Version des Sozialen frei. Die Gesellschaft des Sicherheitsdispositivs der Resilienz besteht aus einer Reihe miteinander zusammenhängender Funktionssysteme, die gleichwohl nicht bloß sozial, sondern ebenso technisch und natürlich sind. Dadurch schließt das Buch an Debatten an, die eine Überwindung der »Soziologie des Sozialen« (Latour 2007) gefordert haben und die Gesellschaft nicht länger bloß als selbstbezüglichen und seltsam weltfremden Interaktionsraum verstehen wollen. Dieser Anschluss erfolgt hier jedoch nicht dadurch, dass einfach eine »neue Gesellschaft« ausgerufen wird, zu der auch nicht-menschlicher Entitäten wie Dinge, Techniken und Naturkräfte gehören sollen. Vielmehr soll den Problemlagen und Krisenerfahrungen der Gegenwartsgesellschaft gefolgt werden, die ein allzu sozio-zentrisches Gesellschaftsverständnis aus sich heraus überschreiten. Auch grundlagentheoretische Fragen werden also analytisch und nicht abstrakt sozialtheoretisch adressiert. Gefragt wird nach einer historischen Ontologie der Gegenwart, nicht nach einer allgemeinen (Sozial)ontologie.

Die Arbeit gliedert sich in vier Kapitel. In Kapitel 1 werden zunächst die konzeptuellen Grundentscheidungen und Bezugsquellen der Arbeit dargestellt, die Auswahl der untersuchten Fälle begründet und der analytische Zugriff auf diese Fälle erläutert. Ich werde darlegen, wie sich die Analytik der Sicherheit von der Soziologie des Risikos unterscheidet und wie sie diese erweitert (1.1.). Anschließend werde ich die zentralen systematischen (1.2.) und historischen Perspektiven der Analytik der Sicherheit erläutern (1.3.) und schließlich zeigen, wie deren historische Einsichten und heuristische Strategien in dieser Arbeit produktiv gemacht werden (1.3.). Dieses Kapitel behandelt vor allem methodologische und sozialtheoretische Fragestellungen und ist deswegen für Leser\_innen relevant, die sich für eine Weiterentwicklung der Soziologie des Risikos durch eine Analytik der Sicherheitsdispositive und/oder für die Kombination von post-foucaultschen Ansätzen und analytischen Herangehensweisen der *Science*

*and Technology Studies* (STS) bzw. der Akteur-Netzwerk-Theorie (ANT) interessieren.

In Kapitel 2 widmet sich die Arbeit in dem ersten von insgesamt drei inhaltlichen Hauptkapiteln der Regierung der Katastrophe in Deutschland seit dem 11. September 2001. Zunächst gehe ich auf die Problematisierungen der Trennung von Zivil- und Katastrophenschutz in der Folge von Katastrophenereignissen seit der Jahrtausendwende ein (2.1.). Dann vollziehe ich nach, wie es zur Entstehung von Strategien und Institutionen des »Bevölkerungsschutzes« gekommen ist, durch den die Trennung von Zivilschutz und Katastrophenvorsorge überwunden werden soll (2.2.). Diese institutionellen Verschiebungen stellen erste Hinweise auf ein umfassendes Sicherheitsdispositiv dar. Um das Dispositiv nicht lediglich ausgehend von Institutionen, sondern von einer Reihe von Technologien und Rationalitäten der Sicherheit zu untersuchen, gehe ich im Folgenden auf neuartige Gefahrenwahrnehmungen und Interventionsformen ein, die sich sowohl im Bevölkerungsschutz als auch in anderen Bereichen – etwa in der Lebensmittelsicherheit, im Bereich von *public health* und in der Finanzmarktregulierung – finden lassen (2.3. bis 2.5.). Dabei zeigt sich die Zentralität des Problems »systemischer Risiken« für die Regierung der Katastrophe (2.4.). Auf diese systemischen Risiken antworten unterschiedliche Strategien zur Erhöhung der Resilienz gesellschaftlicher und technischer Systeme (2.5.). Dieses Kapitel ist vor allem für Leser\_inen von Interesse, die mehr über die paradigmatischen Veränderungen der Sicherheitslandschaft seit dem 11. September und die grundlegenden Verschiebungen auf der Ebene des Sicherheitsdispositivs erfahren wollen.

Während das erste empirische Kapitel so einen allgemeinen Überblick über die Bildung und die Kontur des Sicherheitsdispositivs der Resilienz in Deutschland geben wird, werde ich in den folgenden zwei Kapiteln auf ausgewählte Fälle und Themenbereiche eingehen, in denen sich das Wirken, aber auch die Einschränkungen und Anfechtungen des Dispositivs genauer beobachten lassen. Zunächst werde ich mich unterschiedlichen Projekten zum Schutz Kritischer Infrastruktur und der Sicherung vitaler Systeme widmen. Dabei wird durch Rekurs auf das von Ernst Forsthoff geprägte Konzept der Daseinsvorsorge auf die historische Genese und Signifikanz der Technopolitik der Versorgungssicherheit eingegangen (3.1.). Vitale Systeme sind aber nicht nur sozio-technische Infrastrukturen, sondern auch »natürliche« Ökosysteme. Im nächsten Schritt gehe ich deshalb anhand exemplarischer Fälle (Hochwasserschutz und Klimawan-

delanpassung) und historischer Entwicklungen (die Entstehung des Vorsorgeprinzips im deutschen Umweltrecht) auf den Einfluss von Umweltschutz und ökologischen Sicherheitstechnologien auf das Sicherheitsdispositiv der Resilienz ein (3.2.). Ökologische Kritik an »großer Infrastruktur«, an der Hybris technischer Sicherheitsstrategien und an den Gefahren der Technokratie sowie das umweltpolitische Beharren, dass Sicherheit Umwelt- und Naturschutz und nicht nur Schutz vor Umwelt und Natur beinhalten muss, hat die Sicherung vitaler Systeme zu einer besonders komplexen Angelegenheit gemacht. Das zeigt sich besonders deutlich am Fall der Energiesicherheit. Hier geraten Klimaschutz und Versorgungssicherheit, Schutz technischer und natürlicher Systeme in einen nachhaltigen Konflikt miteinander. Um das zu zeigen, wird die Verschiebung der Problematik der Energiesicherheit vom Atomstaat zur gegenwärtigen Energiewende verfolgt (3.3.). Dieses Kapitel dürfte Leser\_innen ansprechen, die sich für die interdisziplinären Debatten um Biopolitik und die *social studies of infrastructure* interessieren.

Schließlich geht die Arbeit im vierten und letzten Kapitel auch auf die Regierung der Katastrophe im privaten Sektor ein. Damit kann ich zeigen, dass die Regierung der Katastrophe durch das Dispositiv der Resilienz auch »jenseits des Staates« erfolgt. Im Zentrum steht dabei die in der Geschäftswelt mittlerweile sehr prominente Krisenmanagement- und *disaster preparedness*-Technologie des *Business Continuity Management* (BCM) (4.1.). Die Maßnahmen zur Vorbereitung auf und Verhinderung von Unterbrechungen des Geschäftsbetriebes, die ich hier untersuche, werden nicht staatlich verordnet, sondern verbreiten sich über globale Standards (4.2.). Besonders in der Bankenwelt sind Geschäftsunterbrechungen durch katastrophische Ereignisse gefürchtet und BCM deshalb weit verbreitet (4.3.). Schließlich nehme ich auch konkrete Ereignisse in den Blick (*Hurricane Sandy* in New York und Blockupy in Frankfurt), in deren Kontext die BCM-Systeme von Banken zum Einsatz gebracht, aber auch öffentlich kritisiert wurden (4.4.). Die Arbeit endet so mit konkreten Fällen, die exemplarisch die Komplexität der konkreten Politik der Katastrophenvorsorge zeigen. Dieses Kapitel kann fruchtbare Resonanzen bei Leser\_innen erzeugen, die sich vor allem für Fragen der Organisation von Notfällen und für betriebliche Sicherheitsstrategien interessieren.

Die Analyse von Sicherheitsdispositiven birgt einen gesellschaftstheoretischen Mehrwert, weil Sicherheitsdispositive im besorgten Blick auf Risiken und Verwundbarkeiten Facetten des Sozialen beleuchten, die häu-

fig bloß implizit und im Hintergrund verbleiben. Dieser Mehrwert wird jeweils zum Abschluss eines Kapitels »gesichert«, indem gezeigt wird, von welchem Imaginären des Sozialen die gegenwärtige Regierung der Katastrophe informiert ist (Exkurs I), welche Formen der Biopolitik mit dem Sicherheitsdispositiv einhergehen (Exkurs II) und welche temporale Ontologie der Rationalität der Resilienz zugrunde liegt (Exkurs III). Hier kommen Leser\_innen auf ihre Kosten, die vor allem an gesellschaftstheoretischen und übergreifenden zeitdiagnostischen Fragestellungen interessiert sind.

Durch diese materialreiche Studie versuche ich einen sowohl systematischen wie auch zeitdiagnostischen Beitrag zur aktuellen soziologischen Diskussion zu liefern. Die Studie unterbreitet einen Vorschlag, wie Rahmungen und Verfahrensweisen der Sicherheit soziologisch analysiert werden können und vertieft damit das Verständnis eines ebenso wichtigen wie auch allzu oft von der Soziologie vernachlässigten Moments der Gegenwartsgesellschaft. Sicherheit ist ein zentrales politisches Versprechen, das gerade, weil es niemals vollständig eingelöst werden kann, umso nachhaltiger das Regierungshandeln und soziale Praktiken antreibt und herausfordert. Sicherheit ist die Antwort auf die Krisen und Katastrophen, die auch im 21. Jahrhundert das Leben immer wieder heimsuchen. Indem sie die Versprechen und Probleme der Sicherheit in den Blick nimmt, kann die Arbeit zu einem vertieften Verständnis der Gegenwart beitragen. Sie erreicht dies nicht durch eine totalisierende Gesellschaftsbeschreibung, sondern durch die Analyse eines Netzes von miteinander zusammenhängen Sicherheitstechnologien. Sie versammelt unter dem spezifischen Aspekt der zeitgenössischen Regierung der Katastrophe und der Biopolitik vitaler Systeme eine Reihe zentraler Brennpunkte gegenwärtiger gesellschaftlicher Auseinandersetzungen: vom Terrorismus bis zur Energiewende, vom Klimawandel bis zur Finanzkrise. Diese Phänomene ähneln sich darin, dass sie Problemzusammenhänge darstellen, die analoge Sicherheitstechnologien auf den Plan rufen. Die Arbeit liefert keine unmittelbaren Lösungsvorschläge für die Krisen der Gegenwart und versucht sich auch nicht an einer Evaluation der analysierten Sicherheitsstrategien, die definitive Aussagen darüber verspricht, ob die in Anschlag gebrachten Maßnahmen »erfolgreich« sind oder nicht. Das Buch kann aber dennoch zu einer neuen Sicht auf festgefügte Krisenroutinen anregen und dadurch dazu beitragen, unser gewohntes Verständnis von Sicherheit zu verunsichern.

# 1. Analytik des Sicherheitsdispositivs

Eine soziologische Forschung zu Sicherheit kann nicht umstandslos auf einen gesicherten theoretisch-methodologischen Kanon zurückgreifen. Zwar haben vielversprechende Ansätze aus den *Security Studies* auch in der Soziologie Einzug gehalten. Gleichwohl betritt eine soziologisch ausgerichtete Sicherheitsforschung – gerade im deutschen Kontext – noch immer »relatives Neuland« (Opitz 2012, 23). Wenn es um Themen wie Katastrophen und komplexe Gefährdungslagen geht, wird daher zumeist auf Ansätze aus der etablierten und weitläufigen Soziologie des Risikos zurückgegriffen. Das ist gewiss nicht verkehrt. Allerdings werden so die Wirkungsweisen der Sicherheit übersprungen oder bekommen nur als abgeleitete Phänomene Aufmerksamkeit. Risiko wird also als grundlegendes Geschehen verstanden. Sicherheit wird demgegenüber nur als – zumeist vergeblicher – gesellschaftlicher bzw. politischer Reflex interpretiert.

In diesem Kapitel möchte ich eine Forschungsstrategie entwickeln, die eine Alternative zum dominanten risikosoziologischen Paradigma darstellt. Im Anschluss an Foucault werde ich diese Forschungsstrategie als »Analytik der Sicherheit« bezeichnen. Anstatt Sicherheit als Folge von Risiko zu beschreiben, schlage ich vor, Risiko ausgehend von Technologien der Sicherheit zu analysieren. Zunächst werde ich dafür im Folgenden kursorisch auf die zwei gewiss wirkmächtigsten Ansätze der Soziologie der Sicherheit – Beck und Luhmann – eingehen. Dabei werde ich darlegen, wie sich die von mir vorgeschlagene Analytik der Sicherheit von diesen Ansätzen unterscheidet, welche Leerstellen in der Risikosoziologie sie adressiert und welche zusätzlichen Einsichten sie in Aussicht stellt (1.1.). Anschließend gehe ich auf die wesentlichen analytischen Achsen – Problematisierung, Technologien/Dispositive, Strategien – der Analytik der Sicherheit ein. Dabei wird dargelegt, wie eine Foucault'sche Sicherheitsanalytik durch Bezugnahme auf methodologische Einsichten aus den *Science and Technology Studies* (STS) und der Akteur-Netzwerk-Theorie (ANT) erweitert und ge-

schärft werden kann (1.2.). Im Anschluss zeige ich kurz die historischen und zeitdiagnostischen Perspektiven der Sicherheitsanalytik im Anschluss an Foucault und Arbeiten der *Critical Security Studies* auf (1.3.), um dann darzulegen, wie ich diese Perspektiven und analytischen Strategien für eine Untersuchung zeitgenössischer Formen der Regierung der Katastrophe in der Arbeit mobilisieren werde (1.4.).

### 1.1. Von der Risikosoziologie zur Analytik der Sicherheit

Risiko ist ein zentrales Thema und Schlüsselkonzept der Soziologie. Das Sichtbarwerden einer Reihe von ökologischen Risiken und technischen Katastrophen, das Auftauchen neuer sozialer Risiken durch den Verlust sozialstaatlicher Sicherung, Terrorrisiken und schließlich die Risiken des Finanzwesens haben sich über die vergangenen Dekaden als Themen der Soziologie geradezu aufgedrängt. Zudem eignet sich die Semantik des Risikos auch als Leitmotiv gesellschaftstheoretischer Zeitdiagnosen. Ermöglichte die Moderne grundsätzlich eine vollkommen neue Qualität von Kontingenzerfahrung durch die Herauslösung der sozialen Akteure aus traditionellen Banden (Esposito 2007), so ist die Postmoderne, die zweite Moderne (Beck und Lau 2005) oder flüssige Moderne (Bauman 2000) – unsere Gegenwart also –, so systematisch von Ungewissheit und, wie es neuerdings immer häufiger heißt, Prekarität (Castel und Dörre 2009) durchzogen, dass der Begriff des »Risikos« für umfassende Gesellschafts- und Zeitdiagnosen herangezogen werden kann. Schon in den 1980er Jahren hat Ulrich Beck (1986) die »Risikogesellschaft« ausgerufen und damit eine Flut von soziologischen Studien, Konferenzen und Forschungsprojekten unter diesem Titel ausgelöst. Auch Niklas Luhmann (1998b, 1088–1096) hält Risiko für eine geeignetere »Beschreibungsformel« für funktional-differenzierte Gesellschaften als die lange dominierende Erzählung von der Klassengesellschaft. Und selbst Bruno Latour, der die gängige soziologische Rede von der »Moderne« (Latour 2008) ebenso ablehnt wie die von »der Gesellschaft« (Latour 2007), sieht vor allem in den ökologischen Risiken der Gegenwart den entscheidenden Grund, die moderne Verfassung und ihre Aufteilung von Natur und Kultur in Frage zu stellen (Latour 2001a).

Gleichwohl ist die Risikodebatte keineswegs von Einmütigkeit gekennzeichnet. Wie kommt Risiko in die Welt? Ist Risiko eine Wirklichkeit »da draußen« oder »bloß« eine soziale Konstruktion? Welche Rolle kommt der Soziologie in gesellschaftlichen Auseinandersetzungen um Risiko zu: mahnen und kritisieren oder distanziert analysieren? Solche Kontroversen haben sich häufig an den Theorien und Forschungsrichtungen von Ulrich Beck und Niklas Luhmann herauskristallisiert. Beide Autoren haben Risiko- und Risiko-Soziologien mit einem umfassenden gesellschafts- bzw. sozialtheoretischen Anspruch vorgelegt, die zum Ausgangspunkt für eine Vielzahl wichtiger soziologischer Arbeiten zu Risiko geworden sind: einmal aus systemtheoretischer Perspektive (Baecker 1991, Japp 2003, Stäheli 2007, Esposito 2011), einmal unter Bezugnahme auf das Forschungsprogramm der zweiten Moderne (Lau 1989, Bonß 1995, Arnoldi 2009).

Becks Theorie reflexiver Modernisierung und seine Zeitdiagnose der »Risikogesellschaft« stehen in der Traditionslinie der kritischen Soziologie. Zwar wurde Beck aus dem »kritischen Lager« insbesondere für seine Polarisierung von Risiko- und Klassengesellschaft (1986, 121–160) vielfach angegriffen. Mit etwas zeitlichem Abstand fallen jedoch eher die Kontinuitäten zwischen Becks Theorie und klassischen Ansätzen der kritischen Soziologie ins Auge, so dass die Streitigkeiten beispielsweise über die Frage der Klassengesellschaft eher als Auseinandersetzungen über die legitime Version kritischer Soziologie erscheinen. Wie bereits die kritische Tradition vor ihm, mobilisierte nämlich auch Beck eine Krise für die Verankerung seiner Kritik der Gesellschaft (Koselleck 1973, zum Zusammenhang von Kritik und Krise siehe: Roitman 2013, Folkers und Lim 2014). Nur waren dies bei ihm nicht mehr die Krise des Kapitalismus oder die Legitimationskrisen spätkapitalistischer Staatlichkeit (Habermas 1973), sondern die ökologischen Krisen und technischen Katastrophen, die seit den 1980er Jahren immer offensichtlicher wurden. Zudem hat Beck die Dynamiken, die zur Risikogesellschaft geführt haben, als Drama der modernen, rationalisierten Gesellschaft beschrieben. Damit hat er auf Motive zurückgegriffen, die schon die Frankfurter Schule (Horkheimer und Adorno 2010) zum Ausgangspunkt ihrer Kritischen Theorie gemacht hat: die Paradoxien und Pathologien der Zweckrationalität, die im Anschluss an Max Webers Theorie der Rationalisierung ins Zentrum der Gesellschaftskritik gerückt sind. Die Risikogesellschaft ist insofern nicht einfach nur eine Gesellschaft, die mit Risiken konfrontiert ist. Viel grundlegender ist, dass das operative Rationalitätsschema moderner Gesellschaften durch das Auftauchen dieser



Risiken in Frage gestellt wird. Schließlich war die moderne Gesellschaft auch schon vor Beginn der Risikogesellschaft, die etwa seit dem Zweiten Weltkrieg entstanden ist, mit Risiken konfrontiert. So verheerend sich diese Risiken jedoch im Einzelnen auch ausgewirkt haben mögen – sie konnten der modernen Hoffnung auf eine rationale Beherrschbarkeit der Welt keinen Abbruch tun. Die Kalkulierbarkeit von ungewissen Zukunftsverläufen und die finanzielle Kompensierbarkeit von eingetretenen Schäden durch die im 19. Jahrhundert entstandene Versicherung bestärkte vielmehr die Hoffnung, auch mit Gefahren rational umgehen, sie zähmen, meistern oder gar beherrschen zu können. Die Entstehung des »Vorsorgestaats« (Ewald 1993) – also die Entwicklung eines umfassenden Sozialversicherungssystems gegen die Risiken der Industriegesellschaft (Arbeitsunfälle, Armut, Alter etc.) gegen Ende des 19. Jahrhunderts – wird dementsprechend von Beck als »historischer Lernschritt der frühen Industriegesellschaft« (Beck in: Ewald 1993, 540) verstanden.

In der zweiten Moderne bzw. der Risikogesellschaft entwickelt sich dagegen eine andere und wesentlich düsterere Konstellation. Die paradigmatischen Risiken der »Weltrisikogesellschaft« (Beck 2008) bestehen für Beck im Terrorismus, anthropogenen Klimawandel und in globalen Finanzkrisen (Beck 2008, 37ff.). Wie bei den Risiken der ersten Moderne handelt es sich letztlich ebenfalls um nicht intendierte Nebenfolgen gesellschaftlicher Rationalisierungsprozesse. Terror, Klimawandel und globale Finanzkrisen sind Selbstgefährdungsphänomene, nicht von außen hereinbrechende Katastrophen. Im Gegensatz zu den »sozialen« Risiken der ersten Moderne – Arbeits- und Autounfälle, Armut, Arbeitslosigkeit oder Alter – seien diese Bedrohungen aber *erstens* unkalkulier- und damit unversicherbar. *Zweitens* sei es unmöglich, effiziente Vorbereitungsmaßnahmen im Angesicht dieser Gefährdungen zu treffen. Und *drittens* seien die Gefährdungen zeit-räumlich entgrenzt, sprengen also die Grenzen des Nationalstaats und entfalten zudem ein Gefährdungspotenzial, das auch nachfolgende Generationen betreffen wird. Die Risikogesellschaft ist deshalb zugleich »Weltrisikogesellschaft« (Beck 2008). Die Gefährdungen entziehen sich Beck zufolge den Mechanismen der Risikokontrolle der ersten Moderne, die auf der Versicherbarkeit von Risiken innerhalb eines nationalen Territoriums im Vorsorgestaat basierte.

»Die Großgefahren heben die drei tragenden Säulen des Risikokalküls auf. Mit ihnen sind erstens nicht-eingrenzbare, globale, oft irreparable Schädigungen verbunden: Der Gedanke der (geldlichen) Kompensation versagt. Zweitens ist die

vorsorgende Nachsorge für den schlimmstdenkbaren Unfall ausgeschlossen: Die antizipatorische Folgenkontrolle ist unmöglich. Drittens ist der »Unfall raum-zeitlich unbegrenzt.« (Beck 2008, 61f.)

Zugleich hofft Beck, dass es durch die Proliferation unbeherrschbarer, nicht-intendierter Nebenfolgen der industriellen Gesellschaft auch zu einem gesellschaftlichen Umdenken kommt. Die unintendierten Nebenfolgen von technischem Fortschritt und Naturbeherrschung erfordern mit geradezu imperativer Gewalt – Beck (2008, 94) spricht von »erzwungener Aufklärung« – die Problematisierung ihrer Quellen. Es wird den Modernen klar, dass es so nicht mehr weitergeht: Die Folgen der funktionalen Differenzierung können nicht mit noch mehr Differenzierung gelöst, den Folgen der Rationalisierung kann nicht mit noch mehr Zweckrationalität und Expertentum begegnet, die Folgen der Naturbeherrschung nicht mit noch mehr Naturbeherrschung behoben werden. Diese Problematisierungen haben teilweise bereits zu einem Umdenken geführt. Der blinde Glaube in wissenschaftliche Expertise bröckelt; im Zeitalter der Nebenfolgen kommt es zur Politisierung von Technik und Wissenschaft (siehe Beck in: Beck, Giddens und Lash 1994, 19–112). Das Auftauchen von weltumspannenden Risiken ruft eine kosmopolitische Weltöffentlichkeit ins Leben, die neue Institutionen hervorbringt, die besser mit grenzüberschreitenden Risiken umgehen können (Beck 2008, 94–129). Die positive Dialektik der Rationalität besteht für Beck also im Zusammenhang von Reflex und Reflexion (Beck 2008, 86–93). Reflexhaft erzeugt die gesellschaftliche Rationalisierung Risiken. Das führt aber dazu, dass die zweckrationalistische Vereinseitigung der Moderne aufgehoben wird und der normative Gehalt der Vernunft wieder größere Relevanz erlangt. Die Risikogesellschaft ist in diesem Sinne immer beides: Reflex und Reflexion, Selbstgefährdung und Selbstbesinnung, Krise und Kritik.

In Niklas Luhmann fand Beck seinen Gegenspieler. Luhmann, der dem soziologischen Konnex von »Krisendiagnose und kritische[r] Einstellung« (Luhmann 1991a, 147) stets skeptisch gegenüberstand, verschiebt in seiner Risikosoziologie die Perspektive. Er beobachtet nicht mehr Risiken *per se*, sondern die Beobachtungen von Risiken. Risiko kommt für Luhmann nicht durch diese oder jene Gefahrenquelle – zum Beispiel die Nebenfolgen der industriellen Entwicklung – in die Welt, sondern durch eine bestimmte Weise des Beobachtens, des Ent- und Unterscheidens. Für Luhmann ist nicht die Unterscheidung von erster und zweiter Moderne, sondern die von Gefahr und Risiko maßgeblich (Luhmann 2003, 31ff.).

Die Systemtheorie untersucht also aus einer Beobachterperspektive zweiter Ordnung eine Gesellschaft, die »Unheil in der Form von Risiken zu erfassen sucht« (Luhmann 2003, 2). Von Risiko wird immer dann gesprochen, wenn zukünftige Bedrohungen auf gegenwärtige oder vergangene Entscheidungen bezogen werden. Dadurch unterscheidet sich Risiko von Gefahr, die nicht auf Entscheidungen bezogen und stattdessen der Umwelt des Systems zugerechnet wird.

»Entweder wird der etwaige Schaden als Folge der Entscheidung gesehen, also auf die Entscheidung zugerechnet. Dann sprechen wir von Risiko, und zwar vom Risiko der Entscheidung. Oder der etwaige Schaden wird als extern veranlaßt gesehen, also auf die Umwelt zugerechnet. Dann sprechen wir von Gefahr.« (Luhmann 2003, 30f.)

Die Systemtheorie kontrastiert Risiko also nicht, wie es aus einer Beobachterperspektive erster Ordnung naheliegen würde, mit Sicherheit. Aus einer Beobachtungsperspektive zweiter Ordnung zeigt sich vielmehr, dass die spezifische Art der Zurechnung von möglichen oder eingetretenen Übeln auf Entscheidungen die moderne Risikoerfahrung kennzeichnet.

Gleichzeitig ist auch die systemtheoretische Risikosoziologie historisch angelegt. Damit so etwas wie Risiko in die Welt kommen kann, bedarf es eines spezifischen Verständnisses von Temporalität und Historizität, das sich erst in der Moderne eingespielt hat (Luhmann 1976, 1980, 1992b). Die Zukunft muss in diesem Verständnis nicht nur prinzipiell offen sein, sondern ihr Verlauf muss als von unseren Entscheidungen in der Gegenwart abhängig gedacht werden.

»Wir wissen [...], daß viel von dem, was in künftigen Gegenwarten der Fall sein wird, von Entscheidungen abhängt, die wir jetzt zu treffen haben. Und beides hängt offenbar zusammen: die Entscheidungsabhängigkeit künftiger Zustände und der Bruch der Seinskontinuität von Vergangenheit und Zukunft. Denn Entscheiden kann man nur, wenn und seit nicht feststeht, was geschehen wird.« (Luhmann 1992b, 136)

Den Modernen erscheint die Zukunft, sobald sie mit linearen Fortschrittsvorstellungen gebrochen haben, deswegen zumeist als Risiko (siehe: Luhmann 2003, 41–58).

In diesem Sinne ist die Semantik des Risikos nichts per se Schlechtes, sondern vielmehr ein adäquater Ausdruck einer prinzipiell kontingent gewordenen Moderne, die mit einer Vielzahl von – nicht immer nur positiven – Möglichkeiten konfrontiert ist, zwischen denen man auswählen kann (und muss). Allerdings gibt es auch eine spezifische Gefahr des Risikos,

und das heißt für die Systemtheorie immer: der Kommunikation von Risiko. Anders als Beck, der sich von einer geschärften Wahrnehmung von Risiken und einer gesteigerten Reflexivität ein gesellschaftliches Umsteuern erhofft, sieht Luhmann eine Bedrohung in genau dieser Reflexivität und der Kommunikation von Risiko, dem Warnen und Alarmieren. Wenn zu viele Entscheidungen unter den skeptischen Blick des Risikos gestellt werden, droht das die Entscheidungskapazitäten sozialer Systeme einzuschränken oder gar zu blockieren. »Wir müssen deshalb mit der Möglichkeit rechnen, daß die moderne Gesellschaft zu viel auf Entscheidungen zurechnet und dies auch dort tut, wo der Entscheider (Person oder Organisation) gar nicht identifiziert werden kann.« (Luhmann 2003, 130) Die Gesellschaft muss daher Wege finden, sich vor einer Proliferation von »Risiken«, das heißt einem Anschwellen von Risikokommunikationen, zu schützen (siehe dazu am Fall der Umweltrisiken: Luhmann 2008).

Gerade die Vorschläge zur Risikokontrolle als Kontrolle der Risikobebachtung bringt die Systemtheorie in scharfen Gegensatz zur kritischen Risikosoziologie. Während Beck mehr Reflexion und Deliberation im Angesicht von Risikolagen einfordert, plädiert Klaus Peter Japp für mehr Dezsionismus. Gerade, wenn es schnell gehen muss und Deliberation zu viel Zeit in Anspruch nehmen würde, sind »impressionistische Entscheidungen« (Japp 1990, 34) gefragt. Während Beck (1988) die »organisierte Unverantwortlichkeit« risikoproduzierender Institutionen anprangert,<sup>7</sup> sieht Luhmann im Verschieben von Verantwortlichkeiten und Vertagen von Entscheidungen die zentralen Funktionen von Organisationen: die »Unsicherheitsabsorption« (Luhmann 2000, 184). Unsicherheit absorbieren kann die Organisation dadurch, dass sie die Last der Einzelentscheidung, die auf sich allein gestellt sämtliches Risiko trägt, »in eine Vielzahl von Entscheidungen und deren Sequenzierung« (Luhmann 2003, 205) bzw. ein »Netzwerk der Entscheidung« (Luhmann 2003, 203) auflöst. Während Beck mit der Kopplung von Reflex und Reflexion geradezu eine »List der Geschichte« (Beck 2008, 109) am Werk sieht und sich dadurch bei der idealistischen Geschichtsphilosophie des 19. Jahrhunderts bedient, orien-

---

7 In seinem Buch mit gleichnamigem Titel definiert Beck (1988, 100) organisierte Unverantwortlichkeit folgendermaßen: »Es handelt sich also um ein weitverzweigtes Labyrinth-System, dessen Konstruktionsplan nicht etwa Unzuständigkeit oder Verantwortungslosigkeit ist, sondern die Gleichzeitigkeit von Zuständigkeit und Unzurechenbarkeit, genauer: Zuständigkeit als Unzurechenbarkeit oder: organisierte Unverantwortlichkeit.«

tiert sich Luhmann an der Geschichtsauffassung der Evolutionstheorie. In seinem Buch *Ökologische Kommunikation*, in dem er versucht, die Frage zu beantworten, ob die Gesellschaft sich auf die ökologische Gefährdung einstellen kann, erteilt er jeglichem – auch kybernetischen – Planungsoptimismus eine Absage und argumentiert, dass die Gesellschaft sich nur Schritt für Schritt an Irritationsreize aus der Umwelt anpassen kann – oder auch nicht (Luhmann 2008, 22–26).

Die Auseinandersetzungen zwischen den Anhänger\_innen Becks und Luhmanns sind häufig so zugespitzt und polemisch geführt worden, dass darüber allzu oft die Schwächen übersehen wurden, die beide Ansätze teilen. An entscheidender Stelle neigen nämlich sowohl Becks als auch Luhmanns Risikosoziologie dazu, undifferenziert und dadurch für empirische Analysen ungeeignet zu werden. Wenn Beck die Weltrisikogesellschaft zum Drama moderner Rationalität per se stilisiert und argumentiert, dass sämtliche Rationalisierungsversuche katastrophischer Risiken zum Scheitern verurteilt sind, dann verliert er damit allzu leicht die konkreten Bemühungen aus dem Auge, die versuchen, auch diese Risiken mit wissenschaftlichen Techniken zu antizipieren und rational bearbeitbar zu machen (für eine entsprechende Kritik an Beck siehe: Ericson und Doyle 2004, Collier 2008). Wenn demgegenüber Luhmann Risiken als Konsequenz von Entscheidungen und Entscheidungszurechnung beschreibt, dann fragt sich, was dann im Unterschied dazu überhaupt noch als »Gefahr« betrachtet werden kann. Letztlich kann so unterschiedslos alles Handeln als riskant beobachtet werden.<sup>8</sup> In der Konsequenz spielt es dann – in Becks Begriffen – keine Rolle mehr, mit welcher Rationalität die Akteure auf potenziell bedrohliche Situationen reagieren, es scheint – in der Perspektive Luhmanns – egal, welche Entscheidungen getroffen werden. Letztlich unterminieren beide Ansätze so ihre eigenen Potenziale. Beck versäumt es, die faktischen Reaktionen auf die Beschränkungen und das Scheitern spezifischer Rationalitäten des Risikos zu analysieren. Er kann Reflexivität deshalb nur mahnend einfordern, nicht empirisch untersuchen. Der Systemtheorie ergeht es nicht viel besser: Wenn systemtheoretische Risikoforschung ihre vornehmste Aufgabe darin sieht nachzuweisen, dass

---

<sup>8</sup> Luhmann selbst weist auf die Konsequenzen einer solchen ubiquitären Risikounterstellung hin, wenn er im letzten Kapitel seiner Soziologie des Risikos überlegt, was eigentlich passieren würde, wenn die Gesellschaft selbst Bedrohungssituationen so beobachten würde wie die Systemtheorie. Er kommt darin zu dem Schluss: »So aufgeblasen ist die Welt ein riesiges black box.« (Luhmann 2003, 245f.)

auch und gerade die Versuche, Risiko zu vermeiden, riskant sind (Japp 1992), dann häufig um den Preis, von einer Beobachtung zweiter Ordnung doch wieder auf eine Beobachtung erster Ordnung umzustellen und in einen besserwisserischen Gestus zu verfallen, der nur das Vexierbild des Beck'schen Mahnungseifers ist. Vor allem lässt die systemtheoretische Risikoforschung so letztlich die Unterscheidung von Gefahr und Risiko kollabieren und damit strenggenommen die Grundlage ihrer eigenen Beobachtungen: wenn alles Risiko ist, dann verliert es seine andere Seite und wird undifferenziert, amorph.<sup>9</sup>

Die Intuition dieser Arbeit besteht darin, dass diese Sackgassen der Risikosoziologie vermieden werden können, wenn man das Augenmerk auf die realen gesellschaftlichen Prozesse und Mechanismen richtet, die mit Risiken befasst sind: Institutionen und Maßnahmen der Sicherheit. Hier können die operativen Rationalitäten und Entscheidungen in Situationen der Gefährdung konkret analysiert werden. Der Vorschlag lautet also, Risiko aus der Perspektive der Sicherheit zu analysieren. Das ist gewiss erklärungsbedürftig. Schließlich wird Sicherheit in der soziologischen Debatte geradezu gemieden wie eine unverdauliche Mahlzeit. So hat die Systemtheorie Risiko mit Gefahr kontrastiert, um Mythen absoluter Sicherheit zu zerstreuen. Das heißt aber auch, dass Sicherheit noch nicht einmal die unmarkierte, andere Seite des Risikos darstellt – das ist schließlich die Gefahr –, sondern höchstens das Phantasma einer hysterischen Öffentlichkeit.<sup>10</sup> Sicherheit sei eine »soziale Fiktion« und daher höchstens ein »Ventilbegriff für soziale Forderungen« (Luhmann 2003, 28f.). Das mehrfach

---

9 Die hier vorgebrachte Kritik betrifft gewiss nicht alle Ansätze gleichermaßen, die an die systemtheoretische Risikosoziologie anschließen bzw. an das Forschungsprogramm der zweiten Moderne. Aber charakteristischerweise haben die produktivsten Analyseansätze andere Wege eingeschlagen bzw. Akzente gesetzt. Im Forschungsprogramm der zweiten Moderne ist sicherlich die von Peter Wehling (2006) am konsequentesten vertretene Nichtwissensanalyse am fruchtbarsten. Besonders überzeugend sind vor allem solche systemtheoretischen Ansätze, die mit Bezug auf Luhmanns Ausführungen zur modernen Zeitsemantik die temporale Logik von spezifischen Risikosituationen aufschlüsseln (Esposito 2011, Opitz und Tellmann 2015b).

10 Ich lasse die Frage, ob eine systemtheoretische Risikosoziologie nicht auch mit der Grundunterscheidung von Risiko und Sicherheit operieren könnte, die Luhmann (2003, 28–30) explizit abgelehnt hat, offen. Das Konzept von Sicherheit, das ich hier vorschlagen möchte, ist denn auch nicht formtheoretisch gebildet. Vielversprechende Ansätze, Sicherheit ein stärkeres Gewicht in der Systemtheorie zu geben, lassen sich in Luhmanns (1991b, 501–525) Theorie der sozialen Immunisierung finden. Siehe dazu: Folkers (2013a).

gebrochene Konzept der »Unsicherheitsabsorption« in Luhmanns Organisationssoziologie<sup>11</sup> ist symptomatisch dafür, wie schwer sich die Systemtheorie tut, positiv von Sicherheit zu sprechen. Auch Beck liegt es fern, die Risikogesellschaft einer ehemals oder künftig sicheren Gesellschaft gegenüberzustellen. Weltrisikogesellschaft – das ist für Beck kein temporärer Zustand, der überwunden werden muss oder kann, sondern das unhintergehbare Kennzeichen unserer Gegenwart. Der Untertitel seines 2008 erschienenen Buchs *Weltrisikogesellschaft* (Beck 2008) lautet folgerichtig: »Auf der Suche nach der verlorenen Sicherheit«. Höchstens melancholisch gebrochen wagt man in der Soziologie von Sicherheit zu sprechen. In einer »bedrohlichen Welt« mögen wir auf der Suche nach Sicherheit sein, wie es in einer jüngeren Veröffentlichung Zygmunt Baumanns (2009) heißt, endgültig finden werden wir sie aber nicht. So gibt es im deutschen Sprachraum eine differenzierte und weitläufige Risikosoziologie und sogar eine Katastrophensoziologie (Clausen, Geenen und Macamo 2003, Voss 2006, Felgentreff und Dombrowsky 2008), aber »eine Soziologie der Sicherheit gibt es hierzulande erst in Ansätzen«, wie Sven Opitz (2012, 23) zurecht feststellt.<sup>12</sup> Es wird zumeist vermieden, Sicherheit als »soziale Tatsache« wahrzunehmen und zu untersuchen, wie es Franz Xaver Kaufmann (1970, 6) bereits in den 1970er Jahren gefordert hatte.

Zwar kommen soziologische Arbeiten, die sich mit Risiko beschäftigen, schlechterdings nicht darum herum, sich zur Frage der Sicherheit zu verhalten. Deshalb ist die Risikosoziologie auch alles andere als nutzlos für eine Untersuchung von Sicherheit. Aber es fällt doch auf, dass Sicherheit immer nur indirekt, gleichsam über einen Umweg oder über ihr Anderes in den Blick gerät: Risiko, Gefahr, Ausnahme, Unsicherheit, Prekarität, Ungewissheit, Krise, Notfall, Störung etc. Sicherheit wird, wie man in Anlehnung an eine Formulierung von Georges Canguilhem (1977, 65) formulieren könnte, als Schweigen der Gesellschaftsorgane verstanden. Erst die Störgeräusche der Krise lassen die Gesellschaft beredt werden. Hier zeigt sich vielleicht der lange Schatten der Soziologie als »Krisenwissenschaft«

---

11 Trotz Luhmanns frühem »Lob der Routine« (Luhmann 1971b) widmet sich eine an Luhmann anschließende Organisationssoziologie mit Vorliebe Themen wie Störungen (Baecker 2011), Ausnahmen (Ortmann 2003) und Unterbrechungen (Vollmer 2013). Sie betont dabei, wie diese Formen der Unordnung letztlich Teil der Ordnung des Organisierens werden und sich Routinen der Entstörung einspielen.

12 Wichtige »Ansätze« für eine Soziologie der Sicherheit finden sich unter anderem bei: Hempel, Krasmann und Bröckling (2010), Zoche, Kaufmann und Haverkamp (2011), Opitz (2012), Kaufmann (2012), Langenohl (2013), Laufenberg (2014).

(Koselleck 1982, König 2012, 631), die seit ihrem Entstehen dazu neigt, die Gesellschaft vornehmlich über ihre Pathologien wahrzunehmen. Diese Ausrichtung auf Gefahren und Risiken erschwert es der Soziologie, die Bedeutung von Sicherheit ernst zu nehmen. Sicherheit wird geradezu zum *blind spot* der Soziologie. Sicherheit ist das, was die Soziologie nicht beobachten kann, weil es seinerseits ihre Beobachtungsperspektive strukturiert. Wenn Sicherheit doch einmal vorkommt, dann meist nur als subjektive Erwartung von sich in struktureller Unsicherheit befindenden Akteuren. Dadurch wird jedoch die faktische Wirksamkeit dieser Erwartungen ebenso übersprungen wie die im Dienste der Sicherheit stehenden Praktiken. Sicherheit wird mal – wie bei Beck – als vergebliches, verlorenes Ideal der Risikogesellschaft, mal – wie bei Luhmann – als eine »Ideologie« angesehen, die droht, soziale Systeme durch ihre unbegrenzten Anforderungen zu überlasten.

Aber so, wie das Recht nicht auf das Ideal der Gerechtigkeit reduzierbar ist, sondern einen hochwirksamen und spezialisierten gesellschaftlichen Praxiszusammenhang bzw. ein System bildet, so ist »Sicherheit« nicht auf ein Ideal der Gefahrenlosigkeit reduzierbar, sondern erheischt als Komplex von kalkulierten Techniken zur Gefahrenabwehr eine genuine soziologische Aufmerksamkeit. Deshalb besteht der Einsatz dieser Arbeit darin, Sicherheit als ein Ding von dieser Welt zu beschreiben: als ein Set von Rationalitäten, Technologien und reflektierten Praktiken, die versuchen, die Welt, die Gesellschaft, ihre Leben sicherer zu machen. Um diese Rationalitäten, Technologien und reflektierten Praktiken der Sicherheit in den Mittelpunkt zu rücken, greife ich vor allem auf die Arbeiten Michel Foucaults (2004) und seiner Mitarbeiter (Defert 1991, Ewald 1993) sowie auf die an diese anschließenden *Governmentality Studies* (Krasmann 2003, Ericson und Doyle 2004, Purtschert, Mayer und Winter 2008, Valverde 2011, O'Malley 2012), *Critical Security Studies* (Reid 2006, Dillon und Lobo-Guerrero 2008, Aradau und Munster 2011, Anderson, Adey und Graham 2015) und auf die Biopolitikdebatte zurück (Lemke 2007b, Lakoff und Collier 2008, Folkers und Lemke 2014). Ähnlich wie die Systemtheorie begegnen diese Arbeiten der scheinbaren Evidenz des Risikos mit einer distanzierten Skepsis. Auch sie stellen auf Beobachtungen zweiter Ordnung um. Allerdings stellen sie diese Perspektive in den Dienst der Kritik. Kritik heißt jetzt jedoch nicht mehr Warnung vor Gefahren und Aufzeigen der Paradoxien industrieller Gesellschaften. Vielmehr richtet sich die kritische Aufmerksamkeit auf die Risiken der Sicherheit (siehe: Foucault



2005d). Die Machteffekte und Kontrollwirkungen der Rationalität des Risikos und der Technologien der Versicherheitlichung sind der Gegenstand der Kritik. Die kritische Aufmerksamkeit ist damit gleichsam auf die Thematik der Sicherheit »umgekippt«. Insofern stellt die an Foucault anschließende Debatte um Sicherheit keine bloße Verbindung der etablierten Positionen der Risikosoziologie in Aussicht, sondern eine grundlegendere Verschiebung des Analysegegenstands und der Analyseperspektive: von einer Soziologie des Risikos zu einer Analytik der Sicherheit. Nicht mehr erste und zweite Moderne, Gefahr und Risiko, sondern Risiko und Sicherheit ist das entscheidende Begriffspaar der Analytik der Sicherheitsdispositive.

Die Analytik der Sicherheit untersucht gerade keine Zustände fragloser Gewissheiten und unversehrter gesellschaftlicher Vollzüge. Die von ihr untersuchten Sicherheitsmechanismen bilden sich in Reaktion auf bereits eingetretene Verunsicherungen. Sie gleichen einem Immunsystem, das immer erst nach dem ersten Eintreten von Störungen bzw. dem Eindringen von Erregern aktiviert wird, um anschließend auch vorsorglich tätig werden zu können. Sicherheit ist nicht die Abwesenheit von Gefahr, sondern die Sorge<sup>13</sup> um mögliche Gefahren. Sichernder Sorge geht es nicht um Tatsachen, sondern um »matters of concern« (Latour 2004), Sachen, die einen angehen bzw. Dinge von Sicherheitsbelang. Es geht ihr nicht bloß um schlicht vorliegende Übel, sondern um Gefahren im Verzug. Diese Sorge aktualisiert sich jedoch historisch in stets unterschiedlichen Formen und bildet deshalb einen untersuchbaren Bereich gesellschaftlicher Realität für die Soziologie: Sie ist materialisiert in Wissensformen, in Insti-

---

13 Allein wegen ihrer etymologischen Nähe zu Sicherheit (*se-curitas* heißt dem Wortsinn nach »ohne Sorge«, siehe: Conze (1982, 831f.)) ist Sorge ein zentraler Begriff für die Analytik der Sicherheit. Grundbegrifflich lässt sich Sorge im Anschluss an Heidegger (2006) als zeitlich gegliederter Welterschließungsmodus fassen: Sorge ist immer auch auf das Zukünftige und Kommende gerichtet. Für Foucault ist der Begriff der Sorge nicht nur in seinen späten Arbeiten zur Selbstsorge (Foucault 1989b), sondern auch für seine Arbeiten zur Biomacht als fürsorgende Form der Macht von zentraler Bedeutung (Foucault 1977). Sicherheit von Sorgepraktiken ausgehend zu verstehen, ist dabei auch die spezifische Pointe, mit der es Foucault gelingt, eine Alternative zum Denken der Sicherheit in den Begriffen souveräner Staatlichkeit zu entwickeln (siehe dazu Kapitel 1.3.). In dieser Arbeit werde ich einige Traditionslinien der Sicherheitspolitik analysieren, die gewiss nicht zufällig mit dem Begriff der Sorge assoziiert sind, etwa die Daseinsvorsorge und das Vorsorgeprinzip (siehe Kapitel 3.1.1. und 3.2.1.) sowie das Konzept der Versorgungssicherheit, das hier im weitesten Sinne als Biopolitik vitaler Systeme gefasst wird (siehe Kapitel 3).

tutionen, in materiellen Strukturen, technischen Vorrichtungen und reflektierten Praktiken. Dieser historisch spezifische Realitätsbereich der »Sicherheit«, der auf faktische Verunsicherungen reagiert, bildet den eigentlichen Untersuchungsgegenstand der Analytik der Sicherheit.

Risiko ist hier strenggenommen nicht der primäre Gegenstand, sondern ein abgeleitetes Phänomen, das mit dem grundlegenden Untersuchungsgegenstand zusammenhängt: den Technologien und Dispositiven der Sicherheit. Es wird davon ausgegangen, dass Risiken von Anfang an Produkt und Element historisch spezifischer Sicherheitsmechanismen sind. So hat gerade François Ewald (1993) in seiner Studie über den Aufstieg des »Vorsorgestaates« gezeigt, dass Risiko als Konzept, kalkulative Technik und reflektierte Praxis und damit als soziale Tatsache historisch zunächst in und durch die Versicherung seit Ende des 18. Jahrhunderts in die Welt gekommen ist. Risiken sind also nicht natürlich, sie sind keine vor- oder außersozialen Gefährdungen, aber sie sind auch nicht lediglich das Ergebnis von sozialen Zuschreibungen von Verantwortlichkeit oder Zurechnungen von Ereignissen auf Entscheidungen. Sie entstehen korrelativ zu bzw. in den modernen Apparaten der Regierung, die mögliche Bedrohungen als Risiken vergegenwärtigen, beschreiben und kalkulieren (Foucault 2004, 95). Risiken sind ein wesentliches Produkt von Sicherheitsdispositiven, sie sind aber auch deren Zielscheibe. Sie sind »Effekt und Instrument« (Foucault 1976, 42) der politischen Technologie der Sicherheit. Eine »Risikogesellschaft« ließe sich in diesem Sinne eher als eine Gesellschaft beschreiben, die ihr gesteigertes Bedürfnis nach Sicherheit in einer ganz bestimmten Weise organisiert hat und das paradoxerweise als Proliferation von Risiken erlebt.

Allerdings unterscheidet sich eine Foucault'sche Analytik der Macht und Sicherheit von der Beck'schen Risikosoziologie bereits dadurch, dass sie gerade nicht auf eine gesellschaftliche Gesamtdiagnose zielt. Das ist in den *Studies of Governmentality* bisweilen übersehen worden. So wurden immer wieder gewiss bedeutsame Trends und politische Rationalitäten zu einem integralen Gesellschaftstypus hypostasiert, zum Neoliberalismus (Barry, Osborne und Rose 1996), zur »Aktivgesellschaft« (Dean 1995, Lessenich 2009) etc. Gouvernamentalität wurde so als soziologisches Theorieprogramm positioniert. Das ist zwar durchaus legitim und hat wichtige Ergebnisse geliefert. Darüber wurde allerdings allzu oft eine Ausarbeitung und Fortentwicklung der heuristischen Strategien Foucaults sowie eine Beschäftigung mit den historischen Perspektiven der Macht-

analytik versäumt. Insofern ist die vorliegende Arbeit keine klassische »Gouvernementalitätsanalyse«, sondern untersucht zeitgenössische Konstellationen der Sicherheit durch eine historisch informierte Dispositivanalyse. Sie packt die theoretische und analytische Werkzeugkiste aus, anstatt sich im schlüsselfertigen Haus einer umfassenden Gesellschaftsdiagnose einzurichten. Um diesen Ansatz zu plausibilisieren und zu konturieren, werde ich im Folgenden die Grundzüge der hier in Anschlag gebrachten Analytik der Sicherheit darlegen.

## 1.2. Die Achsen der Dispositivanalyse

Die *Governmentality Studies* sind gut zwanzig Jahre nach ihren Anfängen (Burchell, Gordon und Miller 1991) zu einem eigenständigen und etablierten sozialwissenschaftlichen Paradigma geworden (Bröckling, Krasmann und Lemke 2011). Regierung wurde von den *Governmentality Studies* als »conduct of conduct« (Gordon 1991, 2), als Führung von Selbst-Führung, re-konzeptualisiert. Dadurch konnten Formen von »political power beyond the state« (Rose und Miller 1992) sichtbar gemacht und Begrenzungen traditioneller Ansätze der politischen Soziologie sowie der Governanceforschung überwunden werden. Diese produktive Erweiterung schlägt in Teilen der Forschung aber paradoxerweise in eine Beschränkung um, wenn nahezu ausschließlich das Regieren durch Subjektivierung<sup>14</sup> diskutiert wird und etwa die Steuerung komplexer Prozesse in den Hintergrund tritt. So sind in jüngeren postfoucaultschen Debatten die Grenzen des »conduct-Modells« deutlich gemacht worden. Der Fokus auf Subjekte und deren Verhalten reicht nicht aus, wenn etwa die Regierung des Ökonomischen (Tellmann 2011), sozio-technischer Netzwerke (Collier 2011) oder die Reaktion auf Ereignisse in Sicherheitsdispositiven (Folkers 2014) untersucht werden soll. Auch die Regierung der Katastrophe und die Biopolitik vitaler Systeme lassen sich nicht auf die »Führung von Selbstführungen« reduzieren. Deshalb möchte ich hier eine Alternative zur üblichen Gouvernamentalitätsanalyse vorschlagen, die entlang der drei Achsen Problematisierung, Technologie, Strategie ausgerichtet ist und argumentiert, dass Regieren stets an historisch-spezifische Dispositive der Macht gekoppelt

---

14 Zu dieser – gewiss ungemein produktiven Forschungsrichtung – siehe etwa die Arbeiten von: Rose (1992), Dean (1995), Cruikshank (1999), Lemke (2006), Bröckling (2007).

ist. In einer kurzen Bemerkung in seiner 1978 gehaltenen Vorlesung *Sicherheit, Territorium, Bevölkerung* hat Foucault diese Analyseachsen eingeführt, um seine Untersuchung der Gouvernamentalität von klassischen Formen der Institutionen- und Machtanalyse abzugrenzen.

»Aufs ganze gesehen bestand also die in all diesen Untersuchungen vertretene Auffassung darin, zu versuchen, die Machtbeziehungen hinsichtlich der Institution freizulegen, um sie unter dem Gesichtspunkt der Technologien zu analysieren, sie ebenso hinsichtlich der Funktion freizulegen, um sie in einer strategischen Analyse wiederaufzunehmen, und sie hinsichtlich des Privilegs des Objekts flexibel zu machen, um zu versuchen, sie vom Standpunkt der Konstituierung der Felder, Bereiche und Wissensgegenstände zu positionieren.« (Foucault 2004, 177)

Foucault schlägt hier weder eine alternative Theorie des Regierens oder der Macht vor noch präsentiert er verbindliche methodische Verfahrensweisen. Seine Bemerkungen lassen sich im Anschluss an eine Formulierung von Ann Stoler (2014) eher als »analytical position with methodological yield« verstehen. Es sind begriffliche Markierungen, die einen spezifischen Zuschnitt des Felds der Untersuchung implizieren. Und dieser Zuschnitt hat nicht nur eine Reihe von Vorteilen gegenüber klassischen Ansätzen der politischen Soziologie, sondern bietet gerade für eine Analytik der Sicherheit eine Reihe von Vorteilen gegenüber einer subjektzentrierten Auslegung von Gouvernamentalität. Der Fokus auf Problematisierungen als »Konstituierung der Felder, Bereiche und Wissensgegenstände« erlaubt eine Untersuchung von Risiken jenseits von Realismus und Konstruktivismus. Stehen politische Technologien im Zentrum der Aufmerksamkeit, kann die Regierungsanalytik als Untersuchung von (Sicherheits)dispositiven rekonzeptualisiert werden. Im Zentrum der Aufmerksamkeit stehen dann nicht vornehmlich allgemeine politische Programmatiken, sondern Sets miteinander verbundener Techniken – Dispositive – des Regierens. Schließlich kann die Betonung des strategischen Charakters von *Machtverhältnissen* einen Hang zu einem machttheoretischen Funktionalismus überwinden, für den die Gouvernamentalitätsstudien immer wieder kritisiert wurden (Beck 2008, 150f.). Anstatt von einem monolithischen Machtblock auszugehen, wird es so möglich, die Widerstände gegen und die Kritik an der Macht bzw. an Sicherheitstechnologien als Teil eines komplexen, strategischen Verhältnisses in den Blick zu nehmen.

So verstanden ist die Gouvernamentalitätsanalyse nicht mehr auf eine spezifische Zielscheibe des Regierens festgelegt. Dies erlaubt die »exclusive preoccupation with the fabrication of particular kinds of political subjects«

(Marres und Lezaun 2011, 491) zu überwinden, die nicht zuletzt auch von Vertretern der Akteur-Netzwerk-Theorie (ANT) und der *Science and Technology Studies* (STS) an postfoucaultschen Ansätzen moniert wurden. Sichtbar werden vielmehr die Ähnlichkeiten zwischen der Foucault'schen Machtanalyse und Konzepten und methodologischen Sensibilitäten in den STS. Das viel zu häufig verpasste Gespräch zwischen beiden Forschungstraditionen erlaubt eine wechselseitige Erweiterung und Schärfung der jeweiligen Ansätze. Die Gouvernementalitätsanalyse kann für die Rolle von sozio-technischen Gefügen des Regierens, für Natur-Kultur-Verschrankungen und für die Politik der Materialität sensibilisiert werden. Umgekehrt lässt sich die relative Blindheit der ANT und STS für Fragen der Macht und für die Genealogie politischer Rationalität adressieren.

Im Folgenden werde ich daher unter Rückgriff auf Foucault, die postfoucaultschen Ansätze in den *Governmentality Studies* und in der Anthropologie des Zeitgenössischen (Rabinow 2003, Ong und Collier 2005a) sowie auf Debatten in den STS genauer zeigen, welche Perspektiven sich durch die drei Achsen – Problematisierung (1.2.1.), Technologie (1.2.2.), Strategie (1.2.3.) – für eine Analytik der Sicherheit ergeben.

### 1.2.1. Problematisierung: Jenseits von Konstruktivismus und Realismus

Was Foucault zunächst noch etwas umständlich mit »Konstituierung der Felder, Bereiche und Wissensgegenstände« (Foucault 2004, 177) bezeichnet hat, lässt sich gut mit dem Konzept der Problematisierung fassen, das Foucault (1989a, 1996, 2005b, e) erst relativ spät eingeführt hat, um gleichsam rückwirkend das methodische Vorgehen zu explizieren, das seinen historischen Arbeiten implizit zugrunde liegt (zum Begriff der Problematisierung im Werkskontext siehe: Lemke 1997, 339–343). Zugleich steht das Konzept der Problematisierung aber auch für eine Abkehr von der quasi-strukturalistischen Fokussierung auf »diskursive Ordnungen« und Denksysteme (Rabinow 2003, 44f.) zugunsten eines offeneren, prozessorientierten Problematisierungsgeschehens, das nicht von bereits formierten Wissensregimen oder Epistemen ausgeht, sondern eine Reaktion auf Irritationen und Störungen darstellt (Folkers und Lim 2014). Mittlerweile hat auch die ANT dem Konzept der Problematisierung einen

zentralen Stellenwert eingeräumt (Callon 2006a, b).<sup>15</sup> Paul Rabinow (2003, 13–30) und Noortje Marres (2012, 28–59) haben diese Überlegungen bei Foucault bzw. in der ANT mit der Philosophie John Deweys in Verbindung gebracht, wodurch das Konzept zusätzlich an analytischer Schärfe gewonnen hat.

Foucault hat stets versucht, die Gegenstände, die er untersucht – wie Wahnsinn, Delinquenz oder Sexualität – nicht als historischen Universalien oder gegebene Objekte zu betrachten, sondern zu zeigen, wie diese historisch als Elemente einer bestimmten Art der Machtausübung entstanden sind. Auch Risiko ist das historische Ergebnis von Prozessen der Problematisierung und keine historische Universalie oder ein schlicht gegebenes Objekt. Genauso wenig ist Risiko aber »bloß« konstruiert, denn:

»Problematisierung bedeutet nicht die Darstellung eines zuvor existierenden Objekts, genauso wenig aber auch die Erschaffung eines nicht existierenden Objekts durch den Diskurs. Die Gesamtheit der diskursiven oder nicht-diskursiven Praktiken lässt etwas in das Spiel des Wahren und des Falschen eintreten und konstituiert es als Objekt für das Denken.« (Foucault 2005b, 826)

Von seiner Etymologie her betrachtet, bezeichnet das Wort Problem so viel wie Hindernis auf einem Weg, ein Ding, das den Weg versperrt und stört (Callon 2006b, 150, Flusser 1999, 58). Diese Störquellen erzeugen eine »problematische Situation«, die John Dewey zufolge durch eine »crisis of some sort« bestimmt ist: »a forking of roads of some material, a tendency to go this way and that. It represents something the matter, something out of gear, or in some way menaced, insecure, problematic and strained« (Dewey zitiert nach: Marres 2012, 165). Eine solche Situation zeichnet sich sowohl durch das Vorhandensein von Schwierigkeiten als auch durch ihre Undurchsichtigkeit aus: Objektivität als Obstruktivität und Opazität sind die Kennzeichen eines Problems. Klar ist zunächst nur, dass etwas nicht stimmt und so insistent stört, dass es – was immer »es« auch sein mag – nicht zu ignorieren ist. Etwas hat sich ereignet, das sich zugleich aufdrängt und entzieht und somit Ansprüche an das Denken stellt,<sup>16</sup> also eine Problematisierung notwendig macht.

---

15 Auch das Konzept der »matters of concern« bei Latour (2004) lässt sich mit der Thematik der Problematisierung in Verbindung bringen. Matters of concern bzw. Dinge von Belang sind solche Sachverhalte, die nicht schlicht gegebene Fakten darstellen, sondern einen angehen und zu Problematisierungen anregen.

16 Dieses für Foucault maßgebliche Konzept des Denkens findet sich bei Heidegger (2004, 123–137).

»In Wirklichkeit muss, damit ein Handlungsbereich unsicher oder ein Verhalten in das Feld des Denkens eintritt, eine gewisse Anzahl von Faktoren ihn oder es unsicher gemacht, ihm seine Vertrautheit genommen, oder in dessen Umfeld eine gewisse Anzahl von Schwierigkeiten hervorgerufen haben.« (Foucault 2005e, 732)

Der Prozess der Problematisierung besteht darin, die Elemente der Situation so zu arrangieren bzw. zu versammeln, dass sich ein klares »Lagebild« ergibt und sich eine Antwort auf die Frage einstellt, was zur Schwierigkeit geführt hat. Erst rekursiv bzw. nachträglich stellt sich also heraus, was das Problem war, auf das die Problematisierung reagiert hat bzw. reagiert haben wird.<sup>17</sup> Problematisierungen operieren im Modus des Futur II: »das wird das Problem gewesen sein«. Ist die Problematisierung erfolgreich, kann das Problem zum »obligatorischen Passagepunkt« (Callon 2006b, 149) im neu versammelten Akteur-Netzwerk werden, das antritt, das Problem aus der Welt bzw. aus dem Weg zu schaffen. Das Problem ist aus dem Dunkel des »Plasmas«, also aus dem Bereich dessen, was »noch nicht formatiert, [...] gemessen, [...] sozialisiert, [...] registriert« (Latour 2007, 419) ist, ins Licht der Netzwerke getreten. Es ist mit »Anschlussfähigkeit« (Luhmann 1991b, 62) ausgestattet und stört soziale Operationen nicht mehr, sondern schmiert und beschleunigt sie.

Dabei ergeben sich zumeist Artikulationen des Problems, die von einem höheren Abstraktionsgrad sind als die konkrete Situation, von der sie ausgehen. Indem von einer Reihe von konkreten Elementen der Situation abgesehen wird, können anfangs klar situierte Probleme auf eine Weise übersetzt werden, dass sie unabhängig von ihrem Entstehungsort und der konkreten Situation zirkulieren können; ein Phänomen, das sich in Anlehnung an Latour (1987, 227) mit dem Begriff der »immutable mobiles« bezeichnen lässt. Man mag sich diesen Vorgang in Analogie zur Übersetzung von Bewegungsenergie in elektrischen Strom vorstellen, durch die Energie beliebig durch das Stromnetz zirkulieren und für ganz unterschiedliche Zwecke – Licht, Wärme, Bewegung – eingesetzt werden kann.

Das wird gerade am Fall des Risikos besonders deutlich. Wieder ist ein Rekurs auf die Etymologie hilfreich. Das Wort für Risiko kommt vom italienischen *risco* und heißt zunächst nur so viel wie »das, was aufreißt« und

---

17 Dieses Verständnis von Rekursivität lehnt sich an Hans Jörg Rheinbergers Konzept der »rekursiven Stabilisierung« im wissenschaftlichen Forschungsprozess an, durch die »flüchtige Ereignisse fixiert« und schließlich zu »epistemischen Dingen« (Rheinberger 2002, 114) gemacht werden. Siehe auch das Konzept der »konstitutiven Nachträglichkeit« bei Urs Stäheli (1998).

später dann »Klippe« (Ewald 1993, 209). Klippen waren ein konkretes Problem, ein Hindernis auf dem Weg für den entstehenden Seehandel in der Renaissance. Eine finanzielle Absicherung gegen Schäden durch derartige Fährnisse sollte dieses Hindernis beseitigen. Aus dieser Frühform der Versicherungstechnik ist dann langsam das abstrakte Problem des Risikos entstanden. Mittlerweile können wir eine ganze Reihe von Situationen und Problemen als Risiken beschreiben und handhaben: ein Dachziegel, der einem auf den Fuß fällt, der Eintritt ins Rentenalter, Arbeitslosigkeit, umknickende Strommasten etc. lassen sich alle unter die Kategorie des Risikos bringen und als Risiken adressieren. Risiko ist zu einem »Rationalitätsschema« geworden, zu einer »Art und Weise, bestimmte Elemente der Realität zu zerlegen, neu zusammenzusetzen und zu ordnen« (Ewald 1993, 210). Das verdankt sich vor allem dem Aufkommen der Wissensformen der Statistik und Wahrscheinlichkeitsrechnung (siehe dazu: Daston 1987, Hacking 1990), die es erlaubt haben, Risiko zu formalisieren. Risiko ist also tatsächlich untrennbar mit moderner Rationalität verbunden. Allerdings wäre es ein Fehler, die Rationalität des Risikos als »Rationalisierung des Zufalls« (Foucault 2004, 93) mit Zweckrationalität *per se* gleichzusetzen, wie Beck das tut. Die Grenzen bestimmter Kalkulationsformen des Risikos stellen neue Probleme, sie regen neue Problematisierungen an und sind damit generativ für neue, alternative Formen der Abschätzung und Antizipation des Risikos (siehe dazu u.a.: Bougen 2003, Ericson und Doyle 2004).

Dabei ist Risiko keineswegs die einzige Möglichkeit, auf die Arten von Schwierigkeiten zu reagieren, die wir heute als riskant beschreiben. »Auf ein und dieselbe Gesamtheit von Schwierigkeiten können mehrere Antworten gegeben werden.« (Foucault 2005e, 732) Paul Rabinow betont, dass die Analyse von Problematisierungen unsere Situationswahrnehmung modifiziert: »a modal change from seeing a situation not only as »a given« but also as »a question« (Rabinow 2003, 18).<sup>18</sup> Die Aufgabe der Machtanalytik besteht darin, diesen Effekt sichtbar werden zu lassen, indem sie die vorgefundene Problematisierung zugleich aufnimmt, darstellt, aber eben auch entstellt. Gelingt dies, so kommt es zu einer »Reproblematierung« (Foucault 2005j, 751). Aber auch jenseits solcher Reproblematierungen bleiben die Problematisierungen der Sicherheit vertrackt und

---

18 Eine ähnliche Forschungsstrategie hatte auch Luhmann (1991b, 37) mit seinem Konzept der funktionalen Analyse im Sinn, bei der es nicht nur um das Auffinden von Problemlösungen geht, sondern ebenso um das Fragen nach »funktionalen Äquivalenten«.



problematisch, weil sich das Irritierende und Opake der Situationen, von denen sie ausgehen, niemals vollkommen transparent machen lässt und weil gerade in Unsicherheitssituationen jede Form des Wissens stets von Nichtwissen begleitet wird (Wehling 2006). Trotz der Reinigungsarbeit der Problematisierung haftet jedem Problem immer noch etwas »Plasma« an, ja, der plasmatische Bereich, die dunkle Materie wird gerade durch die Zunahme des Wissens immer größer (Luhmann 1992b), wenn *known unknowns* auf *unknown unknowns* verweisen (Daase und Kessler 2007).

### 1.2.2. Von der Institution zur Technologie

Probleme können nicht unabhängig von den (Macht)Technologien existieren, die sie erzeugen und die ihre Beständigkeit sichern, genauso wenig wie wissenschaftliche Fakten oder epistemische Dinge unabhängig von laborativen Einrichtungen und wissenschaftlichen Apparaturen existieren (Latour und Woolgar 1979). Jenseits der Netzwerke der Macht existiert das Problem als Gegenstand der Regierung genauso wenig wie wissenschaftliche Fakten jenseits der Infrastrukturen der Wissenschaft. Es ist deshalb nicht leicht anzugeben, wo eine Machttechnologie beginnt und wo das Problem endet, weil beide wechselseitig aufeinander verweisen. Das Problem ist eine Zielscheibe der Macht, die durch dieses Zielen überhaupt erst erzeugt wird. Umgekehrt ist die Technologie des Regierens immer auf ein »Außen« bezogen, das sie durch ihre internen Operationen zugleich miterzeugt.<sup>19</sup> Insofern ist die Etablierung eines Problems bereits Teil der Lösung, wenn etwa eine Reihe von diffusen Gefährdungslagen unter die Kategorie des Risikos gebracht und dadurch überhaupt erst regierbar gemacht werden. Durch die Problematisierung kommt es gleichsam zu einer »immunsierenden Hereinnahme« (Lorey 2011) des störenden Außen ins Innere der Netzwerke der Sicherheit nach dem Motto: Gefahr erkannt, Gefahr gebannt. Gerade »Risiko« erlaubt eine solche Immunsierung, weil sie jenseits der quasi räumlichen »Hereinnahme« des Außen ins Innen auch eine »immunsierende Vorwegnahme« der Zukunft in der Gegenwart erlaubt (Folkers

---

<sup>19</sup> Ähnlich hat Karan Barad argumentiert, dass ein wissenschaftlicher Apparat Phänomene hervorbringt und Grenzen zwischen unterschiedlichen Entitäten zieht, die aber letztlich nicht außerhalb dieses apparativen Settings existieren. Zwischen Apparat und Phänomen existiert eine »Äußerlichkeit-Innenhalb-von-Phänomenen« (Barad 2012, 20). Systemtheoretisch könnte man argumentieren, dass die Problemumwelt letztlich durch eine systeminterne Unterscheidung zwischen System und Umwelt erzeugt wird.

2013a, 90). Durch die Kategorie des Risikos werden mögliche Gefahren erwartbar, kalkulierbar, bepreisbar bzw. können in aktuelle Bilanzierungen »eingepreist« werden. Risiko »faltet« damit gewissermaßen das Außen ins Innen und die Zukunft in die Gegenwart und macht damit ein ungewisses und potenziell gefährliches Geschehen regierbar. In den *Governmentality Studies* und den *Critical Security Studies* wird daher häufig von einem »governing through risk« (Ericson 2005, Aradau und Munster 2007) statt »governing of risk« gesprochen. Bei Foucault selbst finden sich eine Reihe zirkulärer Formulierungen, um deutlich zu machen, dass Technologien und Probleme, die Macht und das, worauf sie sich richtet, zusammengehören. Die Seele ist »Effekt und Instrument« (Foucault 1976, 42) der Disziplinarmacht und die Bevölkerung »Subjekt und Objekt« (Foucault 2004, 27) der Sicherheitstechnik.

Technik wird hier in einem erweiterten Sinn verstanden. »Technik« – das sind nicht nur Werkzeuge wie ein Hammer oder Technologien wie ein Computer, sondern ebenso ein bestimmtes know-how, ein operatives Wissen, das nicht nur versucht, die Welt zu erkennen, sondern intervenierend in sie einzugreifen. Auch solches know-how ist materialisiert oder verkörpert und kann in Form von technischen Gegenständen, Lehrsätzen, Verfahrensvorschriften, Übungsanleitungen, Berechnungsformeln etc. zirkulieren. Es ist also nicht bloß individuell, sondern stets bis zu einem gewissen Grad auch seriell. Foucault hat sich in seiner Forschung auf Technologien der Macht bzw. politische Technologien (Foucault 2005a) bzw. Technologien des Selbst (Foucault 2005g) konzentriert, also auf Verfahrensweisen, die andere gefügig machen bzw. das Selbst in einen gewünschten Zustand bringen sollen (siehe für eine Definition von Macht- und Selbsttechnologien: Foucault 2005g, 968). Die STS und ANT haben dagegen stärker als Foucault Technik als sozio-materielle Artefakte verstanden und untersucht. Techniken sind hier sowohl »calculative devices« (Callon und Muniesa 2005), also Wissenstechniken, als auch technische Gegenstände bzw. Netze von Alltagsgegenständen bis hin zur Hochtechnologie. Zu selten wurde hier jedoch die Politik dieser Artefakte explizit thematisiert (für eine Ausnahme siehe: Winner 1980), während umgekehrt bei Foucault häufig der technologische Charakter der Macht zu kurz kam. In dieser Arbeit möchte ich versuchen, beide Forschungsstränge zusammenzuführen und die wechselseitige Durchdringung von Macht- bzw. Sicherheitstechniken und technischen Artefakten herauszuarbeiten.

Das hervorstechende Beispiel für eine Sicherheitstechnologie ist die Versicherung. Wenn wir das Wort Versicherung hören, denken wir wohl für gewöhnlich an eine Versicherungsinstitution, zum Beispiel an eine bestimmte Versicherungsgesellschaft. Foucault hat jedoch gegen einen solchen »Institutionalozentrismus« (Foucault 2004, 175) protestiert und vorgeschlagen, »die Machtbeziehungen hinsichtlich der Institution freizulegen, um sie unter dem Gesichtspunkt der Technologien zu analysieren« (Foucault 2004, 177). In diesem Sinne stellt Ewald in Bezug auf die Versicherung fest:

»Der Begriff der Versicherung bezeichnet jedoch nicht nur bestimmte Institutionen, sondern darüber hinaus das, was die Einheit ihrer Verschiedenheit ausmacht. [...] In diesem erweiterten Sinne bezeichnet Versicherung weniger ein Konzept als eine abstrakte Technologie. Die Versicherung ist [...] die Matrix, die ausgehend von den Prinzipien [...] der Technologie des Risikos, unterschiedliche Versicherungskombinationen herzustellen erlaubt [...]. Die Versicherung als Technologie ist die Kunst, gemäß bestimmten, spezifischen Regeln Elemente der ökonomischen oder sozialen Realität miteinander zu kombinieren, Kombinationen, aus denen verschiedene Versicherungsinstitutionen hervorgehen.« (Ewald 1993, 207)

Auch andere Verfahrensweisen der Sicherheit lassen sich solcherart als »abstrakte Technologien« bzw. »abstrakte Formen« beschreiben, die eine Matrix für konkrete Anwendungen liefern.<sup>20</sup> Eine erste Pointe dieser Vorgehensweise besteht darin, zeigen zu können, wie dieselbe Technologie in ganz unterschiedliche Institutionen eingeschrieben und in unterschiedlichen sozialen Feldern und politischen Kontexten aktualisiert werden kann. Ein und dieselbe Technologie kann dabei unterschiedlichen Interessen dienen und mitunter sogar gegensätzliche Effekte hervorbringen. Gerade aus genealogischer Perspektive zeigt sich die Vielfältigkeit und Polyvalenz einer (Sicherheits)technologie wie der Versicherung. Als Seeversicherung im frühen Handelskapitalismus fungiert sie als »Tochter des Kapitals« (Ewald 1993, 223). Später dient sie der Arbeiterbewegung, die mit neuen Formen der Solidarisierung experimentiert (Defert 1991). Als Sozialversicherung wird sie schließlich das zentrale Instrument des modernen Wohlfahrtsstaates (Ewald 1993, 277ff.). Gegenwärtig lässt sich eine Proliferation finanzmarktlicher Versicherungsprodukte beobachten.

Eine weitere Pointe der »Deinstitutionalisierung« der Analyse besteht darin, zeigen zu können, wie eine bestimmte Sicherheitstechnologie sich in

---

<sup>20</sup> So argumentiert Andrew Lakoff (2007, 254): »Thus, like insurance, preparedness is an abstract form that can be actualized in diverse ways, according to diverse political aims.«

ein größeres Ensemble einfügt. Solche größeren Ensembles von Technologien nennt Foucault »Dispositiv« bzw. »Sicherheitsdispositiv«. Obwohl Foucault selbst nur spärliche Kommentare zum Begriff des Dispositivs gegeben hat (Foucault 1978, 119–125), ist das Dispositiv zu einem seiner meistdiskutierten Konzepte geworden. Allein die Frage, »Was ist ein Dispositiv?« hat mehrere hochkarätige Antworten erhalten (Deleuze 1991, Agamben 2008, Bussolini 2010). Häufig wird die Ähnlichkeit des Dispositivkonzepts mit dem Gestell bei Heidegger (2004, 9–40), der Maschine bzw. dem Gefüge bei Deleuze und Guattari (1997), dem Apparat bei Barad (2012) und dem Netzwerk bei Latour (2007) betont, was es bisweilen nicht erleichtert zu sehen, was genau ein Dispositiv ist. Zudem wird das Konzept mittlerweile so ubiquitär verwendet, dass man sich fragen muss, was denn eigentlich kein Dispositiv ist (diese Frage stellt auch: Walters 2012, 76). Tatsächlich erscheint eine negative Bestimmung geeignet, zentrale Merkmale des Konzepts kontrastiv zur Geltung zu bringen:

(1) Ein Dispositiv ist keine *Technik* oder ein *device* im Sinne der ANT (Muniesa, Millo und Callon 2007, Marres und Lezaun 2011). Erst ein größerer Zusammenhang von Techniken bildet ein Dispositiv. Das Dispositiv ist dann das, was zwischen diesen Techniken eine Verbindung herstellt und sie auf eine spezifische Weise anordnet und ausrichtet. »Das Dispositiv selbst ist das Netz, das zwischen diesen Elementen geknüpft werden kann.« (Foucault 1978, 120) Versicherungstechniken wie Renten- und Arbeiterunfallversicherung sind dann Teile eines größeren Sicherheitsdispositivs der biopolitischen Bevölkerungssicherheit, das etwa auch öffentliche Gesundheits- und Hygienemaßnahmen umfasst.

(2) Ein Dispositiv ist keine *Struktur*, die die Techniken in eine feste Ordnung der Dinge einfügt und das Handeln der Akteure gleichsam »hinter deren Rücken« bestimmt. Ein Dispositiv steht nicht »hinter« dem Geschehen, sondern eben »zwischen« den einzelnen Elementen des Geschehens. Es ist eher das Prinzip der Zerstreung und Dispersion des Wirklichen als dessen taxonomische Ordnung. Ein Dispositiv erzeugt ein Feld konditionierter Möglichkeiten und keinen Determinationszusammenhang.

(3) Ein Dispositiv ist keine *Institution* oder ein *Staatsapparat*, wenn auch Institutionen durchaus Teil eines Dispositivs sein können. Aus der Perspektive des Sicherheitsdispositivs ergibt es deshalb keinen Sinn, die Institution der privaten Versicherung als »Grenzbaum« (Beck 2008, 239) zwischen erster und zweiter Moderne anzusetzen. Vielmehr wäre zu

untersuchen, wie es zu einer Neuverteilung des Risikos innerhalb eines Sicherheitsdispositivs kommt, wenn eines seiner Elemente ausfällt oder überfordert ist.

(4) Ein Dispositiv ist kein *gesellschaftliches Subsystem*, sondern vielmehr ein Prinzip der Verknüpfung und Entdifferenzierung, das isomorphe Formen der Sicherung und isomorphe Problembeschreibungen in ganz unterschiedlichen »Systemen« bzw. sozialen Feldern erzeugt. Nicht »Differenzierung, sondern dispositivartige Kopplung und Macht-Isomorphie« (Saar 2003, 185) sind die Leitbegriffe von Foucaults Analytik.

(5) Ein Dispositiv ist aber auch keine *Gesellschaft*. Zwar zieht sich ein Dispositiv quer durch eine ganze Reihe gesellschaftlicher Bereiche, aber es deckt das soziale Feld nicht ab oder totalisiert es. Das Sicherheitsdispositiv ist nur ein bestimmter Zug, eine Tendenz oder Kraftlinie neben anderen. Die Dispositivanalyse untersucht »Gesellschaft« lateral bzw. transversal und nicht aus der Zentralperspektive.

Aber was macht dann ein Dispositiv abgrenzbar, wo sind die »Grenzen« des Dispositivs? Ein Dispositiv zeichnet sich durch eine Vielfalt von Elementen aus, aus denen es zusammengesetzt ist: »ein entschieden heterogenes Ensemble, das Diskurse, Institutionen, architekturelle Einrichtungen, reglementierende Entscheidungen, Gesetze, administrative Maßnahmen, wissenschaftliche Aussagen, philosophische, moralische oder philanthropische Lehrsätze, kurz: Gesagtes ebenso wie Ungesagtes umfaßt« (Foucault 1978, 119f.). Zugleich herrscht eine relative Knappheit in Bezug auf die Probleme, auf die es reagiert. Korrespondierende Probleme und wandernde Problembeschreibungen vernetzen unterschiedliche Institutionen und Elemente zu einem Dispositiv. Probleme fungieren somit in einem gewissen Sinn als »boundary objects« (Star und Griesemer 1989),<sup>21</sup> die es ermöglichen, die Grenzen zwischen Institutionen und unterschiedlichen gesellschaftlichen Bereichen zu überwinden. Zugleich führen gleichgerichtete Problemwahrnehmungen zu einer kohärenten Ausrichtung einer Reihe teils bestehender, teils neu geschaffener Technologien des Regierens. Gerade Problembeschreibungen von relativ hohem Abstrakti-

---

21 Susan L. Star und James Griesemer (1989, 393) definieren »boundary objects« als »analytical concept of those scientific objects which both inhabit several intersecting worlds [...]. Boundary objects are [...] both plastic enough to adapt to local needs [...] yet robust enough to maintain a common identity across sites.« Sowohl geteilte Probleme als auch Technologien können als boundary objects verstanden werden, die an unterschiedlichen Orten den gegebenen Umständen angepasst werden können und so ein Sicherheitsdispositiv verknüpfen.

onsgrad wie die »soziale Frage« oder »systemisches Risiko« bilden gleichsam ein Gravitationszentrum, um das herum sich unterschiedliche Technologien zu einem Dispositiv anordnen. Die Zusammengehörigkeit unterschiedlicher Technologien zu einem Dispositiv ist den Akteuren in konkreten Institutionen keineswegs stets bewusst. Es ist letztlich die Aufgabe der Forschenden, das Dispositiv abzugrenzen. Die Suche nach korrespondierenden Problemen und gleichgerichteten, paradigmatischen Technologien eröffnet aber ein heuristisches Motiv, das diese Aufgabe anleiten kann.

### 1.2.3. Von der Funktion zur Strategie

Wenn Beck in Analogie zu »failed states« von »failed insurances« (Beck 2008, 249) spricht und die *Governmentality Studies* dafür angreift, dass diese »dem offensichtlich ineffektiven Überwachungsstaat auf den Leim« gehen und »einem falschen Selbstbildnis des Staates« (Beck 2008, 151) anhängen, dann trifft er sicherlich einen wunden Punkt. In der Tat gibt es eine Tendenz in den *Governmentality Studies*, die Macht überall zu sehen und als allmächtig zu verstehen. Die Rede von »governable catastrophes« (O'Malley 2003) scheint zu unterschlagen, wie schwerwiegend Katastrophensituationen Regierungen in Bedrängnis und Erklärungsnöte bringen können. Allerdings geht es der Analyse des Sicherheitsdispositivs gar nicht um Gelingen und Scheitern bzw. eine »funktionelle Bilanz des Mehr oder Weniger [...], dessen [...], was angestrebt war und was tatsächlich erreicht wurde« (Foucault 2004, 176). Vielmehr soll versucht werden, den Gesichtspunkt der Funktion zu suspendieren und stattdessen eine »strategische Analyse« (Foucault 2004, 176) vorzunehmen.<sup>22</sup> Machtdispositive haben keine im Voraus bestimmbaren und eingrenzbaeren Funktionen oder klare Zwecke, die entweder erfüllt werden können oder nicht. Vielmehr ist von einer »funktionelle[n] Überdeterminierung« (Foucault 1978, 121), also einer Pluralität möglicher Funktionen auszugehen. Ein partielles Scheitern kann

---

<sup>22</sup> Foucault hat gleichwohl keinen durchgängigen und einheitlichen Begriff von Strategie. Manchmal bezeichnet Strategie im Gegensatz zu Taktik einen größeren Zusammenhang von Machtpraktiken (Foucault 2005f). Ich werde daher den Begriff der Strategie nicht terminologisch streng verwenden. Wenn es um die analytische Sensibilität geht, die ich hier im Anschluss an Foucault evoziere, werde ich eher situationsangepasst von Kritik oder Problematisierung der Sicherheit oder Repositionierung von Sicherheitstechnologien und dergleichen sprechen.

daher auch durch »strategische [...] Wiederauffüllungen« (Foucault 1978, 121) kompensiert werden. So kann die Proliferation von Versicherungsprodukten auf den Finanzmärkten (wie Katastrophenanleihen, sogenannte *cat bonds*) als »Wiederauffüllung« angesehen werden, weil so das scheinbare Scheitern der Versicherung in eine neue Investitionsmöglichkeit verwandelt wurde (siehe etwa: Bougen 2003). Die »Grenzen« der Risikokontrolle wurden zur *new frontier* kapitalistischer Wertschöpfung und damit zu einem neuen Handlungsfeld der Risikokontrolle ausgerollt. In dieser Hinsicht besteht das Sicherheitsdispositiv aus »[c]ogs and levers that don't work – and yet which ›work‹ in the sense that they produce effects that have meaning and consequences for us« (Rose 1996b, 38).

Dabei ist das Scheitern der Sicherheitsdispositive geradezu strukturell in ihrer Funktionslogik angelegt, weil sie schließlich die Probleme, die sie bearbeiten, überhaupt erst erzeugen und deswegen ihre Probleme grundsätzlich nicht einfach lösen können. Je erfolgreicher Sicherheitsdispositive sind, desto mehr Risiken, Gefahrenquellen und bedrohte Schutzgüter identifizieren sie. Nicht selten führt das zu einer Überforderung, die als Scheitern registriert wird, weil nicht erkannt wird, dass das Sicherheitsdispositiv in einem internen Zusammenhang mit dem Anwachsen von Risiken steht. Häufig führt das zum Ruf nach noch mehr vom Gleichen, nach noch mehr Sicherheit. »When they fail, this only justifies the need for more of the same.« (Dreyfus und Rabinow 1983, 169) Gerade in der »immunisierenden« Operationsweise von Sicherheitsdispositiven liegt auch ihr autoimmunisierender Hang. Gerade dass sie das gefährliche Außen in sich hineinnehmen und es so regierbar machen, führt dazu, dass die eigenen Operationen der Sicherheitsdispositive ihrerseits stets riskant bleiben. Die Topologie der Immunisierung ist immer schon eine »Topologie der Autoimmunität« (Derrida 2003, 58, siehe auch: Folkers 2013a).

So wichtig es ist, Ausweitungen und Umschichtungen der Macht in Reaktion auf ihr eigenes Scheitern zu analysieren, so sehr läuft eine solche Analyseperspektive Gefahr, zu einem erweiterten Funktionalismus à la Luhmann zu werden, wo Störungen wie ein Schmiermittel für soziale Systeme wirken. Gerade im Scheitern läge dann der »Modus der Unabschließbarkeit« (Bröckling 2012, 103), also der ständigen Ausweitung der Sicherheitsdispositive. So bleibt aber unklar, welche Kräfte und Mechanismen Sicherheit in ihre Schranken weisen. Schließlich sind Sicherheitsdispositive trotz ihres unbegrenzten Anspruchs – »man kann nie sicher genug sein« – faktisch in vielerlei Hinsicht begrenzt. Deshalb möchte ich in dieser Arbeit

nicht nur die strategischen Ausweitungen, sondern auch die Formen der Limitierung der Sicherheit untersuchen. Ein Grund dafür liegt nicht zuletzt in den Dynamiken der Kritik an bestimmten Formen der Sicherheit. Eine zentrale Überzeugung dieser Arbeit liegt denn auch darin, dass das Entscheidende am Problem der Sicherheit in der Gegenwart übersehen wird, wenn die sicherheitspolitischen Kontroversen und kritischen Infragestellungen von Sicherheitsstrategien ausgeblendet werden. In Anlehnung an Ansätze, die Kritik und Kontroversen als wirksamen Bestandteil sozialer Prozesse beschreiben – wie die pragmatische Soziologie der Kritik (Boltanski und Thévenot 2007) und die »controversy analysis« (Latour 1987, 21–44, 2007, 41–49, Marres 2007) – werde ich die Foucault'sche Regierungsanalyse weiterentwickeln, indem ich sie für »Praktiken der Kritik« (Celikates 2009) sensibilisiere. Regierung wird dann als »doppelte Bewegung« aus Regierungsausweitungen und ihrer kritischen Begrenzung analysierbar (siehe dazu systematisch: Folkers 2016). Die strategische Analyseachse macht die Regierungsanalyse dadurch beweglich, sie lässt Positionswechsel von Technologien und Reformulierungen von Problematisierungen sichtbar werden und vermeidet so den Eindruck, ein Dispositiv sei ein erstarrter Apparat, der stets vorhersehbare Effekte zeitigt (diesen Verdacht äußert: Thrift 2007, 55).

So lässt sich zeigen, dass Problematisierungen auch ihrerseits – durch Gegengutachten, neue Erkenntnisse, öffentliche Anhörungen etc. – problematisiert werden können. Gerade Situationen der Unsicherheit, die mit Nichtwissen bezüglich der möglichen zukünftigen Gefährdungen einhergehen, weisen ein großes Konflikt- und Politisierungspotenzial auf (Wehling 2006, 316–323). Und auch Technologien der Sicherheit können zum Problem gemacht werden, wenn sie im Verdacht stehen, nicht intendierte Nebeneffekte zu zeitigen, die Freiheit einzuschränken oder ihren legitimen Anwendungsbereich zu überschreiten. Der Verdacht, dass Sicherheitstechnologien zu weit gehen und perverse Effekte haben, begleitet die modernen Sicherheitsdispositive spätestens seit Beginn der liberalen Kritik an der Regierung. Nicht nur die unintendierten Nebeneffekte industrieller Technologien, auf die Beck (1996) so eloquent hingewiesen hat, stellen ein Problem gegenwärtiger Risikopolitik dar. Aus einer Foucault'schen Perspektive wird deutlich, dass und wie auch die perversen Effekte der Technologien der Sicherheit und des Regierens immer wieder einer »technischen Kritik« unterzogen wurden (Collier 2011, 177, Folkers 2016). So wie Probleme einen Doppelcharakter als Zielscheibe und Vehikel



der Sicherheit haben, haben auch Technologien einen *Doppelcharakter als Mittel und Problem*. Sicherheitstechniken sind zugleich politische Technologien und Gegenstände politischer Kontroversen, wobei die technische Kritik der Sicherheit der Operator für das Umkippen, den Gestaltwandel von Instrument zu Problem wird. Die gegenwärtige sicherheitspolitische Konjunktur scheint nicht nur durch die Ausweitung der Sicherheit auf Grund neuer Risiken und Probleme, sondern durch ein Problematisch-Werden der Sicherheit selbst gekennzeichnet zu sein. Deswegen werde ich eine mehrstufige Analytik der Problematisierung durchführen, die sowohl die Prozesse der Identifizierung von Sicherheitsproblemen als auch die Problematisierung von Sicherheit in den Blick nimmt.

Die strategische Analyse hat einen heuristischen und einen kritischen Wert. Einerseits erlaubt sie es, die Selbstverständlichkeit von Gefahrenbeschreibungen und Sicherheitstechniken zu hinterfragen. Im Zustand der Kontroverse sind soziale Sachverhalte keine geronnenen sozialen Tatsachen, sondern offene Streitsachen (Latour 2004). Die Einsätze und Grenzen bestimmter Sicherheitstechnologien werden gerade im und durch den Konflikt deutlich. Die synchrone Nebeneinanderstellung unterschiedlicher Rationalitäten in der Gegenwartsanalytik ergänzt die genealogischen Perspektive, in der diachron unterschiedliche politische Rationalitäten analysiert werden. Jeweils wird ein ähnlicher, wenn auch nicht in allen Punkten gleichgerichteter Distanzierungseffekt erzeugt:<sup>23</sup> jeweils geht es nicht nur darum, was ist, sondern ebenso um dessen Alternativen. Wiederum geht es darum, einen »Modalwandel« zu erzeugen, der eine bestimmte Situation nicht nur als gegeben, sondern als umkämpft, als Kraftfeld sichtbar werden lässt. In diesem Sinn sind sowohl ANT als auch die Foucault'sche Analytik weniger Wirklichkeitswissenschaften denn Möglichkeitswissenschaften. Hier liegt auch der kritische Sinn der Kontroversen und Kritikanalyse. Die

---

23 Für Foucault können Problematisierung sehr langandauernde und grundlegende Konstellationen sein (Rabinow 2003, 55). Ein Beispiel wäre das Problematisch-werden des Lebens in der modernen Biopolitik. Das schließt Konflikte jedoch keineswegs aus, sondern ermöglicht sie geradezu, in etwa so wie laut Wittgenstein (1985) nur ein grundlegender Bereich der Gewissheit den (philosophischen) Zweifel ermöglicht. »Die Arbeit einer Geschichte des Denkens bestünde indes darin, an der Wurzel dieser verschiedenartigen Lösungen die allgemeine Form einer Problematisierung wiederzufinden, die sie möglich gemacht hat – bis hinein in ihren Gegensatz« (Foucault 2005e, 733). Um nicht nur die »Wurzeln«, sondern auch die »Gegensätze« und ihre politischen Einsätze und Effekte in den Blick zu bekommen, bieten sich das situativere Konzept von Problematisierung und die Kontroversenanalyse in den ANT und STS als sinnvolle Ergänzung der Foucault'schen Analytik der Problematisierung an.

strategische Analyse betont die »Umkehrbarkeit« (Foucault 1992, 40) von Machtverhältnissen und zeigt konkrete Optionen, wie Sicherheit gedacht und gemacht werden kann.

Analytische Achse	Alternative zu	Fokus auf
Problematisierung	Realismus und Konstruktivismus	Entstehung von Problembereichen der Sicherheit und Zielscheiben des Regierens
Technologie/ Dispositiv	Institutionalismus	<ul style="list-style-type: none"> <li>– systematisch ausgearbeitete Rationalitäts- und Handlungsschemata der Sicherheit</li> <li>– Verkettung von Technologien zu einem Dispositiv</li> </ul>
Strategie	Funktionalismus	<ul style="list-style-type: none"> <li>– Offenheit und Flexibilität von Regierungstechnologien</li> <li>– autoimmune Effekte von Sicherheitstechnologien</li> <li>– Konflikte, Kontroversen, Kritik (an/um Paradoxien der Sicherheit)</li> </ul>

*Tabelle 1: Die Achsen der Dispositivanalyse*

### 1.3. Genealogie der Sicherheitsdispositive

In Foucaults historischen Forschungen findet sich – zumindest implizit – ein neuartiges Verständnis von Sicherheit. Ähnlich wie seine mittlerweile kanonisch gewordenen Konzepte von (produktiver) Macht und Regierung (als Gouvernementalität) hat Foucault auch versucht, zu einem Konzept von »Sicherheit« zu kommen, das nicht auf die Problematik souveräner Staatlichkeit beschränkt ist, die zumeist die Matrix des Nachdenkens über Sicherheit darstellt.<sup>24</sup> Das Foucault'sche »Problem der Sicherheit«

<sup>24</sup> Gerade in der Politikwissenschaft findet sich klassischerweise ein staatszentriertes Verständnis von Sicherheit. »Sicherheitspolitik« umfasst hier Themen wie militärische Konflikte zwischen Staaten, Diplomatie und bisweilen auch innenpolitische Ausnahmesituationen wie Notstände oder Bürgerkriege. Mittlerweile wird jedoch auch hier verstärkt ein »erweitertes Sicherheitsverständnis« diskutiert, wodurch einige Engführungen der politikwissenschaftlichen Debatte vermieden werden können (siehe u.a.: Buzan, Wæver und De Wilde 1998, Daase 2010). Damit wird nicht zuletzt die faktische Erweiterung des operativen Sicherheitsverständnisses auf der Bühne internationaler Politik seit

(Foucault 2006, 100) ist also ein anderes als das Hobbes'sche. Das, was Foucault als »Sicherheitsmechanismen« (Foucault 2001, 290) bzw. als Machtform der Sicherheit einführt (Foucault 2004, 13–133), steht explizit im Kontrast zum klassischen, Hobbes'sche Sicherheitsstaat, der Sicherheit im Inneren, auch auf Kosten der Freiheit seiner Bürger, gewährleistete und zugleich die Integrität des Territoriums gegen äußere Feinde mit Hilfe eines »ständigen diplomatisch-militärischen Apparat[s]« (Foucault 2006, 18) sicherte. Foucault fokussiert vielmehr auf eine liberale und biopolitische Konfiguration von Sicherheit. Das liberale Sicherheitsverständnis erlaubt anders als das Hobbes'sche keinen *trade-off* von Freiheit gegen Sicherheit.<sup>25</sup> Vielmehr zielen liberale Sicherheitstechnologien auf die *Sicherung der Freiheit* des Individuums und der *Freizügigkeit* der bürgerlichen Gesellschaft. Die liberale »Regierungskunst stellt sich also als Manager der Freiheit dar« (Foucault 2006, 97). Biopolitische Sicherheitstechnologien kümmern sich nicht primär um die Sicherung souveräner Macht und um die Wahrung der Integrität des Territoriums, sondern um die *Aufrechterhaltung und Steigerung des Lebens der Bevölkerung*. Dafür werden Maßnahmen in Anschlag gebracht, die über das Repertoire souveräner Sicherheit, also Militär, Diplomatie und Polizei (im klassischen Sinne), hinausgehen. Biopolitische Sicherheit operiert über eine Reihe von »Sicherheitsmechanismen« bzw. »Regulationsmechanismen« (Foucault 2001, 290), die nicht repressiv-verbietend auf den Gesellschaftskörper einwirken, sondern steuernd und anreizend versuchen, die Bedingungen des Lebens der Gattung bzw. die Kontinuität vitaler gesellschaftlicher Prozesse und Funktionen sicherzustellen. Biopolitische

---

Ende des Kalten Krieges (siehe dazu: Rothschild 1995b) reflektiert (und bisweilen auch performativ vorangetrieben). Mithilfe von Foucaults Konzept des Sicherheitsdispositivs lassen sich diese »Erweiterungsbemühungen« historisch und systematisch vertiefen. Eine Genealogie der Sicherheitsdispositive kann eine Reihe historisch gewachsener Modi der Sicherheit unterscheiden, die bis in die Gegenwart wirksam sind (siehe beispielhaft: Gros 2015). Das Dispositiv souveräner Staatssicherheit ist nur eine, wenn auch unbestreitbar wichtige, Spielart der Sicherheit, die nicht erst seit Ende des Kalten Krieges durch andere Formen der Sicherheit erweitert wurde.

25 Unglücklicherweise wird das Hobbes'sche Problem der Sicherheit häufig mit dem liberalen identifiziert (siehe etwa: Meyer 2009, 30). Frédéric Gros argumentiert sogar, dass letztlich alle modernen Vertragstheorien von Hobbes bis Rousseau auf das gleiche Sicherheitsverständnis hinauslaufen (Gros 2015, 101–121). Dadurch verliert man aber allzu leicht die Differenzen zwischen Hobbes und liberalen Denkern wie John Locke (siehe: Valverde 2011, 10f.) oder David Hume und Adam Smith (siehe: Rothschild 1995a) aus dem Blick, die sich explizit kritisch zum absolutistischen Sicherheitsstaat geäußert haben.

Sicherheit ist eine sorgende Form der Sicherheit: Fürsorge, Vorsorge und Versorgung sind ihre wesentlichen Ziele. Frederic Gros gruppiert diese Strategien in Abgrenzung zur klassischen »Staatssicherheit« unter dem Begriff der »Biosicherheit«<sup>26</sup> und weist zurecht darauf hin, dass die Vorstellungswelt der Biosicherheit in Begriffen wie »Ernährungs-, Energie-, Gesundheitssicherheit, affektive Sicherheit, oder auch menschliche Sicherheit« (Gros 2015, 12) – hinzuzufügen wäre natürlich auch die soziale Sicherheit – anzutreffen ist.

Vorläufer der biopolitischen Sicherheitsmaßnahmen, die sich erst im 19. Jahrhundert systematisch auf die Sicherung des Leben gerichtet haben, finden sich sowohl in pastoral-karitativen Machtformen (Foucault 2004, 173–330) als auch in der vor- und versorgenden »Polizey«, wie sie die Polizeiwissenschaft des 18. Jahrhunderts im Sinn hatte (Foucault 2004, 449–519). Das Auftauchen moderner biopolitischer Sicherheitstechnologien ist allerdings ebenso untrennbar mit dem Aufstieg des Liberalismus verbunden, der gerade den kirchlichen und polizeistaatlichen Quellen der biopolitischen Sicherheit kritisch gegenüberstand und für eine Begrenzung der Regierungstätigkeit eintrat. So ist die Verbindung von liberalen und biopolitischen Zielen und Strategien in modernen Formen der Sicherheit gewiss nicht immer eine Liebesheirat gewesen, sondern eher die Schicksalsgemeinschaft eines Paares, deren Teile zufällig zum gleichen Zeitpunkt auf der historischen Bühne erschienen sind und die nicht mit, aber auch nicht ohne einander auskommen.<sup>27</sup> Die Grundkonstellation moderner Sicherheit ist durch ein potenziell spannungsreiches Verhältnis von liberaler politischer Rationalität und der biopolitischen Substanz moderner Re-

---

26 Ich verwende hier nicht den Begriff der Biosicherheit, um Verwechslungen mit dem Konzept der biosecurity zu vermeiden, das Sicherheitsmaßnahmen in Bezug auf Entwicklungen von Biotechnologien und ansteckende Krankheiten begrifflich fasst (siehe dazu: Lakoff und Collier 2008). Zudem ist Gros' Konzept nicht ausreichend trennscharf, um die Differenzen und Transformationen innerhalb von biopolitischen Sicherheitsdispositiven hervortreten zu lassen.

27 Andere Autor\_innen (Lemke 2011, Tellmann 2013) betonen im Anschluss an Foucault stärker den intrinsischen Zusammenhang von Liberalismus und Biopolitik und beziehen sich dabei vor allem auf epistemologische Wahlverwandtschaften zwischen liberalen Vorstellungen von Ökonomie und der Idee des Lebens, die Foucault (1974) schon in der Ordnung der Dinge herausgearbeitet hatte, sowie auf die Parallelen zwischen der Konzeption der Bevölkerung und des Marktes als natürliche, selbstorganisierende Entitäten (siehe dazu: Foucault 2004). Das ist sicher nicht falsch, droht aber das spezifische Konfliktpotenzial liberal-biopolitischer Sicherheitsdispositive nicht ausreichend zu betonen.

gierungsformen gekennzeichnet, ein Spannungsverhältnis zwischen *Sicherung der Freiheit* und *Sicherung des Lebens und Überlebens*. So bestimmt Foucault Sicherheitstechnologien als »Kehrseite und Bedingung des Liberalismus« (Foucault 2006, 100) und weist mit dieser paradoxen Formulierung bereits auf ein Dilemma hin, das bis heute nichts von seinem politischen Konfliktpotenzial eingebüßt hat. Einerseits sind die Bevölkerung als Ganze als auch jeder Einzelne auf die biopolitischen Sicherungsmaßnahmen angewiesen. Selbst die Freiheit des Marktes ist nur möglich, wenn die gesellschaftlichen »Rahmenbedingungen«, von einer funktionierenden Infrastruktur bis zur rechtlichen Planungssicherheit, gegeben sind. Andererseits können einige dieser vitalen Sicherungsmaßnahmen Freiheiten gefährden und einschränken. So ist es immer wieder zu einer »Ausweitung von Verfahren der Kontrolle, der Beschränkung, des Zwangs [gekommen], die das Gegenstück und Gegengewicht zur Freiheit bilden« (Foucault 2006, 102).

Dieses »Paradox des Liberalismus« (Sennelart 2006, 477) läuft auf etwas anderes hinaus als die Marx'sche Ideologiekritik, die im bürgerlichen Recht auf Sicherheit nur eine »Versicherung [des] Egoismus« (Marx 1969, 366) und damit die Ermöglichung des Kapitalismus erkennen wollte. Von liberal-biopolitischen Sicherheitstechnologien zu sprechen heißt also weniger, eine Struktur für die Erklärung moderner Dynamiken der Sicherheit aufzurichten, als vielmehr, das spannungsreiche Verhältnis von liberaler politischer Rationalität und biopolitischen Sicherheitsmechanismen zum Gegenstand der Analyse zu machen. So ist gerade der Liberalismus historisch immer wieder angetreten, um den Exzess biopolitischer Sicherungsmaßnahmen zu kritisieren. Gleichzeitig hat er zumeist gerade nicht die Substanz der sozialen bzw. biopolitischen Moderne – die Sicherung von Leben, Wohlfahrt und Wohlstand – in Frage gestellt (Ewald 1993, 89–102, Collier 2011). Vielmehr bestand der liberale Einsatz häufig darin zu argumentieren, dass private Vorsorgemaßnahmen und die intrinsischen Regulationsformen des freien Marktverkehrs besser als staatliche Interventionen in der Lage sind, die Sicherheit der Bevölkerung, ihr Leben und Überleben, zu gewährleisten, ohne zugleich die Freiheit des Einzelnen und die Freizügigkeit liberaler Lebens- und Handelsformen zu gefährden (Rothschild 1995a). Die erfolgreichsten Technologien der Sicherheit – wie die Versicherung – sind deshalb zugleich Technologien des Kompromisses, denen es gelungen ist, konfligierende politische Rationalitäten miteinander zu vereinbaren (Ewald 1993).

Zusätzlich kompliziert wird diese liberal-biopolitische Konfiguration der Sicherheit dadurch, dass auch das Problem souveräner Sicherheit nicht verschwunden ist, sondern lediglich durch das Auftauchen liberaler und biopolitischer Rationalitäten und Technologien der Sicherheit ergänzt und rekonfiguriert wurde. Es gibt also weiterhin ein souveränes Sicherheitsdispositiv – Grenzsicherung, Militär, Polizei zur Herstellung öffentlicher Ordnung etc. –, das gemeinsam mit den liberal-biopolitischen Sicherheitsmechanismen wirksam ist.<sup>28</sup> Das historisch gewachsene Feld der Sicherheiten bildet weniger ein festes Gerüst als eine konfliktreiche Konstellation unterschiedlicher Sicherheitsdispositive.<sup>29</sup> »Sicherheitsdispositiv« wäre folglich der Name für eine jeweils spezifische historische Formation von Sicherheit, die sich systematisch ab- und eingrenzen lässt. Im Anschluss an Foucault (2004, 13–133) lässt sich bereits zwischen einem *Dispositiv souveräner Staatsicherheit* und einem *Dispositiv normalisierender Bevölkerungssicherheit* unterscheiden,<sup>30</sup> die zwar zu historisch unterschiedlichen Zeitpunkten entstanden sind, aber dennoch faktisch bis in die Gegenwart nebeneinander bestehen, sich überkreuzen und in Konflikt miteinander geraten können.

Die Geschichte der Sicherheit ist aber keineswegs zu ihrem Ende gekommen. Vielmehr kommt es immer wieder zu Verschiebungen, Akzentverlagerungen, aber auch zu grundsätzlicheren Entwicklungsdynamiken. Gerade seit dem Zweiten Weltkrieg scheint es durch politische Umbrüche, technologische Entwicklung, das Auftauchen der ökologischen Problema-

---

28 Das schwierige Zusammenwirken souveräner und liberal-biopolitischer Formen der Sicherheit gezeigt zu haben ist das Verdienst der Arbeiten zur »illiberalen Gouvernamentalität« (siehe u.a.: Opitz 2008).

29 In seinen Vorlesungen zur modernen Regierungskunst führt Foucault (2004, 13–133) »Sicherheit« zunächst als eigenständige Machtform neben Disziplin und Souveränität ein, verfolgt diese Unterscheidung jedoch nicht systematisch weiter. Ich verwende den Begriff Sicherheitsdispositiv hier nicht als gleichbedeutend mit einem ganz bestimmten Modus der Machtausübung. Vielmehr gehe ich davon aus, dass es mehrere historisch konstituierte »Sicherheitsdispositive« – als relativ kohärentes Set von Problemen, Zielscheiben und Sicherheitstechniken – gibt.

30 Mit der Unterscheidung zwischen souveräner Staatssicherheit und normalisierender Bevölkerungssicherheit nehme ich die Unterscheidung von souveräner Macht und Biomacht auf, die sich bei Foucault (1977, 159–190) findet, und beziehe sie stärker auf die Frage der Sicherheit. Foucaultkennern wird auffallen, dass der Disziplinarmacht, die vor allem in Überwachen und Strafen (Foucault 1976) beschrieben wurde, hier kein eigenständiges Sicherheitsdispositiv zugeordnet wird. Neben darstellungstechnischen Gründen liegt das daran, dass disziplinarische Machttechniken für die in dieser Arbeit verhandelten Fragen keine gesteigerte Bedeutsamkeit haben.

tik und die zunehmende Globalisierung zu massiven Transformationen sicherheitspolitischer Selbstverständlichkeiten gekommen zu sein. Es ist gleichwohl gar nicht so leicht auszumachen, ob diese Verschiebungen bereits das Entstehen eines neuen Sicherheitsdispositivs implizieren. Deswegen möchte ich im Folgenden einen interpretatorischen Vorschlag unterbreiten, indem ich auf vier Dimensionen eingehe, mit denen Foucault die Unterschiede zwischen liberal-biopolitischen und souveränen Sicherheitstechniken markiert hat: Zeit, Raum, Gegenstand und Norm (Foucault 2004, 26f.). Dabei argumentiere ich, dass eine Verschiebung in allen diesen Dimensionen auf ein neues Sicherheitsdispositiv schließen lässt. Die Fokussierung auf die Dimensionen Zeit, Raum, Objekt und Norm lässt historische Verschiebungen sichtbar werden. Sie erlaubt es, gezielte Forschungsfragen zu generieren, die es ermöglichen, das Auftauchen eines neuen Sicherheitsdispositivs zu erforschen. Zudem kann die bestehende Forschungsliteratur zu neuen Techniken und Konfigurationen der Sicherheit entlang dieser Dimensionen systematisch geordnet und auf mögliche Leerstellen hin befragt werden.

### *Zeit*

Technologien der Sicherheit bewegen sich stets in einem spezifischen zeitlichen Horizont. Sie sind zumeist auf zukünftige Gefahren gerichtet, die die Gegenwart dann beschäftigen, wenn sie bereits in der Vergangenheit vorgekommen sind. Wie das Antizipieren, Erinnern und Vergegenwärtigen jedoch genau rationalisiert und operationalisiert wird, ist wiederum zeitbedingt (Leanza 2011): abhängig von historisch veränderlichen Dispositiven der Sicherheit. Der frühneuzeitlichen Souveränität mussten hereinbrechende und aufziehende Übel noch als vollkommen unberechenbare »Heimsuchungs-Ereignis[se]« (Foucault 2004, 68) erscheinen, die letztlich höheren Mächten zugeschrieben wurden. Selbst Machiavelli (1978) hat den Zufall in der Politik noch über Rekurs auf die Glücksgöttin Fortuna eingeführt und argumentiert, dass gegen deren Kapricen nur die ebenso impulsiven wie virtuoson Reaktionen des Fürsten, des Souveräns also, helfen (Folkers 2014, 90–93). Auch die Konjunktur der Notstands- und Ausnahmezustandspolitik am Beginn des 20. Jahrhunderts (Agamben 2004, Schmitt 2004) lässt sich dieser Traditionslinie zuordnen. Wieder soll impulsives souveränes Entscheidungshandeln bzw. Dezisionismus auf eskalierende Krisensituationen wie Kriege, Wirtschaftskrisen und (sozialis-

tische) Revolten reagieren. Allerdings kämpft der Souverän nicht nur mit einer extern hereinbrechenden Ereignismaterie, sondern ebenso sehr mit den internen Hindernissen des bürokratischen Apparats, der als viel zu schwerfällig aufgefasst wird, um auf die immer schneller eskalierenden Krisensituationen zu reagieren (Scheuerman 1999).

Das Aufkommen populationsstatistischen und ökonomischen Wissens über Regelmäßigkeiten von Marktbewegungen und gesellschaftlichen (Unglücks)Phänomenen (wie Selbstmord, Sterblichkeit, Geburtenrate, Arbeitsunfälle etc.) hat es erlaubt, das, was der frühneuzeitlichen Souveränität noch als unabsehbares Unglücksereignis erscheinen musste, als serialisiertes und regelmäßiges Ereignis wahrzunehmen (Foucault 2004, 40). Zwar sind Unglücksereignisse und Zufälle nicht im strikten bzw. kausalen Sinn vorhersehbar. Sie sind aber in ihrer Wahrscheinlichkeit berechenbar. Dadurch wird der Zufall, der nun als »Risiko« beschrieben werden konnte, sowohl epistemisch wie auch praktisch kontrollierbar. Ian Hacking (1990) spricht vom »taming of chance« durch das Aufkommen von Statistik und Wahrscheinlichkeitsrechnung. Sowohl präventive Maßnahmen – wie das Impfen gegen erwartbare Krankheitswellen – als auch nachsorgend-kompensatorische Versicherungsmaßnahmen werden möglich (zur Familienähnlichkeit von Impfen und Versicherung, siehe: Ewald 1993, 464–470).

Genau diese relative Vorhersehbarkeit des Ereignisses gerät allerdings im Angesicht katastrophischer Geschehnisse mit geringer Wahrscheinlichkeit und verheerenden Auswirkungen an ihre Grenzen. Wurde der in der Moderne entstandene radikal offene Zukunfts- bzw. Erwartungshorizont (Koselleck 1979, 349–375) durch statistische Prognostiken gleichsam verstopft, wird in jüngeren Debatten zur Regierung des Katastrophischen eine radikale »Refuturisierung« (Opitz und Tellmann 2015b, 111) bzw. eine »Rückkehr des ungezähmten Ereignisses« (Folkers 2014, 97) diagnostiziert. Politisches und soziales Handeln scheint immer stärker von einem »emergency imaginary« (Calhoun 2004, 376f.) angeleitet, in dem »Zukunft als Katastrophe« (Horn 2014) wahrgenommen wird.

Beck sah in diesem Problem der katastrophischen Zukunft, die nicht mehr durch statistische Prognostiken berechenbar ist, eine Grenze der modernen Zweckrationalität. Forschungen aus dem Bereich der *Governmentality Studies* haben dagegen gezeigt, dass als Reaktion auf die Überforderung statistischer Prognostiken neue Formen und Stile der »Rationalisierung des Zufalls« (Foucault 2004, 93) entstanden sind. So sind gerade im Feld der Versicherung in der jüngeren Vergangenheit viele Verfahren ent-



wickelt worden, die auch katastrophische Ereignisse, wie schwere Naturrisiken oder Terroranschläge, versicherbar gemacht haben (Bougen 2003, Ericson und Doyle 2004). Ähnlich hat Stephen Collier (2008) argumentiert, dass im Angesicht von Katastrophen zwar die Wissensform des »archival-statistical knowledge« (ebd., S. 225) versagt, bei der auf Grundlage bestehender statistischer Datensätze über Ereignisse in der Vergangenheit auf die Wahrscheinlichkeit ihres erneuten Auftretens in der Zukunft geschlossen wird. Als Ersatz und Ergänzung dieser Art der Zukunftsprognostik ist es aber zu einem Aufstieg des sogenannten »enactment based knowledge« (ebd.) gekommen. Bereits in den Planspielen des Kalten Krieges wurde versucht, das »Undenkbare« eines Atomkriegs und seiner Folgen denkbar zu machen (Ghamari-Tabrizi 2005, Lakoff 2007). Gegenwärtig lässt sich eine regelrechte Proliferation derartiger Wissensformen beobachten, die in ganz unterschiedlichen Kontexten zum Einsatz kommen: dazu gehören Katastrophenschutzübungen (Adey und Anderson 2012, Ellebrecht, Jenki und Kaufmann 2013), verschiedene Szenario-Techniken (de Goede 2008), Computersimulationen (Galison 1996), der Stresstest (Langley 2013) und die Delphi-Methode (Collier 2008, 242). Wie statistische Prognostiken beziehen sich alle diese Wissensformen auf etwas Zukünftiges. Allerdings operieren sie dabei nicht mehr im Medium des Wahrscheinlichen, sondern des Möglichen – eines Möglichen, das im Falle seines Eintretens verheerend wäre.

Dieser Befund wirft die Frage auf, wie Sicherheitsmaßnahmen in Bezug auf eine lediglich mögliche, kontingente Zukunft geplant werden können. Wie könnte ein »contingency planning« (Lentzos und Rose 2009) aussehen, das nicht wie klassische Formen der Prävention auf einer relativ gesicherten Wissensbasis aufruhen könnte, sondern lernen müsste, mit Situationen hartnäckigen Nichtwissens umzugehen? Vor allem drei Handlungslogiken spielen in den Debatten der *Critical Security Studies* eine entscheidende Rolle: *precaution* – die vorsorgende Vermeidung (Ewald 2002), *preemption* – die proaktive Verhinderung (Massumi 2007) und *preparedness* – die Vorbereitung auf Katastrophensituationen (Lakoff 2007) (eine Gesamtschau dieser Praktiken liefern: Anderson 2010, Bröckling 2012). Während *precaution* und *preemption* immer noch versuchen, ein Ereignis durch Bekämpfung seiner Ursachen zu vermeiden, geht es der Vorbereitung eher um die Kontrolle der Folgen eines Ereignisses. Interessanterweise hatte Foucault den Versuch, ein Unheilereignis »zu verhindern [...] ihm buchstäblich vorzubeugen« (Foucault 2004, 55), noch als »disziplinarische« Logik gekennzeichnet,

während erst die schrittweise Neutralisierung bzw. Normalisierung des Ereignisses eine liberal-biopolitische darstellt (siehe dazu: Folkers 2014, 93–95). Die Frage ist also, ob *preparedness* überhaupt noch sinnvollerweise als Teil eines der »Dispositive der Vorbeugung« (Bröckling 2012) betrachtet werden kann oder nicht vielmehr Teil eines Sicherheitsdispositivs geworden ist, in dem zwar nicht mehr von der »natürlichen« Neutralisierung eines Ereignisses ausgegangen werden kann, man sich aber ebenso von dem Versuch der vollständigen Vermeidung von Unheilsgeschehnissen verabschiedet hat.

### *Raum*

Im Gegensatz zur ausführlichen Debatte über die veränderte zeitliche Rationalität der Sicherheit wird die räumliche Dimension der Sicherheit in der Debatte geradezu stiefmütterlich behandelt (für Ausnahmen siehe: Collier und Lakoff 2008, Folkers 2012, Opitz 2015). Dennoch sind die historischen Veränderungen ihrer Räumlichkeit ein entschiedenes Merkmal von Sicherheitsdispositiven. Gefahren haben je spezifische Weisen der Verräumlichung, die abhängig von der spezifischen Morphologie der Orte, auf die sie treffen, variieren (zum Beispiel ein Sturm an Land oder auf hoher See) und die somit darüber entscheiden, wie groß die Gefahr tatsächlich ist. Entsprechend besteht in der räumlichen Eindämmung bzw. Kanalisierung einer Gefahr bereits ein sichernder Effekt. Beck (2008) hatte bekanntlich argumentiert, dass die Risiken der zweiten Moderne auch deshalb so schwerwiegend sind, weil sie sich nicht mehr national einhegen lassen, insofern sie sich zu räumlich entgrenzten Weltrisiken ausgewachsen haben. Bei Foucault findet sich eine auf den ersten Blick ähnliche Gegenüberstellung zwischen Territorium und Milieu der Sicherheit, die sich aber sowohl in Bezug auf ihre historische Systematik wie auch in ihrer Heuristik von Becks Weltrisikothese unterscheidet. Foucault hatte liberal-biopolitische Sicherheitstechnologien mit einer Raumartikulation in Verbindung gebracht, die er als »historisch-natürliche[s] Milieu« (Foucault 2004, 42) bezeichnete. Dieses Milieu steht im Gegensatz zum souveränen Sicherheitsraum des Territoriums (Foucault 2004, 52). Der souveränen Macht geht es vor allem um die Wahrung der Integrität des nationalen

Territoriums durch Grenzsicherung und Abwehr externer Feinde.<sup>31</sup> Ein Grenzfall der Verräumlichung souveräner Macht besteht in der Errichtung rechtsfreier Zonen oder Lager zur Regierung von Notständen oder extralegalen Ausübung souveräner (Tötungs)macht.<sup>32</sup> Demgegenüber besteht die Herausforderung für Regulatoren des Milieus darin, dessen »Zirkulationen zuzulassen, zu gewährleisten, sicherzustellen« (Foucault 2004, 52). Zirkulationen umfassen dabei sowohl natürliche wie auch kulturelle und sowohl menschliche wie auch nicht-menschliche Prozessverläufe bzw. »flows«: Luft, Gewässer und Krankheitserreger ebenso wie ökonomisch-technische Operationen, Verkehr und Handel, und die Zirkulation von Menschen. Dabei vermischen sich Dinge und Menschen zu hybriden Mobilitäten.

Wichtiger als die Unterscheidung zwischen menschlich und nicht-menschlich ist die Unterscheidung von guten und schlechten Zirkulationen. Das Problem der Sicherheit besteht darin, »die Zirkulation zu organisieren, das, was daran gefährlich war zu eliminieren, eine Aufteilung zwischen guter und schlechter Zirkulation vorzunehmen und, indem man die schlechte Zirkulation verminderte, die gute zu maximieren« (Foucault 2004, 37). Gerade hier zeigen sich die Komplexität und das Dilemma liberal-biopolitischer Sicherheitstechnologien. Es geht um die Sicherung des *Anschlusses*. Deshalb verbieten sich die souveränen und disziplinarischen Techniken der Aus- bzw. Einschließung. Souveräne und disziplinarische Sicherheitstechniken wie die Grenzschiebung oder die Quarantäne (Füller 2012) können kontraproduktiv werden, wenn dadurch die freie Zirkulation von Waren verunmöglicht wird (Cowen und Smith 2009). Gleichzeitig ist die Pathologie des Zirkulationsmilieus – die gefährliche Ansteckung – die direkte Folge der Herstellung erhöhter Anschlussfähigkeit (wenn etwa die

---

31 Foucaults Darstellung des Territoriums ist gewiss sehr schablonenhaft. Für eine intensivere Beschäftigung mit dem Problem des Territoriums im Anschluss an Foucault siehe: Elden (2007).

32 Auch wenn sich sowohl Lager als auch Territorium als Räumlichkeit souveräner Macht verstehen lassen, so stehen sie doch in einem Spannungsverhältnis zueinander. So argumentiert Agamben (Agamben 2002) überzeugend, dass das Auftauchen der Lager ein Effekt der Krise des Nationalstaats und dessen räumlicher Matrix – des Territoriums – darstellt. Diese Diagnose trifft gewiss auch für die Proliferation von Flüchtlingslagern in allen Teilen der Welt zu (Hailey 2009). Allerdings entfaltet sich hier weniger eine souveräne Thanatopolitik, wie Agamben mit Bezug auf die nationalsozialistischen Konzentrationslager argumentiert hatte, sondern vielmehr eine humanitäre Biopolitik des prekären Lebens (Folkers und Marquardt 2016).

Ausweitung des Handels und der Mobilität gleichzeitig zur Ausbreitung von Krankheitserregern oder internationaler Kriminalität beiträgt).

Heuristisch produktiv ist das Konzept des Milieus bei Foucault, weil es den relevanten Raum der Sicherheit nicht auf eine ganz spezifische Gestalt – etwa wie bei Beck das Globale – festlegt. Vielmehr lässt sich ergebnisoffen analysieren, wie Sicherheitstechniken die räumlichen Horizonte, auf die sie zielen und in denen sie wirksam werden, zuschneiden. Dabei kommen Wissensformen wie der Verwundbarkeitskartierung (Collier und Lakoff 2008), die versucht, die räumliche Ausdehnung unterschiedlicher Katastrophenlagen – der Radius einer Atombombe, die Ausbreitung von Giftgaswolken oder Fluten – abzuschätzen, eine besondere Bedeutung zu. Solche Katastrophenlagen fügen sich Länder- oder Nationengrenzen nicht, sind aber auch nicht zwangsläufig »global«. Statt der Opposition global-national besteht die entscheidende Frage vielmehr darin, wie Sicherheitstechniken versuchen, neue, grenzüberschreitende Gefahren zu »re-territorialisieren«, wie sie Gefahrenmilieus und Sicherheitszonen abstecken, die Katastrophenlagen verorten und damit »regierbar« machen sollen.

Historisch stellt sich dabei die Frage, ob es noch ausreicht, mit Foucault davon auszugehen, dass das »historisch-natürliche Milieu« immer noch die relevante Raumgestalt biopolitischer Sicherheitsdispositive der Gegenwart ist. Die wachsende Besorgnis von Katastrophenschützern um sogenannte »Kritische Infrastrukturen« (Folkers 2012) und die *supply chains* im *Just-In-Time*-Kapitalismus (Cowen 2014) deuten eher auf die wachsende Relevanz technologischer Milieus hin. Und natürlich hat auch die Globalisierung die räumliche Gestalt der Sicherheitsmilieus verändert, aber weniger im Sinne eines globalen kosmopolitischen Universums, sondern vielmehr durch das Entstehen eines globalen »space of flows« (Castells 2010, 407–459), durch den sich neue Abhängigkeiten, Anschlussimperative und Ansteckungsgefahren entwickelt haben. Zudem hat das Aufkommen der ökologischen Sicherheitsproblematik – der Umwelt- und Naturschutz – die Morphologie des Milieus von Sicherheit und Gefährdung verändert. Wiederum zeichnet sich ein Dilemma bei dem Versuch ab, schlechte Zirkulationen zu vermeiden, ohne gute zu unterbinden. Wie kann der »infrastructural globalism« (Edwards 2010, 25), die weltumspannende Mobilität und ein dynamischer Welthandel aufrechterhalten werden, ohne die Atmosphäre, Biosphäre bzw. das Erdsystem mit zusätzlichen CO<sub>2</sub>-Emissionen und damit das Leben auf der Erde insgesamt zu belasten?

*Gegenstand*

Sicherheitsdispositive lassen sich mit Bezug auf ihr spezifisches Schutzobjekt, ihr *matter of security concern*, voneinander abgrenzen. Es gibt in jedem Sicherheitsdispositiv eine spezifische Gruppe von Entitäten, die besondere Aufmerksamkeit auf sich ziehen und vornehmlich geschützt werden sollen. Es mag diese Entitäten in der einen oder anderen Weise auch schon vor deren »Entdeckung« durch das Sicherheitsdispositiv gegeben haben, aber nicht als umgrenzte Zielscheibe und Oberfläche für sicherheitspolitische Interventionen.

Während es der Souveränität vor allem darum ging, das nationale Territorium zu schützen und die souveräne Macht zu erhalten, ist das klassische Objekt biopolitischer Sicherheitsbesorgnis die Bevölkerung: »Nicht mehr Sicherung des Fürsten und seines Territoriums, sondern Sicherheit der Bevölkerung« (Foucault 2004, 101). Zum Problem der Regierung und der Sicherheit konnte die Bevölkerung werden, weil statistische Verfahren es ab dem 19. Jahrhundert erlaubten, die Bevölkerung nicht mehr nur als bloße Ansammlung von Körpern, sondern als Gesamtsubjekt mit internen Regelmäßigkeiten, aber auch intrinsischen Pathologien – Selbstmorde, epidemische Krankheiten, Arbeitsunfälle etc. – wahrzunehmen. Um das Leben der Bevölkerung zu schützen und zu verbessern, wurde eine Reihe von gesundheits- und sozialpolitischen Sicherheitsmaßnahmen eingeführt: öffentliche Gesundheitsversorgung bzw. »Sozialmedizin« (Foucault 2003), Verbesserung der Hygiene (Osborne 1996), bis hin zur Sozialversicherung (Ewald 1993).

Gerade in den beiden Weltkriegen, die wie nie zuvor auch die Zivilbevölkerung betroffen haben, ist die Abhängigkeit des Lebens der Bevölkerung von Kritischen Infrastruktur- und lebenswichtigen Versorgungssystemen in den Fokus sicherheitspolitischer Aufmerksamkeit getreten. Collier und Lakoff (2015) argumentieren mit Bezug auf die Geschichte der Vorbereitungen auf einen Atomkrieg in den USA während des Kalten Krieges, dass es dadurch zu einem Übergang von der »population security« zur »vital systems security« gekommen sei. Als vitale Systeme verstehen sie dabei netzgebundene Versorgungsinfrastrukturen (Energie, Wasser, Strom, Informationstechnologie) ebenso wie sozio-ökonomische Systeme wie das Gesundheitssystem, das Finanz- und Versicherungswesen, den Staat etc. Diese Systeme werden im Zuge der *vital systems security* gleichsam zur Interventionsoberfläche, die geschützt werden muss, um das Leben zu sichern.

Die Unterscheidung von *vital systems security* und *population security* ist ein zentraler Ausgangspunkt dieser Arbeit. Über die wichtigen Hinweise von Collier und Lakoff hinaus lässt sich jedoch fragen, welche *life support systems* heute jenseits von Versorgungsinfrastrukturen und sozio-ökonomischen Organisationen sicherheitspolitisch relevant geworden sind. Wiederum deutet die ökologische Problematik auf eine Fortentwicklung des *vital systems*-Motivs hin. Zu untersuchen wäre, ob nicht auch das »Erdsystem« als ebenso prekärer wie lebenswichtiger Komplex von Bio- und Atmosphären zur Zielscheibe umweltpolitischer Sicherheitsmaßnahmen geworden ist.

Die gerade im Zuge der Finanzkrise zu neuer Prominenz gekommene Kategorie des systemischen Risikos (Collier, Lakoff und Kelty 2011, Langley 2014) scheint aber auch auf ein Problematisch-Werden der Systemsicherheit hinzudeuten. Hier scheint es nämlich das System selbst zu sein, von dem Gefahren ausgehen. Zu untersuchen wäre folglich, wie das System als ambivalente – sowohl lebenswichtige als auch seinerseits gefährliche – Größe zum sicherheitspolitischen Problem der Gegenwart geworden ist und wie es – nicht zuletzt »vor sich selbst« – geschützt werden kann.

### *Norm*

Jedes Sicherheitsdispositiv hat eine normative Ordnung, ein Maßstabssystem, das bestimmte Gefährdungen, Situationen oder Zustände der Schutzobjekte bewertbar macht. Im Übergang von einem Sicherheitsdispositiv zum anderen verschieben sich nicht nur die Richtwerte, die anzeigen, ab wann und zu welchem Zweck sicherheitspolitisch interveniert werden muss. Vielmehr verschiebt sich die normative Grundlage, die Matrix, die diese Werte erzeugt. Das hat grundlegende Implikationen dafür, was überhaupt als Sicherheit verstanden wird.

Foucault (2004, 88–98) hatte die normative Ordnung der im 19. Jahrhundert etablierten Biopolitik als »Normalisierung« bezeichnet und diese von der disziplinarisch-souveränen »Normierung« abgegrenzt. Während die Norm der *Normierung* ein fester, präskriptiver Richtwert ist – entweder ein Gesetz oder ein Standard bzw. eine technische Norm –, wird die Norm der *Normalisierung* empirisch gebildet. Sie beschreibt eine statistische *Normalität* oder einen Zustand des *Gleichgewichts* (zum Beispiel von Angebot und Nachfrage auf dem Markt (Folkers 2014, 93–97)) bzw. den Zustand der Gesundheit eines Organismus (Canguilhem 1977). Ihre Ikone ist die

Gaußsche Normalverteilung, die sowohl einen statistischen Durchschnittswert sichtbar macht wie auch eine gleichmäßige bzw. im Gleichgewicht befindliche Verteilung und Streuung der Elemente bzw. Ereignisse der statistischen Mannigfaltigkeit anzeigt. Während die souveräne Norm durch Sanktionen auch gegen Widerstand durchgesetzt werden soll, wird bei der Normalisierung versucht, der »Natur der Sache« entgegenzukommen. Es wird auf die Homöostase und die Selbstregulation makrosozialer Entitäten ebenso vertraut wie auf die Selbstheilungskräfte des Patienten, dem man natürlich medizinisch auf die Sprünge helfen muss, aber niemals mit Zwang, sondern mit den natürlichen Prozessen (zur Entwicklung der Konzepte Selbstregulation und Homöostase im 19. Jahrhundert siehe: Canguilhem 1979, 89–109). Das Impfen, bei dem nicht gegen den, sondern mit dem Erreger gearbeitet wird, ist deshalb für Foucault (2004, 91–93) die paradigmatische Normalisierungstechnik. Grundsätzlich ist gerade der Zusammenhang von Mikrodiversität und Selbstorganisation (Luhmann 1997) der Population ein normalisierender, den Sicherheitstechnologien entgegenkommender Faktor. In der Technologie der Versicherung ist die Bevölkerung nicht nur Objekt der Normalisierung, sondern auch dessen Agent, weil ihre interne Diversität es ermöglicht, Schäden über die Versicherungspopulation aufzuteilen und so zu neutralisieren (Ewald 1993). Auch Märkte und Risikomodelle auf dem Finanzmarkt nutzen die Diversität und Streubreite von Marktpositionen zur Kontrolle und zum sogenannten *hedgen* von Risiken (Folkers 2014, 95–97).

In der Forschungsliteratur zu gegenwärtigen Formen der biopolitischen Sicherheit wurde immer wieder die Abkehr von einer starken oder ausschließlichen Orientierung an Normalität und Gleichgewicht betont (Cooper 2008, Massumi 2009, Folkers 2014, 97–99). Das wirft die Frage auf, ob eine neue normative Ordnung entstanden ist, die das Regime der »Normalität« ablöst. Hier gilt es vor allem, das Konzept der Resilienz in den Blick zu nehmen. Der vom Ökologen Crawford Holling (1973) geprägte Begriff der Resilienz bezeichnet die Toleranz eines Systems gegenüber Schäden und ist mittlerweile in einer ganzen Reihe sicherheitspolitischer Kontexte zu einem zentralen Stichwort geworden. Entsprechend groß ist die Aufmerksamkeit für Resilienz in den *Critical Security Studies* (Cooper und Walker 2011, Kaufmann 2012, Corry 2014, Braun 2014). Allerdings wurde Resilienz bisher nie systematisch mit Foucaults Analytik der Normalisierung in Verbindung gebracht. Vor diesem Hintergrund wäre

zu fragen, ob Resilienz lediglich einen bestimmten, besonders flexiblen Modus der Normalisierung darstellt oder ob Resilienz eine neue normative Ordnung der Sicherheit etabliert.

Sicherheitsdispositiv	Zeit	Raum	Gegenstand	Norm
Souveräne Staats-sicherheit	Souveräner Dezisionismus und Verhängung temporärer Ausnahmezustände	(nationales) Territorium; extralegale Zonen (Lager)	Recht und Ordnung, Sicherung der territorialen Integrität des Staats	Juridische Norm, Gesetz, Standard → Normierung
Bevölkerungs-sicherheit	Prävention von bzw. Versicherung gegen statistisch kalkulierbare Risiken	Historisch-natürliches Milieu der Zirkulation	Bevölkerung	Statistische, empirische Normalität, Gleichgewicht → Normalisierung

*Tabelle 2: Systematik der Sicherheitsdispositive*

Diese kurze Skizze der Veränderungen der Zeit, des Raums, der Schutzobjekte und der normativen Ordnung der Sicherheit hat nicht nur einen historischen Wert, sondern vor allem einen heuristischen. Empirische Forschungen zu Sicherheitspraktiken der Gegenwart erhalten so eine historische Orientierung und Tiefe. Schließlich spielen sich aktuelle Transformationen von Sicherheitstechnologien nicht im luftleeren Raum ab, sondern schreiben sich in eine längere Geschichte ein. Dabei ist weniger davon auszugehen, dass es zu einer definitiven Ablösung eines Dispositivs durch das andere kommt, sondern eher zu einer Modifikation des »Korrelationssystem« der Sicherheit.<sup>33</sup> Ein neues Dispositiv stellt nicht einfach ein zusätzliches Territorium dar, sondern markiert eine Verschiebung der

<sup>33</sup> Foucault selbst hat einer epochalen Interpretation seiner historischen Machtanalytik, in der jeweils nur ein historisches Macht- bzw. Sicherheitsregime nach dem anderen existieren kann, eine Absage erteilt: »Folglich haben Sie überhaupt keine Serie, deren Elemente eins auf das andere folgen, wobei diejenigen, die zum Vorschein kommen, die vorhergehenden verschwinden lassen. [...] In Wirklichkeit haben Sie eine Serie komplexer Gefüge, in denen sich sicherlich die Techniken selbst, die sich vervollkommen oder sich jedenfalls komplizieren, ändern, doch was sich vor allem ändert, ist die Dominante oder genauer das Korrelationssystem zwischen [...] den Sicherheitsmechanismen.« (Foucault 2004, 22f.)



historisch konstituierten Landkarte der Sicherheit. Gleichwohl ging es mir an dieser Stelle nicht um die Erstellung einer definitiven Landkarte, sondern vielmehr um die Erarbeitung einer *roadmap* für die empirische Forschung, um das Auffinden der Orte und Themenbereiche, die für die Untersuchung aktueller Transformationen der Sicherheit besonders relevant und interessant sind.

#### 1.4. Thematische Fokussierung und Forschungsdesign

Die vorausgegangene Skizze der historischen Transformationen von Sicherheitsdispositiven setzt eine empirische Analyse zu aktuellen Verschiebungen sicherheitspolitischer Selbstverständlichkeiten bereits auf die richtige Spur. Jetzt gilt es, diese Spur aufzunehmen und weiter zu verfolgen. Daher möchte ich im Folgenden zunächst den thematischen Zuschnitt der Arbeit darlegen (1.4.1.). Sodann gehe ich auf die Auswahl des empirischen Materials ein, durch das die dargestellten Themenbereiche untersucht werden (1.4.2.). Schließlich möchte ich mein methodisches Vorgehen plausibilisieren (1.4.3.).

##### 1.4.1. Thematische Fokussierung

Um Transformationen auf der Ebene von Sicherheitsdispositiven zu analysieren, bieten sich empirische Studien an, die an einem konkreten Problembereich der gegenwärtigen Politik der Sicherheit ansetzen. Deshalb untersucht die Arbeit die Fortentwicklung von Sicherheitstechnologien und die Konstitution des kontemporären Problems der Sicherheit vor allem ausgehend von der gegenwärtigen Regierung der Katastrophe und von systemischen Risiken in Deutschland. Ein erster Ausgangspunkt dafür wird die Untersuchung des Wandels im deutschen Katastrophen- und Zivilschutz seit dem 11. September 2001 sein. Diese Fallauswahl hat sich angeboten, weil im Vergleich zu den USA (Collier und Lakoff 2008, Masco 2014) und Großbritannien (Adey und Anderson 2011, Aradau und Munster 2011) nur wenig Analysen zu neuen Verfahrensweisen und Denkformen der Regierung des Katastrophischen aus einer sicherheitsanalytischen Perspektive für den deutschen Kontext vorliegen (für eine Ausnahme, siehe: Kaufmann 2011).

Das ist umso bedauerlicher, als gerade in Deutschland Sicherheit ein zentrales Themenfeld politischer Auseinandersetzungen ist. Nach den Erfahrungen des »Katastrophenzeitalters« (Hobsbawm 1998, 37–281) von 1914 bis 1945 war die Suche nach Sicherheit, wie Eckard Conze (2005) argumentiert hat, zu einem politischen Leitmotiv der Bundesrepublik geworden, die jeder Dekade ihren Stempel aufgedrückt hat: die Rückkehr zum Frieden nach Krieg und nationalsozialistischem Terror in den 1950ern, das Projekt der Wohlstandssicherung der 1960er Jahre, die innere Sicherheit in den 1970er Jahren, ökologische und technische Sicherheitsfragen ab den 1980ern, die neue sicherheitspolitische Situation nach Ende des Kalten Krieges und der Umbau des Wohlfahrtsstaat seit den 1990er Jahren. So lässt sich argumentieren, dass die Bedrohung durch den internationalen Terrorismus und neue entgrenzte und systemische Gefährdungen die Politik etwa seit Beginn der Jahrtausendwende dominieren. Die Regierung von Katastrophen und systemischen Risiken ist daher eine der zentralen Herausforderungen deutscher Politik der Gegenwart. Zugleich haben die Erfahrungen mit dem Nationalsozialismus aber auch für eine besondere Skepsis gegenüber Formen der Staatssicherheit – in der DDR bekanntlich der Name des verhassten Geheimdienstes – gesorgt, die immer wieder neu artikuliert wurde: die sogenannte Spiegelaffäre und die Kritik an den Notstandsgesetzen in den 1960ern, die Kritik am Vorgehen des Staates gegen Linksterrorist\_innen und die linke Szene in den 1970ern, der Widerstand gegen den Atomstaat und die Wiederbewaffnung in den 1980ern bis hin zu gegenwärtiger Kritik an ubiquitärer Überwachung durch Staat und Großkonzerne. Sicherheit ist in Deutschland ein besonders problematisches und umkämpftes Politikfeld. Das gilt auch für die Regierung der Katastrophe, weil sie den Eindruck vermeiden muss, unter dem Deckmantel des Außergewöhnlichen den Ausnahmezustand zu organisieren. Schließlich hat die Besetzung Deutschlands nach dem Zweiten Weltkrieg auch dafür gesorgt, dass die BRD eine ungewöhnliche sicherheitspolitische Ausgangslage hatte. Die Verschiebungen bei der Regierung der Katastrophe seit dem 11. September reflektieren auf ihre Weise auch die Veränderung der sicherheitspolitischen Situation Deutschlands seit der Wiedervereinigung und dem Ende der Blockkonfrontation. All das konstituiert die besondere politische und soziologische Brisanz einer Untersuchung der Regierung der Katastrophe in Deutschland.

Der Umgang mit katastrophischen Gefährdungen ist aber nicht nur aus der Innenperspektive deutscher Nachkriegsgeschichte von Interesse. Viel-

mehr kann der empirische Fokus auf die Entwicklungen in Deutschland auch die internationale Debatte der *Critical Security Studies* bereichern. So wurde hier etwa die Herkunft des *precautionary principle* aus dem deutschen Umweltrecht erwähnt (Aradau und Munster 2011, 41), ohne die Genealogie der »Vorsorge« in sicherheitspolitischen Traditionen Deutschlands weiter zu verfolgen. Bereits Hegel verwendet den Begriff der Vorsorge in seiner Rechtsphilosophie. Im 20. Jahrhundert wird Vorsorge dann über das von Ernst Forsthoff geprägte Konzept der Daseinsvorsorge und in Gestalt des Vorsorgeprinzips zu einer entscheidenden Leitlinie nicht nur deutscher Sicherheitspolitik (siehe dazu Kapitel 3.1. und 3.2.). Vor diesem Hintergrund ist es besonders interessant, die Interaktion dieser sicherheitspolitischen Tradition mit anderen Rationalitäten der Sicherheit wie der Resilienz zu untersuchen. Deutschland ist dabei ebenso wenig wie andere Länder als abgeschlossener Nationalcontainer mit einer nur hier anzutreffenden, integralen »Sicherheitskultur« zu verstehen, sondern als spezifischer historisch und geographisch situierter Ort, der Ausgangspunkt, Drehscheibe und Zielpunkt für eine ganze Reihe unterschiedlicher Sicherheitstechnologien ist.

Entsprechend kann Deutschland oder der deutsche Zivil- und Katastrophenschutz seit dem 11. September in dieser Arbeit auch nicht als fixer Rahmen der Analyse dienen. Vielmehr gilt es, das übergreifende Forschungsinteresse »Analytik des Sicherheitsdispositivs« im Blick zu behalten. Dieses Forschungsinteresse erfordert es zwar, Anhaltspunkte an konkreten Phänomenen zu suchen, würde aber kompromittiert, wenn es von vornherein auf einen fest abgesteckten Gegenstandsbereich eingengt würde. Vielmehr lässt sich für die Dispositivanalyse<sup>34</sup> das methodologische Prinzip des »Folgens« mobilisieren, das in der Kulturanthropologie und der Akteur-Netzwerk-Theorie erfolgreich erprobt wurde (siehe dazu: Appadurai 1986, 5, Latour 1987). Hier wird kein im Voraus eingegrenzter Bereich des Sozialen vermessen (etwa nur das Labor als Ort der Wissenschaft), sondern die Trajektorie eines Dinges, eines wissenschaftlichen Forschungsprozesses oder einer Erfindung abgeschrieben. Es hängt also immer auch

---

34 Wie Bührmann und Schneider (2007) zu Recht bemerken, ist die Dispositivanalyse ein »konzeptuell und forschungspraktisch bisher kaum erschlossenes Feld«. Allerdings weicht mein Ansatz der Dispositivanalyse, der auf die Verschränkung der drei Achsen Problematisierung, Technologie und Strategie fokussiert und dafür postfoucaultsche Ansätze mit analytischen Strategien der STS und ANT in Verbindung bringt, von Bührmanns und Schneiders Vorschlag einer Methodisierung der Dispositivanalyse ab.

vom Gegenstand und dessen netzwerkförmigen Verweisungszusammenhängen ab, welche Territorien des Sozialen dabei gekreuzt werden. Ähnlich werde ich hier verfahren und den relevanten Verbindungen und Verknüpfungen des Sicherheitsdispositivs folgen. Es gilt also, die Spuren aufzunehmen, die von dem anfangs ausgewählten Brennpunkt der Untersuchung aus auf andere relevante Felder und Problembereiche der Sicherheit verweisen. Dieses Vorgehen hat vier systematische Stärken, die ich im Folgenden herausarbeiten möchte. So wird es erstens möglich, über den nationalen Kontext Deutschland hinauszugehen und so einen »methodologischen Nationalismus« zu vermeiden (1). Zweitens lässt sich auf diese Weise mehr als nur ein spezifisches Themenfeld von Sicherheitsproblemen in den Blick nehmen (2). Drittens kann die Analyse über staatliche Politiken hinaus auf den privaten Bereich ausgeweitet werden (3). Und schließlich eröffnet sich so eine historische Analysedimension, indem den Netzen des gegenwärtigen Sicherheitsdispositivs auch in die Vergangenheit gefolgt wird (4).

(1) Der Bezugsraum Deutschland wird hier, wie betont, nicht als abgeschlossener Nationalcontainer betrachtet, sondern als Ausgangsort, durch den die Forschung ihre notwendige Situierung erhält. Immer dann, wenn die intrikaten Pfade des Sicherheitsdispositivs selbst es nahegelegt haben, bin ich mit der Analyse über Ländergrenzen hinausgegangen. Das betrifft im Einzelnen die europäische Zusammenarbeit im Schutz vor Katastrophen, die – wie immer wieder betont wird – »keine Grenzen kennen« (siehe Kapitel 2.1.2.), die Regulation systemischer Risiken auf dem Finanzmarkt auf europäischer und globaler Ebene (siehe Kapitel 2.4. und 2.5.) und schließlich auch das Gefüge des sogenannten *Business Continuity Management* (BCM) in einer global operierenden deutschen Bank (siehe insbesondere Kapitel 4.3.2.). Das heißt, die Analyse geht immer dann über Deutschland hinaus, wenn die Akteure selbst die Begrenzungen national gebundener Sicherheitspolitik problematisieren und Wege transnationaler Kooperation beschreiten. Zudem bewegt sich die Analyse des Sicherheitsdispositivs notwendig auf einer transnationalen Ebene. Sicherheitstechnologien wie *preparedness* und Resilienz sind »mobile Technologien« (Ong 2007), die sich in unterschiedlichen nationalen Kontexten in eine bestehende Ökologie der Sicherheiten einfügen. Ich gehe also von vornherein davon aus, dass das Sicherheitsdispositiv ein globales Phänomen ist, das nichtsdestotrotz nur über seine lokalen Artikulationen und Aktualisierungen vollständig verständlich wird. Das Sicherheitsdispositiv auf diese Weise

als »global assemblage« (Ong und Collier 2005a) zu verstehen, steht im Gegensatz zu einem unproduktiven und vor dem Hintergrund des grenzüberschreitenden Charakters aktueller Sicherheitstechnologien auch unplausiblen Ländervergleich, in dem unterschiedliche »nationale Sicherheitskulturen« voneinander unterschieden werden (so etwa bei: Lentzos und Rose 2009).

Während Beck versucht, den »methodologischen Nationalismus« (Beck und Grande 2010) der Soziologie durch seine Theorie der »Weltrisikogesellschaft« zu kritisieren, werde ich versuchen, den faktischen »global assemblages« (Ong und Collier 2005a) der Sicherheit zu folgen. Die Ebene des Globalen ist dabei aber dennoch nicht der Ausgangspunkt der Analyse, sondern wird vielmehr selbst als Effekt der Versammlung und Koordination (durch Standards, *benchmarks*, *best practices*, mobile Technologien und wandernde Problembeschreibungen) lokaler Operationen analysiert. Bruno Latour hat eine ähnliche Forschungsperspektive auf das Globale im Rahmen seiner Akteur-Netzwerk-Theorie auf die drei griffigen Formeln »das Globale lokalisieren, das Lokale neu verteilen und Orte verknüpfen« gebracht (Latour 2007, 299–423). Die Analyse soll also von Ort zu Ort fortschreiten und zeigen, wie das Globale hergestellt wird; ein Vorgang, der natürlich stets an lokalen und nationalen Beharrungskräften scheitern kann. Ein lokaler Ausgangspunkt ist für eine Analyse mit globaler Orientierung also kein Widerspruch, sondern ihre notwendige Voraussetzung.

(2) Anstatt nur ein Praxisfeld der Sicherheit zu untersuchen, geht es mir in dieser Studie darum, die Isomorphien und Familienähnlichkeiten, die Resonanzen und Beeinflussungsmuster der Politiken der Sicherheit in unterschiedlichen Themengebieten (von der Terrorabwehr zum Hochwasserschutz, vom Schutz Kritischer Infrastrukturen bis zur Finanzmarktregulation) und sozialen Feldern (von der Ökonomie bis zur Politik, vom Staat bis zur privatwirtschaftlichen Organisation) in den Blick zu nehmen. Ein Dispositiv der Sicherheit wird in seiner Wirksamkeit und Operationslogik erst dann sichtbar, wenn seine Ausweitung und Anschlussfähigkeit in unterschiedlichen sozialen Feldern und Institutionen aufgezeigt werden kann. Zudem gilt, dass ein Sicherheitsdispositiv seine Fälle und Probleme eigenlogisch festlegt. Die thematische Festlegung auf ein spezifisches Sicherheitsproblem würde deshalb Gefahr laufen zu übersehen, wie das Sicherheitsdispositiv relevante Gefahren auswählt, priorisiert und gruppiert.

Fokussiert man auf den entdifferenzierenden Charakter von Sicherheitsdispositiven, also darauf, wie unterschiedliche Bereiche und Institutionen im Namen der Sicherheit koordiniert werden, dann rücken zunächst einmal die Ähnlichkeiten zwischen unterschiedlichen Handlungsfeldern in den Vordergrund. Gleichzeitig ist es gerade durch die so erzielte thematische Streubreite möglich, die »performative Flexibilität« (Marres 2012, 71) bzw. strategische Offenheit der Technologien eines Sicherheitsdispositivs in den Blick zu bekommen. Welche Einsätze und Auswirkungen die abstrakten Technologien der Sicherheit jeweils haben, wird nur durch die Analyse ihres Wirkens in einem konkreten Operationsbereich sichtbar. Erschlossen werden so die Binnendifferenzen innerhalb des Sicherheitsdispositivs, anstatt von einer grundsätzlichen Differenzierung zwischen unterschiedlichen sozialen Feldern oder Systemen auszugehen, wie es etwa ein systemtheoretisches Vorgehen nahelegen würde (wie etwa in: Luhmann 2008). Zudem reflektiert dieses Vorgehen die Eigenlogik katastrophischer und systemischer Gefahrenereignisse, die sich eben weder um nationalstaatliche Grenzen noch um Grenzen sozialer Systeme scheren und so existenzielle Probleme der Regierung erzeugen, die die Problemlösungskapazitäten einzelner Regierungsapparate überlasten.

(3) Ebenso unterläuft die Dispositivanalyse die klassische Unterscheidung von öffentlichem und privatem Sektor bzw. von *public* und *corporate governance*. Vielmehr kommen gerade im Feld des Schutzes Kritischer Infrastrukturen eine Reihe von »politisch-ökonomischen Indifferenzzonen« (Vogl 2015, 8) bzw. – in der Sprache der untersuchten Akteure – Formen »vernetzter Sicherheit« in »Public Private Partnerships« in den Blick. Aus der Perspektive der Gouvernementalitätsforschung besteht die Regierung der Katastrophe und systemischer Risiken nicht nur in staatlichen Vorschriften, Regulationen und Interventionen, sondern vor allem in einer Reihe von Sicherheitstechnologien, die sowohl von staatlichen als auch privaten Akteuren in Anschlag gebracht werden. Dennoch weisen viele Untersuchungen zur Regierung der Katastrophe in den *Critical Security Studies* de facto einen Staatsbias auf. Wenn überhaupt einmal die Regierung der Katastrophe im Privatsektor untersucht wird, dann meist mit Bezug auf private Versicherungen gegen Katastrophenfälle (Ericson und Doyle 2004, Collier 2014). Die ausführliche Auseinandersetzung mit *Business Continuity Management* insbesondere in Banken adressiert dieses Desiderat, indem sie Formen der Katastrophenvorbereitung auf der Ebene einzelner Unternehmen untersucht (siehe Kapitel 4).

Die Thematik Kritischer Infrastrukturen nimmt auch jenseits der Frage nach Kooperationsmustern von privaten und staatlichen Akteuren in dieser Arbeit einen zentralen Stellenwert ein. An keinem anderen sicherheitspolitischen Feld lassen sich gegenwärtig so deutlich das Ineinandergreifen, die interne Verweisung, aber auch die Grenzen der Technologien und Probleme des Sicherheitsdispositivs der Resilienz analysieren. Diese Arbeit wird nicht nur die spezifischen Bedingungen und Operationsweisen des Schutzes Kritischer Infrastrukturen in Deutschland beleuchten, sondern auch versuchen, ein erweitertes Verständnis der Trajektorien und gegenwärtigen Effekte des Schutzes der kritisch gewordenen Infrastrukturen zu etablieren. Im Zentrum meiner Analyse der Infrastruktursicherung in Deutschland steht die Verschränkung von Techno- und Biopolitik sowie von Umwelt- und Sicherheitspolitik (siehe Kapitel 3). Obwohl in der florierenden interdisziplinären Debatte zu Infrastruktur die sozio-technischen Netze immer wieder als Vermittlungsinstanzen zwischen Natur und Gesellschaft beschrieben werden (Edwards 2003, Gandy 2005, Carse 2012), ist die Forschungslage zum Zusammenhang von ökologischer Sicherheit und Infrastrukturschutz bislang leider recht überschaubar (wichtige Ausnahmen sind: Hodson und Marvin 2009, Braun und Wakefield 2014b).

(4) Schließlich habe ich nicht nur thematisch, räumlich und institutionell, sondern auch in zeitlicher Hinsicht die Netze des gegenwärtigen Sicherheitsdispositivs verfolgt. Die historische Einbettung gegenwärtiger Sicherheitspolitiken ist ihrerseits selbst Teil der Etablierung eines neuen Sicherheitsdispositivs. So werden sicherheitspolitische Paradigmenwechsel angemahnt und ausgerufen, grundlegende weltpolitische und gesellschaftliche Transformationen skizziert und neue Gefährdungshorizonte beschworen, um sicherheitspolitische Veränderungen anzustoßen bzw. zu legitimieren. Im zweiten Kapitel habe ich vor allem diese Arbeit der Akteure an und mit der Geschichte des Sicherheitsdispositivs analysiert, um zu zeigen, wie der Problemhintergrund erzeugt wurde, der zur Etablierung des Resilienzdispositivs in Deutschland beigetragen hat. Im dritten und vierten Kapitel habe ich genealogische Analysen erstellt, um die Prozesse der Gegenwart auf neue Weise in den Blick zu nehmen. Dabei ging es mir nicht nur um Brüche zwischen Vergangenheit und Gegenwart, sondern – im Sinne einer »Geschichte der Gegenwart« (Foucault 1976, 43) – darum, die Herkunft und Kontinuität bestimmter sicherheitspolitischer Denk- und Handlungsformen aufzuzeigen.

Dabei habe ich mich auf solche Zusammenhänge konzentriert, die in den Debatten der *Critical Security Studies* bisher vernachlässigt wurden und/oder vor allem auf Spezifika der deutschen Politiken der Sicherheit bezogen sind. So habe ich einen historischen Schwerpunkt auf die Beleuchtung der Tradition des Vorsorgedenkens deutscher Sicherheitspolitik (das Konzept der Daseinsvorsorge und das umweltpolitische Vorsorgeprinzip) gelegt (Kapitel 3.1.1. und 3.2.1.). Zudem habe ich die Hinterlassenschaften des Atomzeitalters in Bezug auf gegenwärtige Problematisierungsweisen und Techniken der Sicherheit beleuchtet. Während die Kritik des Atomstaats von den 1970er Jahren bis heute sowohl Formate wie Inhalte gegenwärtiger Debatten um Energiepolitik in Deutschland prägt (Kapitel 3.3.1.), leben die Techniken des *Continuity of Government Planning*, mit denen im Kontext des Kalten Krieges die Fortsetzung der Regierungstätigkeit im Falle eines Atomkrieges gewährleistet werden sollte, im gegenwärtigen *Business Continuity Management* fort (Kapitel 4.1.). Schließlich werde ich zeigen, wie bestimmte Sicherheitsrationalitäten – insbesondere das Konzept der Resilienz – nicht bloß das Ergebnis eigenlogischer Entwicklungen innerhalb von Sicherheitsapparaten sind, sondern ebenso die Folge von ökologischer Kritik an technokratischen Steuerungsphantasmen und Sicherheitsstrategien (Kapitel 3.2. und 3.3.2.).

Zusammengenommen bearbeitet die vorliegende Untersuchung ein breites thematisches, institutionelles und historisches Terrain. Nur so kann dem analytischen Anspruch, die aktuelle Transformation der Sicherheit und das mögliche Auftauchen eines neuen Sicherheitsdispositivs in der Gegenwart zu erforschen, entsprochen werden. Zugleich erhält die Studie durch dieses übergreifende Forschungsanliegen die notwendige Kontur und Rahmung. Es geht also nicht um betriebliche Governance, Finanzmarktkrisen, Infrastrukturen, Energiepolitik etc. *per se*, sondern um die Einsätze und Effekte eines Dispositivs der Resilienz in diesen Feldern, dessen Emergenz ich nachzeichnen möchte.

#### 1.4.2. Materialauswahl

Um diese heterogenen Themenfelder zu untersuchen, habe ich einen entsprechend heterogenen Materialkorpus analysiert. Dabei habe ich die Inhalte des Materialkorpus nicht im Vorhinein festgelegt, sondern zunächst wiederum versucht, den Netzwerken der Macht und Dispositiven der Sicherheit zu »folgen«. Anhand der Arbeit mit dem Material konkretisiert



sich die Strategie des Folgens empirisch: Gefolgt bin ich den Querverweisen in Strategiepapieren auf bestehende oder zu erarbeitende Programmatiken, den kooperativen Verbindungslinien zwischen Institutionen, den Verweisen auf Gesetze, den Empfehlungen zur Implementierung neuer Sicherheitstechniken, den dokumentarischen Serien (regelmäßige Berichte und Stellungnahmen) sowie der Diagnose von Problemfeldern. Erst dadurch bin ich auf Themen, Probleme und Zusammenhänge gestoßen, die mir durch eine allzu strikte Festlegung des Materials verschlossen geblieben wären.<sup>35</sup>

Ausgangspunkt meiner Zusammenstellung des Materialkorpus war zunächst das 2004 neu geschaffene Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), weil hier die institutionellen und konzeptuellen Veränderungen deutscher Sicherheitspolitik seit dem 11. September ihren sichtbarsten Ausdruck haben. Tatsächlich ist das BBK – wie es in seiner Selbstbeschreibung immer wieder heißt – ein »Netzknoden« der Sicherheit. Es ist aber eben nur ein Knoden, der auf weitere Verbindungslinien und Orte des Sicherheitsdispositivs verweist. Diesen Spuren und losen Enden, die ich durch meine Analyse des BBK gefunden habe, bin ich in unterschiedliche Richtungen gefolgt.

Für eine Gouvernementalitätsanalyse gelten strengere Regeln für die Auswahl des Materials, als sie von den an Foucault anschließenden diskursanalytischen Verfahren zumeist angelegt werden, in denen vornehmlich Medienbeiträge, linguistische Eigenarten von Diskursen oder »Kollektivsymbole« untersucht werden (Jäger 2004). Vielmehr gilt es in der Gouvernementalitätsanalyse, die jeweils für die Regierungstätigkeit angemessenen »Formen der Veridiktion« (Foucault 2009a, 17)<sup>36</sup> zu identifizieren. Diese »Formen der Veridiktion« sind historisch veränderliche Wahrheitsspiele, bezeichnen also die Art und Weise, unter welchen *Bedingungen* etwas in Erscheinung treten und »wahr« werden bzw. Realität erlangen

---

35 Marilyn Strathern hat für die anthropologische Forschung darauf aufmerksam gemacht, dass das Prinzip des »Folgens« eine nicht-lineare Methode der Versammlung von Daten impliziert: »Rather than devising research protocols that will purify the data in advance of analysis, the anthropologist embarks on an exercise which yields materials for which analytical protocols are often devised after the fact.« (Strathern 2003, 5)

36 Ein offensichtlich an Foucault anschließendes Konzept der Veridiktion findet sich auch bei Latour (2014, 99ff.). Wie bei Foucault wird auch bei Latour Wahrheit bzw. die Wahrheitsprozedur der Veridiktion nicht lediglich als eine Aussage über einen Sachverhalt der »Außenwelt« betrachtet. Gerade Latour betont dabei die materiellen Verfahren – etwa Experimente im Labor –, die daran beteiligt sind, etwas »wahr« zu machen.

kann. Die Formen der Veridiktion der Gouvernementalität stecken ab, welche Aussagetypen, Formate und Sachverhalte als Bestandteile der Regierungspraxis relevant werden können, wie ein Problem für die Operationen des Regierens intelligibel werden kann. Veridiktionen selbst bezeichnen die spezifischen Prozeduren des »Wahrmachens« und zur Geltung Bringens. Zur Abgrenzung solcher Formen der Veridiktion hilft das von Paul Rabinow und Hubert Dreyfus (1983, 48) im Anschluss an Foucault in die Debatte eingebrachte Konzept der »serious speech acts«. Veridiktionen oder *serious speech acts* sind nicht auf Sprechakte im engeren Sinne beschränkt, sondern umfassen eine ganze Reihe von Techniken und Artefakten des Wissens – Berichte, Karten, Graphiken, Charts, aber auch Preise auf Märkten (zu letzterem siehe: Foucault 2006, 57) etc. –, die etwas in ein institutionalisiertes Wahrheitsspiel eintreten lassen. Diese Wahrheitsspiele sind keine beliebigen Sprachspiele, die sich in gewöhnlichen Alltagssituationen ereignen, weil ihnen stets eine bestimmte institutionelle Wirksamkeit zukommt.

»Foucault requires that the situation in question contain institutionally legitimated claims to truth or one or another type of sanctioned seriousness; Dreyfus and I called them »serious speech acts«. Without the presence of serious speech acts, there is no problematization in the strict sense of the term, although obviously there could be problems.« (Rabinow 2003, 20)

*Serious speech acts* bzw. Veridiktionen sind also immer Teil eines institutionellen Settings, auf das sie zugleich einwirken, und zwar weil und insofern sie durch ihren institutionellen Status mit Wirkmächtigkeit ausgestattet sind.<sup>37</sup> Dabei sind sie nicht auf diesen Kontext reduzierbar, weil sie ihren

---

37 Der Institutionenbegriff wird hier in einem sehr weiten Sinne der sanctioned seriousness verstanden. Bei der Abgrenzung der serious speech acts, verstanden als Äußerungen von Gewicht, wird der einfache Sachverhalt reflektiert, dass Foucault stets Wahrheitsprozeduren von einem relativ hohen Professionalisierungsgrad untersucht hat (Wissenschaft, Vertreter von Kirche, Staat, Ökonomie etc.). Mit seinem Konzept des »Wahrheitsspiels« (Foucault 2005b, 826) grenzt Foucault diese Art des Diskurses von Sprachspielen in Alltagssituationen ab. Einen Spezialfall der serious speech acts stellt die antike Praxis des Wahrsprechens, der parrhesia dar, die Foucault (1996, 2010) in seinen letzten Vorlesungen analysiert hat. Diese geht nämlich weder von einer institutionalisierten Position aus, noch hat sie klar kodifizierte Effekte. Vielmehr versucht sie gerade die Regeln eines dominanten Wahrheitsspiels und die damit einhergehenden Machtpositionen und Wirkungen in Frage zu stellen. In Foucaults Analyse der parrhesia wird aber deutlich, dass diese sich als serious speech act konstituieren kann, weil sie in ein asymmetrisches Machtverhältnis interveniert und dadurch ernsthaft wird, dass sie potenziell gefährliche Konsequenzen für die Person des Wahrsprechers hat. Versteht man die Pra-

Kontext bis zu einem gewissen Grad performativ mit hervorbringen und dadurch ständig verändern.

In meinem Material lassen sich zwei unterschiedliche Arten von *serious speech acts* zunächst grob unterscheiden: Zum einen habe ich primär debatten- und problemorientierte Dokumente analysiert. Dazu gehören Bundestagsdebatten, Problemstudien von Ministerien und Bundesämtern, sogenannte Grünbücher und Weißbücher, wissenschaftliche Studien im Auftrag des Bundes oder solche, auf die immer wieder Bezug genommen wird, Berichte an den Bundestag, Jahres- und Projektberichte von relevanten Regierungsbehörden, aber auch kritische Stellungnahmen von Nichtregierungsorganisationen, unabhängigen Forschungseinrichtungen oder privatwirtschaftlichen Akteuren. Daneben gibt es eine Reihe von Beiträgen, die einen unmittelbareren Vollzugscharakter haben. Dazu gehören natürlich Gesetze, aber auch Standards und Leitfäden, die klare Vorgaben für Sicherheitsmaßnahmen auf unterschiedlichen Ebenen enthalten, Strategiepapiere und bereits auf ministerieller oder Bundesebene verabschiedete Programmatiken. Gerade anhand dieser Dokumente werden nicht nur Problematisierungen analysierbar, sondern auch die mit diesen verbundenen Sicherheitstechnologien, institutionellen Veränderungen und Sicherheitsmaßnahmen sichtbar.

Dokumente geben aber nicht nur Hinweise auf Sicherheitstechnologien, sondern sind selbst bereits eine Technologie der Sicherheit. Nicht selten enthalten die von mir analysierten Dokumente neben reinem Text auch Elemente wie Checklisten, Leitfäden, *flow charts*, Risikoanalysematrizen etc., die als Techniken zur Strukturierung generischer Vorbereitungsmaßnahmen dienen. Die Dokumente enthalten zudem Aufforderungen zur weiteren Dokumentation: Ablauf und Umgang mit wirklichen oder inszenierten Katastrophen(übungen) sollen dokumentiert, Lehren aus diesen Ereignissen sollen festgehalten werden, um sie für die Erstellung zukünftiger Notfallpläne nutzbar zu machen. Diese Notfallpläne müssen ihrerseits dokumentiert, kopiert und zirkuliert werden und im Ernstfall in handlicher Form verfügbar sein. Dokumentation ist eine Kerntätigkeit von Katastrophenschützern, die naturgemäß nur selten mit tatsächlichen Katastrophenereignissen beschäftigt sind. Katastrophenschutz ist immer auch die »Ar-

---

xis der *parresia* als Matrix für moderne Formen der Kritik des Machtwissens und Regierens (siehe dazu: Folkers 2016), dann lässt sich öffentliche Kritik an (staatlichen) Institutionen klarerweise als *serious speech act* qualifizieren, wenn die Kritik in relevanter Weise auf bestimmte Rationalitäten und Operationsformen des Regierens Bezug nimmt.

beit und Anwendung einer dokumentarischen Materialität« (Foucault 1981, 15). Die virtuelle Welt der kommenden Katastrophe existiert in den Akten, Szenarien, Berichten und Notfallplänen der Sicherheitstechniker\_innen. Gerade diese Notfallpläne haben bisweilen den Charakter von »fantasy documents« (Clarke 1999), die jedoch nichtdestotrotz reale Effekte haben. Sie simulieren in der Gegenwart Sicherheit in Bezug auf künftige Ereignisse, und wenn doch einmal etwas schiefgeht, dokumentieren sie den verantwortlich-vorausschauenden Umgang mit potenziellen Gefahren.

Dokumente werden hier also nicht nur auf ihren Inhalt, sondern auch auf ihre Materialität und Performativität hin untersucht. Als »paradigmatic artifacts of modern knowledge practices« (Riles 2006, 2) insbesondere in bürokratischen Kontexten fungieren Dokumente als »inscription devices« (Latour und Woolgar 1979, 51), die es ermöglichen, die flüchtige Ereigniszeit des Katastrophischen mit der auf Langfristigkeit, Regelmäßigkeit und Routine ausgelegten Zeit der Bürokratie, Verwaltung und Organisation zu versöhnen. Erst dadurch wird es möglich, Sicherheitsmaßnahmen zwischen ganz unterschiedlichen, institutionell und räumlich entfernten Settings zu koordinieren und ein Dispositiv zu verknüpfen. Dieser Fokus auf die Medialität, Temporalität und Mobilität von Dokumenten, der vor allem in der politischen Ethnographie und der Wissenschafts- und Technikforschung erfolgreich praktiziert wurde, ergänzt die Foucault'sche Orientierung auf den Inhalt der Dokumente, auf die diskursiven Regelmäßigkeiten und Variationen, die Probleme generieren und Sicherheitstechnologien ausarbeiten.

Ergänzt wurde diese umfassende Analyse von Dokumenten durch leitfadengestützte Expert\_inneninterviews. Insgesamt habe ich sechs solcher Interviews geführt, die jeweils zwischen einer und zwei Stunden gedauert haben. Drei Interviews habe ich mit Vertreterinnen des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe geführt, die schwerpunktmäßig mit dem Schutz Kritischer Infrastrukturen befasst sind. Zwei der interviewten Mitarbeiterinnen hatten jeweils einen zusätzlichen Schwerpunkt, einmal im Bereich »Anpassung an den Klimawandel« und einmal im Bereich der Kritischen Infrastruktur der Stromversorgung. In den Interviews ging es mir vor allem darum, einen vertieften Einblick in das Schwerpunktthema meiner eigenen Untersuchung – Schutz Kritischer Infrastrukturen und Sicherung vitaler Systeme – zu erhalten. Die anderen drei Interviews sollten mir ein vertieftes Verständnis privatwirtschaftlicher Strategien der Infrastruktursicherung liefern und wurden entsprechend mit

Experten im Bereich *Business Continuity Management* geführt. Dabei habe ich ein Interview mit einem Unternehmensberater geführt, der Firmen im Prozessmanagement und im Kontinuitätsmanagement berät. Das Interview hat mir vor allem einen Einblick in die Breite des Anwendungsbereichs des betrieblichen Krisen- und Kontinuitätsmanagements gegeben. Die zwei weiteren Interviews habe ich mit *Business Continuity*-Managern einer großen deutschen Bank geführt. Ein Gesprächspartner war Leiter des Krisen- und Kontinuitätsmanagements des Standorts der Bank in Frankfurt und gleichzeitig Koordinator der BCM-Strategien zwischen den unterschiedlichen Standorten der Bank weltweit. Eine weitere Gesprächspartnerin war zuständig für das lokale Business Continuity Management der Bank in New York. Beide Interviews haben vor allem Einsichten in die spezifischen Strategien und Problematiken des BCM im global operierenden Finanzwesen gegeben. Zugleich habe ich durch die Interviews zusätzlich Aufschluss über den Umgang mit zwei konkreten Ereignissen erhalten, die zu Einsatzpunkten von Kontinuitätsstrategien geworden sind: die Demonstrationen und Aktionen des kapitalismuskritischen Bündnisses Blockupy in Frankfurt und der Hurrikan Sandy in New York.

Insgesamt ging es mir bei den Expert\_inneninterviews darum, mehr über den institutionellen Alltag und die organisatorischen Routinen des Regierens der Katastrophe zu erfahren – beides ist durch die Analyse von Dokumenten allein nur schwer zu erschließen. Außerdem dienten mir die Interviewten stets als Informant\_innen, um Einschätzungen über die praktische Relevanz von Gesetzen, Handlungsempfehlungen und Strategien zu erlangen. Darüber hinaus kamen auch Probleme und Herausforderungen des Katastrophenschutzes zur Sprache, die keinen Eingang in die offiziellen Dokumente und Programmatiken gefunden haben. Die Struktur meines Interviewleitfadens (Flick 1999) folgte dabei meinen Forschungsinteressen: Offene Erzählaufforderungen sollten den Interviewten zunächst Gelegenheit geben, Relevanzen selbst festzulegen und Probleme und Sachverhalte zur Sprache zu bringen, die ihnen als Funktions-träger\_innen vor dem Hintergrund ihrer institutionellen Praxis als besonders wichtig erschienen. Die so generierten Einblicke in die Relevanzsysteme der Akteure wurden durch Aufrechterhaltungsfragen vertieft, die den Akteuren zusätzliche Impulse geben sollten, ihr Wissen zu entfalten, zu interpretieren und zu exemplifizieren (Helfferich 2004, 91f.). In diesen Phasen des Gesprächs habe ich versucht, möglichst flexibel auf – mitunter auch unerwartete – Themensetzungen der Interviewten zu reagie-

ren. Im späteren Interviewverlauf habe ich zudem versucht, auch solche Themen anzusteuern, die im Rahmen der von mir analysierten Dokumente als zentral für den Schutz Kritischer Infrastrukturen und die Sicherung vitaler Systeme identifiziert wurden. Hier habe ich zum einen versucht, einen Abgleich zwischen den Relevanzsystemen der Dokumente und denjenigen der Akteure zu vollziehen, aber zum anderen auch der Frage nachgespürt, welche Relevanz die Dokumente selbst für die institutionelle Praxis der Akteure haben.

Die Interviews sind, insofern sie ausnahmslos mit institutionell verankerten Expert\_innen geführt wurden, ebenfalls *serious speech acts*, die entsprechend auch ebenso ausgewertet wurden wie die übrigen Dokumente.<sup>38</sup> Allerdings sind es klarerweise keine rein institutionellen Artefakte, sondern Artefakte, die ich selbst mitproduziert habe. Von Seiten der Interviewten wurde ich als Ko-Experte wahrgenommen und adressiert. Im Rahmen der Interviews wurde Interesse an meiner Forschung und meiner Perspektive geäußert, Antworten wurden in Antizipation eines geteilten Wissenshorizontes formuliert und bisweilen wurden meine Fragen (etwa zu bestimmten Szenarien) als Hinweise für die eigene Arbeit aufgefasst. Einige meiner Gesprächspartner\_innen hatten selbst ein sozialwissenschaftliches Studium absolviert und verfügten über eine entsprechend differenzierte Vorstellung von der möglichen sozialwissenschaftlichen Relevanz ihrer beruflichen Tätigkeiten. Der Dialog fand auch deshalb oft »auf gleicher Augenhöhe« (Pfadenhauer 2009) statt.

Aber auch wenn die Interviews von Informant\_innen und Forschenden koproduzierte Artefakte darstellen, so sind es dennoch wichtige Informationsquellen (Bogner und Menz 2009). Angemessen reflektiert eröffnen sich gerade aus dem besonderen Setting des Expert\_inneninterviews vertiefte und alternative Perspektiven, die Aufschluss über das Selbstverständnis

---

38 Zu diesem Zweck habe ich alle Interviews möglichst leserfreundlich und authentisch transkribieren lassen. Vor dem Hintergrund meines Forschungsinteresses und meines analytischen Vorgehens habe ich mich dabei für eine Form der Transkription entschieden, die den Interviewtext an die Schriftsprache annähert, sprachliche Besonderheiten (etwa Lachen oder längere Pausen) und auffällige Betonungen dabei aber durch entsprechende Markierungen beibehält (für pragmatische Richtlinien der Gesprächstranskription siehe: Dittmar (2004, 77ff.)). Für die sorgsame Transkription möchte ich an dieser Stelle Franca Schirmacher danken. Die Namen der Interviewten sind sämtlich anonymisiert worden. Im Fall der Interviews mit Business Continuity-Managern wurden zudem die entsprechenden Institutionen – Banken bzw. Wirtschaftsberatungsunternehmen – anonymisiert.

und die Rechtfertigungsstrategien der Akteure ebenso liefern wie über die Nähe des Forschers zu seinem Gegenstand. So wurde ich bei einer Interviewanfrage von einer Mitarbeiterin des BBK im Bereich Kritische Infrastrukturen gefragt, ob ich auch mit der Akteur-Netzwerk-Theorie arbeite. Dadurch wurde ich für die performativen Effekte der von mir verwendeten Theorien sensibilisiert. Theorien sind weder bloß Abbilder der Wirklichkeit noch »Brillen« oder Rahmungen, um diese angemessen zu beschreiben, sondern strukturieren mitunter bereits das, was man mit ihnen beobachten möchte.

Die historischen Analysen zur Entstehung des Vorsorgeprinzips (Kapitel 3.2.1.) und zum *Continuity of Government Planning* (Kapitel 4.1.) habe ich weitgehend aus bestehenden historischen Arbeiten rekonstruiert und auf die in dieser Arbeit untersuchten Zusammenhänge so bezogen, dass sie jeweils als »Geschichte der Gegenwart« (Foucault 1976, 43) kenntlich werden. So habe ich etwa versucht zu zeigen, wie die Technologien, die beim *Continuity of Government Planning* während des Kalten Krieges entwickelt wurden, in gegenwärtigen Strategien des *Business Continuity Management* fortleben und dadurch mehr als bloße Relikte einer vergangenen Epoche sind. Genealogie der Gegenwart heißt in diesem Zusammenhang also, die Geschichte strategisch mit der Gegenwart kurzzuschließen, anstatt das Vergangene lediglich »so wie es war« abzubilden. Ähnlich bin ich auch bei den historischen Ausflügen zum Konzept und zur Praxis der Daseinsvorsorge (Kapitel 3.1.1.) und zur Kritik am Atomstaat (Kapitel 3.3.1.) und der Herkunft des Konzepts der systemischen Resilienz (Kapitel 2.5.1.) verfahren. Allerdings habe ich hier auch historisches Quellenmaterial untersucht. Dabei habe ich mich jeweils auf die Autor\_innen konzentriert, welche die entsprechenden Konzepte bzw. die spezifische Spielart der Kritik geprägt haben: Crawford Holling für die Entwicklung des Denkens systemischer Resilienz, Ernst Forsthoff für das Konzept der Daseinsvorsorge und Robert Jungk, Amory und Hunter Lovins für die Kritik am Atomstaat. Diese Autor\_innen können jeweils auf ihre Weise als paradigmatische Denker\_innen gelten, die in Reaktion auf eine bestimmte historische Situation und vor dem Hintergrund einer spezifischen intellektuellen und politischen Positionierung eine Problematisierung vorgenommen haben, die ihre unmittelbare Situiertheit transzendiert hat. Sie sind damit gewissermaßen zu »technicians of general ideas« (Rabinow 1995, 9) geworden, deren eloquente Problembeschreibungen eine besondere historische Wirkmächtigkeit entfaltet haben.

### 1.4.3. Auswertung des Materials

Bei der Auswertung des Materials habe ich mich an methodologischen Richtungsanweisungen orientiert, die von Vertreter\_innen der STS und von Forscher\_innen im Anschluss an Foucault vorgeschlagen wurden. Dabei handelt es sich nicht um genau festgelegte methodische Auswertungsprotokolle. Vertreter\_innen der Akteur-Netzwerk-Theorie (Law 2004), der poststrukturalistischen Diskursforschung (Feustel und Schochow 2010) und der *Governmentality Studies* (Bröckling und Krasmann 2010) haben gleichermaßen deutlich gemacht, dass Methodenkritik Teil des Selbstverständnisses und der Verfahrensweise ihrer Forschungsprogramme ist. Schließlich setzt eine Methode klassischerweise den Gegenstandsbe- reich voraus, der erforscht werden soll, während in der ANT und der an Foucault anschließenden Analytik der Macht die Entstehung von Gegen- ständen, Problemen und Handlungsfeldern selbst untersucht wird. Eine stabile Ontologie des Sozialen, in der eine Methode ihr sicheres Funda- ment finden könnte, wird also abgelehnt.<sup>39</sup> Diese Reserviertheit gegenüber standardisierten Methodenprogrammen ist keiner »naiven Methodenskep- sis« (Diaz-Bone 2005b) geschuldet, sondern einer reflexiven und autologi- schen Forschungstradition, die sich mit den Bedingungen und Effekten der (eigenen) Wissensproduktion auseinandersetzt. Das impliziert nicht, dass

---

<sup>39</sup> Methodische Programme sind keine unschuldigen Verfahren zur Auffindung des Wirk- lichen, sondern setzen in einem meist nicht explizierten Vorgriff immer schon voraus, was diese Wirklichkeit überhaupt ist und sein kann. Anders formuliert: Sie setzen eine zumindest regionale Ontologie oder Metaphysik voraus und präformieren damit auch die möglichen Ergebnisse empirischer Untersuchungen. Foucaults »historischer Ontolo- gie« und auch Latours Forschung, die sich als »empirische Metaphysik« (Harman 2009, 3) charakterisieren lässt, geht es dagegen gerade darum, ein empirisches Vorgehen vor- zuschlagen, das starken ontologischen Setzungen entsagt und stattdessen die Entstehung historischer bzw. regionaler Metaphysiken beschreiben und kritisieren kann. Diaz-Bone kritisiert poststrukturalistische Positionen dafür, dass diese die »Grenzen der Metaphy- sikkritik« überschreiten und bekennt sich zu einer Metaphysik des Sozialen: »Diese methodologische Position zeichnet sich eben dadurch aus, dass eine Theorie eine Metaphy- sik (des Sozialen) einbringt, welche dann die Methodologie und damit in die konkretesten methodischen Schritte einfließen soll.« (Diaz-Bone 2005b) Die empirisch ausgelegten Programme der historischen Ontologie bzw. empirischen Metaphysik sind durch ihre experimentelle Forschungshaltung in der Lage, mit der latenten Paradoxie je- der metaphysikkritischen Position, dass auch eine Kritik von metaphysischen Funda- mentalismen von irgendwelchen Fundamenten ausgehen muss, umzugehen. So lassen sich auch die eigenen Positionen und ontologischen Grundannahmen in sukzessiven Forschungsvorhaben und in Auseinandersetzung mit den untersuchten Gegenständen hinterfragen.



keine Rechenschaft über die eigenen Auswertungstechniken gegeben werden kann. Orientierung für die Auswertung geben aber weniger feste Regeln, sondern vor allem »analytische Strategien«<sup>40</sup> und methodologische Sensibilitäten.

Eine solche Forschungsstrategie bzw. Methodologie (im Gegensatz zu einem festen Methodenprotokoll) lässt sich im Konzept der »interpretativen Analytik« finden, das von Hubert Dreyfus und Paul Rabinow (1983, 122) geprägt wurde, um Foucaults Forschungspraxis zu charakterisieren.<sup>41</sup> Während der analytische Teil dieser Methodologie auf die Existenzbedingungen und historischen *Gründe* des untersuchten Phänomens fokussiert, komplettiert der interpretative Teil die Forschung durch eine Untersuchung der *Effekte* des Phänomens.

Dreyfus und Rabinow (1983, 122) vergleichen das analytische Vorgehen Foucaults mit der Analytik bei Kant und Heidegger und geben damit entscheidende Hinweise zum Verständnis der interpretativen Analytik als Forschungsprogramm. Sowohl Kant (in seiner transzendentalen Analytik) als auch Heidegger (in der Daseinsanalytik) sind von konkreten Phänomenen (Praktiken, Konventionen, Begriffen, Affekten) ausgegangen, die sie in der Wirklichkeit vorgefunden haben (zum Beispiel die Pflicht in Kants (1968) »Grundlegung« oder die Angst in Heideggers (2006) Daseinsanalytik). Ihre analytische Arbeit besteht darin zu zeigen, was diese Phänomene implizieren und was sie ermöglicht hat bzw. worin sie begründet sind. Dadurch werden die Phänomene auf einer höheren Abstraktionsebene intelligibel, so dass ihre unmittelbar-konkrete Selbstverständlichkeit einer philosophischen Reflexion zugänglich wird. Es geht darum zu erkennen, was das Phänomen »enthält«, und darum, es durch »Abstechung heben und desto heller hervorscheinen zu lassen« (Kant 1968, 22), bzw. ein distanzierendes Verhältnis zum »ontisch Nächste[n] und Bekannte[n]«

40 Diese Wendung übernehme ich von dem PhD-Workshop »Foucault, Governmentality, Biopolitics – Analytical strategies for critique of power«, der im Dezember 2013 an der Copenhagen Business School von Kasper Villadsen, Mitchell Dean, Thomas Dumm und Jeffrey Bussolini angeboten wurde und an dem ich teilnehmen konnte.

41 Rainer Diaz-Bone (2006, 70) charakterisiert die interpretative Analytik insofern zurecht als methodologische Position, im Gegensatz zu einem methodischen Verfahren (siehe auch: Diaz-Bone 2005a). Allerdings legt Diaz-Bone die interpretative Analytik dabei lediglich als diskursanalytische Methodologie aus. Sowohl für Foucault wie auch für Dreyfus und Rabinow ist aber klar, dass sich die interpretative Analytik nicht nur zur Untersuchung von Diskursen eignet. Gerade das veränderte, pragmatische Verständnis von Interpretation (s.u.) legt nahe, dass es von vornherein nicht nur um die Analyse von Begriffen und die Interpretation sprachlichen Sinns gehen kann.

einzunehmen, indem man es auf das »ontologisch Fernste« (Heidegger 2006, 43) bezieht. Kant gelangt durch seine Analyse des Pflichtbegriffs zum Sittengesetz als implizitem Gehalt und Bedingung der Möglichkeit der Pflicht. Heidegger vom Phänomen der Angst zur zeitlichen Struktur des endlichen und mit Selbstverständnis ausgestatteten Daseins. Ausgehend von einem konkreten Phänomen (einer sozialen Konvention und einer affektiven Disposition) werden so universelle Möglichkeitsbedingungen und Grundsätze der Moralität bzw. Wesensstrukturen (menschlicher) Existenz aufgezeigt.

Auch Foucault geht von konkreten Phänomenen und Problemen aus, die er durch seine Analyse »hebt«, sie auf ihren impliziten Gehalt und ihre ermöglichenden Faktoren hin befragt, um sie dadurch auf Distanz zu bringen und ihnen ihre Selbstverständlichkeit zu nehmen. Bei ihm führt die Analyse aber gerade nicht zu Universalien, sondern zu historisch spezifischen Formationen.

»Foucault accepts this project [die Analytik, A.F.] but rejects the attempts to find a universal grounding in either thought or Being. Analytics today must find a way of taking seriously the problems and conceptual tools of the past, but not the solutions and conclusions based on them. Foucault (like later Heidegger) replaces ontology with a special kind of history.« (Dreyfus und Rabinow 1983, 122)

Diese »special kind of history« hat Foucault (2005i, 702) als »historische Ontologie« bzw. »Ontologie der Gegenwart« charakterisiert.

Wie die transzendente Analytik und die Daseinsanalytik nimmt auch die interpretative Analytik die Probleme der Gegenwart ernst. »Analytics respects established problems and concepts, recognizing that they are concerned with something important.« (Dreyfus und Rabinow 1983, 204) Sie bezieht sie aber nicht auf universelle Möglichkeitsbedingungen, sondern auf historisch spezifische Existenzbedingungen (Dreyfus und Rabinow 1983, 52–58). Die Herausforderung der interpretativen Analytik besteht darin, vorgefundene Probleme mit einem allgemeineren Begriff in Verbindung zu bringen, der als Name für eine historische Konstellation von Wissen und Macht steht. Das Problem der Bevölkerung etwa wird auf den Begriff der Biomacht, die Praxis des Geständnisses auf das Sexualitätsdispositiv gebracht, so wie sich etwa das Problem des »systemischen Risikos« möglicherweise auf ein neues Sicherheitsdispositiv beziehen lässt.

Man kann in diesem analytischen Vorgehen, das von einem Problem zu einem Begriff fortschreitet, den theoretischen Einsatz der Analytik der Macht sehen. Tatsächlich erfordert die Entwicklung von Begriffen einen

gewissen spekulativen Sprung über das unmittelbare empirische Material hinaus. »The resulting interpretation is neither a subjective invention nor an objective description, but it is an act of imagination, analysis, and commitment.« (Dreyfus und Rabinow 1983, 253) Genau dieser spekulative Überhang ist aber notwendig, um die Probleme nicht einfach nur nachzuerzählen, sondern zu einer Neubeschreibung der Probleme, einer »Reproblematisierung« zu gelangen. Gleichwohl hat man es auch nicht mit einer klassischen Art der Theorie zu tun, die eine eigene theoretische Problematik an den untersuchten Bereich herantragen kann, insofern sie radikal mit der Perspektive der Akteure bricht. Im Gegenteil wird die begriffliche Diagnose immer ausgehend von den vorgefundenen Problemen entwickelt, mit denen sich der Forscher identifizieren kann, weil er sie bis zu einem gewissen Grad teilt.<sup>42</sup> Reproblematisierung besteht im Akt einer begrifflichen Neuversammlung, nicht in einem kompletten Wechsel der Problemstellungen. Der interpretative Analytiker »is able to diagnose our problems because he shares them. We can no longer do theory« (Dreyfus und Rabinow 1983, 125). Theorie in ihren klassischen Varianten, als Gesellschaftstheorie, Sozialtheorie, normative Theorie oder Sozialphilosophie, wird ersetzt durch ein empirisch-theoretisches Format, das man mit einem von Bourdieu (1992, 15–49) geprägten Begriff als »fieldwork in philosophy« bezeichnen kann.<sup>43</sup> *Fieldwork in philosophy* heißt, die spontanen

---

42 Dieses Vorgehen ist daher gerade nicht, wie Diaz-Bone (2006, 78) argumentiert, an der Bachelard'schen Epistemologie des Bruchs zwischen Alltagsgeschehen und wissenschaftlicher Forschung orientiert (siehe zum Konzept des Bruchs mit der Alltagserkenntnis: Bachelard 1974, 19f.). Eher ist die epistemologische Position Canguilhem's maßgeblich, der diese in Auseinandersetzung mit und Kritik des Selbstverständnisses der Lebenswissenschaften entwickelte. Der Physiologie, so argumentiert Canguilhem (1977), geht die Pathologie und damit auch das Pathos, das Leiden des Patienten, voraus, weshalb sich Biologie und Medizin nicht gänzlich von ihren (bio)normativen und lebensweltlichen Grundlagen abkoppeln können. Reproblematisierung ist in diesem Sinne einer ärztlichen Diagnose vergleichbar, die von den unmittelbaren Beschwerden des Patienten ausgehen und diese ernst nehmen, sie aber zugleich überschreiten muss, um zu einer gehaltvollen Diagnose zu gelangen. Im Fall der Analysen bzw. Diagnosen in den Sozial- und Kulturwissenschaften ist gleichwohl Leiden und Diagnostizität nicht so klar verteilt wie in der medizinischen Analogie. Schließlich geht die Machtanalytikerin von einem geteilten Unbehagen, einem »common distress« (Dreyfus und Rabinow 1983, 253) aus.

43 Für diese Arbeit sind gleichwohl die (Foucault'schen) Aneignungen dieses Konzepts durch Paul Rabinow (2003, 84ff) und Ann Stoler (2014) maßgeblicher als Bourdieus Ansatz. Eine ähnlich empirisch-philosophische Ausrichtung haben aber auch Konzepte

und impliziten, aber bisweilen auch ganz explizit vorgetragenen »Philosophien«, die in den Stellungnahmen des untersuchten Feldes zum Vorschein kommen, in ihrer Performativität ernst zu nehmen und zu erkennen, dass die beobachteten Akteure selbst theoretisch beobachten und reflektieren. *Fieldwork in philosophy* heißt, die von bestimmten Technologien (der Macht) ins Werk gesetzten Ontologien zur Sprache und auf den Begriff zu bringen. *Fieldwork in philosophy* ist ein Modus theoretisch ambitionierter empirischer Forschung, die »Theorie« nicht unabhängig von konkreten Fällen und Problemen entwickelt und Empirie nicht als bloßes Registrieren und Berichten von Daten gestaltet. In diesem Sinne handelt es sich um eine Variante »theoretischer Empirie« (Kalthoff, Hirschauer und Lindemann 2008).

Während Foucault sich selbst auf das Konzept der Analytik berufen hat, stand er dem Begriff der Interpretation stets skeptisch bis ablehnend gegenüber. Zu sehr ist Interpretation beladen mit Vorstellungen von der Suche nach einem in der Tiefe verborgenem Sinn und der Entschlüsselung des subjektiv Gemeinten. Das ist aber nur der Fall, solange man Interpretation unter Maßgabe eines traditionellen Sinnverständnisses begreift. Wenn man Sinn nicht als tiefen Bedeutungsgehalt oder eine der Welt angeklebte Symbolschicht, sondern als eine Form praktischer Relevanzbildung begreift, die korrelativ mit den Operationen sozialer Gefüge entsteht, dann heißt auch Interpretation nicht mehr Suche nach tiefen Bedeutungsschichten und subjektiven Absichten. Interpretation wird gewissermaßen dehermeneutisiert: »Foucault's method is interpretive but not hermeneutic.« (Dreyfus und Rabinow 1983, 124) Stattdessen bekommt Interpretation eine pragmatistische Schlagseite. Es geht nicht mehr um tiefe Bedeutungsschichten, sondern um Oberflächenereignisse. Es geht auch nicht mehr um die subjektiven Sinnzuschreibungen einer Handlung oder einer Aussage, sondern um deren *Effekte* und damit um die Ebene, die den Akteuren aufgrund ihrer Verwobenheit in den Vollzug sozialer Operationen systematisch entgeht. »Die Leute wissen, was sie tun; häufig wissen sie, warum sie das tun, was sie tun; was sie aber nicht wissen, ist, was ihr Tun tut.« (Foucault zitiert nach: Dreyfus und Rabinow 1994, 219) Die Interpretation untersucht also Oberflächen und keine Tiefenschichten, Relevanzereignisse und nicht Bedeutungen, Effekte und nicht Intentionen.

---

und Forschungsstrategien in den STS bzw. in der ANT, etwa Annemarie Mols (2002, vff.) Konzept der »empirical philosophy«.

Konkretisiert wird die Untersuchungsstrategie der interpretativen Analytik in dieser Arbeit durch eine Systematisierung des Materials entlang der drei Achsen der Sicherheitsanalytik: Problematisierung, Technologie und Strategie. Auf der Achse der Problematisierung geht es darum, im Material wiederkehrende Argumentations- und Rationalitätsmuster zu identifizieren. Die Herausarbeitung diskursiver Regelmäßigkeiten und Häufungen ermöglicht es zunächst, auf den geteilten Raum der Problematisierung zu schließen. Die bloße diskursive Häufung bildet aber noch nicht den Problemraum selbst. Deshalb muss die Häufung auf eine begrenzte Zahl paradigmatischer Probleme als zentrale Zielpunkte der gouvernementalen Sicherheitsbemühungen bezogen werden.<sup>44</sup> Immer wiederkehrende Problematisierungen von Interdependenz, Ansteckung, kaskadenartiger Ausbreitung, Übervernetzung, Abhängigkeit und Komplexität lassen sich dann auf die konzeptuelle Kategorie des systemischen Risikos beziehen, die als paradigmatisches – wenngleich nicht unbedingt explizit als solches benanntes – Problem die Bemühungen zur Regierung der Katastrophe anleitet. Die paradigmatische Analyse geht analogisch vor (Agamben 2009, 37), indem sie ähnliche Problematisierungsmuster in unterschiedlichen Feldern analysiert. Der höhere Abstraktionsgrad, der durch diese Untersuchung erzielt wird, ist nicht zuletzt notwendig, um zu untersuchen, ob und inwiefern analoge Problembeschreibungen verschiedene Handlungsfelder miteinander verzahnen.

Auf der Achse der Technologien geht es darum, in den vielfältigen institutionellen Innovationen, regulatorischen Maßnahmen und praktischen Interventionen eine Reihe analoger Technologien zu identifizieren. Auch hier gilt es, die unmittelbare Fülle der Maßnahmen auf eine Weise zu ordnen, die überhaupt erst so etwas wie abstrakte Formen und Technologien

---

44 Foucaults geradezu statistisches Vokabular in der Archäologie des Wissens, seine Rede von »diskursiven Regelmäßigkeiten« (1981, 33ff.), »Serien« (33ff.), »Häufung« (172) lässt bisweilen den Eindruck entstehen, dass die zu identifizierenden Regeln der (diskursiven) Praktiken gleichsam durch die Kenntnis über ihren Durchschnitt rekonstruiert werden könnten. Das würde allerdings den paradigmatischen oder idealtypischen Charakter der Foucault'schen Analytik übersehen (siehe dazu: Rabinow 2003, 36ff.). Idealtypen – so hat schon Weber (1988a, 190f.) argumentiert – sind eben keine Durchschnittstypen, sondern entstehen durch »Steigerung«. Paradigmen sind bisweilen drastische und zugespitzte Phänomene, die aber gerade dadurch auch andere Phänomene intelligibel machen (Agamben 2009, 11–39). Der Fokus auf das Paradigmatische ist dennoch keine gänzliche Absage an die Analyse der Wiederholungen und Regelmäßigkeiten, weil sich ja erst durch diese Analyse zeigen kann, was sich in Bezug auf Wiederholungen als paradigmatisch bzw. idealtypisch abheben lässt.

zum Vorschein kommen lässt. So können beispielsweise Maßnahmen zur Ressourcenbevorratung, zum Aufbau von Puffern, zum Aufbau zusätzlicher Katastrophenbewältigungskapazitäten und organisatorische Kontingenzplanungen als Technologie der *preparedness* sichtbar gemacht werden. Ein Dispositiv kann dann ausgemacht werden, wenn unterschiedliche Technologien in ihrem Zusammenspiel aufgezeigt werden können. Auf dieser Untersuchungsebene geht es dann auch darum, wie Technologien und Probleme zusammenhängen, indem gezeigt wird, wie auf bestimmte paradigmatische Probleme systematisch bestimmte Arten von Technologien antworten (etwa Technologien der Verwundbarkeitsreduktion, die auf das paradigmatische Problem des systemischen Risikos antworten).

Mit Blick auf die Analyseachse der Strategien werden die im Material vorgefundenen Problematisierungen und Technologien zusätzlich als interessengeleitete und politisch motivierte Einsätze aufgeschlüsselt. Im Gegensatz zum Fokus auf Analogien, Regelmäßigkeiten und Häufungen auf der Problem- und Technologieachse geht es bei der Analyse der strategischen Ebene eher um Modifikationen und die Streubreite der Probleme und Technologien, also gewissermaßen um die Differenzen in den Wiederholungen. Gerade weil ganz unterschiedliche Problematisierungen auf einen gemeinsamen Problemraum und unterschiedliche Technologien auf ein Dispositiv bezogen werden können, indem Analogien, Ähnlichkeiten und diskursive Regelmäßigkeiten herausgearbeitet werden, ist es auch möglich, die vorgefundene empirische Diversität als strategische Variationen innerhalb des etablierten Problemraums kenntlich zu machen. Prinzipiell ist jede Positionierung, jede Aussage, jede Problematisierung, jede vorgesehene oder durchgeführte Maßnahme strategisch: sie steht im Dienste konkreter Interessen und/oder politischer Ziele: »keine Macht, die sich ohne eine Reihe von Absichten und Zielsetzungen entfaltet« (Foucault 1977, 116). Deswegen werden auf der strategischen Analyseebene auch keine anderen Aussagen, sondern dieselben Aussagen anders, also unter einem anderen Blickwinkel analysiert.

Die Analyseachse der Strategien enthält darüber hinaus auch die Analyse von Kontroversen und Kritik. Diese Streitigkeiten und Anfechtungen machen die Einsätze der Problematisierungen und Technologien deutlich, sie zeigen, worum es geht, was auf dem Spiel steht. Dabei können in Kontroversen auch Positionen vorkommen, die abseits des etablierten Problemraums stehen, die diesen grundsätzlich kritisieren oder ihm Widerstände entgegensetzen. Gerade solche Positionierungen sind wichtig, um die

Mächte der Sicherheit angemessen kartieren zu können. Denn erst Widerstände machen die Machtformationen nicht als geronnene Strukturen, sondern als umkämpfte und umkehrbare Verhältnisse sichtbar (siehe: Foucault 2005f, 273).

Bei der Analyse des Materials habe ich auf standardisierte Auswertungsprotokolle und Computerprogramme verzichtet. Vielmehr habe ich zunächst in einer explorativen Untersuchungsphase Material erschlossen, Experten\_inneninterviews geführt und erste analytische Überlegungen angestellt, die ich systematisch protokolliert habe. Aus dieser ersten induktiven Codierung des Materials haben sich thematische Cluster ergeben, die sich in der Struktur der Arbeit widerspiegeln und im Weiteren ein an die jeweiligen Schwerpunkte angepasstes Auswertungsverfahren ermöglicht haben. Anschließend habe ich die Dokumente sowie die transkribierten Interviews thematisch sortiert und erneut detailliert untersucht. Hierfür habe ich in der Auseinandersetzung mit dem jeweiligen thematischen Sachgebiet angemessene Kategorien gebildet und diesen Kategorien relevante Passagen und Schlüsselbegriffe im Text zugeordnet. Schließlich habe ich die Kategorien und die ihnen zugeordneten Passagen und Begriffe in *mind maps* systematisiert. *Mind maps* eignen sich für diese Systematisierung, weil sie ähnlich wie digitale Codierungsprogramme eine (hierarchisierte) Codestruktur erzeugen, die zudem eine gute Übersicht über das Material ermöglicht und flexibel auf die eigene Forschung zugeschnitten werden kann.

Die Darstellung der Ergebnisse hat eine aus dem Erkenntnisinteresse der Arbeit resultierende Logik. Die Darstellung muss das Ethos der interpretativen Analytik auf- und annehmen, die Gegenwart »auf einen Begriff« zu bringen, sie in einer Weise zu präsentieren, die Distanz zu den unmittelbaren Geschehnissen erzeugt, um das, was ist, anders wahrnehmen zu können. Es geht mir folglich darum, signifikante und bisweilen auch riskante Berichte (zur Bedeutung des Schreibens riskanter und guter Berichte siehe: Latour 2007, 211–243) über meine Auseinandersetzung mit meinem Material, mit den Feldern und Themen, die ich untersucht habe, zu geben. Nicht selten habe ich mich entschieden, eine narrative Form der Darstellung zu wählen, die der Chronologie der untersuchten Ereignisse folgt, um sie als exemplarische Fälle eines emergenten Sicherheitsdispositivs verständlich zu machen. Die stärker theoretisch-spekulativen Überlegungen finden sich zumeist am Ende der einzelnen Abschnitte und Kapitel. Sie sollen zeigen, auf welchen größeren Einzugsbereich sich die empirischen

---

Fälle beziehen lassen. Es ging mir also gleichsam darum, die Rahmungen der einzelnen Fälle spekulativ zu überfluten, anstatt diese mit einem allgemeinen theoretischen Rahmen zu überfrachten. Am Ende des Tages bzw. am Ende der Arbeit geht es weder um Theorien, die zu beweisen oder zu widerlegen sind, noch um Methoden, die besonders elegant oder konsequent angewendet werden sollen; es geht nicht um die Größe und Zusammensetzung des Materialkorpus, sondern darum, ob man Antwort geben kann auf eine Frage, die sich spätestens seit Beginn der Aufklärung stellt: Was ist die Gegenwart? »Welchen Unterschied führt sie heute gegenüber gestern ein?« (Foucault 2005i, 689) An dieser Frage müssen sich die theoretischen, empirischen und darstellerischen Werkzeuge und Praktiken messen lassen.



## 2. Die Regierung der Katastrophe

Auf den ersten Blick erscheint die Regierung der Katastrophe als ein aussichtsloses Unterfangen. Wie kann etwas regiert werden, das sich der Kontrolle und Beherrschung so systematisch entzieht? Es lässt sich gleichwohl nicht übersehen, dass der Schutz vor Katastrophen zur Praxis von und zum Anspruch an Regierungen westlicher Staaten geworden ist. Bürger\_innen erwarten, vor katastrophischen Verheerungen geschützt oder zumindest bei der Bewältigung ihrer Folgen von staatlichen Institutionen unterstützt zu werden. Schon immer war die Katastrophe eine Bewährungsprobe für die Regierenden. Aber seit etwa einhundert Jahren geht es für Regierungen nicht mehr nur darum, situativ auf Katastrophen zu reagieren, sondern auch, vorsorglich Kapazitäten für den Katastrophenfall zu mobilisieren. Die Katastrophe ist zum expliziten Thema des Regierens geworden. Treibende Kraft dafür waren zunächst die beiden Weltkriege, die in zuvor unbekanntem Maße auch die Zivilbevölkerung betroffen haben. Wie ich im Folgenden nachzeichnen werde, wurden aus dieser Erfahrung heraus im Kalten Krieg beträchtliche Anstrengungen zum Zivilschutz unternommen. Der Katastrophenschutz ist zumeist im Fahrwasser dieses Zivilschutzes mit vorangetrieben worden. Deswegen hat auch das Ende des Kalten Krieges eine Zeit der Umorientierung in der Regierung der Katastrophe ausgelöst, die vor allem seit dem 11. September 2001 eine spezifische Gestalt und Richtung angenommen hat. In einer ganzen Reihe westlicher Staaten wurde jetzt daran gearbeitet, Institutionen zu bilden bzw. umzubilden sowie Strategien aufzulegen, die ein Management von Großschadenslagen ermöglichen sollten, das sich nun nicht mehr vornehmlich am Kriegsfall orientierte. So sind etwa in direkter Folge des 11. Septembers das Department of Homeland Security in den USA und etwas später das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe in Deutschland geschaffen worden. Bereits kurz vor dem 11. September entstand in Großbritannien das Civil Contingencies Secretariat. Aber auch

dort, wo – wie etwa in Frankreich – keine Institutionen neu gegründet wurden, kam es zu vielfältigen Transformationen der Katastrophenschutzpolitik.

In dieser Arbeit stehen allerdings nicht die institutionellen Transformationen, sondern vor allem die Verschiebungen und Entwicklung auf der Ebene der Sicherheitstechnologien im Vordergrund. Auch und gerade auf dieser Ebene lassen sich ähnliche Entwicklungen in unterschiedlichen Ländern identifizieren. So wurde in Studien zur Regierung der Katastrophe in Ländern wie den USA (Collier 2008, Lakoff 2007), Großbritannien (Adey und Anderson 2011), Frankreich (Lentzos und Rose 2009, 238f.), Schweden (Amin 2013), der Schweiz und Indien (Deville, Guggenheim und Hrdličková 2014) ähnliche Regierungstechnologien und Rationalitäten identifiziert: der Bedeutungsgewinn der Interventionsform der Vorbereitung, die Orientierung am Leitbild der Resilienz, die Fokussierung auf eine Vielzahl unterschiedlicher Katastrophen (*All-Hazards Approach*). Diese ähnlichen Entwicklungen sind gewiss keine reinen Zufälle, sondern ein Hinweis auf die hohe Mobilität von Politiken der Sicherheit, die häufig das Ergebnis expliziter Koordinierungsbemühungen auf europäischer und globaler Ebene sind. Regierungstechnologien im hier verstandenen Sinn sind also stets »mobile technologies« (Ong 2007) bzw. »abstract form[s]« (Lakoff 2007, 254), die in unterschiedlichen Ländern aktualisiert werden können.

Gleichwohl geschieht diese Aktualisierung nicht im luftleeren Raum. Vielmehr treffen neue Technologien und Denkweisen der Sicherheit auf eine bestehende und mitunter sehr beharrliche Ökologie aus Institutionen und Routinen der Sicherheitspolitik. Das gilt auch und gerade für Deutschland. Schließlich hat sich im Nachkriegsdeutschland auf Grund von Besatzung, Teilung und nicht zuletzt wegen der historischen Belastung deutscher Verteidigungs- und Sicherheitspolitik eine sehr spezifische Konstellation des Zivil- und Katastrophenschutzes herausgebildet. Neue Sicherheitstechnologien ersetzen diese Konstellation nicht einfach, sondern schreiben sich in sie ein, indem sie bestehende Traditionen kritisieren, aber auch aufnehmen und für ihre Zwecke mobilisieren.

In diesem Kapitel folge ich bestimmten operativen Technologien der Sicherheit in Deutschland, die Katastrophen regierbar machen sollen. Dabei führt mich diese Folge- und Suchbewegung über den Bereich des Katastrophen- bzw. Bevölkerungsschutzes im engeren Sinne hinaus. Auch in Bereichen wie Lebensmittelsicherheit, Umweltschutz und Finanzmarkt-

gulation finden sich Rationalitäten und Technologien, die auf eine Regierung von Katastrophensituationen bzw. eine Kontrolle systemischer Risiken zielen. Ich versuche hier also einen großangelegten Überblick über analoge Technologien und Problemstellungen in einer ganzen Reihe gesellschaftlicher Felder zu geben. Zusammengenommen bilden die vielfältigen Transformationen in unterschiedlichen Institutionen und Bereichen, die Kombination alter und neuer Technologien der Sicherheit, eine spezifische Konfiguration, die ich als Sicherheitsdispositiv der Resilienz beschreiben und systematisch von historisch konstituierten Dispositiven der Sicherheit – der Souveränität und der Normalisierung – abgrenzen werde.

Dafür werde ich zunächst auf die Problematisierungen der institutionellen Verfasstheit und der strategischen Ausrichtung des deutschen Katastrophen- und Zivilschutzes in der Folge des 11. September eingehen. Dabei setze ich nicht einfach einen bestehenden sicherheitspolitischen Kontext voraus, in den sich die neuen Sicherheitstechnologien versuchen einzuschreiben. Vielmehr will ich zeigen, wie die Problematisierungen selbst diesen Kontext beschreiben, wie sie durch ihre Problematisierungen den sicherheitspolitischen »Hintergrund« in den Vordergrund rücken (2.1.). Anschließend gehe ich auf die institutionellen Veränderungen ein, die sich im Zuge dieser Problematisierungen ergeben haben und im strategischen Ansatz des »Bevölkerungsschutzes« und der Etablierung des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK) ihren deutlichsten Ausdruck finden (2.2.). Diese institutionellen Veränderungen genügen aber noch nicht, um von der Herausbildung eines Sicherheitsdispositivs der Resilienz zu sprechen. Deswegen gehe ich in den folgenden drei Teilen des Kapitels auf die Charakteristika der neuen Regierungsformen der Katastrophe im Hinblick auf die vier Dimension – Zeit, Raum, Objekt, Norm – ein, die ein Sicherheitsdispositiv abgrenzbar machen. Zunächst gehe ich auf die Risikoanalytik im Bevölkerungsschutz ein und zeige die zeitliche und räumliche Dimensionierung der Sicherheitstechnologien zur Regierung der Katastrophe (2.3.). Danach zeige ich, wie das »System« einerseits zum zentralen Schutzobjekt geworden ist – als vitales System bzw. Kritische Infrastrukturen –, andererseits aber auch durch die Kategorie des systemischen Risikos auf neue Weise als Gefährdungszusammenhang beobachtet wird (2.4.). Schließlich analysiere ich eine Reihe von Sicherheitstechnologien, die auf derartige systemische Risiken in ganz unterschiedlichen Bereichen reagieren und alle auf ihre Art dem normativen Leitbild der Resilienz folgen (2.5.). Das Kapitel schließt mit einer Betrachtung über die Konse-

quenzen, die kontemporäre Beobachtungsweisen und Regierungsformen der Katastrophe für das Denken des Sozialen haben (Exkurs I).

## 2.1. *Problematisierung*: Neuverhandlung des Katastrophen- und Zivilschutzes

Die Terroranschläge vom 11. September auf das World Trade Center in New York City und das Pentagon in Washington D.C. haben die weltweite Sicherheitspolitik nachhaltig verändert. Vertreter\_innen der *Critical Security Studies* haben diese Veränderungen – wenn auch eher selten in Bezug auf den Katastrophenschutz – aufgezeigt und kritisiert (siehe exemplarisch: Bigo und Tsoukala 2008). Zugleich haben sie davor gewarnt, den 11. September zum alleinigen Ausgangspunkt dieser Transformationen zu stilisieren und sich damit eine allzu suggestive Chronologie der Ereignisse zu eigen zu machen, die von den Sicherheitsapparaten selbst nahegelegt wird. Es besteht nämlich die Gefahr, wie Didier Bigo (2006) zurecht argumentiert hat, diese Veränderungen als notwendige Folge und angemessene Reaktion auf eine veränderte und zugleich verschärfte »Gefahrenlage« zu interpretieren. Die *Critical Security Studies* haben darauf unter anderem mit genealogischen Untersuchungen reagiert. So konnte gezeigt werden, dass Sicherheitstechnologien, die seit dem 11. September vermehrt zum Einsatz kommen, vielfach bereits im Kalten Krieg entwickelt wurden (Aradau und Munster 2011, Collier und Lakoff 2015). Damit ist aber noch nicht geklärt, wie es dazu kommen konnte, dass dem 11. September eine solche Bedeutung zugeschrieben wird. Wie wurde 9/11 in Dispositiven der Sicherheit mobilisiert und was hat diese Mobilisierung auslöst und ermöglicht? Diesen Fragen möchte ich mich in diesem Kapitel widmen. Ich werde nachvollziehen, wie genau der 11. September in Deutschland zum problematischen Ereignis und dann zur fraglosen Evidenz in Sicherheitsdispositiven werden konnte. Dafür werde ich zunächst die spezifische Ereignislogik von 9/11 untersuchen (2.1.1.). Anschließend werde ich darauf eingehen, wie das Ereignis des 11. September als Ausgangspunkt für Problematisierungen der traditionellen Aufteilung von innerer und äußerer Sicherheit, von Katastrophen- und Zivilschutz in Deutschland genutzt wurde (2.1.2.). Danach gehe ich auf eines der Grundprobleme der Kontingenzplanung

ein, nämlich die Frage der angemessenen Ressourcenallokation für sehr unwahrscheinliche und seltene Ereignisse (2.1.3.).

### 2.1.1. Das Ereignis des 11. September

Das Datum 11. September oder 9/11 ist bis heute ein unvermeidlicher Bezugspunkt sicherheitspolitischer Debatten. »Die Ereignisse vom 11. September 2001 haben [...] innerhalb weniger Stunden die Welt so entscheidend und grundlegend verändert wie wenige Ereignisse zuvor.« (BBK 2005a, 10) Deswegen bietet sich das Datum als Ausgangspunkt der Untersuchung über die Veränderungen der Regierung katastrophischer Risiken in Deutschland an. Gleichwohl geht mit diesem Zugeständnis nicht einher, sämtliche Evidenzeffekte des 11. September unhinterfragt zu lassen. Zuzugestehen, dass die Terroranschläge Effekte hatten und vielleicht sogar, dass sie bestimmte sicherheitspolitische Folgen haben mussten, schließt gerade nicht aus, zu fragen: *was* genau war das Ereignis, *wie* ist es so wirksam geworden?

Diese Fragen zu stellen heißt, zwischen zwei Verständnissen des Ereignisses zu unterscheiden. Zunächst bewirkt ein Ereignis, im emphatischen Verständnis Michel Foucaults (2005c, 29), einen »Bruch der Evidenz«. Es ist dann ein Ereignis, wenn es aus einem gewohnten und erwartbaren Verlaufsgeschehen, aus der »Serie der Ereignisse« (Foucault 2004, 40), ausschert. Ein solches Ereignis erzeugt eine Verunsicherung, die zur Problematisierung anregt. Im Zuge von Problematisierungen kann das Ereignis wiederum zum Anker bzw. Referenzpunkt für die Produktion neuer Evidenzen werden. Das Ereignis wird rekursiv zum Objekt und zur Zielscheibe von Wissensformen und Machttechnologien und wechselt so seinen Modus. Zunächst ist es ein Wahrheitsereignis, weil es einen Riss im Kontinuum des Wahren darstellt, »a tear in the fabric of our epistemological web« (Butler 2001). Dies ist der Moment, wo dem Ereignis noch mit rat- und sprachlosem Staunen begegnet wird. Erst rückwirkend kann das Ereignis zum »moment that reveals truth« (Roitman 2013, 4) werden. Es wird für politische Programmatiken und Forderungen mobilisierbar und kann nun zum Ausgangspunkt einer neuen Serialisierung von Ereignissen werden.

»Die Ereignisse vom September 2001 sollten die Notwendigkeit entsprechender Maßnahmen deutlich gezeigt haben und alle Verantwortlichen zum unverzüglichen Handeln anregen.« (Schutzkommission 2001, 7). Das

Zitat entstammt einer Stellungnahme der sogenannten »Schutzkommission beim Bundesminister des Inneren« – eine Gruppe von Wissenschaftler\_innen, die die Bundesregierung in Fragen des Katastrophenschutzes berät. Hier, wie in anderen institutionellen Stellungnahmen, bekommt das Katastrophenereignis des 11. September neben seinem Wahrheitswert einen normativen Mehrwert. Es erlangt imperativen Charakter, weil es eine politische Reaktion herausfordert. Der 11. September fungiert, gemeinsam mit den »Hochwasserlagen von 2002« (BBK 2010b, 13),<sup>45</sup> geradezu als Gründungsszene für eine sicherheitspolitische Neuorientierung in Deutschland, die rechtliche und institutionelle Schritte angeregt hat und gerechtfertigt erscheinen lässt. Sein und Sollen, Wahrheit und Normativität des Ereignisses gehen Hand in Hand. Denn die institutionellen Maßnahmen antworten auf Leerstellen und Lücken bisheriger Sicherheitspolitik, die durch das Ereignis beleuchtet wurden.

»[D]iese Ereignisse und ihre Folgen [haben] die Verwundbarkeit einer hoch technisierten, global agierenden und von zahlreichen Systeminteraktionen abhängigen Gesellschaft zu Beginn des 21. Jahrhunderts auf dramatische Weise verdeutlicht.« (BBK 2010b, 20) Erst durch die Krise konnte eine bereits bestehende latente »Verwundbarkeit« bewusst werden. Die Bezugnahme auf den 11. September als »weltveränderndes Ereignis« ist also eine typische Mobilisierung von Krisenereignissen als »Wahrheitsprozedur« (Folkers und Lim 2014, 49), die etwas sichtbar macht, das ohne sie im Verborgenen geblieben wäre.

Die intensive Debatte über »neue« Sicherheitsprobleme und die grundlegende Verwundbarkeit westlicher Gesellschaften zu Beginn des neuen Jahrtausends verweist gleichwohl auch auf eine Atmosphäre der Verunsicherung, die eine gesteigerte Aufmerksamkeit für die Katastrophe vom 11. September begünstigt hat. Die Furcht vor neuen und »asymmetrischen« Bedrohungen ist aber keine Erfindung des 21. Jahrhunderts. Spätestens mit dem Ende des Kalten Krieges begann nicht nur in der Bundesrepublik eine Debatte über veränderte Gefährdungslagen und Spekulationen über neue Bedrohungen. Schon 1996 heißt es im damaligen Bericht der Schutzkommission:

»Die Rahmenbedingungen für die Planung und Durchführung von Maßnahmen zum Schutze der Bevölkerung gegen die Gefahren bei Großkatastrophen und im

---

45 Im August 2002 gab es in Mitteleuropa viele schwerwiegende Hochwasser. Betroffen waren vor allem die Elbe und die Donau.

Verteidigungsfall haben sich mit dem Wandel der allgemeinen sicherheitspolitischen Lage, der Öffnung der Gesellschaft in einem vereinigten Europa, der technologisch bedingten Veränderung der Gesellschaft und der Zunahme des Terrorismus in den letzten Jahren grundlegend verändert.« (Schutzkommission 1996, 3)

Zugleich blieb die neue Gefährdung stets diffus und ungewiss. Das Ende der Blockkonfrontation und der klar identifizierbaren Bedrohung durch das »feindliche Lager« hinterließ ein beunruhigendes Vakuum. So hieß es in den verteidigungspolitischen Richtlinien von 1992 entsprechend vage: »Der mögliche Verlauf von Krisen und Konflikten läßt sich kaum nach Wahrscheinlichkeiten und Bedrohungsgrad voraussagen.« (BMVg 1992) Die Gründe für die große Resonanz, die die Ereignisse vom 11. September in sicherheitspolitischen Kreisen auslösten, müssen also auch in dieser Ungewissheit nach dem Kalten Krieg gesucht werden. In einer Situation, in der Sicherheitsstrategen nur im Trüben nach möglichen Gefahren fischen konnten, verlieh der 11. September der diffusen Besorgnis vor den neuen Gefahren des 21. Jahrhunderts mit einem Mal eine ebenso schrille wie unabweisbare Evidenz. Das Gespenst der diffusen Bedrohung hatte sich manifestiert, die anonyme Gefahr ein Gesicht bekommen. In dieser Perspektive erscheint der 11. September weniger als ein vollkommen singuläres Ereignis, das einen »Einschnitt« darstellte, sondern vor allem als Ereignis mit einer besonders hohen Anschlussfähigkeit (Luhmann 1991b, 62). Dabei sichert hier nicht Gewohnheit, Routine und Wiederholung die Anschlussfähigkeit, sondern gerade das Ungewöhnliche und Problematische, das Aufmerksamkeit bindet und gleichsam einen neuen paradigmatischen Verteidigungsfall aufgerufen hat.

Ebenso wie das Ereignis einen Vorlauf in der Vergangenheit hatte, ermöglicht es auch ein Vorgehen in die Zukunft. Diese komplexe Temporalität des 11. September als Trauma, das aus der Zukunft kommt, hat Jacques Derrida beleuchtet:

»Der Beweis des Ereignisses hat als tragisches Korrelat nicht etwa das, was derzeit passiert ist, sondern das vorlaufende Zeichen dessen, was zu passieren droht. Die Zukunft macht die Nichtaneignbarkeit des Ereignisses aus, weder die Gegenwart noch die Vergangenheit. [...] Es handelt sich um ein Trauma und also um ein Ereignis, dessen Temporalität weder vom gegenwärtigen Jetzt noch von der gegenwärtigen Vergangenheit ausgeht, sondern von einem Un-Darstellbaren, das noch kommen wird.« (Derrida und Habermas 2004, 130)

»Kann das wieder geschehen? Kann das auch bei uns geschehen? Was kann sonst noch geschehen?« lauten die obligatorischen Fragen *nach* der

Katastrophe, die in Hinsicht auf die erst noch *kommende* Katastrophe gestellt werden. So beschwörte etwa die Schutzkommission in ihrem Bericht unmittelbar nach dem 11. September eine ganze Serie möglicher, durch Terrorismus ausgelöster Katastrophenszenarien herauf:

»Die Terroranschläge in den USA am 11. September 2001 haben deutlich gemacht, dass im Rahmen des Zivil- und Bevölkerungsschutzes bisher nicht für möglich gehaltene Szenarien berücksichtigt werden müssen. Wenn Mitglieder fanatisierter Gruppen in präzise geplanten und koordiniert durchgeführten Selbstmord-Attentaten die Maximierung des Schadens anstreben, sind folgende Anschläge nicht mehr undenkbar: Störung der Regierungs- und Wirtschaftsfunktionen durch Beeinträchtigung nationaler und internationaler Computernetzwerke [...], Zerstörung von Versorgungseinrichtungen (Energie, Wasser) mit möglichen Spätfolgen wie Lebensmittelverknappung, Anschläge auf Regierungs- oder Verwaltungssitze, auch internationaler Behörden, Anschläge auf den Bahnverkehr (auch hier sind Unfälle mit Hunderten von Toten möglich), Sprengung von Talsperren mit anschließender Überflutung weiter Gebiete, Anschläge auf vollbesetzte Sportstadien, Verbreitung von radioaktiven, biologischen oder chemischen Gefahrstoffen in Luft oder Wasser, Anschläge auf Bauwerke oder Veranstaltungen mit großer symbolischer Bedeutung für Deutschland, Europa oder die Welt.« (Schutzkommission 2001, 13–4)

Der 11. September hat einen geschärften Sinn für das Mögliche der Katastrophe erzeugt. Diese Sinnesschärfung wird von Sicherheitsexperten kultiviert und intensiviert. Eine Serie von konkreten Szenarien wird aufgerufen, für die zusätzliche Sicherheitsmaßnahmen eingefordert werden. Dabei vermengen sich Realität des geschehenen Ereignisses und Fiktion über mögliche zukünftige Ereignisse häufig zu einem amorphen Evidenzblock.

»Auch die Größenordnung der Anschläge vom 11. September 2001 mit mehreren Tausend Toten und Verletzten sowie möglicher anderer Anschlagsszenarien mit radioaktiven nuklearen, chemischen oder biologischen Massenvernichtungswaffen [...] zeigen [sic!], dass Vorbereitung, Abwehrplanung und Schadensbekämpfung in diesen Fällen nicht alleine Aufgabe des Katastrophenschutzes und der für den Katastrophenschutz zuständigen Behörden sein kann« (BBK 2010b, 25).

Der 11. September kann also als Ausgangspunkt dienen, um die zeitgenössische Regierung der Katastrophe in Deutschland zu analysieren, aber nur, wenn das Ereignis aus der gewohnten chronologischen Serie herauslöst wird, in der es im Zuge eines längeren Problematisierungsprozesses seinen Platz eingenommen hat. Zu zeigen, welche Techniken zu dieser »Ereignishaftmachung« (Foucault 1992, 30f.) beigetragen haben, heißt zugleich eine Re-serialisierung (Walters 2012, 131) vorzunehmen, indem



Problematisierungen nachvollzogen werden, welche die Signifikanz des Ereignisses überhaupt erst möglich gemacht haben.

### 2.1.2. »Katastrophen kennen keine Grenzen« Kritik des deutschen Katastrophenföderalismus

Mit dem 11. September ist aber nicht nur ein neuartiges Sicherheitsproblem auf den Plan getreten. Der gegebene institutionelle und rechtliche Rahmen der Sicherheitspolitik ist selbst zum Problem geworden. Vor allem die klassische Aufteilung von Zivilschutz und Katastrophenhilfe wurde immer wieder als entscheidendes Hindernis für einen effektiven Schutz der Bevölkerung angeführt. Während der Zivilschutz im Falle eines Angriffskrieges auf die BRD laut Artikel 73 des Grundgesetzes Aufgabe des Bundes bzw. der Bundeswehr ist, fällt die Aufgabe des Katastrophenschutzes in den Aufgabenbereich der Bundesländer. Die Idee, die dieser Aufteilung zugrunde liegt, ist die Abgrenzung von »äußeren« und »inneren« Gefahrenquellen. Für die innere Sicherheit ist die Polizei (auf Länderebene) sowie auf kommunaler Ebene Feuerwehren und Sanitätsdienste zuständig, während für die Landesverteidigung der Bund und die Bundeswehr zuständig sind. Diese grundsätzliche Aufteilung zwischen Landesverteidigung und innerer Sicherheit kann auf eine lange Tradition nicht nur in Deutschland zurückblicken. Die zunehmende Auflösung dieser klaren Trennung von innerer und äußerer Sicherheit ist in einer Reihe von Analysen globaler Sicherheitspolitik hervorgehoben worden.<sup>46</sup>

Der 11. September hat im Verbund mit anderen Katastrophenereignissen aber die ohnehin bestehende Tendenz zur Auflösung der Unterscheidung von innerer und äußerer Sicherheit intensiviert. Dabei sind diese Veränderungen gerade in Deutschland aus historischen Gründen besonders heikel. Die spezifische Aufgabenteilung zwischen Bund und Ländern ist schließlich vor allem ein Ergebnis der Entstehung der bundesrepublikanischen Verfassung, in der die Lehren aus dem Nationalsozialismus gezogen werden sollten. Erst die berüchtigten Notstandsgesetze in den 1970er Jahren hatten die strikte Trennung von äußerer und innerer Sicherheit

---

<sup>46</sup> So haben Michael Hardt und Antonio Negri (2002) argumentiert, dass im *Empire* – der neuen globalen Weltordnung, die kein Außen mehr kennt – auch militärische Interventionen als Operationen einer neuen Weltpolizei verstanden werden müssen. Didier Bigo (2001) hat in ähnlicher Absicht die Verschlingungen von äußerer und innerer Sicherheitspolitik seit dem Ende des Kalten Krieges betont.

durch den Artikel 35 erstmals eingeschränkt, der unter anderem besagt, dass bei Katastrophenlagen und »zur Wiederherstellung der öffentlichen Ordnung« die Länder Unterstützung durch die Bundespolizei und die Bundeswehr erhalten können. Der beträchtliche Widerstand gegen diese Gesetze unter anderem seitens der damaligen Studierendenbewegung offenbart das damalige Misstrauen gegen zentralstaatliche Machtkonzentration und den politischen Wert, der der Trennung von innerer und äußerer Sicherheit zugesprochen wurde.

Vielen Sicherheitsstrategen und Katastrophenforschern erscheint diese Trennung heute dennoch zunehmend problematisch und unangemessen. In einer Studie zu möglichen Weiterentwicklungen des deutschen Zivilschutzes aus dem Jahr 2002, die zur Grundlage für den Beschluss zu einer neuen Strategie des Bevölkerungsschutzes im Jahr 2004 werden sollte, bemerkt der Sicherheitsexperte Wolfram Geier etwa:

»Die Anforderungen an einen effektiven [...] Schutz der Bevölkerung sind aufgrund der Komplexität von Gefahren, Verletzlichkeiten und Risiken so umfangreich und vielschichtig, dass sie nur durch eine wesentlich stärkere Integration der Fähigkeiten und Potenziale aller administrativen Ebenen und eine konzeptionell beschriebene Überbrückung der bisherigen Trennlinien zwischen Bundes- und Länderzuständigkeiten erfüllt werden können.« (BBK 2010b, 63)

Zunächst einmal wird die Trennung »innen-außen« von der Gefahrenseite her kritisiert. Internationaler Terrorismus lasse sich weder eindeutig als Gefährdung der inneren Sicherheit noch eindeutig als äußere Aggression verstehen. Terrorismus wird als neue »asymmetrische Bedrohung« gesehen, dem mit den klassischen Mitteln der Landesverteidigung alleine nicht beizukommen ist (siehe etwa: BMVg 2006, 2).

Zudem zeige sich immer wieder, dass sich beim Schutz der Bevölkerung ähnliche organisatorische Herausforderungen stellen, egal ob es sich dabei um eine »Naturkatastrophe« oder einen Terroranschlag handelt. Zum Beispiel stelle ein sogenannter »Massenanfall von Verletzten« (BBK 2010b, 37) eine wichtige Herausforderung dar, die jeweils ähnliche katastrophenmedizinische Vorbereitungen erfordert. Schließlich liegt es geradezu in der »Natur« von katastrophischen Gefährdungen, dass diese sich nicht an Zuständigkeits- und Ländergrenzen halten: »Katastrophen kennen keine Grenzen« heißt es immer wieder in Veröffentlichungen von Katastrophenschützern. Die räumliche Realität der Gefährdung steht im schrillen Kontrast zur politischen Willkürlichkeit rechtlicher und institutioneller Gebietsaufteilungen. Sinnfällig formulierte der sächsische Umwelt-

minister Hermann Onko Aekens 2012 anlässlich des nationalen Bevölkerungsschutzkongresses: »Weil sich Hochwasser nach geographischen Gegebenheiten und nicht nach Ländergrenzen richtet, muss der Hochwasserschutz Landesgrenzen überwinden.« (Bevölkerungsschutzkongress 2012, 14)

Die entgrenzte »Natur der Gefährdung« kann dabei durchaus auch sozial oder technisch sein. Es geht jeweils um eine »Natur der Sache«, die der Logik der institutionellen Aufteilungen gegenübergestellt wird. So kann unter der Überschrift: »Kritische Infrastrukturen: Zusammenarbeit liegt in der Natur der Sache« (BBK 2007b, 25) mehr Zusammenarbeit zwischen Wirtschaft und Staat, Ländern und Kommunen gefordert werden. Mitunter lässt sich sogar etwas vom Beck'schen Pathos der »Weltrisikogesellschaft« vernehmen. So hieß es 2005, nach der Tsunamikatastrophe im Indischen Ozean, im Jahresbericht des im Jahr zuvor eingerichteten Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe:

»Ereignisse wie Sandoz 1986, Elbehochwasser 2002 und die chemische Verunreinigung des Flusses Songhua in China 2005 haben gezeigt, dass große Schadensereignisse keine Ländergrenzen – und wie die Tsunami-Katastrophe gezeigt hat – nicht mal kontinentale Grenzen kennen.« (BBK 2005b, 58)

Hierin liegt auch der Grund, warum ausgerechnet das Elbehochwasser für die Problematisierung der klassischen Aufteilung in der deutschen Sicherheitspolitik am Beginn der 2000er Jahre eine solche Bedeutung bekommen konnte. War der 11. September der paradigmatische Fall für eine asymmetrische Bedrohung, die die Trennung von Landesverteidigung und Katastrophenschutz in Frage stellt, so waren die Hochwasser des Jahres 2002 der Paradefall für eine grenzüberschreitende Gefährdung, die die Notwendigkeit ebenfalls grenzüberschreitender Zusammenarbeit im Katastrophenschutz unterstrich.

Die Trennung von Katastrophenschutz und Zivilschutz erscheint in den Problematisierungen von 11. September und Hochwasserereignissen als arbiträres institutionelles Artefakt: ein Relikt aus einer anderen Zeit mit anderer Gefahrenlage, einer anderen Welt mit Blockkonfrontation und nuklearer Bedrohung, aber ohne Europäisierung, Globalisierung und internationalen Terrorismus. Nach dem Ende der Blockkonfrontation wurde in den 1990er Jahren zunächst eine Reihe von Maßnahmen des Zivilschutzes, die retrospektiv als geradezu bizarre Relikte des Kalten Krieges erscheinen – vom Bunkerbau über die massenhafte Bevorratung von Arzneimitteln und sonstigen knappen Ressourcen bis hin zu einem weitgespannten Sire-

nennetz – zurückgebaut. Im Gefahrenbericht der Schutzkommission von 1996 wird der Rückbau folgender »Sonderstrukturen« benannt:

»die staatliche Förderung des Schutzraumbaus; de[f] Bau und die Vorhaltung von Hilfskrankenhäusern; die dauerhafte Bevorratung umfangreicher Arzneimittel sowie von Geräten und Ausstattungsgegenständen in Sanitätslagern; de[f] Bundesverband für den Selbstschutz« (siehe hierzu: Schutzkommission 1996, 6).

Stattdessen wurde verstärkt auf die lokalen »Abwehrkräfte« gegen Katastrophen vertraut. »Wesentliche Aufgaben sollen in Zukunft, aufbauend auf den bei den Ländern für die Zwecke der Gefahrenabwehr in Friedenszeiten ohnehin vorzuhaltenden Einrichtungen und Organisationen von diesen mit übernommen werden.« (Schutzkommission 1996, 6) Die meisten dieser Veränderungen werden von Sicherheitsexpert\_innen als sinnvolle Anpassungen an eine neue Sicherheitslage und nicht nur als Zugeständnis an eine schwierige Haushaltssituation verstanden. Allerdings wird auch auf die Sicherheitslücken hingewiesen, die durch den Rückbau der Zivilschutzmaßnahmen entstanden sind. Problematisiert wird vor allem die »nach dem Wegfall der flächendeckenden Sirenenwarnung entstandene ›Warnlücke« (Schutzkommission 2001, 8), also der Verlust der Möglichkeit, die Bevölkerung auch jenseits der bestehenden – stets verwundbaren – Rundfunk- und Telekommunikationskanäle vor Gefahren zu warnen. Vor allem aber wird bemängelt, dass es an Vorrichtungen fehlt, die den neu entstehenden Risiken begegnen können:

»Zivile Verteidigung und Zivilschutz in Deutschland wurden nach dem Ende des Kalten Krieges an die Erkenntnisse und Erfordernisse der frühen 90er Jahre angepasst, die u.a. davon ausgingen, dass der Zivilschutz nicht mehr in der Lage sein müsse, aus dem Stand heraus alle Kräfte zur Abwehr einer existenzbedrohenden Aggression zu mobilisieren. Nach den Anschlägen vom 11. September 2001 wurde deutlich, dass dieser Status aufgrund neuer, erst jetzt bewusst zur Kenntnis genommener Bedrohungsformen nicht mehr aufrechterhalten werden darf.« (BBK 2010b, 22)

Wenn auf mangelnden Kapazitäten im Angesicht einer veränderten Gefährdungslage hingewiesen wird, dann betrifft dies zum einen tatsächlich »neue« Bedrohungen: von ABC-Waffen in Terroristenhand über Cyberanschläge oder neue Pandemien, die sogenannten *emerging infectious diseases*.

Jenseits dessen stellen sich auch weniger spektakuläre Herausforderungen, die gleichwohl einige grundsätzliche Schwierigkeiten des Bevölkerungsschutzes in der Gegenwart beleuchten. Der sogenannte »Massenanfall von Verletzten«, kurz MANV (siehe u.a.: BBK 2006a), ist ein immer

wiederkehrendes Problem des Katastrophenschutzes, das gerade zu Beginn der Neuorientierung der Sicherheitspolitik im Zentrum der Aufmerksamkeit stand. Brisant ist dieses Thema allein wegen der moralisch-ethischen Dilemmata, die die Katastrophenmedizin generell durchziehen und die in der Praxis der »Triage« ihren deutlichsten Ausdruck bekommen.<sup>47</sup> Letztlich liegt aber auch der moralischen Schwierigkeit der Katastrophenmedizin ein organisatorisches Problem zu Grunde, das in Forderungen nach »Verbindlichkeit medizinischer Behandlungsalgorithmen beim Massenanfall sowie Sichtungskategorien/Triagestufen« (BBK 2010b, 56) nur besonders sichtbar wird: Wie kann man knappe zeitliche, personelle und materielle Ressourcen im Ernstfall möglichst effektiv einsetzen und verteilen? Bezogen auf eine mögliche Bedrohung in der Zukunft muss gefragt werden, welche Ressourcen überhaupt zur Verfügung stehen und für welche Fälle diese ausreichen. In seiner Studie zum Zivilschutz von 2002 bemerkt Wolfram Geier, dass ein MANV von »weit über 1.000 betroffenen Menschen lokal bzw. regional auftreten kann« (BBK 2010b, 38). Diese Zahl würde weit über den bisherigen »Planungsparametern für Großschadensfälle in Deutschland« liegen, die lediglich Maßzahlen von »je nach Region und Planungsvorhaben zwischen 50 und 300 Verletzten« (BBK 2010b, 38) vorsehen. Nicht nur wäre in einem solchen Fall die regionale bzw. kommunale Ebene, die für die medizinische Versorgung der Bevölkerung zuständig ist, schnell überfordert, so dass andere bzw. höhere Ebenen ins Spiel gebracht werden müssten. Vor allem müssten, um höheren »Planungsparametern« gerecht zu werden, mehr materielle Ressourcen vorgehalten werden. Es bestehe ein Mangel an

»sofort und in ausreichendem Umfang zur Verfügung stehenden Medikamenten- und medizinischen Verbrauchsgüternvorräten (Notfaldepots), geeigneten mobilen und nach vergleichbaren Kriterien gestalteten Behandlungskonzepten vor Ort (Verletzensammelstellen, Behandlungsplätze, mobilen Notfaldepots, Sichtungskriterien etc.), ausreichenden Behandlungs- und Bettenkapazitäten in Krankenhäusern, ausreichenden Spezialbehandlungsplätzen für Verbrennungspatienten, polytraumatisierte Patienten und infizierte, hoch kontagiöse Patienten, ausreichendem, sofort zur Verfügung stehendem medizinischen Fachpersonal (Ärzte, Pflegekräfte).« (BBK 2010b, 39)

---

47 »Triage« bezeichnet Strategien zur Priorisierung medizinischer Hilfeleistungen in Situationen, in denen für ein hohes Aufkommen von Verletzten zu wenig medizinisches Fachpersonal zur Verfügung steht. Zur Praxis der Triage im Humanitarismus und der Katastrophenmedizin siehe: Redfield (2008), Ellebrecht (2009).

### 2.1.3. Vom »Gießkannenprinzip« zur Risikozone

Was hier deutlich wird, ist, dass die Regierung von Katastrophen die Anhäufung und Lagerung von materiellen Ressourcen beinhaltet: von Bunkern bis zum Sirennennetz, von Medikamentendepots bis zu Krankenhausbetten. Im privaten Bereich umfasst die Lagerung Konservenbüchsen, Kerzen, Taschenlampen, Batterien, Verbandskästen etc. (für eine vollständige Auflistung, siehe: BBK 2013b). Dabei handelt es sich zumeist um Ressourcen, die im besten Fall nie zum Einsatz kommen, aber im Ernstfall das Überleben von Menschen ermöglichen sollen. Gleichzeitig sind es Ressourcen, in die investiert werden muss, die gewartet, überprüft, erneuert etc. werden müssen, die rumstehen und Platz wegnehmen. Es werden also Kapazitäten für mögliche Fälle verausgabt, die an anderen Stellen möglicherweise fehlen. Der randvoll mit Konservenbüchsen, Gaskartuschen und Wachskerzen gefüllte »Familienbunker« ist zum Aushängeschild für eine ebenso panische wie hilflose Vorbereitungskultur im Kalten Krieg geworden. Der Spott und Schauer über die »Bunkermentalität« unserer Eltern und Großeltern sollte aber nicht davon ablenken, dass in dieser Mentalität ein grundlegendes und bis heute für die Katastrophengouvernmentalität entscheidendes Organisationsprinzip enthalten ist: in der Gegenwart Kapazitäten aufbauen, um für den möglichen Ernstfall in der Zukunft gewappnet zu sein.

Dieses Organisationsprinzip der Vorratshaltung, das schon im Alten Testament in den Joseph-Geschichten zum Vorschein kommt und das möglicherweise am Ursprung der ersten Form der Staatlichkeit stand,<sup>48</sup> gerät aber spätestens unter Bedingungen »fortgeschritten liberaler« (Rose 1993) Regierungsrationalitäten unter Druck. Wie Nikolas Rose (1993, 295) argumentiert, zeichnet sich die klassische Wohlfahrtspolitik westlicher Staaten durch eine Dominanz substanzieller Rationalität aus, das heißt die Zielvorgaben der Regierenden – wie Gesundheitsversorgung der Bevölkerung – wurden durch die Allokation entsprechender Ressourcen adressiert. Auch die Expertise der Katastrophenvorsorge, die bisher besprochen wurde, folgt in diesem Sinne einer »substanziellen Rationalität«: für einen

---

48 Michael Mann (1984, 126) verweist auf die frühgeschichtliche Entstehung von Staatlichkeit aus Praktiken der Lagerhaltung: »The redistributive state seems to have been particularly appropriate, as anthropologists and archeologists argue, in the early history of societies before the exchange of commodities was possible. Different ecological niches delivered their surpluses to a central storehouse which eventually became a permanent state.«

möglichen Schadensfall wird kalkuliert, wie viele substanzielle Ressourcen (Betten, Medikamente etc.) benötigt werden, um angemessen auf diesen Vorfall vorbereitet zu sein. Dagegen zeichnet sich, so Rose, fortgeschritten liberales Regieren durch eine formale Rationalität aus.<sup>49</sup> Die Mittel zur Erreichung eines gegebenen substanziellen Ziels werden durch formale Kalkulationen auf ihre Effizienz überprüft.

»The calculative regimes of positive knowledges [...] are to be replaced by the calculative regimes of accounting and financial management. And the enclosures of expertise are to be penetrated through a range of new techniques of exercising critical scrutiny over authority – budget disciplines, accountancy and audit being three of the most salient.« (Rose 1993, 295)

Gerade Budgets sind in diesem Sinne Werkzeuge einer Kritik, die als formale Rationalität wirksam wird und versucht, die Regierungstätigkeit zu begrenzen und von Ressourcenverschwendung abzuhalten (siehe dazu auch: Collier 2005). Diese durch Budgetierung und formale Rationalität auferlegte Reflexivität steht aber häufig im scharfen Kontrast zu der immer wieder eingeforderten Risikoreflexivität, nach der auch für sehr unwahrscheinliche Gefährdungen vorzusorgen ist. Kosten-Nutzen-Kalküle für Risikovorsorgemaßnahmen mit sehr ungewisser bzw. geringer Eintrittswahrscheinlichkeit sind schwer bis gar nicht durchzuführen. Die Versicherung als Sicherheitstechnologie, die von vornherein formalen Kalkülen angepasst ist, gerät genau deshalb in Schwierigkeiten. Historisch gesehen war es das Vorrecht des Militärs – gewiss noch mehr als der Politik der Wohlfahrt –, Erwägungen der formalen Rationalität und der Haushaltsdisziplin nicht zur Kenntnis nehmen zu müssen, sondern recht ungezügelt »wirtschaften« und Ressourcen verausgaben zu können. Es ist jedoch fraglich, ob unter den gegenwärtigen fiskalischen Rahmenbedingungen und unter der Voraussetzung, dass der Schutz der Bevölkerung »ziviler« werden soll, dieser Stil der Ressourcenallokation weiter bestehen bleiben kann. Zumindest liegt hier eine Sollbruchstelle für Konflikte um die Sicherheitspolitik – und zwar eine, bei der es nicht darum geht, ob es eine reflexive Sicherheitspolitik gibt, sondern darum, welche Art der Reflexivität und welche kalkulativen Prozeduren zum Zug kommen: eine Risikoreflexivität, die Sicherheitsmaßnahmen auch dann vorsieht, wenn deren Kosten sehr hoch sind und nicht durch statistische Risikokalkulationen gerechtfertigt

---

<sup>49</sup> Die Unterscheidung von formaler und substanzieller bzw. materialer Rationalität wird bereits in Webers *Wirtschaft und Gesellschaft* (2005, 60) definitorisch eingeführt.

werden können, oder eine ökonomische Reflexivität, die gerade durch die Kontrolle von Kosten die unbegrenzten Ansprüche der Sicherheit begrenzt?

An einem konkreten Beispiel – dem Konflikt um die Vorhaltung von Krankenhausbetten im Katastrophenfall – lässt sich exemplarisch der Konflikt von substanzieller und formaler Rationalität im Katastrophenschutz zeigen. Zeitgleich zur Debatte über die Neuorientierung des Katastrophenschutzes wurde in Deutschland auch die Reform des Gesundheitswesens diskutiert. Während von Seiten der Katastrophenschutzexpert\_innen die Vorhaltung von mehr Bettkapazitäten gefordert wurde, zielten die Reformen des Gesundheitssystems darauf, dieses mithilfe ökonomischer bzw. marktorientierter kalkulativer Techniken effizienter zu machen, was wiederum von Bevölkerungsschützern kritisiert wurde:

»Mit der vom Bundesgesundheitsministerium geplanten Einführung von Abrechnungs-Komplex-Gebühren (Diagnosis Related Groups, DRG) werden ökonomische, auch gewinnorientierte Verfahrensweisen primär in der stationären, sekundär in der ambulanten Versorgung weiter an Bedeutung zunehmen. Unter diesen Umständen [...] werden personelle wie materielle medizinische Vorhaltungen zur zügigen und sicheren Bewältigung von Katastrophen so gut wie nicht mehr vorhanden sein; zumal die erforderliche (mindestens) 10% Reserve von Krankenhausbetten wird unter diesen Vorgaben nicht zur Verfügung stehen können, da die DRGs zu einer kompletten Bettenauslastung zwingen.« (Schutzkommission 2001, 81)

Diese Problematik wurde 2002 in den Empfehlungen für eine neuen Strategie des Bevölkerungsschutzes erneut aufgegriffen (BBK 2010b, 39). 2006 wurden dann bereits die faktischen Auswirkungen des neuen Abrechnungssystems im Gefahrenberichts moniert (Schutzkommission 2006, 59ff.). Dennoch findet sich im Beschluss der Innenministerkonferenz vom 6. Dezember 2002 in Bremen zur Verabschiedung der »Neuen Strategie zum Schutz der Bevölkerung in Deutschland« folgende Protokollnotiz, die dem Anliegen der Bevölkerungsschützer eine deutliche Absage erteilt:

»Einzelne Punkte des Berichts »Neue Strategie zum Schutz der Bevölkerung in Deutschland« gehen über das hinaus, was an Vorsorge leistbar ist. So ist u.a. die Reduzierung von Krankenhausbetten im Hinblick auf die Finanzierung des Gesundheitswesens alternativlos.« (BBK 2010b, 83)

Man mag darin den Sieg ökonomischer Sachzwänge über die Sicherheitsbelange der Bevölkerung sehen. Es ist aber auch ein Konflikt um differierende Kalkulations- und Rationalitätsformen. Wenn die Mittelzuweisung



für Krankenhäuser über tatsächlich anfallende Fallpauschalen ermittelt wird, dann wird es schwer, weiterhin die Vorhaltung zusätzlicher Krankenhausbetten vorsehen zu können. Die Finanzierung und Ausstattung der Krankenhäuser bezieht sich dann nämlich auf die aktuellen und das heißt durchschnittlichen bzw. (statistisch) normalen Krankenfälle, während im Katastrophenschutz für einen außergewöhnlichen, nicht normalen Fall vorgesorgt werden soll. Das Kalkül der Bevölkerungsschützer sieht also vor, substanzielle Ressourcen für einen Katastrophenfall vorzuhalten, während die Mittelzuweisung über Fallpauschalen auf ein Gesundheitssystem zielt, das formalen Ansprüchen an Effizienz und Wirtschaftlichkeit genügt. Beide Kalküle sind Ausprägungen instrumenteller Rationalität bzw. von Zweckrationalität, ermöglichen aber jeweils unterschiedliche Formen der Reflexivität und führen zu sehr unterschiedlichen Ergebnissen. Becks (1986) Unterscheidung von instrumenteller Rationalität und Reflexivität reicht an dieser Stelle nicht aus, um die Problematisierung von konkurrierenden Sicherheitsstrategien zu analysieren.

Ein ähnlicher Konflikt zwischen Haushaltsdisziplin und Katastrophenvorsorge findet sich auch in den Beschlüssen zur sogenannten Schuldenbremse, die seit 2009 in den Grundgesetzartikeln 109 und 115 geregelt wurde. In diesem Fall ist der Konflikt aus Sicht des Katastrophenschutzes jedoch scheinbar günstiger ausgegangen. Zwar verpflichtet eine Reihe von Änderungen des Grundgesetzes den Bund und die Länder zu Haushaltsdisziplin. Aber zugleich sind explizit Ausnahmen für den Fall von »Naturkatastrophen oder außergewöhnlichen Notsituationen, die sich der Kontrolle des Staates entziehen« (GG, Artikel 109, Absatz 3), vorgesehen worden, mit denen die Regelungen der Schuldenbremse temporär außer Kraft gesetzt werden können. Der Konflikt zwischen zwei unterschiedlichen Rationalitäten des Regierens wird trotzdem deutlich. Beide Prinzipien schließen sich aus, weshalb nur Ausnahmeregelungen die Vereinbarkeit gewährleisten können.

Dieser Konflikt kann gleichwohl nicht nur extern beobachtet werden, sondern wird von den Katastrophenschützer\_innen sehr bewusst wahrgenommen und – wie gesehen – auch als solcher adressiert. Das geschieht nicht nur in polemischer Absicht, sondern auch, um Kompromisse zwischen substanzieller Rationalität (verstanden als Effektivität) einerseits und formaler Rationalität (verstanden als Effizienz) andererseits schmieden zu können. Es soll »eine solide Planung mit Hilfe moderner und wirkungsvoller Planungsverfahren und Planungsinstrumenten [...] (*Effektivität*)« mit

Gesichtspunkten des »wirtschaftlichen Mittelfluss (*Effizienz*)« (BBK 2010b, 30, Hervorhebung im Original) verbunden werden. Erreicht werden soll dieses Ziel zum Beispiel durch neue Prinzipien der Ressourcenverteilung im Bevölkerungsschutz, die sich stärker als bisher an Gefahren und Verletzlichkeiten, also an Risikoanalysen und weniger an arbiträren institutionellen Aufteilungen orientieren soll. Konkret wird vorgeschlagen, »das bisherige undifferenzierte Gießkannenprinzip und den ungeeigneten Königsteiner Schlüssel« (BBK 2010b, 30) abzulösen. Der Königsteiner Schlüssel bezeichnet das Berechnungsverfahren, das darüber entscheidet, wie die Bundesländer an der Finanzierung von Gemeinschaftsaufgaben beteiligt werden (zum Beispiel an der Finanzierung von Forschungseinrichtungen wie dem Max Planck Institut). Als generisches Verteilungsprinzip, bei dem Steueraufkommen und Bevölkerungszahl einfach miteinander verrechnet werden, trägt der Königsteiner Schlüssel nicht der faktischen Gefährdungslage von bestimmten Ländern, Regionen oder Städten Rechnung. Statt des »Gießkannenprinzips« bei der Finanzierung und Verteilung von Katastrophenschutzvorrichtungen soll deshalb eine risikoangemessene Umverteilung stattfinden:

»Oberstes Planungsziel ist die Gewährleistung eines qualifizierten flächendeckenden *Grundschatzes* für die Bevölkerung Deutschlands bei größeren Schadensereignissen. Dieser Grundschatz muss aus den Potenzialen der alltäglichen Gefahrenabwehr und einem – regional durchaus variierbaren – definierten Zusatzpotential bestehen. Besonders gefährdete Regionen Deutschlands mit hoher Bevölkerungsdichte bzw. Menschenagglomerationen, politische und wirtschaftlich-industrielle Zentren sowie Zentren mit Kritischen Infrastrukturen [...] müssen über diesen Grundschatz mit einem risiko- und vulnerabilitätsorientierten *Sonder- oder Spezialschutzpotential* ausgestattet sein. Das Staatsgebiet Deutschlands wäre dabei in unterschiedliche Risikokategorien und unterschiedliche, damit korrespondierende Stufen eines schutzzielorientierten Versorgungskonzeptes einzuteilen.« (BBK 2010b, 30, Hervorhebung im Original)

Diese Vorschläge enthalten einen doppelten Angriff auf die bisherige föderale Struktur von Zivilschutz und Katastrophenhilfe. Zum einen wird die bisherige Finanzierung überregionaler Aufgaben in Frage gestellt. Zum anderen kommt der Vorschlag der Aufteilung des »Staatsgebietes« in »Risikoazonen« (BBK 2010b, 52) einer Erneuerung der politischen Landkarte der Sicherheit gleich.

Projekte zur »Neubestimmung der Grenzen des Regierens« bzw. das »re-figuring [of] the territory of government« (Rose 1996a) gelten zurecht als allgemeine Tendenz des Regierens in der Gegenwart (siehe u.a.: Castel

2000, Barry 2006, Ong 2006, Easterling 2014). Regiert wird nicht mehr der Einzugsbereich des nationalen Territoriums, das in sich ebenfalls nach territorialen Prinzipien gegliedert sein kann (wie im Fall der BRD nach Bundesländern). Stattdessen kommt es zu einer Reterritorialisierung des Regierens, etwa auf der Ebene der »communities« (Rose 1996a) einzelner, als problematisch angesehener Stadtquartiere (Castel 2000, 370–374), oder gemäß unterschiedlicher Kriterien ausgewählter Zonen (Barry 2006, Ong 2006, Easterling 2014). Häufig geht die Zersplitterung des einheitlichen nationalen Territoriums des Regierens einher mit dem Verweis auf die Grenzen und Widersprüche zentraler Regierung, mit der Aufforderung zu mehr Eigenverantwortung auf lokaler Ebene, oder auch mit der Implementierung von außerstaatlichen Räumen der Regierung. Der Vorschlag zur Einführung von abgestuften »Risikozonen« im Katastrophenschutz ist dagegen gerade keine Absage an zentrale Planung oder staatliches Regieren. Es geht lediglich darum, durch eine angemessenere zentrale Planung verfügbare Ressourcen lokal besser zu verteilen. Dabei soll der Zuschnitt der Zone der »Natur« der Risiken entsprechen und nicht mehr willkürlichen und künstlichen Grenzziehungen folgen – »Katastrophen kennen keine Grenzen«. Dabei können die entstehenden Risikozonen bzw. Zonen der Sicherheitspolitik sowohl kleiner sein als das nationale Territorium – einzelne Regionen mit bestimmtem Risikoprofil, besonders verwundbare Städte und Stadtzentren oder bedrohte Knotenpunkte der Infrastruktur – als auch die nationale Ebene deutlich überschreiten, so dass beispielsweise eine Zusammenarbeit auf EU-Ebene erforderlich würde. Idealerweise soll stets die sozio-technische (Infrastruktur) und die naturräumliche (Flussverläufe, Küsten etc.) Beschaffenheit und nicht die politisch-rechtliche Zusammengehörigkeit über das Profil einer Risikozone entscheiden. Die »Risikozone« entspricht also eher dem räumlichen Arrangement eines »historisch-natürlichen Milieus« (Foucault 2004, 42), in dem eine »Serie von Ereignissen« auf spezifische natürliche und technische Faktoren trifft, und nicht einem Territorium, das gegen äußere Feinde verteidigt werden soll. Hier liegt ein weiterer Konfliktpunkt, den die Problematisierungen des Katastrophenschutzes seit dem 11. September sichtbar gemacht haben: der Konflikt zwischen dem »künstlich-juridischen« Raum des Territoriums und dem »historisch-natürlichen« bzw. »natürlich-technischen« Raum des Risikos.

Die Problematisierungen der deutschen Sicherheitspolitik seit dem 11. September sind nicht folgenlos geblieben. Als Konsequenz aus diesen

Problematisierungen wurde eine Reihe von institutionellen Veränderungen an der bisherigen Struktur des deutschen Zivil- und Katastrophenschutzes vorgenommen. Es wäre gleichwohl verkehrt, in diesen Problematisierungen eine bloße »Programmierung« institutioneller Veränderungsprozesse zu sehen, um sodann zu fragen, ob es diesen Programmen gelungen ist, sich zu »verwirklichen«.<sup>50</sup> Problematisierungen stehen der institutionellen Wirklichkeit nicht als Maßstab gegenüber, sondern sind Teil ebendieser. Sie nehmen von einer laufenden institutionellen Praxis ihren Ausgang und intervenieren zugleich in diese hinein. Darin liegt der heuristische Mehrwert der Analyse von Problematisierungen: Sie beleuchten den »Kontext«, die »Institution«, die »Strukturen«, die sie zugleich durch ebendiese Reflektionen verändern.

So konnten in diesem Kapitel mithilfe der Analyse der Problematisierungen der deutschen Sicherheitspolitik seit dem 11. September die »strukturellen« Ausgangsbedingungen der deutschen Sicherheitspolitik beleuchtet werden – das Ende des Zivilschutzes der Nachkriegszeit in den 1990er Jahren, die neue Gefahrenlage seit Ende des Kalten Krieges, die Aufteilung von Zivilschutz und Katastrophenhilfe in Bund- und Länderangelegenheiten, der Konflikt zwischen der »Effektivität« und »Effizienz« staatlicher Planungsvorhaben, die Reformen im Gesundheitswesen, eine spezifisch deutsche Sicherheitskultur etc. – ohne objektivierend einen »Kontext« zu unterstellen, der die problematisierenden Äußerungen »immer schon« eingeht hat und weiter einhegen wird. Stattdessen wurde gezeigt, dass Problematisierungen sich nicht einfach in einem gegebenen Umfeld bewegen, sondern in einem offenen, dynamischen Kraftfeld, das durch den »Text« der Problematisierungen ko-konstituiert und transformiert werden kann.

Wenn im weiteren Verlauf der Arbeit die institutionellen Veränderungen der Regierung der Katastrophe in Deutschland nachverfolgt werden,

---

50 Beiträgen der *Governmentality Studies* wird immer wieder vorgeworfen, mit der Analyse auf einer »programmatischen Ebene« stehen zu bleiben und die »Wirklichkeit« der Regierungspraxis zu vernachlässigen. Diese Kritik übersieht aber die komplexe Perspektive der Problematisierungsanalytik. Stattdessen wird häufig ein positivistisches Verständnis von Diskurs einerseits und institutioneller Realität andererseits zugrunde gelegt. Diskurse und Institutionen oder Praktiken sind nicht zwei separate Bereiche, die durch einen Hiatus – Vorstellung und Realität, Möglichkeit und Wirklichkeit, Programm und Praxis – voneinander getrennt sind. Es sind Elemente des Wirklichen, die durch ein Set von Relationen miteinander verbunden sind. Deswegen kann es auch nicht darum gehen, einen Diskurs mit der Wirklichkeit »abzugleichen«.

geht es also nicht darum zu untersuchen, ob die hier analysierten Problematisierungen »erfolgreich« gewesen sind oder nicht. Nicht nur ist eine einfache Umsetzung oder Verwirklichung der Problematisierungen ohnehin nicht möglich, sondern würde überdies noch nicht einmal einen soziologisch sonderlich interessanten Fall darstellen. Gerade dort, wo eine Problematisierung übergangen wird, eine Forderung auf Widerstände stößt, eine Diagnose Abwehrreaktionen provoziert, liegen die interessanten Sachverhalte – die Konflikte, Friktionen und Paradoxien, die sich nicht auflösen lassen und deshalb überhaupt als »Probleme prozessier[t]« (Bröckling 2007, 21) werden müssen.

## 2.2. *Institutionalisierung*: Bevölkerungsschutz als »Neue Sicherheitsstrategie«

Neue, entgrenzte Gefährdungen – so die Problematisierung einer Vielzahl von Sicherheitsexpert\_innen – haben die Begrenzungen deutscher Sicherheits- und Katastrophenvorsorgepolitik deutlich werden lassen. Der Zivilschutz als Bundesangelegenheit bewegt sich mit seinem Mandat im »Verteidigungsfall« noch im Rahmen territorialer und souveräner Sicherheitspolitik. Die Katastrophenhilfe auf Länderebene stützt sich ebenfalls auf institutionelle Grenzen, die nicht der räumlichen Ausdehnung von Gefährdungen entsprechen und im Zweifelsfall die Zusammenarbeit erschweren. Vor diesem Hintergrund liegt es nahe, einer netzartig wuchernen Gefährdungslage mit einer Strategie »vernetzter Sicherheit«<sup>51</sup> zu begegnen, die in der jüngeren Vergangenheit von Sicherheitsexperten immer wieder proklamiert und angepriesen wurde. So klar und sinnfällig das klingen mag, so schwierig ist es, diesen neuen Zielvorstellungen innerhalb der gewachsenen institutionellen Landschaft bundesrepublikanischer Sicherheitspolitik Geltung zu verschaffen. In diesem Abschnitt möchte ich die

---

51 Der Begriff der »vernetzten Sicherheit« hat sich in der Politik internationaler Beziehungen entwickelt und bezeichnet einen Ansatz, der betont, dass zur Lösung internationaler Konflikte ein Zusammenspiel von diplomatischen, humanitären und militärischen Initiativen notwendig ist. Entsprechend tauchte der Begriff etwa im Weißbuch der Bundeswehr als neuer Ansatz deutscher Sicherheitspolitik auf (BMVg 2006, 20–22). Im Bevölkerungsschutz wird der Begriff zumeist verwendet, um die Zusammenarbeit von Bund, Ländern und Kommunen sowie die Kooperation zwischen Staat und privaten Unternehmen zu beschreiben.

institutionellen Veränderungen und strategischen Verschiebung bei der Regierung der Katastrophe untersuchen. Die Konzentration auf die institutionelle Ebene bereitet die Untersuchung der Transformationen auf der Ebene der Technologien vor, indem sie das veränderte institutionelle Selbstverständnis durch neue sicherheitspolitische Strategien und Programmatiken analysiert. Institutionen sind, auch wenn sie nicht den primären Gegenstand der hier verfolgten Sicherheitsanalyse konstituieren, entscheidende Orte, an denen neue Sicherheitstechnologien wirksam werden.

Im Folgenden werde ich zunächst die Verabschiedung der *Neuen Strategie zum Schutz der Bevölkerung in Deutschland* (BBK 2010b) in den Blick nehmen (2.2.1.). Eine entscheidende institutionelle Neuerung im Rahmen dieser Strategie besteht dabei in der Einrichtung des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK) (2.2.2.). Ein wesentliches Merkmal dieser Institution ist ihre Ereignisorientierung (2.2.3.). Schließlich werde ich die konzeptuelle Frage stellen, inwiefern diese institutionellen Veränderungen es bereits rechtfertigen, von einem neuen Sicherheitsdispositiv zu sprechen (2.2.4.).

### 2.2.1. Die »Neue Strategie zum Schutz der Bevölkerung in Deutschland«

Bereits im Jahr 2002 hat die Innenministerkonferenz (IMK) die *Neue Strategie zum Schutz der Bevölkerung in Deutschland* (BBK 2010b) verabschiedet. Sie ist darin weitgehend den zuvor in Auftrag gegebenen *Überlegungen für eine gemeinsame Rahmenkonzeption zur Weiterentwicklung des Zivilschutzes* (BBK 2010b, 18–63) gefolgt. Der Kern dieser Strategie liegt darin, dass mit dem »Bevölkerungsschutz« ein integrierter sicherheitspolitischer Ansatz vorgeschlagen wird, der sowohl Zivilschutz als auch Katastrophenhilfe umfasst.<sup>52</sup> Damit wurde ein Begriff geschaffen, der ein neues Aufgabenfeld absteckt, das der »Gefahrenlage im 21. Jahrhundert« Rechnung tragen und »Trennlinien überwinden« (BBK 2010b, 63) soll. Mit der aufgegebenen »Trennlinie« zwischen Zivilschutz und Katastrophenhilfe fällt auch eine entscheidende Grenzziehung auf der Gefahrenseite. Bevölkerungsschutz fokussiert auf alle national bedeutsamen Gefahren, die das Leben und

---

<sup>52</sup> Der Begriff »Bevölkerungsschutz« wird auch schon vor der Verabschiedung der Strategie verwendet, bekommt aber erst durch die Strategie den spezifischen Sinn, einen Ansatz darzustellen, der Zivilschutz und Katastrophenhilfe umfasst.

Überleben der Bevölkerung bedrohen. Es wird nun nicht mehr nach »äußeren« und »inneren«, aber auch nicht mehr zwischen menschengemachten und Naturgefahren unterschieden.

Gleichwohl hat bereits die IMK betont, dass an der institutionellen Struktur zur Abwehr von Gefahren und damit auch an der grundsätzlichen Trennung von äußerer und innerer Sicherheit nichts geändert werden muss und soll, weil »Bund und Länder ein funktionierendes System zur Bewältigung auch von Großschadensereignissen haben.« (BBK 2010b, 81) Dieses »System« ist nach kommunaler, Länder- und Bundesebene gegliedert und umfasst öffentliche wie private Träger.

»Deutschland hat ein gegliedertes, zum großen Teil auf Ehrenamtlichkeit und Freiwilligkeit beruhendes einheitliches Hilfesystem: In den Kommunen zur flächendeckenden Bekämpfung alltäglicher Gefahren unter Einschluss überörtlicher nachbarlicher Hilfe. Rückgrat des örtlichen Hilfeleistungssystems sind die Feuerwehren und Rettungsdienste. Die Länder ergänzen oder unterstützen die örtlichen Einheiten bei der Abwehr regionaler und überregionaler Gefahren, ggf. durch Spezialeinheiten für den überörtlichen Einsatz. Der Bund sorgt für den Schutz der Bevölkerung vor kriegerischen Gefahren und ergänzt hierzu den Katastrophenschutz der Länder bzw. leistet Amtshilfe bei der Abwehr überregionaler und die gesamte Nation betreffender Gefahren.« (BBK 2010b, 68)

Lediglich für einige wenige »außergewöhnliche Gefahren«, »die auf Grund ihrer Dimension eine Fortentwicklung der bestehenden Systeme erfordern« (BBK 2010b, 81), sind Erweiterungen und Zusätze vorgesehen. Die »neue Strategie« ist in der Folge zu einer obligatorischen Referenz in sicherheitspolitischen Debatten geworden. Eine rechtliche Verankerung haben viele der schon in der »neuen Strategie« angekündigten Maßnahmen allerdings erst relativ spät, nämlich im Jahr 2009 mit der Novellierung des Zivilschutzgesetzes erfahren (ZSKG 2009), die eine stärker koordinierende Rolle des Bundes zur Bewältigung überregionaler Gefahrenlagen vorsieht.

Tatsächlich sind die institutionellen Veränderungen, die durch die »neue Strategie« in Kraft gesetzt wurden und auf neue entgrenzte Gefahren reagieren sollen, ihrerseits begrenzt. Allerdings enthält die Strategie bereits erste Hinweise auf Verschiebungen des institutionellen Selbstverständnisses und auf Transformationen der Technologien zur Regierung der Katastrophe. Die im Begriff »Bevölkerungsschutz« zum Vorschein kommende Verpflichtung auf »Schutz« haben Nikolas Rose und Fillipa Lentzos als Indiz für eine spezifisch deutsche Ausprägung von Sicherheit interpretiert. Bevölkerungsschutz deutscher Prägung ziele darauf, »to place the popula-

tion under a kind of guardianship or patronage designed to secure each and all from the threat of harm or danger.« (Lentzos und Rose 2009, 240) Tatsächlich fällt bei einem Vergleich der »neuen Strategie« mit der *National Strategy for Homeland Security* (DHS 2007) der USA aus dem Jahr 2007 ein rhetorischer Unterschied auf. Hier wird explizit eine »Culture of Preparedness« (DHS 2007, 41) beschworen, die eben nicht die vollkommene Abwendbarkeit von Gefahren verspricht, sondern auf den Aufbau von Kapazitäten für den Umgang mit unvermeidbaren und teilweise katastrophischen Risiken fokussiert. Ähnlich orientiert sich der neu formierte Zivilschutz in Großbritannien sehr explizit am Leitbild der Resilienz (Lentzos und Rose 2009, 241–243, Anderson und Adey 2012). In der bundesdeutschen »neuen Strategie« hingegen werden derartige Begriffe und ihre deutschen Pendanten eher sparsam verwendet. Darin liegt jedoch weniger eine »typisch« deutsche Sicherheitsmentalität, sondern eine rhetorische Markierung, die darauf zielt, eine eigenständige Sicherheitsstrategie zu entwickeln, die eher europäisch als transatlantisch orientiert ist. Explizit Bezug genommen wird folglich nicht auf den US-amerikanischen Heimatschutz, sondern auf die europäische Strategie der »civil protection« (BBK 2010b, 28).

Eine genauere Auseinandersetzung mit den vorgeschlagenen Maßnahmen (statt bloß mit den verwendeten Begriffen) bestätigt diese Deutung. Hier zeigt sich, dass auch die Programmatik der »neuen Strategie« von Risiken ausgeht, die als niemals gänzlich vermeidbar angesehen werden. Schon der grundsätzliche Ansatz des Katastrophen- und Zivilschutzes geht schließlich davon aus, dass sich Katastrophen tatsächlich ereignen können. Und dieser Ansatz hat auch in Deutschland mit der Problematisierung von »unvorhersehbaren« und »undenkbaren« Gefahren seit dem 11. September an Bedeutung gewonnen. Im deutschen Bevölkerungsschutz ist die Formel, dass es keine »vollkommene Sicherheit« gibt, geradezu zum Mantra geworden.

### 2.2.2. Das BBK als »Zentralstelle und Netzknoten«

Der sichtbarste Ausdruck der neuen Sicherheitsstrategie besteht in der Gründung des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK) am 1. Mai 2004. Das BBK ist gleichwohl keine vollkommen neue Institution, sondern tritt die Nachfolge des Bundesamtes für Zivilschutz (BZS) an, das 1999 aufgelöst wurde und dessen fortbestehende



Aufgaben bis zur Gründung des BBK vom Bundesverwaltungsamt übernommen wurden. Zwar wurde durch die Einführung des BBK tatsächlich eine »optische« Aufwertung des Bevölkerungsschutzes erreicht. Gleichwohl ist das BBK kein Superministerium mit eigenen operativen Kompetenzen wie das Department of Homeland Security (DHS) in den USA, das 200.000 Mitarbeiter umfasst und über ein Budget im zweistelligen Milliardenbereich verfügt. Die personelle und finanzielle Ausstattung des BBK ist im Vergleich zu den zuvor bereits der Zivilschutzabteilung im Bundesverwaltungsamt zur Verfügung stehenden Mitteln nur unwesentlich aufgestockt worden (Bundesregierung 2003, 1f.).

Das neugegründete Bundesamt stellt also keine Institution zur Organisation einer umfassenden Notstandsregierung im Katastrophenfall dar. Als Bundesamt untersteht das BBK dem Bundesinnenministerium (BMI). Es hat folglich auch keine operativen Kompetenzen im Friedensfall. Dafür hätte die Aufteilung von Zivilschutz und Katastrophenschutz zwischen Bund und Ländern grundsätzlich aufgehoben werden müssen. Zuständig ist das BBK für die »nicht-operativen Dienstleistungen und Serviceangebote des Bundes« (Bundesregierung 2003, 4). Das heißt die Länder können auf die Dienste des BBK zurückgreifen, müssen dies aber nicht tun. Entsprechend kann das BBK nicht von sich aus Dienste übernehmen, ohne einen entsprechenden Auftrag erhalten zu haben. Wichtiger als die operative Funktion ist folglich die Koordinierungsfunktion der neuen Behörde gerade bei

»großflächigen oder bei national bedeutsamen Gefährdungslagen. In der Sache geht es im Wesentlichen darum, [...] die Hilfspotentiale des Bundes und die der Länder besser miteinander zu verzahnen sowie [...] vor allem neue Koordinierungsinstrumente für ein effizienteres Zusammenwirken des Bundes und der Länder, insbesondere verbesserte Koordinierung der Informationssysteme, zu entwickeln, damit die Gefahrenabwehr auch auf neue, außergewöhnliche Bedrohungen angemessen reagieren kann.« (Bundesregierung 2003, 4)

Die Doppelaufgabe als Dienstleister einerseits und Koordinationssstelle andererseits prägt das Selbstverständnis des BBK. Es sieht sich als *Partner im Bevölkerungsschutz* (BBK 2007b), der Unterstützungsaufgaben in Notsituation wahrnimmt. Noch ausgeprägter ist aber das Selbstverständnis als Koordinierungsstelle zwischen Bund, Ländern, Kommunen, privater Wirtschaft, europäischer und internationaler Ebene. Das BBK beschreibt sich selbst als »Knotenpunkt«, als »Netzknoten, Scharnier und Wissensdrehscheibe« (BBK 2007b, 42), als »Bühne« (BBK 2008a, 16) oder auch als

»Plattform, wo die Länder sich treffen können« (Interview 1). Als »Netz-knoten« soll es aber nicht nur die Zusammenarbeit von Bund und Ländern koordinieren, sondern darüber hinaus auch als Vermittlungsinstanz einer sehr weit ausdifferenzierten Schutzlandschaft in Deutschland agieren. Die Liste der Akteure, mit denen das BBK bei unterschiedlichen Projekten zusammenarbeitet, ist entsprechend lang und umfasst Hilfsorganisationen wie das Rote Kreuz, Ministerien und Behörden, das Robert Koch-Institut, den Wetterdienst und natürlich das Technische Hilfswerk (THW), das seinen Sitz unmittelbar neben dem BBK in Bonn hat und seit seiner Gründung als Bundesbehörde für Zivil- und Katastrophenschutz zuständig ist.<sup>53</sup> In der Selbstbeschreibung als Vermittlungsinstanz wird vor allem die Verpflichtung auf die Strategie »vernetzter Sicherheit« deutlich und das Selbstverständnis als zusätzliches Instrument in einer verzweigten Sicherheitslandschaft und nicht als übergeordnetes Superministerium mit operativen Aufgaben.

Allerdings wird an einigen Stellen auch deutlich, dass sich das BBK durchaus nicht nur als nebeneordnete, sondern als – wenn auch nicht institutionell, so doch gleichsam »epistemisch« – übergeordnete Instanz versteht. Zwar hat das BBK nicht die Führungskompetenz einer zentralstaatlichen Institution, aber es soll sich zumindest den zentralen Blick eines Staates zu eigen machen, es soll »wie ein Staat sehen« (Scott 1998).<sup>54</sup> Das BBK ist nicht nur ein Knoten im »Netzwerk der Akteure« (BBK 2010d, 12), sondern auch so etwas wie eine Aussichtsplattform, die das Netzwerk überblicken können soll. Eine »länderübergreifende Schadenslage [braucht] einfach einen Blick aus der Vogelperspektive [...], die [sieht]: Wie ist die Lage in Land A, wie wird sie sich in Land C entwickeln und wie können wir diese Länder unterstützen?« (Interview 1) Diese doppelte Selbstpositionierung als »Zentralstelle und Netzknoten« (BBK 2007b, 6) ist Ausdruck des Kompromisses zwischen der Beibehaltung des etablierten Sicherheitssystems und dem Willen, neue Kapazitäten für außergewöhnliche, großflächige Gefahrenlagen zu schaffen, die mehr Übersicht benötigen.

---

53 Diese Auflistung ist exemplarisch und soll nur einen Eindruck von der Vielzahl an Akteuren liefern, die am Bevölkerungsschutz beteiligt sind.

54 In seinem Buch *Seeing like a State* hat James C. Scott (1998) gezeigt, dass moderne Staatlichkeit stets mit der Etablierung von bestimmten Sichtbarkeitsregimen einherging, die eine zentralperspektivische Übersicht über das regierte Territorium gewährleisten sollten und dadurch zentralstaatliche Machtausübung erst ermöglichen.

So ist mit dem Gemeinsamen Melde- und Lagezentrum (GMLZ), das beim BBK in Bonn angesiedelt ist und bereits seit 2002 besteht, ein konkretes technisches Hilfsmittel geschaffen worden, das einen solchen übergeordneten Blick ermöglichen soll. Lagezentren sind gängige Einrichtungen der Sicherheitspolitik und des Katastrophenschutzes. So haben auch die Bundesländer eigene Lagezentren, die rund um die Uhr besetzt sind und zumeist beim jeweiligen Landesinnenministerium angesiedelt sind. Wie bereits sein Name signalisiert, ist das GMLZ aber eine gemeinschaftliche Einrichtung, die in der Lage sein soll, relevante Informationen über Schadenslagen zu erfassen, zu kommunizieren und Einsätze auch zwischen den einzelnen öffentlichen und privaten Hilfsorganisationen zu koordinieren und eventuell auch bei internationalen Gefahrenlagen tätig zu werden (siehe exemplarisch die Übersicht über Einsätze im Jahr 2009: BBK 2010d, 15). Zusätzlich zu dieser zentralen Koordinationsstelle ist mit dem sogenannten Deutschen Notfallvorsorge-Informationssystem (deNIS II)<sup>55</sup> eine Infrastruktur zur »dezentralen Datenintegration« (BBK 2006b, 4) geschaffen worden, die den Informationsfluss aus den Lagezentren von Bund und Ländern aufeinander abstimmen soll.

Wesentliche Aufgabe des GMLZ als auch des Informationssystems deNIS II ist die Erzeugung und Verbesserung der Sichtbarkeit von Gefahrenlagen. Bildschirme, auf denen Informationen über Gefahrenentwicklung, Schutzgüter und Hilfspotenziale flimmern, prägen das Erscheinungsbild des Lagezentrums. Zentrales Visualisierungsinstrument sind geographische Informationssysteme, die einen schnellen kartographischen Überblick über die »Lage« bzw. die Gefahrensituation vermitteln sollen. Das GMLZ und deNIS II haben eine informationelle Vernetzung der deutschen Katastrophenhilfe geschaffen, die verschiedene Akteure durch eine geteilte und zentral koordinierte Informationsinfrastruktur vernetzt. Durch das GMLZ wird das BBK als »Netzknoten« zur Koordinierung von Einsätzen verstreuter Akteure materialisiert, indem es eine »boundary infrastructure«<sup>56</sup> für die gemeinsame Arbeit etabliert.

---

55 Bei deNIS II handelt es sich um eine der Öffentlichkeit zugängliche Internetplattform mit Informationen und einer Linksammlung zum Thema Katastrophenschutz, die vor allem das Selbsthilfepotenzial der Bevölkerung stärken beziehungsweise unterstützen soll.

56 Mit ihrem Konzept der *boundary infrastructure* betonen Susan Leigh Star und Geoffrey Bowker die sozio-technischen Voraussetzungen von organisationaler und interorganisationaler Zusammenarbeit. »Any working infrastructure serves multiple commu-

Das Lagezentrum ist aber nicht nur ein Ort der Koordination der Einsätze verstreuter Akteure der Notfallbearbeitung, sondern auch ein paradigmatischer Ort der Kontrolle und Machtausübung. Beim Blick auf das Lagezentrum stellen sich Assoziationen zu Orten ein, die so etwas wie die Heterotopien der kybernetischen Kontrollprojekte darstellen. Die »dispatching center« der großen Stromnetzbetreiber (Hughes 2004, 53) können dabei als Vorläufer der »electronic control centers« (Edwards 1997, 39) betrachtet werden, die zuerst während des Kalten Kriegs etabliert wurden: die *mission control rooms* in der Raumfahrt, der *operations room* im Militär, der *situation room* des US-Präsidenten, die *war rooms* in Atomschutzbunkern der Regierungen, aber auch das Kontrollzentrum des *cybersyn*-Projekts von Stafford Beer, der in Chile während der Allende-Regierung die sozialistische Planwirtschaft von einem solchen Raum aus organisieren wollte (Pickering 2004). In diesen mit digitaler Informations- und Überwachungstechnik hochgerüsteten Räumen scheint Benthams Panopticon (Foucault 1976, 251ff.) seine kontrollgesellschaftliche Entsprechung zu finden. Das Panopticon war eine Überwachungsarchitektur, die von einer Aussichtsplattform aus die kreisförmig angeordneten Parzellen eines Gefängnisses überblicken lässt. Das Lagezentrum entspricht demgegenüber eher einer Überwachungsinfrastruktur, die informatorischen Netze über ein weites Gebiet ausstretet und an einem zentralen Ort zusammenlaufen lässt, an dem die Informationen auf Bildschirmen visualisiert werden. Das Lagezentrum ermöglicht dadurch nicht nur die Überwachung im Inneren eines »Einschließungsmilieus« (Deleuze 1993, 255), sondern weitet sie über den offenen Raum des Milieus der Sicherheit aus. Mit Latour (1987, 215ff.) lassen sich diese Räume als »centres of calculation« verstehen, die dadurch, dass sie Wissen über entfernte Ereignisse an einem Punkt zusammenlaufen lassen, das Kunststück vollbringen können, aus der Distanz zu handeln bzw. zu regieren.

Häufig haben diese Projekte, so wichtig und wirksam sie bisweilen sind, einen phantasmatischen Überhang, weil sie glauben machen wollen, mit der Kontrolle von Informationen zugleich die Welt als solche im Griff zu haben. Zudem wird häufig die Selektivität der panoptischen Überwachung übersehen. Schließlich mangelt es der zentralen Perspektive häufig an Kenntnissen über Details am Ort des Geschehens *on the ground*. Das pan-

---

nities of practice simultaneously be these within a single organization or distributed across multiple organisations.« (Bowker und Star 2000, 313)

optische Phantasma ist bisweilen auch im Bevölkerungsschutz wirksam, wenn es beispielsweise heißt:

»Welcher Krisenmanager wünscht sich nicht einen umfassenden und schnellen Lageüberblick? Ein Blick aus dem All kann oft in einem einzigen Bild eine Situation sichtbar machen. Ganz gleich ob Überflutung, Erdbeben oder technische Katastrophe, aktuelle Satellitenbilder sind ein unverzichtbares Hilfsmittel im Krisenmanagement geworden.« (BBK 2010d, 13)

Der Blick aus dem »All« darf aber nicht mit Allmacht verwechselt werden. Schließlich bringt bei Katastrophen ein noch so guter Informationsfluss nichts, wenn nicht gleichzeitig auch Ressourcen zur Verfügung stehen, die auf Grundlage der Informationen bewegt und gesteuert werden können. Man kann daher im neuen Lagezentrum und der neuen Informationsinfrastruktur des Bevölkerungsschutzes eine wichtige Ergänzung der Sicherheitsstruktur der BRD sehen, die auf die Erfahrung grenzüberschreitender Gefährdungen und gleichzeitiger Organisationsdefizite reagiert hat. Man kann darin aber auch eine Verlegenheit des integrierten bundesdeutschen Bevölkerungsschutzes sehen, den es zwar geben soll, der aber nicht mit eigenen operativen, sondern eben »nur« informatorischen Befugnissen ausgestattet ist. Der Testfall ist hier natürlich der Notfall, bei dem die Logistik der Hilfe aber mindestens so wichtig ist wie deren Informatik.

### 2.2.3. Ereignisorientierung und ambulante Gouvernamentalität

Die Einrichtung des BBK für »außergewöhnliche« Gefahren macht ein weiteres wiederkehrendes Motiv der Selbstpositionierung des Bundesamtes verständlich. Das BBK versteht sich als »ereignisorientierte Behörde« (siehe exemplarisch: BBK 2008a, 6). Sie hat insofern keinen klar festgelegten Aufgabenzuschnitt, der gemäß einer klaren internen Logik fortlaufend bearbeitet wird, sondern folgt in ihrer Arbeit dem, was »draußen« passiert. Das prägt das Professionsverständnis der Mitarbeiter\_innen, die sich gewissermaßen als Expert\_innen des Außergewöhnlichen sehen, für die Krisensituationen Routine sind.

»Anders als in – ich sage mal – standardisierten Arbeitsbereichen oder in Arbeitsbereichen der Massenverwaltung haben wir in dem Sinne keinen klassischen Arbeitsalltag, dass man rein kommt und schon ganz genau weiß, das und das mache ich heute, das und das mache ich morgen.« (Interview 1)

Die Ereignisorientierung hat dabei einen doppelten Sinn. Zunächst einmal ist das Ereignis der Gegenstand, mit dem sich das BBK befasst, und der Punkt, an dem die Behörde zum Einsatz kommt. »Sobald draußen irgendetwas [...] passiert kommen Anfragen hinein.« (Interview 1) In diesem Sinn ist die Aufgabe des BBK gewissermaßen *event management*: die Bearbeitung des »Außergewöhnlichen« verhindert einen »standardisierten« Aufgabenzuschnitt.

Für eine derartige ereignisbasierte Regierung von Risiken hat der Bund neben den erweiterten Ressourcen für Planung, Koordination und Informationsübermittlung im BBK auch einige Spezialressourcen für operative Einsätze aufgebaut, die nicht so sehr »flächendeckende Grundversorgung«, sondern vor allem »Spezialfähigkeiten zur Abwehr besonderer Risiken« ermöglichen sollen, wie es der damalige Innenminister Wolfgang Schäuble im Vorwort des Jahresberichts des BBK von 2008 formuliert hat (siehe: BBK 2009b, 4). Diese Spezialfähigkeiten umfassen beispielsweise eine Anzahl von Rettungshubschraubern, die der Bund den Ländern zur Verfügung stellt. Vor allem aber wurde vom Bund eine sogenannte medizinische und analytische Task Force gebildet. Die Einsetzung von Task Forces geht auf den Beschluss der IMK zur »neuen Strategie« zurück, der unter anderem einen »Sonderschutz mit Hilfe von Spezialkräften (Task Forces) für von Bund und Ländern gemeinsam definierte besondere Gefahren« (BBK 2010b, 70) vorsieht. In der »neuen Strategie« wurde zwischen vier Versorgungsstufen unterschieden, die jeweils unterschiedliche Schutzpotenziale erfordern. Die Task Forces sind für die vierte Versorgungsstufe – »Sonderschutz« – vorgesehen. Die Analytische Task Force (ATF) ist spezialisiert auf die Detektierung und Dekontamination chemischer, biologischer, radiologischer und nuklearer Gefahrenquellen (sogenannte CBRN-Gefahren), für die gewöhnliche Rettungsdienste weder das entsprechende know-how noch technische Hilfsmittel zur Verfügung haben. Dementsprechend wurden insgesamt sieben »operativ tätige ATF Standorte« (BBK 2009b, 37) eingerichtet, die mobil zu entsprechenden Einsatzorten gebracht werden können. Die Medizinische Task Force (MTF) folgt einem ähnlichen Prinzip. Sie soll allgemein bei Katastrophen mit vielen Verletzten eingesetzt werden. Dafür wurden insgesamt 61 Standorte eingerichtet, die so über das Bundesgebiet verteilt sind, dass eine Task Force ihren Einsatzort in mindestens 60 bis 90 Minuten erreichen kann. Mit den Task Forces sind also ereignisorientierte Kapazitäten für besonders schwere Gefahrenlagen geschaffen worden, die jenseits der »stationären« eine »ambulante« und mo-

bile Regierung der Katastrophe gewährleisten sollen. Die Mobilität der Task Forces soll eine Re-Territorialisierung der Sicherheit ermöglichen, ohne die territorialen Grundprinzipien in Frage zu stellen.

In Erwartung von Ereignissen werden aber nicht nur Ressourcen mobilisiert, das Ereignis wird im Bevölkerungsschutz auch für die eigene Arbeit rekrutiert. Das katastrophale Ereignis ist nicht nur das, was zum Arbeiten anhält und bearbeitet werden muss, sondern auch das, was bemüht wird, um die eigene Arbeit zu legitimieren, für Gefahren zu sensibilisieren und neue Verwundbarkeiten zu erkennen und zu analysieren. Die Mobilisierung von Ereignissen zu Zwecken der Legitimierung der eigenen Arbeit unterscheidet sich nicht sonderlich von den Argumentationen, die bereits zur Einrichtung des BBK geführt haben. Auch in Stellungnahmen des BBK wird die eigene Existenz immer wieder mit den Ereignissen vom 11. September 2001 und der Flutkatastrophe im Jahr 2002 gerechtfertigt. Für die alltägliche Arbeit des BBK ist die sensibilisierende Wirkung von Gefahrenereignissen aber sicher wichtiger als die legitimierende. Denn die Mitarbeiter\_innen des BBK müssen Wege finden, andere Akteure für ihre Belange zu »interessieren«,<sup>57</sup> weil viele Angebote, Vorgaben und Anregungen des BBK letztlich auf freiwilliger Zusammenarbeit basieren. Ereignisse, die Aufmerksamkeit für bestimmte Gefährdungen erzeugen, kommen in dieser Situation gelegen, um andere Akteure für die Zusammenarbeit mit dem BBK zu rekrutieren.

»Wenn wir erzählt hätten, 2001/2002 von einem großflächigen Stromausfall, bei dem 250.000 Menschen in Deutschland über Tage betroffen werden, hätte das keinen interessiert. Erst mit dem Münsterland<sup>58</sup> ist es tatsächlich auch öffentlichkeitswirksam in den Fokus der Energieunternehmen gekommen, und seitdem läuft ein Projekt nach dem anderen zum Thema Stromausfall.« (Interview 1)

---

57 Der Begriff des *interessement* wird hier aus der Akteur-Netzwerk-Theorie übernommen. Dort ist das *interessement* ein Vorgang während der Knüpfung eines Akteur-Netzwerks. Michel Callon (2006b, 151–156) weist auf die Etymologie des Begriffs des Interesses hin, der vom lateinischen *inter-esse*, dazwischen-Sein stammt. In diesem Sinne wird nicht davon ausgegangen, dass Akteure mit formierten Interessen bestehen, sondern dass sich die Interessen und das Verhältnis der Akteure in einem Vermittlungsprozess erst einspielen.

58 Gemeint ist der Stromausfall im Münsterland im Jahre 2005, bei dem in der Folge schwerer Schneefälle einige Strommasten umgeknickt waren und einen Stromausfall ausgelöst haben, von dem circa 250.000 Menschen bis zu vier Tage lang betroffen waren.

Schließlich haben Ereignisse aber auch einen heuristischen Wert, insofern sie Aufschluss über Verwundbarkeiten und über mögliche bisher nicht wahrgenommene Gefährdungen geben. Ereignisse haben damit einen potenziellen Wahrheitswert. Sie regen zu einer Analyse an, die neue Erkenntnisse generieren kann:

»Im Jahr 2005 [...] brach in der Schweiz das gesamte Eisenbahnnetz zusammen. [...] Wir haben damals eben überlegt – ereignisorientierte Behörde – kann das auch bei uns passieren? Wir haben uns mit Experten unterhalten und sind zu dem Schluss gekommen: Nein, das kann hier nicht passieren. Die Schweiz hat ein Rundnetz in der Energieversorgung ihrer Bahnen. Deutschland hat mehrere kleine Netze, die nach und nach abschaltbar sind.« (Interview 1)

Dabei muss es sich bei den Ereignissen keineswegs um »reale« Vorfälle handeln. Schließlich geht es ja gerade darum, sich auf das zukünftig-mögliche Ereignis vorzubereiten. Dafür kann es nachgerade schädlich sein, sich nur auf das Gewesene, also nur auf vergangene Ereignisse zu stützen und nicht auch mögliche zukünftige in Rechnung zu stellen. Hier hat die »Übung« ihren Platz in der neuen Architektur des deutschen Bevölkerungsschutzes. Übungen gehören zum Standardrepertoire des Notfallmanagements: vom Probefeueralarm in der Grundschule bis hin zum großangelegten militärischen Planspiel. Entsprechend ist nicht die Übung selbst eine Innovation der neuen Bevölkerungsschutzstrategie, sondern lediglich ihre Größenordnung.<sup>59</sup> Die sogenannte Länderübergreifende Krisenmanagement-Übung/Exercise (LÜKEX) ist ein bereits in der »neuen Strategie« vorgesehenes Instrument, um die Zusammenarbeit im Bevölkerungsschutz auf Bundesebene »länderübergreifend« zu verbessern. Mit Akteuren aus dem gesamten Bundesgebiet wird der Umgang mit ausgewählten Szenarien geübt, welche eine länderübergreifende Kooperation notwendig machen würden. Die Übungen finden in zweijährigem Rhythmus mit einer langen Vor- und Nachbereitungszeit statt. Die Übungsleitung liegt stets beim BBK. Bei den tatsächlichen Übungsereignissen sind dann Akteure von Bund und Ländern, von Unternehmen (insbesondere Betreiber Kritischer Infrastrukturen), aber auch Medienvertreter\_innen beteiligt, so dass an einer Übung bis zu 3.000 Personen teilnehmen können (siehe: BBK 2013a). Geübt wird jeweils der Umgang mit einem bestimmten Szenario, das möglichst komplex sein soll und daher häufig mehrere Gefährdungen

---

59 Für eine ausführlichere Darstellung der Übung in Vergangenheit und Gegenwart des Bevölkerungsschutzes siehe: Ellebrecht, Jenki und Kaufmann (2013).



umfasst. So wurde bereits der Umgang mit folgenden Bedrohungen geübt: »winterliche Extremwetterlagen mit großflächigem Stromausfall« (2004), »terroristische Anschläge im Zusammenhang mit der Fußball-WM 2006« (2005), »weltweite Influenza-Pandemie« (2007), »terroristische Bedrohung mit konventionellen Sprengstoffen, chemischen und radioaktiven Tatmitteln (»schmutzige Bombe«)« (2009/10), »Cyberattacke« (2011) und »[a]ußergewöhnliche biologische Bedrohungslage« (2013).

In solchen Übungen kommen die unterschiedlichen Anforderungen des »ereignisorientierten« Bevölkerungsschutzes idealtypisch zusammen. Die Übung erfüllt sowohl die inter-essierende als auch die heuristische Funktion des Ereignisses. Die Übung bringt Akteure zu einem konkreten Projekt zusammen und ermöglicht somit die Einübung von Zusammenarbeit im Ernstfall.

Die anschließende Auswertung soll etwaige Schwachstellen der Krisenbewältigung offenlegen und so neue Einsichten und Erkenntnisse für den Bevölkerungsschutz mobilisieren. In dieser Hinsicht ist die Übung eine wesentliche Form des »enactment based knowledge« (Collier 2008).

»Jede Übung wird sorgfältig ausgewertet. Die gewonnenen Erkenntnisse und die daraus abgeleiteten Handlungsempfehlungen werden in einem Auswertungsbericht zusammengefasst. Er ist Ausgangspunkt für die weitere Optimierung der Strukturen und Verfahren des strategischen Krisenmanagements.« (BBK 2013a)

Die Übung ist damit nicht nur ein Test, sondern bereits selbst eine Vorbereitungsmaßnahme, weil durch ihren Vollzug praktisches Wissen generiert wird, das für einen tatsächlichen Einsatz bereitstehen soll. Umgekehrt ist jeder tatsächliche »Ernstfall« zugleich auch eine Übung für die kommende Katastrophe. In der Übung kommen Techniken des Wissens und der Macht, epistemische und praktische Verfahren zusammen. Test und praktischer Vollzug der Macht vermischen sich hier und werden tendenziell ununterscheidbar.

#### 2.2.4. »Vernetzte Sicherheit« oder Sicherheitsdispositiv?

Die institutionellen Innovationen, die auf die »neue Gefahrenlage« seit dem 11. September reagieren, sind vielfältig und zugleich limitiert. Der bundesweite Bevölkerungsschutz im BBK ist eine Koordinierungsstelle mit begrenzten Interventionsmöglichkeiten. Das neue institutionelle Arrangement, das unter dem Namen Bevölkerungsschutz firmiert, ist ein

Kompromiss. Ein Kompromiss, der seinerseits aufschlussreich ist, insofern er auf das Kraft- und Konfliktfeld deutscher Sicherheitspolitik verweist, aus dem er hervorgegangen ist. Schon die Ausgangsüberlegungen, die zur neuen Bevölkerungsschutzstrategie führten, legten eine Kompromisslösung nahe, insofern eine Fortentwicklung des bestehenden Schutzsystems ohne dessen grundsätzliche Infragestellung vorgesehen wurde. Die Einflussfaktoren dafür waren vielfältig und reichen von der formalen Organisation des deutschen Katastrophenföderalismus bis zu sehr grundsätzlichen und teils historisch begründeten Vorbehalten gegenüber Kompetenzakkumulation in der deutschen Sicherheitspolitik. Es wird viel Wert darauf gelegt, dass die mit der »neuen Strategie« zusammenhängenden Maßnahmen keine Überschreitung von Zuständigkeitsgrenzen implizieren. So bemerkte der damalige Parlamentarische Staatssekretär beim Bundesminister des Inneren Fritz Rudolf Körper in der Aussprache zur Einrichtung des BBK im Bundestag:

»In diesem Zusammenhang möchte ich eines unmissverständlich klarstellen und damit auch einer gelegentlich geäußerten Befürchtung eindeutig entgegenreten: Mit der Einrichtung des neuen Bundesamtes maßt sich der Bund keine neuen Zuständigkeiten an.« (Bundestag 2004, 8450)

Diese institutionellen Begrenzungen implizieren aber nicht, dass es keine grundlegende Transformation deutscher Sicherheitspolitik auf der Ebene des Sicherheitsdispositivs gegeben hat. Die Entwicklung eines Dispositivs hängt nämlich nicht nur mit institutionellen Veränderungen zusammen, sondern vor allem mit Transformationen von Problematisierungen und Technologien der Macht. Auch wenn Institutionen ein wichtiger Indikator für Veränderungen sein können, geht die Regierung in und durch ein Dispositiv doch immer über Institutionen hinaus. Der Ort des Dispositivs ist nicht die Institution, sondern eine umfassendere Topologie des Regierens, in der institutionelle Grenzziehungen nur relative Markierungen und keine substanziellen Gebietsunterteilungen darstellen, in der Limitierungen der Regierungstätigkeit in einer Institution zur Intensivierung des Regierens in einer anderen beitragen können. Ein Dispositiv ist keine einheitliche Institution oder ein abgrenzbarer Staatsapparat, sondern ein

»entschieden heterogenes Ensemble, das Diskurse, Institutionen, architekturelle Einrichtungen, reglementierende Entscheidungen, Gesetze, administrative Maßnahmen, wissenschaftliche Aussagen, philosophische, moralische oder philanthropische Lehrsätze, kurz: Gesagtes ebenso wie Ungesagtes umfaßt.« (Foucault 1978, 119f.)

Eine Reihe der hier genannten Elemente wurde bereits zusammengetragen: Debatten und Expert\_innengutachten über neue Gefahrenlagen, eine ganze Armada von Hilfsorganisationen, alten und neuen Institutionen, das gemeinsame Melde- und Lagezentrum, ritualisierte Katastrophenschutzübungen, das Gesetz für Zivilschutz und Katastrophenhilfe, die Formulierung einer neuen Sicherheitsstrategie etc. Aber ein Dispositiv besteht nicht nur aus Elementen, sondern aus der Art der Beziehung zwischen diesen Elementen.

»Das Dispositiv selbst ist das Netz, das zwischen diesen Elementen geknüpft werden kann. Zweitens möchte ich in dem Dispositiv gerade die Natur der Verbindung deutlich machen, die zwischen diesen heterogenen Elementen sich herstellen kann. [...] [Es gibt] zwischen diesen Elementen [...] ein Spiel von Positionswechseln und Funktionsveränderungen« (Foucault 1978, 120)

Es sind also nicht die Elemente, nicht die Relata, sondern es sind die Relationen, die ein Dispositiv ausmachen. Auch solche institutionellen oder technischen Elemente des Sicherheitsdispositivs, die schon lange vor dem 11. September bestanden – wie etwa die Hilfsorganisationen oder der Katastrophenschutz der Länder –, können demnach durch »Positionswechsel« Teil eines neuen Sicherheitsdispositivs werden.

»Positionswechsel« finden aber nicht nur beim Übergang von einem Dispositiv zum anderen statt, sondern auch innerhalb eines Dispositivs. Das liegt daran, dass Dispositive immer auf Probleme reagieren und damit gegenüber einem Außen geöffnet bleiben, das sie ver- und bearbeiten.

»Drittens verstehe ich unter Dispositiv eine Art von – sagen wir – Formation, deren Hauptfunktion zu einem gegebenen historischen Zeitpunkt darin bestand hat, auf einen Notstand (urgence) zu antworten.« (Foucault 1978, 120)

Es ist offensichtlich, dass ein Dispositiv zur Regierung der Katastrophe auf Notstände und Notfälle reagieren muss. Wichtig festzuhalten bleibt aber, dass es nicht nur zu einem gegebenen historischen Zeitpunkt auf einen Notstand reagiert hat, sondern fortwährend »ereignisorientiert« ist und sein soll. Katastrophen sind die Situationen, in denen sich die Elemente des Sicherheitsdispositivs versammeln, in denen aber immer auch Positionswechsel stattfinden und neue Elemente des Dispositivs hinzutreten. Die Katastrophenschutzübungen sollen ja gerade diesen Fall simulieren und inszenieren, indem sie immer wieder neue Akteure hinzuziehen, die jedes Mal, von Fall zu Fall verschieden, in einer anderen Konstellation zueinander stehen, was Bruce Braun als »ad hoc assemblage« (Braun 2014, 51)

bezeichnet hat, um den situationellen Charakter der Regierung der Katastrophe zu betonen. Die Ereignislogik ist ein Grund für die Offenheit und die Dynamik des Feldes des Bevölkerungsschutzes in Deutschland. Verbindungen, Verantwortlichkeiten und Verfahrensweisen sind zwischen den Akteuren nicht immer eindeutig und klar verteilt und können aufgrund der »Unvorhersehbarkeit« der Gefährdungen auch nicht ein für alle Mal festgelegt werden. Vieles bleibt im Vagen – und zwar durchaus mit System: Nur eine offene Organisationsstruktur kann angemessen auf die Offenheit der Zukunft reagieren. Es gelingt gerade nicht, dem Ereignis wie einer sorgfältig angeordneten Schlachtreihe gegenüberzutreten, wie dies der Begriff des Dispositivs in seiner militärischen Bedeutung nahelegen würde. Eher schwirrt das Gefüge um das Ereignis wie Motten um eine Lichtquelle, nur um sich wieder zurückzuziehen, wenn die Ereignisse ihre Strahlkraft verloren haben.

Wenn man also die Betonung der Strategie »vernetzter Sicherheit« und das Selbstverständnis des BBK als Netzknoten bedenkt, liegt die Analyse des Bevölkerungsschutzes als heterogenes Sicherheitsgefüge nah – allzu nah vielleicht. Schließlich war eine Rekonstruktion der Regierung als »System [...] von mehreren Gouvernamentalitäten« (Foucault 2006, 115), die gerade nicht den vorgegebenen institutionellen Unterteilungen, Aufteilungen und Abteilungen in Ressorts und rechtlich zugeschriebenen Zuständigkeiten folgt, für Foucault ein heuristisches Instrument, um bei einer Analyse des Staates nicht den Blick und das Raster des Staates selbst einfach nur zu reproduzieren.<sup>60</sup> Lässt sich dieser heuristische Vorzug der Dispositivanalyse, die das kapillare Netzwerk der Macht statt der zentralen Machtinstitution untersuchen soll, heute noch erhalten, wenn sich die Institution selbst als Netzwerk oder »Netzknoten« oder sogar als »Kräftedispositiv« (TAB 2011, 43) versteht, wie es in Bezug auf das deutsche Krisenmanagementsystem in einem Bericht des Büros für Technikfolgenabschätzung im Deutschen Bundestag heißt? Dieser Vorzug kann nicht nur erhalten, sondern sogar noch gestärkt werden, wenn es gelingt, die Heuristik des Dispositivs schärfer zu konturieren und nicht nur einer zentralistischen Staatslogik einen dezentrale Netzlogik gegenüber zu stellen. Wie Marieke de Goede (2012) überzeugend argumentiert, ist das

---

60 Auf diese Gefahr hat auch Pierre Bourdieu (1998, 93) hingewiesen: »Beim Nachdenken über den Staat läuft man immer Gefahr, staatliches Denken zu übernehmen, staatlich produzierte und gestützte Denkkategorien auf den Staat anzuwenden und also eine ganz grundlegende Wahrheit über den Staat zu verkennen.«

Netzwerk in jüngerer Zeit zu einer Sicherheitsrationalität ersten Ranges aufgestiegen: sowohl als Figur der Gefährdung wie auch als bevorzugte Strategie im Umgang mit Risiken. Es kommt also darauf an, das »Netzwerk« anders zu verstehen und zu kartieren.

Eine solche andere Kartierung beginnt beim eigenen Blick auf das Netzwerk. Zwar versteht sich das BBK nicht als übergeordnete Steuerungsinstanz des Bevölkerungsschutzes, aber gleichwohl doch als zentraler Aussichtspunkt. Während der Bevölkerungsschutz also einen panoptischen Blick für sich reklamiert, aus dem das Netzwerk der Sicherheit wie aus einer »Vogelperspektive« überblickt werden kann, ist die Perspektive der Dispositivanalyse »oligoptisch«. Der Begriff der »Oligoptik« wurde von Bruno Latour (2007, 302–316) geprägt und der »panoptischen« Perspektive gegenübergestellt. Latour betont den stets partialen und situierten Charakter oligoaptischer Perspektiven, die nicht zentral auf die Phänomene schauen, sondern gleichsam lateral den Windungen und Wendungen eines Netzwerks folgen. Diese veränderte Epistemologie ist die notwendige Folge einer grundsätzlich anderen Ontologie der Sicherheitsnetze. Ein Sicherheitsnetz für Strateg\_innen »vernetzter Sicherheit« hat eine ganz andere Seinsweise als ein Sicherheitsdispositiv im Foucault'schen Sinne. So müssen Strateg\_innen vernetzter Sicherheit davon ausgehen, dass ihre Netze tatsächlich existieren, dass sie entweder bereits vorliegen oder noch geschaffen werden können und müssen. Das Dispositiv dagegen ist keine Gegebenheit und bezeichnet auch nicht die Möglichkeit einer zukünftigen, also zu realisierenden Gegebenheit. Es ist die Bedingung der Möglichkeit für das Gegebene, das Wirkliche, die Positivitäten. Das Dispositiv ist nicht das Positive, sondern das Streuungs- oder Verteilungsprinzip des Positiven. Das Dispositiv ist nicht dasselbe wie die Elemente des Wirklichen. Es konstituiert sich durch die Relationen. Schließlich ergibt sich die Funktion eines Elements innerhalb des Dispositivs erst durch dessen Stellung bzw. Position. Die Bevölkerungsschützer\_innen müssen dagegen notwendigerweise von bereits formierten Funktionen und Identitäten der einzelnen Elemente in ihren Netzen ausgehen, um sie gezielt für ihre Interessen rekrutieren zu können. Die Schwierigkeit der Dispositivanalyse besteht also darin, einerseits den Wegen, Verknüpfungen und Verbindungen zu folgen, die die Akteure selbst herstellen, aber andererseits die Sichtweise der Akteure auf die so geschlungenen Netze nicht einfach zu übernehmen.

Dieser komplexen Herausforderung möchte ich mich im weiteren Verlauf dieses Kapitels stellen, indem ich versuche, das operative Dispositiv

zur Regierung der Katastrophe in Deutschland auch jenseits der Institutionen des Bevölkerungsschutzes zu beleuchten. Als entscheidende Indikatoren für die Herausbildung eines Dispositivs gelten mir dabei vor allem die Machttechnologien, die Institutionen eine neue Ausrichtung, ein neues Prinzip des Handelns und des Wissens geben. Im Anschluss an die in Kapitel 1.3 skizzierten Dimensionen werde ich im Folgenden deutlich machen, wie die zeitliche, räumliche und normative Ordnung des Sicherheitsdispositivs sowie die Herausbildung eines neuen distinkten Objekts der Sicherheit in jüngeren sicherheitspolitischen Debatten und Entwicklungen in der Bundesrepublik verortet werden können.

### 2.3. *Zeit und Raum*: Die Analyse katastrophischer Risiken

Technologien zur Antizipation katastrophischer Risiken bilden einen wesentlichen Bestandteil der Regierung der Katastrophe. Risikoanalysen sollen helfen, mögliche Risiken zu detektieren, zu antizipieren, in ihrer Gefährlichkeit und Wahrscheinlichkeit ein- und abzuschätzen, um sich so auf sie vorbereiten zu können. Damit etablieren sie einen spezifischen Problembereich, auf den sich das Dispositiv richtet. Gleichzeitig wird dieser Problem- und Aufgabenbereich nicht nur von den epistemischen Techniken der Risikoanalyse etabliert. Er muss zudem institutionellen Anforderungen, in diesem Fall der Struktur des Bevölkerungsschutzes in Deutschland, gehorchen. Die Risikoerfassung muss also versuchen, einerseits der Komplexität der Risikolagen gerecht zu werden, andererseits Risikoklassifikationen vorzunehmen, die den Bedürfnissen der mit den Risiken befassten Regierungsapparate genügen. Die Risikoanalytik kann als »Rationalisierung des Zufalls« (Foucault 2004, 93) begriffen werden. Durch die Prävention der Vorhersagbarkeit von Gefahren trägt sie dazu bei, die Verunsicherung über die mögliche bedrohliche Zukunft zu mildern. Sie verwandelt das erschreckend Udenkbare in etwas Gedachtes und Erwartetes und beruhigt damit nicht nur die Affekte von besorgten Subjekten, sondern ermöglicht vor allem eine gezielte institutionelle Bearbeitung der Risiken – und zwar nicht zuletzt dadurch, dass sie sie auf die Bedürfnisse der Institution zugeschnitten klassifiziert und aufbereitet.

Mit Blick auf die Entwicklung einer Risikoanalytik im deutschen Bevölkerungsschutz lässt sich Becks (2008, 61f.) Behauptung, die katastrophischen

schen Risiken der Weltrisikogesellschaft seien prinzipiell nicht wissenschaftlich prognostizierbar, nur schwer aufrechterhalten. In Debatten der *Critical Security Studies* wurde bereits auf eine Vielzahl von Katastrophenantizipationstechniken hingewiesen (Collier 2008, Ericson und Doyle 2004, de Goede 2008). Während ein Großteil der Forschung dabei vor allem auf die zeitliche Dimension von Risikoanalysen eingeht – auf die Abschätzung der Wahrscheinlichkeit und die Inszenierung und Simulation zukünftiger Gefährdungen (siehe u.a.: Grusin 2004, de Goede 2008, Opitz und Tellmann 2015b) –, möchte ich hier auch die räumliche Dimension der Risikoanalytik durch Verwundbarkeitskartierungen betonen, die – bis auf wenige Ausnahmen (Collier und Lakoff 2008) – noch unterbelichtet ist. Dadurch kann ich zeigen, inwiefern sich die Etablierung neuer Sicherheitstechnologien im Bevölkerungsschutz auf die zeitliche und räumliche Achse des Sicherheitsdispositivs auswirkt. In der Risikoanalytik wird ein zeitlicher Horizont der möglichen und verheerenden, wenngleich nicht sehr wahrscheinlichen und dadurch schwer prognostizierbaren Gefährdung aufgespannt. Es wird aber auch ein Sicherheitsraum abgesteckt, in den diese bedrohliche und gleichwohl ungewisse Zukunft eingeschrieben wird.

Wenn ich die Risikoanalysen im Bevölkerungsschutz hier als Techniken zur »Rationalisierung des Zufalls« beschreibe, möchte ich damit nicht suggerieren, dass die Sicherheitsapparate »alles im Griff« haben, wie es bisweilen in den *Governmentality Studies* mit der Rede von »governable catastrophes« (O'Malley 2003) nahegelegt wird. Vielmehr möchte ich gerade auf die mannigfaltigen Schwierigkeiten und Wissenslücken im Rahmen der Risikoanalyse hinweisen und zeigen, inwiefern Analytiken zur Abschätzung katastrophischer Risiken nicht nur Wissenstechniken, sondern ebenso Nicht-Wissenstechniken darstellen, die es erlauben sollen, mit Nicht-Wissen umzugehen und es strategisch zu mobilisieren. Dazu werde ich zuerst darauf eingehen, wie die für den Bevölkerungsschutz relevante Gefahrengruppe zusammengestellt und abgegrenzt wird (2.3.1.). Anschließend werde ich auf die mittlerweile standardisierte Risikoanalytik im Bevölkerungsschutz eingehen und dabei zeigen, wie hier Zeit und Nicht-Wissen verhandelt werden (2.3.2.). Schließlich werde ich Strategien zur Kartierung von Risiken und Verwundbarkeiten daraufhin untersuchen, wie sie einen operativen Sicherheitsraum versammeln (2.3.3.).

### 2.3.1. Die »bundesrelevante Katastrophe«

Seit der Einführung der *Neuen Strategie zum Schutz der Bevölkerung* durch die Innenministerkonferenz im Jahr 2002 ist in Deutschland eine Vielzahl von Berichten erstellt worden, die einen genaueren Überblick über die Gefährdungslage aus Sicht des bundesweiten Bevölkerungsschutzes liefern sollen (Schutzkommission 2006, 2011, ZöS 2008, BBK 2005c, 2006c). Seit 2010 wird der Bundestag zudem jährlich von der Bundesregierung über die *Risikoanalyse im Bevölkerungsschutz* unterrichtet (Bundestag 2010, 2011a, 2012, 2013). Die Berichte unterscheiden sich in einzelnen Einschätzungen, im Ton und in der Dringlichkeit, aber auch hinsichtlich ihrer Wirk- und Bedeutsamkeit innerhalb der institutionalisierten deutschen Sicherheitslandschaft. Sie ähneln sich gleichwohl darin, dass sie alle ein Gefährdungsprofil entwerfen, das einer bestimmten Art von Ereignissen Gestalt gibt und damit den Gegenstand und Problembereich des »ereignisorientierten« Bevölkerungsschutzes konstituiert und konturiert.

Die institutionelle Struktur des Bevölkerungsschutzes, die dem Bund neue Zuständigkeiten für besonders schwerwiegende Gefahren zugetragen hat, macht sich in den Berichten bemerkbar, insofern diese sich vornehmlich mit »Gefahrenarten mit potenzieller Bundesrelevanz« beschäftigen (Bundestag 2011a, 2). Neben der Schwere eines Ereignisses ist es vor allem seine räumliche Ausbreitung und seine zeitliche Dauer, die Bundesrelevanz erzeugt. So ist etwa ein »langdauernder und großräumiger Stromausfall« (TAB 2011) ein bundesrelevantes Ereignis, das auf dem Radar von Risikoanalysen auf Bundesebene erscheint. Gerade die räumliche Ausbreitung über die Grenzen eines Bundeslandes hinaus ist ein sinnfälliger Hinweis auf Bundesrelevanz. Denn »wenn das Ereignis ein so großes räumliches Ausmaß hat, dass mehrere Bundesländer gleichzeitig betroffen sind, [müssen] umfangreiche Ressourcen des Bundes zum Einsatz kommen« (Bundestag 2011a, 2). Auch dann, wenn die Kosten die Grenzen der Länderhaushalte überschreiten und vor allem, wenn deren operationelle Hilfskapazitäten nicht ausreichen, liegt ein bundesrelevantes Gefahrenereignis vor.

Dieser Fall könnte insbesondere dann eintreten, wenn es zu gravierenden und außergewöhnlichen Risiken kommt, also bei Gefahren, die sehr selten und damit kaum abschätzbar oder prognostizierbar, aber zugleich schwerwiegend sind und die ein hohes Schadensausmaß haben – sogenannte *low probability, high impact risks*. In Anlehnung an Nassim Talebs (2007) Buch über außergewöhnliche Gefahren auf Finanzmärkten wird im



Hinblick auf diese Risiken auch von »schwarzen Schwänen« (Bundestag 2011a, 5) gesprochen.

Schließlich sind die als bundesrelevant antizipierten Gefährdungsergebnisse komplex. Sie können sich miteinander verketten und/oder unvorhergesehene Folgen haben. Es handelt sich um »komplexe Risiken«: »Gefahren können sowohl einzeln als auch in Kombination und Wechselwirkung miteinander auftreten, wodurch besonders gravierende Schäden verursacht werden können.« (Bundestag 2011a, 5) So nimmt ein Typus von Gefahrenereignis Gestalt an, der großflächig und langanhaltend ist, eine geringe Eintrittswahrscheinlichkeit und ein großes Schadensausmaß hat und zudem komplexe Verlaufsmuster aufweist, insofern im Zuge seines Eintretens unvorhergesehene Folgeschäden und Kaskadeneffekte auftreten können. In der Klassifikation einer bundesrelevanten Katastrophensituation vermischen sich also epistemische Definitionen des Risikos über Eintrittswahrscheinlichkeit und Komplexität von Katastrophenszenarien mit institutionellen Fakten wie Ländergrenzen und Budgets. Die bundesrelevante Katastrophe ist ein epistemisch-institutioneller Hybrid, mit dessen Hilfe die deutschen Sicherheitsapparate sowohl eine äußere Bedrohungslage als auch ihre eigene interne Struktur reflektieren.

Ereignisse, die eines oder mehrere dieser drei Kriterien aufweisen und häufig in den Berichten erwähnt werden, sind unter anderem: Terroranschläge, Hochwasser, Kriege, Stromausfälle, Epidemien und Pandemien, Stürme, Unfälle in der Chemieindustrie, Sabotage und Cyberangriffe. Häufig werden diese Ereignisse nochmals in unterschiedliche Kategorien wie Naturkatastrophen, von Menschen gemachte (anthropogene) oder technische (technogene) Katastrophen unterteilt (siehe etwa: BBK 2010a, 11). Aber auch, wenn sich diese Gefahren in Bezug auf ihre Ursache bzw. ihre Urheber unterscheiden mögen, sind es die gleichförmigen Effekte der Gefahren, die im Fokus der Reaktion auf die Ereignisse stehen. Hier zeigt sich bereits die Orientierung an der Sicherheitstechnologie der Vorbereitung. Angestrebt wird nämlich weniger ein vorbeugendes als vielmehr ein vorbereitendes Risikohandeln, das »unabhängig von der Ursache des jeweiligen Ereignisses« (Bundestag 2011a, 3) möglich ist.

Für eine an der Sicherheitstechnologie der Vorbereitung orientierte Risikoanalyse sind die Ereignisse ebenso singular, im Sinne von außergewöhnlich, überraschend, unvorhersehbar und einschneidend, wie generisch, das heißt in Bezug auf Folgen und notwendige Reaktionsformen gleichförmig. Niemand weiß, wann ein bestimmtes Ereignis eintreten wird,

aber alle sind überzeugt, dass stets mit dem Eintreffen eines bestimmten Typus von Ereignis, der generischen Katastrophe, gerechnet werden muss. Die Akteure des vorbereitenden Katastrophenschutzes gehen geradezu von der Notwendigkeit des Kontingenten aus. Der generische Charakter der Risikoanalysen auf Bundesebene wird dabei eigens betont. »Die Risikoanalysen des Bundes erfolgen in abstrahierter, generischer Art und Weise.« (Bundestag 2012, 3) Eine zu große Genauigkeit würde nämlich die Flexibilität der Reaktionen auf den tatsächlichen und immer bis zu einem gewissen Grad »undenkbaren« Ereignisfall mindern und die Vorbereitungsmaßnahmen möglicherweise auf einen zu spezifischen Fall einschränken. Das Generische der Risikoanalyse ist damit aus Sicht der Bevölkerungsschützer der Offenheit und Unvorhersehbarkeit der Zukunft und der faktischen Unbestimmtheit der Bedrohung geschuldet.

Programmatisch wird diese generische Sicht auf Gefahren als »All-Gefahren Ansatz« (BMI 2009, 7) gefasst, der mittlerweile in einer Reihe von Ländern die Gefahrenwahrnehmung im Katastrophen- und Zivilschutz charakterisiert. Ebenso salopp wie treffend hat Brian Massumi argumentiert, die Gruppierung von Ereignissen im »All-Hazards Approach« erfolge entlang der »polar extremes of war and weather« (Massumi 2009, 154). Es ist wenig verwunderlich, dass der All-Gefahren-Ansatz immer wieder kritisiert wurde. Schließlich haftet einem solchen generischen Ansatz der Makel jeder Art der Abstraktion an: Es wird vom Einzelfall ebenso abstrahiert wie von den Ursachen, und auch die spezifische Betroffenheit der Bevölkerung droht in den Hintergrund zu geraten. Allerdings ist eine solche Abstraktion der Spezifik von Risiken in Technologien der Sicherheit keineswegs ungewöhnlich oder neu. So fand im Zuge der historischen Entwicklung des »Vorsorgestaates« (Ewald 1993) bereits eine alles andere als selbstverständliche Versammlung von Risiken unterschiedlichster Art statt. Ereignisse wie Arbeitsunfälle, Alter, Arbeitslosigkeit, Krankheit und Armut wurden unter die generische Kategorie des »sozialen Risikos« gebracht (Ewald 1993, 414). Auch diese Sachverhalte ähnelten sich nicht in ihren Ursachen, sondern nur darin, dass sie statistisch normal und über die Bevölkerung verteilt auftraten. Das erlaubte wiederum die Anwendung der »generischen« Technik der Sozialversicherung. Der Zuschnitt und die Kategorisierung von Risiken gehorchen historisch wie aktuell den Anforderungen der jeweiligen Sicherheitstechnologien: also etwa der Versicherung oder der Vorbereitung auf den Katastrophenfall. Durch die Konstitution ihrer Fälle und Aufgabenbereiche erschaffen Sicherheitsdispositive biswei-

len seltsam anmutende Ordnungssysteme: das 65. Lebensjahr und der Verlust von Gliedmaßen an einer Kreissäge sind sich plötzlich ähnlich, genauso wie ein Wintersturm und eine terroristische Cyberattacke. Ohne das Erstaunen über solche seltsamen Ereignisversammlungen mildern zu wollen, scheint aus der Perspektive der Analytik des Sicherheitsdispositivs die Bündelung zu einheitlichen Kategorien – sei es das soziale Risiko oder die generische Katastrophe – nicht weiter erstaunlich. Bemerkenswert sind vielmehr die historischen Unterschiede zwischen den beiden Serien von Ereignissen. Im Fall der sozialen Sicherheit handelt es sich um genuin »soziale« und statistisch normale Ereignisse, während die Ereignisse der Regierung der Katastrophe vorläufig nur negativ als nicht-normale und post-soziale Ereignisse charakterisiert sein sollen. Aber welche Wahrnehmungsmuster und Handlungsschemata produziert diese Allgemeinheit, die dem All-Gefahren-Ansatz zugrunde liegt? Wie produziert das Dispositiv die Art der Gefahren, auf die es sich richtet?

### 2.3.2. Die Risiko-Matrix: Zeit und Nichtwissen in der Risikoanalyse

Ein wesentlicher Effekt und zugleich ein zentrales Instrument eines Dispositivs besteht in der Etablierung eines Rasters der Intelligibilität,<sup>61</sup> also einer Matrix, die auftretende Probleme registrieren und einordnen kann. Im Idealfall liefert dieses Raster die »Problemstellungen fix und fertig, quasi verwaltungstechnisch in Schubladen sortiert« (Deleuze 1989, 26). Eintretende oder drohende katastrophische Ereignisse müssen dann nicht jedes Mal als Bruch mit den Selbstverständlichkeiten und Erwartungen verstanden werden, sondern können gemeinsam mit anderen, analogen Fällen serialisiert und erwartbar gemacht werden. Erst das erlaubt es dem Sicherheitsdispositiv, nicht mehr nur situativ auf einen »Notstand« zu antworten, sondern sich systematisch darauf vorzubereiten.

Die Entwicklung einer einheitlichen »Methode für die Risikoanalyse im Bevölkerungsschutz« (BBK 2010a) – ein Projekt, das sowohl in der »neuen Strategie« wie im Zivilschutzgesetz-Paragraph 18, Absatz 1 vorgesehen wurde (ZSKG 2009) – soll dementsprechend eine »vergleichende Gegenüberstellung verschiedener Risiken durch unterschiedliche Gefahren in

---

61 »[G]rid of intelligibility« ist ein Übersetzungsvorschlag für »Dispositiv« von Dreyfus und Rabinow (1983, 121). Zwar stellt diese Übersetzung zu sehr auf die Wissensdimension des Dispositivs ab. Sie lässt aber auch deutlich werden, dass jedem Dispositiv systematische Wahrnehmungs- und Bewertungsschemata eigen sind.

einer Risiko-Matrix« etablieren und damit zur »Grundlage für alle Planungen im Bevölkerungsschutz« (BBK 2010a, 21) werden. Ziel ist es, die Zusammenarbeit zwischen den unterschiedlichen Behörden zu verbessern, indem verbindliche Vorgaben für die Bewertung und Erfassung von Risiken katastrophischen Ausmaßes bereitgestellt werden. Denn:

»Sollen die Ergebnisse der Risikoanalyse verschiedener Gebietskörperschaften auf gleicher Ebene verglichen oder auf der übergeordneten Ebene zusammengefasst werden, bedarf es der Verwendung von einheitlichen Szenarien, Schadensparametern und Indikatoren zu deren Operationalisierung sowie von einheitlichen Schwellenwerten für die Klassifizierung der Eintrittswahrscheinlichkeit und des Schadensausmaßes.« (BBK 2010a, 51)

Vertreter\_innen der *Science and Technology Studies* haben in jüngerer Zeit vermehrt auf die Rolle von Standards in der Wissenschaft (Edwards 2010) und in großen Organisationen (Lampland und Star 2009) hingewiesen. Standards ermöglichen erst eine Koordinierung und die Kooperation unterschiedlicher Akteure, ohne immer wieder von neuem komplexe Kommunikations- und Übersetzungsarbeit leisten zu müssen. Standardisierung sowohl von materiellen, technischen Elementen – wie »connection standards« (Barry 2006, 239) in großtechnischen Systemen – als auch von Methoden und Routinen erlaubt so erst die Etablierung großer Infrastrukturen: globale wissenschaftliche Arbeitszusammenhänge, große Organisationen bzw. Organisationsnetzwerke, technische Infrastrukturnetze. Diese Einsichten lassen sich auch für die Analytik der Sicherheit fruchtbar machen. Sicherheitsdispositive sind auf Normierungen und Standardisierungen angewiesen, um verstreute Akteure und Elemente zu koordinieren. So ist gerade die Strategie »vernetzter Sicherheit« auf die Etablierung von Standards angewiesen, um die Anschlussfähigkeit und Kompatibilität der unterschiedlichen Elemente der Sicherheitsinfrastruktur zu gewährleisten. Generisch ist die Gefährdung also auch in dem Sinne, dass sie in einer einheitlichen Matrix erfasst und nach einem vorgegebenen Protokoll abgearbeitet wird.<sup>62</sup> Die einheitliche Methode soll genutzt werden, um »auf allen administrativen Ebenen Risikoanalysen im jeweiligen Zuständigkeitsbereich« (Bundestag 2010, 6) durchzuführen. Wiederum zeigt sich, dass die Risikoanalyse immer auch institutionellen Ansprüchen,

---

<sup>62</sup> Die Risikoanalyse ist nicht nur für Deutschland standardisiert, sondern orientiert sich auch an international praktizierten Risikoanalysetechniken, wie sie etwa im ISO-Standard 31000 für Risikomanagement beschrieben werden (Bundestag 2010, 15).

in diesem Fall der Zusammenarbeit unterschiedlicher Regierungsapparate, genügen muss.

Im Mittelpunkt der Methode der Risikoanalyse steht die »Risiko-Matrix«, ein Raster mit 25 Feldern, die sich aus den beiden Koordinatenachsen »Schadenausmaß« und »Eintrittswahrscheinlichkeit« ergeben. Die farbige Matrix ist das sichtbare Endprodukt der Risikoanalyse. Um zu diesem Ergebnis zu gelangen, wird zum einen das Schadensmaß anhand von fünf Parametern – Mensch, Umwelt, Wirtschaft, Versorgung, immateriell – abgeschätzt. Zum anderen wird die Eintrittswahrscheinlichkeit auf einer Skala von eins (sehr unwahrscheinlich) bis fünf (sehr wahrscheinlich) festgehalten. Dabei wird davon ausgegangen, dass sich ein mit dem Wert »eins« versehenes Ereignis alle 100.000 Jahre wiederholt, während ein als »fünf« klassifiziertes Ereignis durchschnittlich alle zehn Jahre vorkommt (siehe: BBK 2010a, 27). Die Kombination von Eintrittswahrscheinlichkeit und Schadensmaß gibt dann das Risiko eines bestimmten Szenarios an. Es wird also der schon lange gültigen Praxis gefolgt, einen Risikowert durch Multiplikation von Schadensmaß und Eintrittswahrscheinlichkeit zu generieren.

Bei der Risikomatrix steht offensichtlich deren politische Kommunizierbarkeit und Übersichtlichkeit, also Komplexitätsreduktion im Vordergrund. Die Matrix wird als Gitternetz mit 25 Kästchen dargestellt, die von grün (geringes Risiko) über gelb (mittelgroßes Risiko) bis rot (hohes Risiko) reichen. Einzelne Szenarien können dann in Form eines schwarzen Pünktchens in die Matrix eingetragen werden und bieten so eine handliche Übersicht über mögliche Gefahren. Die Matrix zeigt buchstäblich an, ob Alarmstufe rot besteht oder noch »alles im grünen Bereich« ist und erlaubt so einen intuitiven Zugang zum »Udenkbaren«. Dadurch kann sie

»als Grundlage für Entscheidungen im Risikomanagement, Notfallplanung und Krisenmanagement dienen. Hierzu zählen Priorisierung von Maßnahmen zur Minimierung von Risiken und zur Vorbereitung auf unvermeidliche Ereignisse und deren Bewältigung.« (BBK 2010a, 40)

Diese Übersichtlichkeit hat gleichwohl einen Preis. Die Komplexitätsreduktion bei der »Visualisierung des Risikos« (BBK 2010a, 39) muss in Kauf genommen werden. Zugleich wird aber auch die Objektivität und Wissenschaftlichkeit der Risikoanalyse behauptet und dem politischen Prozess von Entscheidungsfindung und öffentlicher Kommunikation gegenübergestellt.

»[W]ährend die Analyse der Risiken ein nüchterner, wissenschaftlicher Prozess ist, werden die Risikobewertung und die daraus folgende Abwägung und Auswahl von risikomindernden Maßnahmen in erheblichem Umfang von politischen und gesellschaftlichen Aspekten mitbestimmt.« (BBK 2010a, 46)

Dieses Beharren auf »Wissenschaftlichkeit« ist keineswegs selbstverständlich. Nicht nur gibt es bisweilen bereits eine deutliche Abkehr von derartigen Wissenschaftlichkeitsansprüchen in vergleichbaren Projekten zur Risikoanalyse.<sup>63</sup> Zudem ist fraglich, ob es für die Vorbereitung auf Katastrophen überhaupt einer quantitativen Bemessung von Risiken bedarf.<sup>64</sup> Vor allem wimmelt es in den Berichten zur Risikoanalyse von Verweisen auf mangelnde Informationen und unüberwindbare Ungewissheiten.

»Bei der Durchführung der Risikoanalyse ist das richtige Maß an wissenschaftlichem Anspruch und pragmatischem Vorgehen zu finden. Immer dann, wenn keine oder zu wenige statistische/wissenschaftliche Erkenntnisse vorliegen, müssen Wissensdefizite (zunächst) durch begründete Annahmen und Schätzungen kompensiert werden können.« (BBK 2010a, 17)

Die mangelnde Datenlage wird sowohl einem Mangel an Kooperationen zwischen den Behörden und Unternehmen zugeschrieben als auch den in der »Natur der Sache« liegenden Faktoren: sehr unwahrscheinliche Ereignisse kommen einfach zu selten vor, um signifikante statistische Schlüsse zuzulassen. Trotzdem werden die Ergebnisse der Risikoanalyse quantitativ präsentiert. »Grundsätzlich hat sich Deutschland entschieden, einen mit der EU vergleichbaren Weg bei der Erarbeitung von Risikoanalysen zu gehen und auf einer *wissenschaftlich abgesicherten Basis eher quantitativ* ausgerichtete Risikoanalysen durchzuführen.« (Bundestag 2011a, 2, Hervorhebung A.F.)

Noch deutlicher wird die Schwierigkeit, auf dem Pfad reiner Wissenschaft zu bleiben, bei der Berechnung des Schadensausmaßes. Denn zum einen müssen hier inkommensurable Schadensgrößen – Schaden in Personenzahlen in der Kategorie »Mensch«, Schaden in Hektar in der Kategorie »Umwelt«, Schaden in Euro in der Kategorie »Wirtschaft«, Dauer der Un-

---

63 So grenzt die OECD in einem Bericht zur Methodik der Risikoanalyse diese von »exakter Wissenschaft im klassischen Sinne« (zitiert nach: Bundestag 2012, 9) ab.

64 Am Fall des sogenannten *Business Continuity Management* werde ich in Kapitel 4 auf eine betriebliche Katastrophenvorbereitungstechnik eingehen, die nicht nur auf quantitative Risikobemessung, sondern sogar auf die Verwendung spezifischer Katastrophenszenarien bei ihrer Risikoanalyse verzichtet.

terbrechung in der Kategorie »Versorgung«, und ohnehin nicht quantifizierbare »Ausmaße« in der Kategorie »immateriell« (siehe: BBK 2010a, 37f.) – auf einen Nenner gebracht werden. Jeweils werden *score*-Werte von eins bis fünf zugeordnet und am Ende miteinander verrechnet. Zudem muss unter Umständen ein sogenannter »Aversionsfaktor« berücksichtigt werden, bei dem der »Schadenswert, der deutlicher berücksichtigt werden soll [...] mehrfach gezählt« (BBK 2010a, 37) wird. Spätestens hier muss also nicht nur geschätzt werden, weil *Zahlen* fehlen, sondern zudem auch eine Wertung vorgenommen werden, weil einheitliche *Skalen* zur Messung von Katastrophenschäden fehlen.

Das Festhalten an quantitativen Risikoabschätzungen hängt sicher mit dem tief verwurzelten Vertrauen in Zahlen zusammen. Mit quantitativen Größen wird Objektivität und Unparteilichkeit assoziiert: zentrale Werte nicht nur in der modernen Wissenschaft, sondern auch in modernen Bürokratien.<sup>65</sup> Aber wie kann der Anspruch der Wissenschaftlichkeit aufrechterhalten werden, obwohl an allen Ecken und Enden Defizite und Wissenslücken sichtbar werden? Eine Strategie, auf diese Schwierigkeiten zu reagieren, besteht in einer geradezu ostentativen Reflexivität im Umgang mit Nicht-Wissen, die den Wissenschaftlichkeitsanspruch der Risikoanalyse stabilisieren soll. Das Nicht-Wissen wird gerade nicht bestritten, sondern explizit betont, um Wissenschaftlichkeit unter Beweis zu stellen. Als Kronzeuge für diesen Umgang mit Nicht-Wissen wird ein Wissenschaftler herangezogen – nämlich der Soziologe Niklas Luhmann –, um zu betonen, dass Nicht-Wissen ein legitimes und notwendiges Problem der Wissenschaft in Risikolagen darstellt.

»Luhmann (2003, S. 166) [Zitation im Original, A.F.] stellt nüchtern fest, dass das Typische an Risikolagen ist, dass man nicht genug weiß. Die Annahmen, die bei Entscheidungen und Analysen zugrunde gelegt werden, können selbstverständlich in Zweifel gezogen werden und überholen sich möglicherweise im Laufe der Zeit. Letztlich geht es darum, zu entscheiden, mit welchem Maß an Ungewissheit die (Mehrheit der) Gesellschaft zurzeit leben kann.« (BBK 2010a, 47)

---

65 In seiner wichtigen Studie *Trust in Numbers* hat der Wissenschaftshistoriker Theodore Porter (1996) die Bedeutung von Zahlen und quantitativen Berechnung in Wissenschaft und öffentlichem Leben untersucht. Dabei argumentiert er, dass die Verwendung quantitativer Verfahren immer auch eine politische Funktion hat. Ihnen wird zugetraut, Objektivität und Unparteilichkeit zu gewährleisten und damit politische Streitigkeiten stillzustellen.

Hier wird eine Wissenschaftlichkeit vertreten, von der seriöserweise gerade keine vollständige Gewissheit erwartet werden kann, die gerade deshalb wissenschaftlich ist und bleibt, weil sie weiß, was sie nicht weiß.

Man könnte nun aus soziologischer Perspektive die Selektivität und vielleicht sogar die schlichte Fehlinterpretation von Luhmanns Risikosoziologie seitens der Risikoanalytiker\_innen des Bevölkerungsschutzes monieren. Schließlich geht es Luhmanns Risikotheorie nicht nur darum, dass »man nicht genug weiß«, um angemessene probabilistische Risikoberechnungen zu erstellen. Schließlich ist der systemtheoretische Risikobegriff gerade nicht probabilistisch, sondern possibilistisch (Baecker 1991, 121). Kein Wahrscheinlichkeitskalkül kann jemals das »Risiko« einer Situation angemessen erfassen, weil die Entscheidungen, die in Bezug auf diese scheinbar gesicherte Wissensgrundlage getroffen werden, das, wovon sie ausgingen, zugunsten von »offenen Situationen, die von der Entscheidung erst geschaffen werden«, ersetzen (Baecker 1991, 119). Nicht-Wissen ergibt sich damit geradezu notwendig durch die Performativität von Beobachtungen und Entscheidungen in Risikolagen (siehe dazu auch: Esposito 2013). Es geht mir hier aber nicht um die richtige Luhmanninterpretation oder die Betonung der Performativität von Risikoabschätzungen, sondern vielmehr um die Performativität von Luhmanns Theorie im Feld des Katastrophenschutzes, also um die Effekte des Bezugs auf eine soziologische Theorie durch Akteure des Regierens. Die Stellungnahmen im analysierten Material sind schließlich keine rein wissenschaftlichen Äußerungen, sondern mit institutionellen Weihen ausgestattete Berichte, die auf konkrete politische Effekte abzielen. Insofern ist im hier auffindbaren Umgang mit Nicht-Wissen auch eine Strategie des Regierens zu sehen, die »vorsorglich« die Mängel der Vorsorge betont und so ihre eigenen Begrenzungen zugleich reflektiert als auch legitimiert. Unsicherheiten sollen auch deshalb offen kommuniziert werden, um überzogene Erwartungen an komplette Schadensvermeidung zurückzuweisen. Der Bevölkerung wird nämlich eine »Vollkasko-Mentalität« (siehe: Bundestag 2012, 47) unterstellt, die verhindern, dass sie sich stärker auf ihre Selbsthilfefähigkeit besinnt, anstatt sich auf umfassenden Schutz durch den Staat zu verlassen.

»Dabei muss allen Beteiligten deutlich gemacht werden, welche Erkenntnisse bewiesen und belastbar sind und welche noch auf Annahmen beruhen. Hierdurch kann dargelegt werden, dass ein vollständiger Schutz der Bevölkerung durch staatliche Einrichtungen nicht gewährleistet werden kann und dass eine entsprechende ereignisabhängige Vorbereitung der Bürger (Auf- und Ausbau der Selbsthilfefähigkeiten) gefordert und gefördert wird.« (BBK 2010a, 46f.)



Obwohl in den Berichten zur Risikoanalytik im Bevölkerungsschutz kein allwissender und allmächtiger Vorsorgestaat auftritt, kommt doch eine spezifische Artikulation von staatlicher Sicherheitsrationalität zum Tragen. So sorgt sich der Staat neben unvorhersehbaren Risiken auch vor den vorhersehbaren Reaktionen der Öffentlichkeit bei Eintreten dieser Risiken, die von ihm mehr fordern, als er zu leisten im Stande oder willens ist. Letztlich bleibt die Bevölkerung dabei das Objekt des »Bevölkerungsschutzes«. Sie wird weniger als aktiver Akteur einbezogen, sondern vor allem als Störfaktor behandelt, der nicht nur mangelhaft auf Katastrophen vorbereitet ist, sondern das Risikomanagement zudem auch noch mit überzogenen Erwartungen belastet.<sup>66</sup>

Eine zweite Strategie des Umgangs mit Nicht-Wissen und Ungewissheit besteht in der Betonung des Prozesscharakters der Risikoanalyse.

»Abschließend wird hier noch einmal betont, dass die Risikoanalyse als Prozess zu verstehen ist. Erkenntnisse, verwendete Daten und methodisches Vorgehen sind regelmäßig zu überprüfen, zu aktualisieren und ggf. an neue Rahmenbedingungen anzupassen. Bei Bedarf sind zusätzliche Szenarien für neu identifizierte Gefahren zu entwickeln. Erkenntnislücken können durch gezielte Forschungsvorhaben geschlossen werden. Auf diese Weise kann eine realistische Einschätzung der aktuellen Risiken erfolgen, die je nach bereits ergriffenen Maßnahmen im Rahmen des Risiko- und Krisenmanagements zu einer Verbesserung der Risikolandschaft führt.« (Bundestag 2013, 16)

Nicht-Wissen ist hier nicht nur ein dunkler Fleck auf der Landkarte des Risikos, der durch zusätzliche Forschungen beseitigt werden kann. Denn die »Risikolandschaft« ist nicht statisch und ein für alle Mal zu kartieren, sondern permanent in Bewegung, so dass es auch keine abschließende Risikoanalyse geben kann. Die Betonung des Prozesscharakters der Risikoanalyse verweist bereits auf das sicherheitspolitische Leitmotiv der Resilienz. Sicherheit verstanden als Resilienz wird hier nicht als Zustand, sondern eher als Anpassungsprozess an eine sich ständig verändernde Ökologie der Gefahr bzw. eine »Risikolandschaft« verstanden. Deshalb

---

<sup>66</sup> Mit dem Katastrophensoziologen Wolf Dombrowsky (2013) kann man darin einen generellen Zug deutscher Sicherheitsbehörden erkennen. Aus einer Haltung heraus, in der sich Fürsorglichkeit und Paternalismus mischen, wird von einer mangelnden Selbsthilfefähigkeit der Bevölkerung ausgegangen, die im Katastrophenfall bestenfalls passives Schutzobjekt ist und im schlimmsten Fall selbst eine Quelle der Bedrohung. Gleichwohl zeigt die explizite Problematisierung der »Vollkasko-Mentalität« der Bevölkerung auch, dass es den Sicherheitsbehörden gegenwärtig um eine verstärkte Aktivierung der Selbsthilfekapazitäten der Bevölkerung geht.

geht auch das Intelligibilitätsraster des Bevölkerungsschutzes nicht in der je aktuellen »Risiko-Matrix« mit ihren grünen, gelben und roten Kästchen auf. Es ähnelt eher dem Paradigma einer Normalwissenschaft im Sinne Kuhns (1976). Die Matrix ist kein enzyklopädisches Verzeichnis aller möglichen Risiken, sondern ein Set von Regeln, Methoden, Standards und Verfahrensvorgaben, die von unterschiedlichen Akteuren geteilt werden und die es so erlauben, immer neue paradigmatische Problemlagen zu identifizieren. Der Mehrwert dieser Matrix liegt weniger darin, die Welt komplett im Griff zu haben, sondern eine Grundlage zu liefern, die auch und gerade im Falle von Fehlschlägen konkrete Handlungsmöglichkeiten und Handlungsbedarfe ausweist. Immer wieder blitzt in den Berichten zur Risikoanalyse die Hoffnung auf, dass die perfekte Risikoanalyse möglich ist, wenn nur noch mehr Akteure beteiligt, noch mehr Daten gewonnen und noch mehr Erfahrungen mit Verwundbarkeiten gesammelt worden sind. Diese Hoffnung ist gewiss ein Phantasma – aber ein wirksames. Es transformiert Nicht-Wissen, den Mangel an Daten und Informationen, in eine Herausforderung, eine Aufgabe und ein Projekt. Dieser »Wille zum Wissen« ähnelt einem unersättlichen Begehren, dass durch Versagung nur noch mehr angetrieben wird.

Die kritische Soziologie hat sich, sowohl wenn sie als Ideologiekritik als auch wenn sie als Sozialkonstruktivismus auftritt, auf die Entlarvung von objektivistischen Geltungsansprüchen als Scheinwahrheiten spezialisiert.<sup>67</sup> Allerdings scheinen diese etablierten kritischen Werkzeuge im Fall der Risikoanalyse unbrauchbar zu sein. Schließlich wird hier gerade nicht die Objektivität eines Verfahrens behauptet, die man durch einen Blick in die *black box* der Wissensproduktion ihres konstruierten Charakters überführen könnte. Vielmehr ist ein *savoir ignore*<sup>68</sup> zum *savoir faire* des Staates geworden. In jüngeren Debatten um strategisches Nicht-Wissen (McGoey 2012,

---

67 Vor allem Bruno Latour (2004) hat diesen Fokus der kritischen Soziologie und des Sozialkonstruktivismus kritisiert. Dabei sind viele seiner Vorwürfe gegen die kritische Tradition gewiss überzogen und polemisch. Allerdings macht er überzeugend darauf aufmerksam, dass das Verhältnis von Wissen(schaft) und Politik nicht mehr einfach gemäß eines technokratischen Modells gedacht werden kann. An die Stelle der technokratischen »rules of experts« (Mitchell 2002) sind gerade in Situationen der Ungewissheit Konflikte um Wissens- und Wahrheitsansprüche getreten (zu derartigen Konflikten siehe auch: Callon, Lascoumes und Barthe 2009).

68 Die Formel des *savoir ignore* geht auf Condorcet zurück, der damit sowohl die philosophische Methode beschreibt als auch den angemessenen Einsatz von Wissen in der Politik (siehe dazu: Rothschild 2001, 178).

Marquardt 2016) wird zurecht betont, dass auch dieses Wissen um Nicht-Wissen Machteffekte zeitigen kann und deshalb ebenso kritisch betrachtet werden muss wie klassische Wahrheitsansprüche. So können auch in den beiden soeben aufgezeigten Umgangsweisen mit Nicht-Wissen spezifische Machtstrategien gesehen werden. Einerseits wird das Nicht-Wissen gegenüber der Bevölkerung und der Öffentlichkeit als Grund für die begrenzte Reichweite staatlicher Schutzpolitik ins Feld geführt. Andererseits dient die Identifizierung von Wissenslücken dazu, die Netzwerke des Sicherheitsdispositivs auszuweiten: mehr Akteure sollen einbezogen, mehr Daten gesammelt, mehr Problembereiche aufgedeckt werden.

### 2.3.3. Verwundbarkeitskartierung. Der Raum der Katastrophe

Neben der zeitlichen Unbestimmtheit stellt die Verräumlichung von Katastrophen – die Reichweite eines Hochwassers, die Ausbreitung toxischer Gase, die Übertragungswege einer Ansteckungskrankheit – eine zentrale Herausforderung für Risikoanalysen im Bevölkerungsschutz dar. Schließlich ist diese Verräumlichung eine weitere Quelle von Unbestimmtheit. Denn neben der Eintrittswahrscheinlichkeit muss auch die »Flächenausdehnung des Ereignisses« (Allianz 2008, 31) abgeschätzt werden. Erst diese Räumlichkeit entscheidet darüber, ob ein Ereignis das Zeug zur Katastrophe hat oder sich leicht einhegen lässt. Gleichzeitig bietet der Raum aber auch so etwas wie einen Anker im Meer der Unbestimmtheit. Schließlich können Schutzgüter und Hilfspotenziale in Bezug auf mögliche Gefahren verortet und kartiert werden, um so bereits in der Gegenwart Einsicht in bestehende Verwundbarkeiten und Schutzpotenziale zu erhalten. Deswegen spielt die räumliche Kartierung von Verwundbarkeiten eine mindestens ebenso große Rolle für den Bevölkerungsschutz wie die Abschätzung der Wahrscheinlichkeit zukünftiger Katastrophen.

Techniken zur Verwundbarkeitskartierung bzw. zum »vulnerability mapping« kamen in den USA schon während des Kalten Krieges zum Einsatz, um das räumliche Ausmaß eines Atombombenangriffs zu ermes- sen (Collier und Lakoff 2008, 17f.). Über die geographische Karte eines Bezugsgebietes wurde eine Folie gelegt, die die räumliche Ausbreitung der Zerstörungskraft der Bombe angeben sollte. So konnte zwar nicht die Frage nach dem Wann und Ob eines solchen Angriffs beantwortet werden, die mögliche Katastrophe konnte aber zumindest verortet werden, was dabei helfen sollte, die lokalen Verwundbarkeiten zu reduzieren und so

bereits in der Gegenwart ein Interventionsfeld für Sicherheitstechnologien zu eröffnen.

Diese räumliche Dimensionierung ist auch ein fester Bestandteil der Risikoanalyse im deutschen Bevölkerungsschutz. Insofern ist die Risikoanalyse nicht nur eine zeitlich orientierte Matrix, sondern auch ein »Gefährdungskataster« (Dombrowsky, Horenczuk und Streitz 2003, 38); ein »Kataster der Staat, Gesellschaft und Wirtschaft in Deutschland potenziell bedrohenden Gefahren« (BBK 2010a, 11). Insbesondere mit Hilfe von computergestützten Anwendungen geographischer Informationssysteme (GIS) werden Verfahren möglich, die an Techniken des *vulnerability mapping* anschließen. Die Möglichkeiten moderner Informationstechnologie haben die zunächst noch analogen Verwundbarkeitskartierungstechniken in Bezug auf Analysefähigkeit und Darstellungstechnik dabei deutlich erweitert.

Die Erstellung eines »Gefährdungskatasters« mithilfe von GIS wurde schon vor der Verabschiedung der »neuen Strategie« im Projekt der Erstellung eines Schutzdatenatlas geplant (siehe: Dombrowsky, Horenczuk und Streitz 2003), hat aber durch die Entwicklungen seit dem 11. September neue Brisanz und vermehrte Anwendungen insbesondere im Notfallinformationssystem deNIS II bekommen. Stets besteht das Ziel dieser Projekte in der Sammlung, Zusammenführung und analytischen Auswertung raumbezogener Informationen zur Erlangung eines möglichst umfassenden Lagebildes, das sowohl als Grundlage der Vorbereitungsplanung dienen als auch als Koordinierungshilfe im Ernstfall zum Einsatz kommen kann.

Dafür werden unterschiedliche Karten eines ausgewählten Gebiets mit je spezifischen Informationen über Schutzobjekte, natürliche Gegebenheiten, Gefährdungen und Schutzpotenziale erstellt, um diese dann so miteinander in Bezug zu bringen, dass Verwundbarkeiten sichtbar werden. Die Autor\_innen des *Schutzdatenatlas* unterscheiden dabei zwischen Grundlegenkarten, Gefahrenkarten und Karten über das Schutzpotenzial (siehe: Dombrowsky, Horenczuk und Streitz 2003, 7f.), die jeweils mit unterschiedlichen durch GIS ermöglichten Analyseinstrumenten traktiert werden können. »Grundlegenkarten« dienen dem Katastrophenschutz vor allem zur Kartierung von Schutzgütern und »natürlichen« geographischen Gegebenheiten auf dem entsprechenden Einzugsgebiet. Dafür erfasst werden

»Informationen zur allgemeinen Geographie des Bezugsgebietes (z.B. Klima, Landnutzung) sowie zur Bevölkerung (z.B. Einwohnerzahl und -dichte), Umwelt

(z.B. geschützte Gebiete), Wirtschaft (z.B. Wirtschaftsleistung, Gewerbesteuererinnahmen) und Versorgung (Hauptinfrastrukturen der Strom- und Trinkwasserversorgung).« (BBK 2010a, 23)

Dabei ist es mit GIS möglich, die Daten nicht nur topographisch auf einer Karte zu verorten, sondern auch deren »topologische« Eigenschaften – die »Lagebeziehung zu anderen Geobjekten (Topologie)« (Dombrowsky, Horenczuk und Streit 2003, 89) – also die Relationen zwischen den unterschiedlichen Objekten zu erfassen. Das geschieht sowohl mit der sogenannten »Nachbarschaftsanalyse«, mit der sich bestimmen lässt, welche Objekte aneinander grenzen und wo es gefährliche räumliche Verknüpfungen gibt, als auch mit »Netzwerkanalysen«, die »Beziehungen von Netzwerken (z.B. Elektrizitätsnetze, Straßennetze, Gewässernetze) [...] ermitteln und [...] berechnen.« (Dombrowsky, Horenczuk und Streit 2003, 94). Analysen der relationalen Strukturierung eines Gebietes sind für die Analyse von Vulnerabilitäten deshalb so wichtig, weil gerade die räumliche Verflechtung von »Schutzobjekten« potenziell gefährlich werden kann. Zum Beispiel kann die räumliche Nähe einer Chemiefabrik und eines Wohngebietes ein Problem darstellen, aber auch die Konzentration von interdependenten Infrastrukturen ist ein Faktor der Verwundbarkeit.

Gefahrenkarten sollen vor allem Aufschluss über die »räumliche Ausdehnung« (BBK 2010a, 26) eines Ereignisses geben. Abhängig von Szenarien wird der Umkreis möglicher Ereignisse simuliert. Dies geschieht zu meist mit Hilfe von sogenannten »Pufferberechnungen« (Dombrowsky, Horenczuk und Streit 2003, 93), mit denen räumliche Ausbreitungen von Gefahrenstoffen berechnet werden. Dabei kann es sich um Schadstoffe, Sturmfluten, nukleare Wolken oder auch um Lärm handeln. Die Pufferberechnung versucht gleichsam den »glatten Raum« (Deleuze und Guattari 1997, 657ff.) einer Gefährdung zu bestimmen, der sich nicht an institutionelle und physische Einkerbungen und Grenzziehungen hält. Ein Raum, der häufig von einer volatilen Materialität konstituiert wird – Wasser, Sturm, Strahlung, Giftstoffe –, die an fixen Grenzen nicht halt macht. Sichtbar wird diese entgrenzende Qualität der Gefährdung durch eine sogenannte »Verschneidung« bzw. einen »Overlay« (Dombrowsky, Horenczuk und Streit 2003, 95) der Karte eines Puffers mit einer Grundlagenkarte. Die Karten werden so übereinandergelegt, dass sich abschätzen lässt, welche Schäden im Einzugsgebiet entstehen könnten, wenn es zum simulierten Ereignis käme. Ebenso können Verwundbarkei-

ten kenntlich werden, etwa durch die Positionierung eines Atomkraftwerkes in einem Erdbebengebiet.

Zur Abschätzung des tatsächlichen Schadensausmaßes muss diese Karte aber auch noch mit der »Karte des Schutzpotentials« in Beziehung gesetzt werden. Die Verwundbarkeit in einem Gebiet ist nämlich nicht nur abhängig von den strukturellen Beziehungen zwischen Gefährdungen und Schutzgebiet, sondern auch von den vor Ort verfügbaren operationellen Schutzressourcen. Deshalb verspricht man sich von der Kartierung von Verwundbarkeiten in Relation zu den Schutzpotenzialen die Überwindung eines »verdinglichte[n] Katastrophenverständnis[ses]« (Dombrowsky, Horenczuk und Streit 2003, 36), das nur die äußere Gefährdung in den Blick nimmt und nicht erkennt, dass eine »Katastrophensituation aus mindestens zwei Bestandteilen, dem Ereignis« und den »Bewältigungsstrategien der Gesellschaft« (BBK 2005c, 3) besteht. Entsprechend werden systematisch die Einrichtungen von Ersthelfer\_innen kartiert, etwa die Standorte von Krankenhäusern, Feuerwehren und Polizeistationen. Sichtbar werden so die Verteilung der Schutzeinrichtungen im Verhältnis zu potenziellen Gefährdungen und damit auch eventuelle räumliche Über- oder Unterversorgungen. Zur Bestimmung des Versorgungsniveaus im Ernstfall ist vor allem die »raum-zeitliche Reichweite« (Dombrowsky, Horenczuk und Streit 2003, 148) der Einrichtungen wichtig: Wie schnell ist ein Rettungsteam an einem Einsatzort, welchen Radius deckt eine Feuerwehr ab? Wiederum sind es die relationalen Raumeigenschaften, die ausschlaggebend sind. Es geht um das »korrekte Abbilden topologischer Beziehung« (Dombrowsky, Horenczuk und Streit 2003, 94). Dies geschieht mit Hilfe von »Netzwerk- bzw. Graphenanalysen«, die »zwischen zwei Orten die optimalste Verbindung« (Dombrowsky, Horenczuk und Streit 2003, 94) ermitteln.

Die Verschneidung von Grundlagenkarten, Gefahrenkarten und Karten des Schutzpotenzials vermittelt Einsichten für die korrekte Vorsorgeplanung. So können abhängig von Gefährdungsintensität und Wahrscheinlichkeit die Dislozierung von Hilfseinrichtungen geplant und die »optimalen Positionen für Ambulanzgaragen« (Dombrowsky, Horenczuk und Streit 2003, 94) gefunden werden. Die Dislozierung der Task Forces im Bevölkerungsschutz (siehe 2.1.3.) basiert auf ähnlichen Erwägungen. Immer geht es um die Berechnung davon, wie schnell ein bestimmter Helfer\_innentrupp – Feuerwehr, Polizei, Krankenwagen etc. – am Einsatzort sein kann und muss. Der Raum der Sicherheit, der durch Verwundbar-

keitsanalysen mit Geodaten in Szene gesetzt wird, erscheint hier als komplexe Ökologie unterschiedlicher räumlicher Modi. Topographische Räumlichkeiten (metrische Lage von bestimmten Objekten) und topologische bzw. relationale Räume (Beziehungen, Nachbarschaften sowie Vernetzungen von Räumen), Einkerbungen (Bezirksgrenzen, Deiche) und glatte Räume (Schadstoffausbreitung und Sturmfluten) müssen miteinander in Bezug gebracht werden.<sup>69</sup> Hinzu kommt eine zeitliche Dimensionierung des Raumes der Risikoanalyse als Raum der Sicherheit. Mögliche Ereignisse werden in ihrer Ausbreitung, mögliche Hilfspotenziale in ihrer »zeit-räumlichen« Entfernung zum Einsatzort dargestellt. So wird ein Sicherheitsraum eröffnet, der einige Eigenschaften des »Milieus« aufweist, das Foucault als operativen Raum der Sicherheitsdispositive beschrieben hat.<sup>70</sup> »Der Sicherheitsraum verweist also auf eine Serie möglicher Ereignisse, er verweist auf [...] ein Zeitliches und Aleatorisches, die in einem gegebenen Raum eingeschrieben werden müssen.« (Foucault 2004, 40) Der Raum ist dabei bereits ein relationaler Raum, der nicht nur aus »euklidischen« Distanzen, sondern ebenso aus topologischen Beziehungen entsteht. Trotzdem dient der Raum als ein in der Gegenwart verfügbares und gestaltbares Setting, in dem die mögliche Gefahrenzukunft präsent gemacht werden kann. Die Verwundbarkeitskartierung eröffnet damit das »Gefahrenmilieu« als Interventionsfeld vorsorgender Sicherheitstechnologien.

Die Zeitlichkeit des Sicherheitsraumes wird noch augenscheinlicher bei der Verwendung von Geodaten bei der Einsatzplanung und Koordinierung über das deutsche Notfallinformationssystem deNIS II, insofern in diesem Fall nicht nur mögliche Risiken simuliert, sondern aktuelle Bedrohungen und deren Bearbeitung eingefangen werden sollen. Karten werden hier für drei Funktionen genutzt: das Lage-, Ressourcen- und Meldemanagement (BBK 2006b). Für das Lagemanagement wird eine Grundlagen-

69 Die Unterscheidung von glattem und gekerbtem Raum geht auf Gilles Deleuze und Félix Guattari (1997, 658–693) zurück. Während gekerbte Räume der Effekt von Ab-, Ein- und Grenzziehungen sind, sind glatte Räume nicht in gleicher Weise festgelegt. Vielmehr breiten diese sich eigengesetzlich aus und überfluten – bisweilen sprichwörtlich – territorialisierende Einkerbungen.

70 Foucaults Konzept des Milieus als Raum der Sicherheit changiert zwischen historischem und systematisch-operativem Begriff. Hier steht die systematische Dimension seines Milieukonzepts im Vordergrund. Anders als das Territorium – der Raum souveräner Sicherheitsdispositive – ist das Milieu kein abgrenzbarer Raum, sondern ein zeit-räumliches Gefüge, das nicht so sehr über seine Grenzen, sondern seine internen Relationen definiert ist. In Kapitel 3 steht dagegen die historische Transformation des Milieukonzepts im Vordergrund (siehe insbesondere Exkurs II).

karte mit einem »Ereignislayer« versehen, das Informationen zu faktisch vorliegenden Schadensfällen gibt (BBK 2006b, 6). Für das Ressourcenmanagement können zusätzlich die lokal verfügbaren Hilfspotenziale angezeigt werden (BBK 2006b, 6). Schließlich ermöglicht das Meldemanagement einen Überblick über laufende oder bereits abgeschlossene Bearbeitungen des Ereignisses. »In einer Meldeliste werden alle Meldungen und erteilten Aufträge zur Lage mit dem aktuellen Status (zum Beispiel »Auftrag erledigt«) zusammenfassend dargestellt.« (BBK 2006b, 6) Zusätzlich zu den Karten, die auch für die Vorbereitungsplanung Verwendung finden, werden für die Einsatzkoordination also auch Praktiken der Hilfeleistungen kartiert.

Die »Lage« wird sichtbar als komplexes Geschehen, das aus der Interaktion unterschiedlichster Parameter entsteht. Ob ein solches Geschehen überhaupt zu einer Katastrophe wird und wie schwerwiegend sich diese auswirkt, hängt dann genau von der Interaktion von Objekten, Beziehungen, Ereignissen und Praktiken ab und nicht nur von der Schwere eines äußeren, singulären Ereignisses. Die »Lage« zeigt sich als eine »Serie von Ereignissen« – sowohl Schadensereignisse als auch Rettungsaktivitäten. Sie ist ein dynamischer und relationaler Zeit-Raum. Wiederum ist Foucaults Konzept des Milieus hilfreich, um dessen Charakteristika zu denken.

»Die »Sicherheit« [wird] versuchen, ein Milieu im Zusammenhang mit Ereignissen oder Serien von Ereignissen oder möglichen Elementen zu gestalten, Serien, die in einem multivalenten und transformierbaren Rahmen reguliert werden müssen.« (Foucault 2004, 40)

Anders als bei der Verwundbarkeitskartierung im Rahmen der Vorbereitungsplanung ist das Milieu im Fall der Einsatzplanung und Koordination nicht nur ein Raum, in dem mögliche Ereignisse vorsorglich eingeschrieben werden können, sondern ein aktueller Ereignisraum. Das Milieu ist hier nicht nur der Ort, sondern auch das zeitliche »Mittendrin« der sich entfaltenden oder noch abzuwendenden Katastrophe bzw. »Lage«. <sup>71</sup>

Sowohl im Rahmen der Vorbereitungs- als auch der Einsatzplanung erlaubt die computergestützte Risikoanalyse die Visualisierung eines erstaunlich hohen Grades der Komplexität solcher Milieus. Deshalb sind Risikokarten gerade für die operative Seite des Bevölkerungsschutzes eine

---

71 Dieser sowohl räumliche als auch zeitliche Sinn liegt schon im französischen Wort *milieu*. Einen ähnlichen Doppelsinn hat auch das deutsche Wort »Lage«, das als technischer Begriff eine wichtige Bedeutung im deutschen Notfallwesen hat.



so bedeutende Wissenstechnik. Das über Karten funktionierende Informationssystem fungiert dabei wiederum zur Koordinierung unterschiedlicher Akteure. Die Karte selbst kann als »boundary object« (Star und Griesemer 1989) verstanden werden, das die Zusammenarbeit von Akteuren durch die Etablierung von »coincident boundaries« ermöglicht.<sup>72</sup> Die Akteure können sich in der Karte auf je spezifische Art und mit ihren eigenen Daten einschreiben und so im Verhältnis zu anderen Akteuren verorten. Das ermöglicht nicht zuletzt, dass eine zentrale Koordinierung »aus der Distanz« eines Lagezentrums wie dem GMLZ erfolgen kann. Das Informationssystem deNIS II bettet die einzelnen Karten also in ein größeres Netz ein, so dass eine »boundary infrastructure« entsteht.<sup>73</sup> Die Situation der Katastrophe kann gewissermaßen in den »Situationsraum« des Lagezentrums gebracht werden. Wie die standardisierte Risikomatrix ermöglicht auch das Kartensystem von deNIS II das praktische Knüpfen der Netze des Sicherheitsdispositivs.

Allerdings stellt die Kartierung der Vulnerabilität auch eine Alternative zur quantifizierenden Risikomatrix dar. Der Vorteil besteht hier darin, dass die Karte nicht allzu abhängig von statistischen Daten über vergangene Ereignisse ist und gleichzeitig nicht nur mit imaginierten Zukünften operieren muss, sondern sich an konkreten räumlichen Fixpunkten orientiert. Dadurch eröffnet sich zugleich ein Feld der Intervention für Techniken der vorbereitenden Katastrophenbewältigung: der Sicherheitsraum oder das »Milieu« in seiner materiellen Strukturiert- und Vernetztheit, an dem

---

72 In ihrem klassischen Text, der das Konzept der *boundary objects* eingeführt hat, verweisen Star und Griesemer explizit auf die Bedeutung von Karten als *boundary objects*, insofern diese ein Gebiet mit gemeinsamen Grenzen umschreiben, auf dem dennoch ganz unterschiedliche Daten eingetragen werden können (im Fall der Regierung der Katastrophe unter anderem Schadenslage, Ressourcen und bereits bearbeitete Aufträge). Karten sind also »common objects which have the same boundaries but different internal contents. They arise in the presence of different means of aggregating data and when work is distributed over a large-scale geographic area. The result is that work in different sites and with different perspectives can be conducted autonomously while cooperating parties share a common referent« (Star und Griesemer 1989, 411).

73 Mit dem Konzept der *boundary infrastructure* haben Star und Bowker das Konzept der *boundary objects* erweitert. »Boundary infrastructures [...] deal in regimes and networks of boundary objects (and not of unitary, well-defined objects).« (Bowker und Star 2000, 314) Einer Analyse des Sicherheitsdispositivs hilft dieses Konzept zu erkennen, welche konkreten sozio-technischen Vorrichtungen die Koordination und Zusammenarbeit unterschiedlicher Akteure ermöglichen.

bereits in der Gegenwart gearbeitet werden kann, um Verwundbarkeiten zu reduzieren.

Gleichwohl gehen mit dem kartenbasierten Risikomanagement auch etliche Probleme einher. Beispielsweise kann es zu Fehlallokationen bei der räumlichen Verteilung von Hilfsressourcen kommen. Gerade weil das Katastrophenpotenzial immer nur relativ zu der Vulnerabilität des jeweiligen Gebietes und den dortigen operativen Hilfsressourcen besteht, können Fehlplanungen auch harmlosere Ereignisse in katastrophische Ausmaße eskalieren lassen. So heißt es im Bericht zur Risikoanalyse des Bundestages aus dem Jahr 2010: »[U]nglückliche Verkettungen von Ereignissen und Fehlentscheidungen gehören ebenso in den Katalog akuter Gefahren, die Deutschland als Ganzes oder aber in Teilen betreffen können« (Bundestag 2010, 7). Unter Bedingungen begrenzter Budgets und verfügbarer Ressourcen werden alle Verbesserungen in der »Risikolandschaft«, alle Fortschritte in der Versichertheitlichung mit einer Erhöhung von Anfälligkeiten und Verwundbarkeiten an anderer Stelle erkaufte.

Eine weitere Zwickmühle betrifft die Verfüg- und Handhabbarkeit von Daten. Einerseits wird stets ein Mangel an verfügbaren Daten beklagt (Dombrowsky, Horenczuk und Streit 2003, 125). Andererseits drohen die Katastrophenschützer\_innen aber auch in einem »Meer von Daten« (Dombrowsky, Horenczuk und Streit 2003, 25) unterzugehen, dass nicht nur aus signifikanten Informationen, sondern vor allem auch aus nicht-signifikantem Rauschen besteht. Die Informationen, die eigentlich als Entscheidungshilfe dienen sollen, drohen die Entscheidung faktisch zu erschweren. Gerade Luhmann hat immer wieder betont, dass Entscheidungshandeln durch zu viele Informationen eher belastet wird und formuliert scheinbar paradox: »Die Last der fehlenden Information ist die Voraussetzung für die Lust am Entscheiden.« (Luhmann 2000, 188)

Und selbst wenn es möglich wäre, alle relevanten Daten zu sammeln und mit der so erzeugten Komplexität angemessen umzugehen: Ein bestimmter Blick auf Risiken, der gerade gegen Ende des vergangenen Jahrzehnts immer prominenter wurde, müsste selbst dann noch eine Unterkomplexität sowohl der zeitlichen als auch der räumlichen bzw. raumzeitlichen Methoden zur Risikoanalyse diagnostizieren. Radikal genug gedacht sprengen systemische Risiken die Raster – die Matrix und das Kataster – der Risikoanalyse. Systemische Risiken beschreiben Gefahrenlagen und Verwundbarkeiten, die so komplex sind, dass einzelne, isolierte oder sporadische Risikoanalysen nicht mehr ausreichen. Sie nötigen zu

einer Reflexivität, die etwas in den Blick geraten lässt, das in jüngerer Zeit mehr als einmal in der Soziologie wie auch in öffentlichen Diskussionen verabschiedet wurde: die Gesellschaft.

#### 2.4. *Gegenstand:* Das »System« als Schutzobjekt und Gefährdungszusammenhang

Seit der jüngsten Finanzkrise sind systemische Finanzmarktrisiken zu einem ebenso viel wie kontrovers diskutierten Thema in den Sozialwissenschaften (siehe unter anderem: Willke, Becker und Rostásy 2013, Langley 2014), aber auch in einer breiteren Öffentlichkeit geworden. Weniger öffentliche Beachtung finden dagegen systemische Umweltrisiken oder systemische Risiken in Infrastruktursystemen (siehe dazu: Renn und Keil 2008, Collier, Lakoff und Keltly 2011). Gleichwohl sind letztere ebenso wie die systemischen Finanzmarktrisiken zu zentralen *matters of concern* sicherheitspolitischer Strategien geworden.

Systemische Zusammenhänge stellen dabei nicht nur Probleme, sondern zugleich auch zentrale Schutzziele innerhalb des Sicherheitsdispositivs der Resilienz dar. Collier und Lakoff (2015) haben gezeigt, dass bereits im Rahmen der Zivilschutzplanungen während des Kalten Krieges in den USA miteinander zusammenhängende Versorgungsleistungen und Infrastrukturen, die als »vital« für die Kriegsführung und die Sicherheit der Bevölkerung angesehen wurden, zum sicherheitspolitischen Problem aufgestiegen sind. Im Zuge dieser Überlegungen hat sich eine neue Sicherheitstechnologie entwickelt, die Collier und Lakoff als »vital systems security« bezeichnen und von der klassischen biopolitischen Bevölkerungssicherheit abgrenzen. Um das »Heimatland« und das Leben der Bevölkerung zu schützen, muss die Integrität »vitaler Systeme« gewahrt werden. Unter dem Stichwort »Schutz Kritischer Infrastrukturen« bilden derartige Überlegungen einen mittlerweile fest etablierten Topos in Sicherheitsstrategien einer Reihe westlicher Staaten (siehe dazu: Der Derian und Finkelstein 2008, Dunn Caveltly 2008, Aradau 2010, Folkers 2012). Dabei geht es längst nicht mehr nur um den Schutz von »kriegswichtigen Infrastrukturu-

ren« und Systemen, sondern allgemeiner um »gesellschaftswichtige« oder »lebenswichtige« Strukturen und Leistungen.<sup>74</sup>

Was sich gegenüber der Zeit des Kalten Krieges geändert hat, ist allerdings, dass die »vitalen Systeme« nicht mehr nur als extern – von feindlichen Atombombenabwürfen etwa – bedroht angesehen werden, sondern dass ihnen ein intrinsisches Gefahrenpotenzial zugeschrieben wird. Gefahr entsteht nicht ausschließlich durch Schocks aus der Umwelt, sondern hängt ebenso mit systeminternen Resonanzeffekten zusammen. Genau das drückt die Kategorie »systemisches Risiko« aus. Zwar wird bisweilen gegargwöhnt, dass die Rede von systemischen Risiken auf eine Dekulpation von Verantwortungsträgern hinauslaufe und somit bloß eine Semantik »organisierter Unverantwortlichkeit« (Beck 1988) sei, indem mit Verweis auf die Komplexität systemischer Zusammenhänge politische und rechtliche Haftungsansprüche abgewiesen werden. Systemisches Risiko ist aber auch eine reflexive Risikorationalität, weil sie zur Selbstbeobachtung, zur Reflexion der »eigenen« Strukturen und Verwundbarkeiten nötigt. Im gegenwärtigen Dispositiv der Sicherheit nimmt das »System« deshalb eine ambivalente Stellung ein. Es ist sowohl *Schutzobjekt* – Gegenstand der Sicherheit – als auch *Gefahrenherd*. Das daraus resultierende Sicherheitsproblem besteht darin, dass sich die systemischen Risiken nicht einfach dadurch bekämpfen lassen, dass man die Systeme, von denen diese ausgehen, beseitigt. Der Ausstieg erscheint nicht als Option, um der selbstgewebten systemischen Gefährdung zu entgehen, weil die Gesellschaft von dem, was sie gefährdet, zugleich existentiell abhängt.

In diesem Kapitel werde ich eine Reihe von exemplarischen Problematierungen systemischer Risiken in unterschiedlichen Feldern – von der Lebensmittelsicherheit bis zum Finanzmarkt – analysieren. Mein Analysefokus wird im Folgenden also über den deutschen Katastrophen- und Bevölkerungsschutz hinausgehen. Dadurch werden die Familienähnlichkeiten zwischen den Sicherheitsrationalitäten im Katastrophenschutz und anderen Bereichen sichtbar, die sich ebenfalls der Regierung der Katastrophe (als systemisches Risiko) verschrieben haben. Auch wenn in diesen Bereichen nicht immer der Begriff »systemisches Risiko« verwendet oder das Schutzobjekt als »System« beschrieben wird – ebenso häufig wird von »komplexen Risiken« und »Ereignisverkettungen« gesprochen, die »Liefer-

---

74 Ich werde in Kapitel 3.1. genauer auf die historischen Entwicklungen in Deutschland eingehen, die zur Etablierung des Topos der Lebenswichtigkeit von Infrastrukturen beigetragen haben.

ketten« oder »Infrastrukturen« betreffen –, ähneln sich die sicherheitsstrategischen Problematisierungen doch so sehr, dass sie als Teil ein und desselben Sicherheitsdispositivs verstanden werden müssen.

Im Folgenden werde ich zunächst auf den Aufstieg der Kategorie des systemischen Risikos zum Kardinalproblem der Regierung der Katastrophe eingehen (2.4.1.). Danach wird gezeigt, wie das *system of systems* als allgemeiner Horizont gegenwärtiger Sicherheitsdispositive figuriert (2.4.2.). Sodann werde ich herausarbeiten, welche systemischen Risiken in jeweils spezifischen Bereichen – vom Schutz Kritischer Infrastrukturen bis zur Seuchenkontrolle – identifiziert werden (2.4.3.). Der Finanzmarkt stellt dabei einen Sonderfall dar, weil die Aufmerksamkeit für systemische Risiken hier besonders groß ist (2.4.4.). Schließlich wird die Frage aufgeworfen, wie sich die herausgearbeiteten Ähnlichkeiten in den Problematisierungen systemischer Risiken im Rahmen einer Dispositivanalyse interpretieren lassen (2.4.5.).

#### 2.4.1. Der Aufstieg des systemischen Risikos

Die Terroranschläge des 11. September 2001 haben ein Jahrzehnt vielfältiger Neuorientierungen der Sicherheitspolitik in Deutschland eingeleitet. Knapp zehn Jahre später, am 11. März 2011, sollte ein anderes Ereignis die Erde und mit ihr die Gefüge der Sicherheit erschüttern: das Tohoku-Erdbeben in Japan und seine Folgen. Einschneidend war der 11. März 2011, weil sich nicht nur *ein* Ereignis, sondern eine »Dreifach-Katastrophe« aus Erdbeben, Tsunami und Nuklearkatastrophe im japanischen Atomreaktor Fukushima Daiichi an der japanischen Ostküste ereignete. Der natürliche Auslöser des Ereignisses lag fernab menschlicher Einflussmöglichkeiten: 130 Kilometer vor der japanischen Küste und 24 Kilometer unter der Erdoberfläche hatte eine Bewegung von Erdplatten die Erschütterungen ausgelöst. Die tektonische Begegnung der Erdplatten ließ jedoch nicht nur Land und See erbeben, sondern versetzte zugleich eine Reihe von sozio-technischen Systemen in Schwingung. Das Beben hat Unterscheidungen zwischen vermeintlich getrennten Bereichen oder »Systemen« im wahrsten Sinne des Wortes in sich zusammenbrechen lassen und an deren Stelle ein vibrierendes materielles Gefüge, eine »resonance machine« (Connolly 2011, 124) gesetzt, in der Rückkopplungseffekte eine katastrophische Ereignisseskalation bewirkt haben. Was an der Mehrfach-Katastrophe in Japan selbst für ausgewiesene Sicherheitsexpert\_innen so schockierend war, war

kein singuläres, undenkbares oder noch nie dagewesenes Ereignis, wie es beim 11. September der Fall gewesen war. Jedes der Ereignisse vom Katastrophemärz in Japan hatte historische Vorläufer. Noch nie dagewesen und unerwartet waren jedoch die spezifische Verkettung der Ereignisse und ihre kaskadierende Ausweitung.

Dies lässt sich an den jeweils kurz nach den Ereignissen vom 11. September 2001 und 11. März 2011 veröffentlichten Gefahrenberichten der Schutzkommission ablesen. Nach dem 11. September hieß es etwa: »Die Terroranschläge in den USA am 11. September 2001 haben deutlich gemacht, dass zukünftig im Rahmen des Zivil- und Bevölkerungsschutzes bisher nicht für realistisch gehaltene Szenarien berücksichtigt werden müssen.« (Schutzkommission 2001, 7) Zehn Jahre später heißt es dann:

»Die in Japan durch das zeitliche Zusammenwirken von drei in höchstem Maße katastrophalen Ereignissen eingetretene Lage entspricht einer Ereigniskaskade (Domino-Effekt) in einem bislang nach dem Prinzip der »Wahrung praktischer Vernunft« bei klassischen Risikobetrachtungen als »unwahrscheinlich« (sog. »seltenes Ereignis«) dem sog. »Restrisiko« zugeordnetes Ereignis.« (Schutzkommission 2011, 19)

Zwar wurde in beiden Fällen gefordert, bisher nicht für möglich gehaltene Szenarien zu berücksichtigen. Was sich jedoch verändert hat, ist die Quelle der Unsicherheit: einmal ist es das singuläre Ereignis selbst, das andere Mal sind es seine Folgen bzw. die fatale Serie unglücklicher Ereignisse.

Neben der japanischen Mehrfach-Katastrophe waren es zuletzt vor allem die Krisen der Finanzökonomie, die dazu beigetragen haben, ein zwar bekanntes, aber zugleich wenig beachtetes Risikoverständnis mit Nachdruck auf die Agenda der Sicherheitsapparate zu setzen. Die weltweite Finanzkrise der Jahre 2007 und 2008 sowie die seit 2011 perennierende Eurokrise haben es weit über die Kreise von Sicherheitsexpert\_innen und Finanzmarktakteuren hinaus üblich werden lassen, von Ansteckungsgefahren, *toxic connections*, *financial meltdown* und immer wieder auch von systemischen Risiken zu sprechen. Das ökonomische Risikomanagement ist dadurch zu einem weiteren »Epizentrum« der Aus- und Umarbeitung des Sicherheitsdispositivs geworden.

Die japanische Katastrophenserie wie auch die weltweiten Finanz- und Schuldenkrisen stellen Ereignisse mit paradigmatischem Mehrwert dar, insofern sie eindrücklich die Grenzen eines spezifischen Risikoverständnisses und mithin die Grenzen der Analyse katastrophischer Risiken sichtbar machten. Das heißt nicht, dass die bisherigen Analysen katastrophischer

Risiken vollkommen hinfällig geworden wären. Allerdings konzentriert sich das Sicherheitsdispositiv etwa seit dem Ende des ersten Jahrzehnts des neuen Jahrtausends verstärkt auf systemische Risiken mit unterschiedlichen Morphologien: Ereigniskaskaden, Dominoeffekte, selbstverstärkende Feedbacks etc. Dabei knüpft ein systemisches Verständnis der Katastrophe in vielerlei Hinsicht an die bisher geschilderte »generische« Gefährdungsauffassung an – gerade das macht es für das entstehende Sicherheitsdispositiv auch so anschlussfähig. Allerdings sprengt »systemisches Risiko« konsequent genug gedacht die *zeitlichen*, *räumlichen* und *sachlichen* Grenzen der generischen Gefährdungsauffassung und der Ausarbeitung der Risikoanalytik im Bevölkerungsschutz.

Die *zeitliche* Grenze betrifft die Bestimmung des Risikos durch die Multiplikation von Eintrittswahrscheinlichkeit und Schadensausmaß. Unter dem Eindruck des »Fukushima Schocks« merkt der Gefahrenbericht der Schutzkommission kritisch an:

»Die Katastrophe in Japan und die draus folgenden Reaktionen in Deutschland machen deutlich, dass im Zusammenhang von ›Seltenen Ereignissen mit extrem hohem Schadensschwere‹ [sic!] die für sehr viele Betrachtungsfälle zweckdienliche und bewährte Auffassung des Risikos als Produkt aus Schadensschwere und Eintrittswahrscheinlichkeit gesellschaftspolitisch unzulänglich ist.« (Schutzkommission 2011, 19)

Schließlich ist es nicht nur die Wahrscheinlichkeit eines einzelnen Ereignisses, sondern auch die Wahrscheinlichkeit einer bestimmten Verkettung von Ereignissen, die in einer systemischen Perspektive bestimmt werden müssten. Der isolierte Punkt in der Risikomatrix ist daher wenig aussagekräftig.<sup>75</sup> In einem Bericht des Zukunftsforums Öffentliche Sicherheit – ein parteiübergreifender Zusammenschluss von Bundestagsabgeordneten – heißt es programmatisch:

»Die Mitwirkenden des ›Zukunftsforums Öffentliche Sicherheit‹ sind sich einig, dass die physische und politische Existenz der Bundesrepublik Deutschland nur in extremen Ausnahmefällen von einem singulären Ereignis bedroht oder gar zerstört werden kann. [...] Viel wahrscheinlicher sei, dass sich existenzgefährdende, natio-

<sup>75</sup> Dementsprechend müssen Szenarien komplexe Ereignisverkettungen berücksichtigen.

So entwirft das Zukunftsforum Sicherheit in seinem *Grünbuch* ein Szenario mit eng gekoppelter Ereignisfolge, in der ein Hochwasser in einem Hitzesommer zur Vermehrung von Mücken und zur Ausbreitung einer Pandemie führt, die aufgrund der durch Hochwasser und Hitze gebundenen Hilfskapazitäten nur schwer eingedämmt werden kann. Siehe: ZÖS (2008, 36).

nale Notlagen aus dem Zusammenwirken mehrerer Negativereignisse ergeben. Durch Dominoeffekte können natürliche, technische, soziale und ökonomische Faktoren interagieren und [...] zu sehr unterschiedlichen Schadensverläufen führen.« (ZöS 2008, 14)

Zwar ist die *räumliche* Kartierung von Vulnerabilität in der Lage, die Komplexität von kaskadischen Ereignisverläufen in den Blick zu bekommen. Die radikale Ausfransung eines Ereignisses, die sich aus komplexen Risikolagen ergeben kann, lässt aber auch die Limitation des geographischen *vulnerability mapping*, und damit die Grenzen der räumlichen Dimensionierung der Risikoanalytik im Bevölkerungsschutz, deutlich werden. Schließlich soll sich die Kartierung von Gefährdung und Verwundbarkeit »immer auf die geschlossene Einheit eines bestimmten räumlichen Bezugsgebietes« (BBK 2010a, 23) beziehen. Aber was ist, wenn, wie im Falle der Mehrfach-Katastrophe, Beeinträchtigungen und Zerstörungen der japanischen Infrastruktur zu Lieferengpässen und Produktionsausfällen noch in der deutschen Automobilindustrie führen? Was ist, wenn eine Gefährdung keine »geschlossene Einheit«, sondern eine Reihe offener und zugleich interdependenter Systeme betrifft? Bereits in dem für die globale Sicherheitslandschaft einflussreichen Bericht des PCCP von 1997 wurde auf die »new geography« aufmerksam gemacht, die durch Globalisierung und Digitalisierung entstanden sei und damit zugleich eine neue Topologie der Gefährdung erzeugt habe (siehe: PCCP 1997, 7ff.). So sei zum einen ein virtueller Raum entstanden, der vollkommenen anderen Spielregeln gehorche als physische Räume. »[T]he day may be coming when an enemy can attack us from a distance, using cyber tools [...]. The new geography is a borderless cyber geography whose major topographical features are technology and change.« (PCCP 1997, 7) Ganz ähnlich hat zwanzig Jahre später auch das Bundesamt für Sicherheit in der Informationstechnik den mittlerweile etwas angestaubten Topos des *cyber space* aufgerufen und auf eine neue »Gefährdungslage im Cyber-Raum« (BSI 2017, 5) hingewiesen. Zugleich, so wird argumentiert, ist die physische Vernetzung und damit die Verwundbarkeit für physische Bedrohungen weitläufiger, komplexer und unübersichtlicher geworden. »In the networked world of today, the effects of such physical attacks could spread far beyond the radius of a bomb blast.« (PCCP 1997, 5) Dabei ist die Bezugnahme auf den »radius of a bomb blast« eine deutliche Anspielung auf das klassische *vulnerability mapping*, bei dem der Umkreis bzw. Puffer eines Atombombenabwurfs mit einem abgegrenzten Bezugsgebiet verschnitten wurde, um dessen Verwundbarkeiten



zu ermitteln – eine Prozedur, die in der »vernetzten Welt der Gegenwart« nur noch von begrenztem Nutzen ist.

Schließlich zeichnen sich die komplexen Gefährdungen aber nicht nur durch eine räumliche und zeitliche, sondern auch durch eine *sachliche Entgrenzung* aus. Die Mehrfach-Katastrophe ist schließlich gerade durch die Resonanz zwischen »natürlichen« und »soziotechnischen« Ereignissen und Systemen entstanden.

»Die konventionelle Einteilung in die drei Kategorien Naturkatastrophe, technische oder man-made Katastrophe verführt dazu, die nachfolgenden Schutzmaßnahmen jeweils nur innerhalb dieser gedanklichen Schublade zu entwickeln. Mit einer neuen Kategorie »Systemversagen« kann zumindest mehr Augenmerk auf die komplexen systemischen Zusammenhänge und Interdependenzen gerichtet werden, um Katastrophen verhüten zu können.« (Allianz 2008, 49)

Im Angesicht von komplex-vernetzten Gefahrenlagen wird daher immer wieder eine »Abkehr von sektorbezogenen Betrachtungen von Gefahrenlagen hin zu einem Systemverständnis« empfohlen (Schutzkommission 2011, 130). Das System ist in diesen Ansätzen also eine Figur, die »konventionelle Einteilungen« und »sektorbezogene Betrachtungen« überwinden soll. Sie problematisiert damit gesellschaftliche und institutionelle Differenzierungen als willkürliche Grenzlinien, die eine angemessene Reaktion auf entgrenzte Gefährdungen erschweren. Dabei steht bei diesen Ansätzen, die sich als »ganzheitliche, vernetzte, kybernetische, systemische« (Allianz 2008, 18) verstehen, das Eigene, das »System«, und nicht die »Umwelt« im Vordergrund.

»Katastrophen entstehen demnach nicht aus heiterem Himmel und nicht durch singuläre Ursachen (Naturgewalt, technisches oder menschliches Versagen), sondern durch ein sogenanntes Systemversagen. Das bedeutet, dass ein System (z.B. Verkehrssystem, Energieversorgung, Gesundheitswesen) deshalb ausfällt, weil der Mensch die materiellen und immateriellen Elemente des Systems nicht sorgfältig genug aufeinander abgestimmt hat.« (Allianz 2008, 17)

Die generische Gefährdungsauffassung wird mit der systemischen Perspektive nicht außer Kraft gesetzt, sondern intensiviert und erweitert. Der generische Horizont der Gefährdung hat sich sogar noch einmal erweitert: »Alles kann Auslöser sein« (ZöS 2008, 20). Auch sehr unscheinbare Ereignisse können eine gleichsam enorme Wirkung entfalten, so wie laut der Chaostheorie schon der Flügelschlag eines Schmetterlings einen Orkan auf einem anderen Teil der Erde auslösen kann (siehe: Gleick 1990, 20–53). Die generische Gefährdung geht nun aber nicht mehr aus dem

unendlichen »All« äußerer Gefahren hervor, sondern letztlich aus der internen Beschaffenheit dessen, was doch eigentlich vor diesen Gefahren geschützt werden soll. Dabei geht es nicht nur darum, dass das System Irritationen oder Störimpulse aus der Umwelt immer systemspezifisch verarbeiten muss, wie Luhmann (2008) in *Ökologische Kommunikation* betont. Vielmehr ist das »System« ein substanzieller Gefahrenzusammenhang, in dem systemeigene Prozesse sich zu gefährlichen Resonanzen auswaschen können, die nachhaltige Schäden produzieren. Zudem sind die Resonanzen zwischen den Systemen nicht nur kommunikativ, sondern materiell, insofern die Systeme durch störungsanfällige Infrastrukturen und substanzielle Versorgungsleistungen miteinander gekoppelt sind.<sup>76</sup>

#### 2.4.2. Das »system of systems« als Horizont des Sicherheitsdispositivs

Im Zuge der verstärkten Aufmerksamkeit für systemische Risiken sind »Systeme« aber nicht nur zum Gefahrenherd, sondern immer mehr auch zum vorrangigen Schutzobjekt von Sicherheitsdispositiven geworden. Häufig hat nämlich der Zusammenbruch systemische Zusammenhänge überhaupt erst sichtbar werden lassen, wo vorher nur isolierte Elemente gesehen werden konnten. Der Zusammenbruch des Finanzmarktes hat erst das Ausmaß der Interdependenzen zwischen den wichtigsten Finanzinstitutionen sichtbar gemacht. Die *ripple effects* der Finanzkrise haben die Abhängigkeit westlicher Gesellschaften von der Finanzwirtschaft hervortreten lassen. Der Zusammenbruch von Infrastrukturen lässt regelmäßig deren Bedeutung für das Funktionieren einer technisierten Gesellschaft bewusst werden. Und erst seit man begonnen hat, sich um die Integrität eines Netzes miteinander verwobener Infrastrukturen wie Wasser- und Stromversorgung, Verkehr, Behörden und Gesundheitswesen zu sorgen, ist so etwas wie eine infrastrukturelle Totalität, nun als Kritische Infrastruktur angesprochen, in Erscheinung getreten. Aber auch abseits vom Schutz Kritischer Infrastrukturen und systemwichtiger Finanzinstitutionen zeichnen

---

<sup>76</sup> Luhmann betont zwar durchaus das Problem der Resonanz, das zur Überlastung von sozialen Systemen führen kann. Im Blick hat er dabei aber nur die kommunikative Resonanz, die durch die allgemeine Erregung und Besorgnis über ökologische Risiken verstärkt durch Regulierungsaufgaben des politischen Systems die Subsysteme überlasten kann (Luhmann 2008, 143–148). Die materiellen Resonanzphänomene, die im Fall systemischer Risiken eine Rolle spielen, lassen sich eher durch Rekurs auf Connollys (2011, 124–147) Konzept der »resonance machines« begreifen.

sich Systeme, komplexe Zusammenhänge und Netzwerke immer deutlicher als distinkter und bisweilen wichtigster, wenn auch schwieriger *Gegenstand der Sicherheit* ab: Etwas, das geschützt werden muss, weil wir von ihm abhängen, auch und gerade weil es ein hohes endogenes Störungspotenzial aufweist. Die vitalen Systeme sind in einem doppelten Sinne kritisch: Sie sind einerseits von entscheidender Bedeutung für das Funktionieren der Gesellschaft, sie sind andererseits aufgrund ihrer hohen Komplexität aber auch krisenanfällig und damit in einem potenziell kritischen Zustand.

Mit diesem neuen, schwierigen Gegenstand der Sicherheit verändert sich zugleich das Verständnis von Sicherheit. Der Zustand der Sicherheit besteht dann vor allem im reibungslosen Funktionieren eben dieser Systeme. »Unter diesen Bedingungen bedeutet ›Öffentliche Sicherheit‹ in erster Linie, dass komplexe Prozesse und Systeme – lokale, nationale bis hin zu transnationalen – möglichst problemlos funktionieren.« (ZöS 2008, 44) Dieses Verständnis von »öffentlicher Sicherheit« als Sicherstellung »problemloser Funktion« von »Prozessen und Systemen« unterscheidet sich auf den ersten Blick von der Zielsetzung der »neuen Strategie«, die als Ziel den »Schutz der Bevölkerung vor besonderen Gefahren« bzw. den »umfassende[n] und wirkungsvolle[n] Schutz der Bevölkerung und ihrer Lebensgrundlagen« (BBK 2010b, 19, 48) angegeben hatte. Gleichwohl kommt es nicht zu einer schlichten Ersetzung des einen durch ein anderes Schutzobjekt, sondern zu einer Verlagerung und Umgruppierung. Die Bevölkerung bleibt weiterhin entscheidend, aber sie ist nicht länger die primäre Interventionsoberfläche zur Herstellung der Sicherheit. Sie ist das Ziel, aber nicht die Zielscheibe, also nicht der unmittelbare Ansatzpunkt der Sicherheitstechnologien. Diesen geht es darum, die Systeme vor Gefahren zu schützen und im Notfall das Funktionieren der Systeme aufrechtzuerhalten. Allerdings müssen die Systeme auch vor sich selbst geschützt werden, indem deren interne Verwundbarkeit reduziert wird.

Verwundbar ist ein System durch seine internen Verflechtungen, aber auch durch seine Abhängigkeiten von anderen Systemen. Die Systemperspektive steht deshalb nicht für eine »sektorale« Logik, der es jeweils nur um spezifische gesellschaftliche »Subsysteme« geht, die so unterschiedlich operieren, dass sie jeweils nur aus ihrer eigenen Logik heraus analysiert werden können. Stattdessen steht die »systemische« Perspektive hier für einen »ganzheitlichen« Ansatz, der das »Ganze« der Systeme in den Blick bekommt. »Sowohl die Risikosteuerung als auch das Krisenmanagement müssen von einer sektoralen Betrachtung zu einer prozessualen und ganz-

heitlichen Betrachtung kommen.« (Zös 2008, 26) Die Systeme sind aufeinander angewiesene Gebilde, die in ihrem Zusammenhang betrachtet werden müssen.

»Jedes der verschiedenen Systeme (z.B. Verkehrswesen, Energieversorgung, Gesundheitswesen) ist für sich allein katastrophenanfällig. Weil alle durch Stromversorgung sowie Informations- und Telekommunikationstechnologie aneinander gekoppelt sind, ist es möglich, dass deshalb alle Systeme gemeinsam versagen.« (Allianz 2008, 46)

»Man guckt auf das ganze System und man guckt, wie die Systeme untereinander interagieren.« (Interview 2). Diese Interaktionsebene, das »system of systems« (Interview 2), bildet dann den ultimativen Horizont des Katastrophenschutzes. Das *system of systems* ist ein interdependentes Netz von operativen Einheiten, die füreinander funktionsnotwendige Dienste produzieren.

Aber weil die Störung in einem dieser Systeme sich schnell auf andere ausbreiten kann, betreffen die systemischen Risiken letztlich die »ganze Gesellschaft« (Zös 2008, 16). Die Problematisierung systemischer Risiken bekommt dadurch eine geradezu soziologische Dimension. Durch die Konzeption eines ebenso interdependenten und störanfälligen *system of vital systems* wird sich die Gesellschaft ihrer selbst als fragiles und komplexes Funktionsnetzwerk gewahr. Dabei werden zwei Charakteristika auf die gesamte Gesellschaft übertragen, mit denen Charles Perrows (1987) bereits in den 1980er Jahren versucht hat, die Normalität von Katastrophen in hochtechnologischen Systemen wie Atomkraftwerken zu beschreiben: enge Kopplung und hohe Komplexität. Die Gesellschaft ist erstens so vernetzt und interdependent, dass sich Schockereignisse schnell fortsetzen, ausweiten und verstärken und im schlimmsten Fall zu Zusammenbrüchen führen (»enge Kopplung« (Perrow 1987)). Diese Komplexität besteht nicht nur in einer Vernetzung, die zum Übertragungsweg für Gefahrenereignisse werden kann, sondern auch in einer Opazität der Netze, Wege und Interdependenzen. Die Gesellschaft ist hier eine eng verzahnte Mega-Maschine: hochsensibel für Störungen und gleichzeitig undurchschaubar.<sup>77</sup>

Dafür wird immer wieder die »komplexe technische Vernetztheit« der »Industriegesellschaft« verantwortlich gemacht, die durch ihre Vernetzung

---

<sup>77</sup> In jüngeren Veröffentlichungen hat Perrow (2011) seinerseits seine *Normal Accident Theory* auf Zusammenhänge jenseits einzelner Organisationen bzw. hochtechnologischer Systeme erweitert.

»hochsensibel« geworden sei (siehe: Schutzkommission 2011, 46). Die informatorische Vernetzung kommt dabei nicht nur als zusätzlicher Zweig zu bisherigen industriellen Prozessen hinzu. Vielmehr ist die gesamte moderne Technik zunehmend auf Informationstechnologien angewiesen.

»Die hohe Abhängigkeit von IKT [Informations- und Kommunikationstechnologie, A.F.] wird in den kommenden Jahren weiter steigen. Damit werden Störungen – insbesondere bei kritischen Prozessen – zunehmend intolerabel. Die eingesetzten IKT Architekturen werden aber gleichzeitig komplexer. Damit sind sie tendenziell fehleranfälliger und störungsempfindlicher.« (ZöS 2008, 18)

Zudem wird in sozio-technischen Großprojekten wie der »Industrie 4.0« bzw. dem »Internet der Dinge« die Vernetzung zwischen technischen Geräten und IT-Funktionen immer intensiver, was neue Risiken mit sich bringt. »Die zunehmende Vernetzung von IT-Komponenten und daraus erwachsende Abhängigkeiten führen zu einer erhöhten Verletzlichkeit der eingesetzten Systeme.« (BSI 2017, 5)

Schließlich wird die Globalisierung als Grund für die Intensivierung gesellschaftlicher Vernetzung und Komplexität mobilisiert. Unter der Überschrift »Globalisierung birgt neue Risiken« stellt das *Grünbuch* des Zukunftsforums Öffentliche Sicherheit fest: »Globalisierung gilt als wichtigster Megatrend bis 2020, denn die Interdependenz von Gesellschaft wird weiter wachsen.« (ZöS 2008, 12) Und schon heute sind »globale Vernetzungen, Kopplungen und Abhängigkeiten von Wirtschaftssystemen, Waren-, Geld- und Informationsflüssen« (Allianz 2008, 43) Faktoren, die die gesellschaftliche Anfälligkeit gegenüber Katastrophen erhöhen.

Dass es sich bei den angeführten »Megatrends« um Komplexitätssteigerung, Technisierung, Digitalisierung und Globalisierung handelt, unterstreicht die Problematik bei der Sicherung vitaler Systeme. Denn die Sicherheitsprobleme ergeben sich tatsächlich aus gesellschaftlichen Trends, die sonst zumeist als Fortschritte, zumindest aber gesellschaftliche Notwendigkeiten verstanden werden. Hatte Perrow seine Diagnose über eng gekoppelte und hochkomplexe Technologiesysteme noch mit der Empfehlung verbinden können, größere Sicherheit sei nur durch den Abschied von diesen Technologien zu erreichen, so scheint diese Exit-Option hier versperrt zu sein. Denn die Prozesse und Systeme, die geschützt werden sollen, sind es gleichzeitig, die so große Sicherheitsprobleme bereiten.

### 2.4.3. Sektorspezifische Systemrisiken

Gleichwohl ist systemisches Risiko, das durch Vernetzung, Interdependenz und Komplexität ausgelöst wird, mehr als nur eine Metaerzählung über die Gegenwartsgesellschaft. Auf der Ebene einzelner Systeme oder Systemkomplexe werden gefährliche Verknüpfungen und Verwundbarkeiten adressiert und analysiert, ohne gleich auf die Ebene der Gesamtgesellschaft oder des *system of systems* zu springen. So lassen sich mittlerweile Problematisierungen systemischer Risiken und komplexer Katastrophen in einer ganzen Reihe von Bereichen identifizieren. Vernetzungsrisiken werden in Infrastrukturnetzwerken, Waren- und Lebensmittelketten, im Finanzsystem und im globalen Verkehrswesen identifiziert. Damit erscheinen systemische Risiken auf dem Radar von Sicherheitsexperten weit über den Bevölkerungsschutz hinaus. *Public Health* und nationale Sicherheit, Finanzmarktregulation und Lebensmittelkontrolle kämpfen mit ähnlichen Problemen wie der Katastrophenschutz und schreiben sich dadurch in das entstehende Sicherheitsdispositiv ein.

Die sogenannten Kritischen Infrastrukturen bilden einen zentralen Problemkomplex, der sich im Zuge der wachsenden Besorgnis um Komplexitäts- und Vernetzungsrisiken als Interventionsfeld der Sicherung vitaler Systeme herausgebildet hat. So hat die Bundesregierung eine *Nationale Strategie zum Schutz Kritischer Infrastrukturen* (BMI 2009) und zum *Schutz Kritischer Informationsinfrastrukturen* (BMI 2005) aufgelegt. Kritische Infrastrukturen umfassen sowohl klassische sozio-technische Installationen - wie Verkehrsinfrastruktur, Wasser und Strom- bzw. Energieversorgung (BMI 2009) - als auch die digitalen Netze der Informationsinfrastruktur (BMI 2005). »Kritisch« werden Infrastrukturen durch die Abhängigkeit der Bevölkerung und des gesellschaftlichen »Lebens« von ihren Diensten. Kritische Infrastrukturen sind »lebenswichtig« (BMI 2009, 7) bzw. »unverzichtbare [...] Lebensadern moderner, leistungsfähiger Gesellschaften« (BMI 2009, 2). »Kritisch« werden sie darüber hinaus aber auch durch ihre Verletzlichkeit gegenüber externen Ereignissen und gezielten Manipulationen sowie durch ihre interne Interdependenz.

»Durch die große Abhängigkeit von infrastrukturellen Dienstleistungen ist die Gesellschaft sehr verletzlich geworden, wobei diese Verletzlichkeit nicht nur durch Gefahren und Risiken von außen, sondern auch aufgrund der hohen Interdependenzen zwischen einzelnen Infrastruktursystemen im Inneren stark angewachsen ist. Die Folge von Störungen oder Ausfällen können sogenannte Domino- oder Kaskadeneffekte sein« (BMI 2009, 7).

Diese Thematisierung der Kritischen Infrastruktur rückt insbesondere die technische Vernetzung der Gesellschaft in den Vordergrund. Die physischen und technischen Verbindungen – Schienen, Glasfaserkabel, Stromtrassen etc. – sind so etwas wie der Unterbau (das lateinische *infra* heißt soviel wie »unterhalb«) des sozialen Zirkulations- und Operationsgeschehens. Physische Infrastrukturen gelten als die materiellen Manifestationen und Voraussetzungen der Funktionsfähigkeit einer globalisierten Netzwerkgesellschaft.

Die Definition Kritischer Infrastrukturen erlaubt aber eine weiterführende Interpretation, die nicht nur netzgebundene Infrastrukturleistungen und technische Infrastrukturnetze betrifft. Laut der vom Bundesinnenministerium herausgegebenen »nationalen Strategie« sind

»Kritische Infrastrukturen [...] Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.« (BMI 2009, 3)

Wie Schützer\_innen Kritischer Infrastrukturen zugestehen, ist dies eine »sehr, sehr weite und sehr offene Definition«, die aber gerade deshalb »Raum für Interpretationen auf jeder Ebene gibt« (Interview 1). Tatsächlich erlaubt es diese weite Definition, das Modell der Infrastruktur auf die gesamte Gesellschaft bzw. das »Gemeinwesen« umzulegen. In Strategien zum Schutz Kritischer Infrastrukturen werden gegenwärtig neun Kritische Infrastruktursektoren unterschieden, zu denen neben Energie, Informationstechnologie, Wasser, Verkehr und Energie auch Bereiche wie Kultur, Staat sowie Finanz- und Versicherungswesen gezählt werden. In dieser Offenheit des Topos »Kritische Infrastrukturen« – Infrastrukturen als technischer Unterbau der Gesellschaft und Gesellschaft selbst als infrastruktureller Zusammenhang – liegt die besondere Bedeutung des Schutzes Kritischer Infrastrukturen für das gegenwärtige Sicherheitsdispositiv.

Aber auch unabhängig von Strategien zum Schutz Kritischer Infrastrukturen und vom institutionalisierten Katastrophenschutz lässt sich in ganz unterschiedlichen Bereichen eine vergleichbare Problemwahrnehmung erkennen, die versucht, vitale gesellschaftliche Funktionen vor einem systemischen Kollaps zu schützen. Analoge und sich mit dem Feld des Infrastrukturschutzes auf vielfältige Weise überschneidende Probleme stellen sich etwa im Bereich der *Logistik* und der »Sicherung von Warenketten« (BMBF 2011). Weltweiter Handel, verteilte Produktionsstandorte, *outsourcing* und *just-in-time*-Produktion sorgen für eine zeitliche und räumli-

che Anspannung des Warenverkehrs. Die Sensibilität der Logistik für Unterbrechungen aller Art ist damit noch gewachsen (zum Problem der Logistik aus der Perspektive der *security studies* siehe: Lobo-Guerrero 2012, Cowen 2014).

»Mit der weiter zunehmenden Vernetzung und Komplexität der Warenketten steigt jedoch nicht nur das Angebot von Waren und Gütern. Ebenso erhöht sich die Wahrscheinlichkeit, dass lokale Störungen, wie technische Unfälle und Naturkatastrophen, aber auch Sabotageakte und Anschläge, zu längeren Unterbrechungen globaler Warenketten [...] führen.« (BMBF 2011)

Die Warenkette versammelt eine Vielzahl von Themen, Akteuren, Wirtschaftszweigen und Politikfeldern. Hafen- und Containersicherheit steht hier ebenso auf der Agenda wie der Schutz des Seehandels vor Piraterie und die Sicherung der »Lebensmittelwarenkette« (siehe: BMBF 2011). Die Risiken global vernetzter Warenketten sind Themen für den Verbraucherschutz ebenso wie für die Geopolitik. So ist die Sorge um sichere Handelswege auf globaler Ebene, die sich unter anderem in der Angst vor Piraterie zeigt, schon länger ein Thema *nationaler Sicherheit* bzw. militärischer Geopolitik. So heißt es bereits im *Weißbuch* der Bundeswehr aus dem Jahr 2006: »Deutschland, dessen wirtschaftlicher Wohlstand vom Zugang zu Rohstoffen, Waren und Ideen abhängt, hat ein elementares Interesse an einem friedlichen [...], an einem offenen Welthandelssystem und freien Transportwegen.« (BMVg 2006, 14) Daraus wird gefolgert: »Dies erfordert, Risiken und Bedrohungen für unsere Sicherheit vorzubeugen und ihnen rechtzeitig dort zu begegnen, wo sie entstehen. [...] [D]ie Überschneidungen zwischen innerer und äußerer Sicherheit [haben] zugenommen.« (BMVg 2006, 14) Hier ist die Globalisierung der grundlegende Prozess, der zur intensivierten Vernetzung, Abhängigkeit und Verwundbarkeit Deutschlands beiträgt, und zugleich ist das »Territorium«, das fortan im Sinne der nationalen Verteidigung geschützt werden muss, globalisiert. Auch das Militär orientiert sich also zunehmend am Zirkulationsraum weltumspannender Netze und nicht mehr nur am Raum des nationalen Territoriums.

Die Frage der Lebensmittelwarenketten verweist dagegen auf das größere Feld der *Lebensmittelsicherheit*, das in jüngerer Zeit immer wieder für Probleme gesorgt hat. Lebensmittelkandale von BSE bis EHEC haben Schlaglichter auf die potenziell gefährlichen Verflechtungen der Lebensmittelproduktion und Konsumption geworfen.



»Warenketten der Lebensmittelversorgung werden zunehmend international vernetzt. Entsprechend steigt die Komplexität der Warenketten und ihre Anfälligkeit gegenüber Störungen. Daher müssen Warenketten auch künftig optimal geschützt werden vor Ausfällen und Unterbrechungen sowie Kontaminationen, etwa durch Bakterien, Gifte, Metalle oder Splitter.« (BMBF 2011)

Lebensmittelsicherheit ist ein sicherheitspolitisches Schnittfeld, das eine ganze Reihe von Akteuren und politischen Themenfeldern zusammenbringt. Vor allem das Landwirtschaftsministerium, beschäftigt sich auf Bundesebene intensiv mit »Strategien der Lebensmittelsicherheit« (BMELV 2013). Die Problematisierung der »systemischen Gefährdung« der Nahrungsmittelproduktion hat dabei in jüngerer Zeit zur Konstitution einer neuen Interventionsoberfläche des Verbraucherschutzes geführt: die Lebensmittelkette. Nur die Überwachung der gesamten Kette von Lebensmittelproduktion, Distribution, Zubereitung und Konsumtion kann den komplexen Gefährdungen, die für Lebensmittelskandale verantwortlich waren, Rechnung tragen.

»[A]lle Maßnahmen zur Gewährleistung der Lebensmittelsicherheit müssen konsequent entlang der gesamten Lebensmittelkette durchgeführt werden. Denn Fehler auf einer einzigen Stufe können sich auf die ganze Kette auswirken. Ein großer Schritt in diese Richtung auf nationaler Ebene war im Jahr 2005 die Zusammenführung von Lebensmittel- und Futtermittelrecht (LFGB). Damit gilt für alle Produktionsstufen vom »Acker bis zum Teller« ein geschlossenes System an Vorschriften und Kontrollen.« (BMELV 2013, 10)

Sicherheitsprobleme entstehen durch die vielen Komponenten der komplexen sozio-technischen Passage, die ein einzelnes Nahrungsmittel »vom Acker bis zum Teller« durchschreitet. Das wird vielleicht am Beispiel der Kühlkette am deutlichsten. Tiefkühlprodukte müssen immer bei minus 18 Grad Celsius gekühlt bleiben, um potenziell gesundheitsschädigende Beeinträchtigungen der Lebensmittel zu vermeiden.<sup>78</sup> Egal ob es zu einer Einnistung von Keimen bei der Lebensmittellagerung oder einer Unterbrechung der Kühlkette kommt: immer sind die Endverbraucher betroffen. Der Mensch, der es dank seiner technischen Überlegenheit nicht nur ans Ende der »Nahrungskette« gebracht, sondern zugleich die gesamte »Le-

---

<sup>78</sup>Zum Problem der Kühlkette aus biopolitischer Perspektive siehe den spannenden Aufsatz von Friedrich und Höhne (2014).

bensmittelkette« in seine Hand genommen hat, findet sich dadurch erneut in einer prekären und bedrohten Position.<sup>79</sup>

Das Feld der Lebensmittelsicherheit ist wiederum eng mit einem anderen Themenkomplex verbunden, der mit ähnlichen Komplexitäts- und Vernetzungsproblemen zu kämpfen hat: der *Seuchenvorsorge*. Das Auftreten der zunächst rätselhaften Erkrankungen mit dem EHEC-Erreger hat nicht nur die verschlungenen Pfade und die Unübersichtlichkeit der Lebensmittelproduktion und -distribution vor Augen geführt. Es hat auch gezeigt, dass die Lebensmittelkette ein Übertragungspfad für schwerwiegende Infektionskrankheiten sein kann. Auf der Suche nach der Ursache für die sich häufenden Krankheitsfälle wurde eine wahre Schnitzeljagd initiiert, bei der zunächst spanische Gurken ins Visier der Fahnder gerieten, bis schließlich ägyptische Sprossen für die ausgebrochene Krankheit verantwortlich gemacht wurden. Als erschwerender Faktor kommt hinzu, dass gefährliche Keime auf Lebensmitteln bisweilen unempfindlich gegen die Behandlung mit Antibiotika sind, weil deren intensiver Einsatz in der industriellen Landwirtschaft zur Entwicklung resistenter Erreger beigetragen hat. Lebensmittelsicherheit heißt deshalb auch: »Verbraucher vor antibiotikaresistenten Keimen zu schützen« (BMELV 2013, 16).

Schließlich sind auch die auf Menschen übertragbaren Tierseuchen ein Schnittfeld von Lebensmittelsicherheit und Seuchenvorsorge. »Ein großes Problem sind die zunehmenden Krankheiten, die von Tieren auf Menschen übertragen werden, den so genannten Zoonosen. Die gesamte Kette vom Erzeuger bis in den Kühlschrank des Verbrauchers muss optimiert werden.« (BMELV 2013, 16) Aber auch jenseits der Bewegung von Keimen und Erregern entlang der Lebensmittelkette ist die Seuchenkontrolle ein Problem, das mit Vernetzung, Komplexität und Globalisierung zusammenhängt und damit auf eine neue Qualität der Problematik ansteckender Krankheiten im 21. Jahrhundert verweist. Neben der Angst vor bioterroristischen Anschlägen steht dabei vor allem das Phänomen der Pandemie im Zentrum der Aufmerksamkeit von Gefügen der *Biosicherheit* (zum Konzept und Feldern der Biosicherheit, siehe: Lakoff und Collier 2008). Pandemien bezeichnen im Gegensatz zur Epidemie Seuchen mit globalem Ausmaß und sehr schneller Ausbreitung (BBK 2007a, 6). Gerade Influenzapandemien, die in jüngerer Zeit im Zentrum der Aufmerksamkeit

---

<sup>79</sup>Jenseits der verstärkten Überwachung auf nationaler Ebene soll eine Reihe von internationalen Standards die Lebensmittelsicherheit und Qualität gewährleisten. Siehe dazu die ausgezeichnete Studie von Stefan Ouma (2010).

der Biosicherheit standen, sind schwer zu kontrollieren. Zum einen sind die genauen Erreger kaum vorhersehbar, weil viele Erreger schnell mutieren (der sogenannte *drift*) oder sich durch eine gleichzeitige Übertragung von Menschen zu Mensch und von Tier (insbesondere von Vögeln) zu Mensch schnell auf gefährliche Weise transformieren können (der sogenannte *shift*) (BBK 2007a, 8). Zum anderen lässt sich die Ausbreitung eines einmal an irgendeinem Ort der Welt ausgebrochenen Grippeerregers schwer verhindern. Entsprechend wird von einer »durch Reiseverkehr erhöhte[n] Ausbreitungsdynamik einer Influenza-Pandemie« (BMG und RKI 2007, 10) ausgegangen. Die mit der Globalisierung einhergehende Verflechtung von Ländern und Kontinenten, die intensiviertere Mobilität und Zirkulation von Menschen und Gütern, haben zugleich die Übertragungswege ansteckender Krankheiten vermehrt und verkompliziert (Braun 2008, Opitz 2015). Der globale »space of flows« (Castells 2010, 407) ist auch ein viraler Raum, ein Raum der Ansteckung.

#### 2.4.4. Systemische Finanzmarktrisiken

Ausbreitungsdynamiken durch Ansteckungen sind schließlich noch in einem anderen Bereich zu einem prominenten Problem geworden: der *Ökonomie*. Die Krisendynamik seit 2007, die mit der US-amerikanischen *subprime*-Krise begann (siehe etwa: Blackburn 2008), sich seit der Lehman-Pleite im Jahr 2008 zur Finanz- und dann zur Wirtschaftskrise ausgewachsen hat (siehe etwa: Arnoldi 2009), schließlich in der Euro-Krise bzw. der europäischen Staatsschuldenkrise ihre Fortsetzung fand (siehe etwa: Vogl 2015), zeigte Verlaufsmuster, die denen einer ansteckenden Krankheit, einer Kernschmelze oder einem Flächenbrand durchaus ähnlich zu sein scheinen. Solche Analogien wurden nach der Finanzkrise gleichsam als Verständnisbrücken mobilisiert, mit denen der Ratlosigkeit und dem Versagen der hegemonialen finanzwirtschaftlichen Modelle seit der Finanzkrise begegnet werden sollte. Durch den konzeptuellen Kurzschluss von Ökonomie und Katastrophenschutz hat sich die Finanzmarktregulation und die Regulation des europäischen Währungsraums nicht nur in die Dynamik des entstehenden Sicherheitsdispositivs eingeschrieben, sondern ist sogar zu dessen wesentlichem Brennpunkt geworden. Die Brisanz des Konzepts systemischen Risikos wird im Fall der Finanzregulation auch deshalb besonders sichtbar, weil es hier besonders umstritten ist: Ist das Konzept des systemischen Risikos ein besonders machtvoller Hebel der

Finanzregulation oder nur eine Entschuldigung für verantwortungslose Banken? Führen Strategien zur Vermeidung systemischer Risiken nur zum Schutz besonders großer und mächtiger Knotenpunkte oder ist eine grundlegende Veränderung der Systemarchitektur in Richtung von mehr Resilienz möglich? Lässt sich die Regulation systemischen Risikos mit den Imperativen ökonomischer Effizienz vereinbaren oder führt sie notwendig zu Profiteinbußen?

Das Konzept des systemischen Risikos in der Ökonomie und insbesondere in der Finanzwirtschaft ist schillernd und vielfältig. Immer wird hier jedoch eine Perspektive auf Risiko eingenommen, die den engen betriebswirtschaftlichen Blick transzendiert, der nur auf die Risiken einer Institution, einer Bank oder Versicherung oder gar nur eines bestimmten Wertpapiers fokussiert. Der mikroprudenzielle, also auf eine Institution begrenzte Blick auf Risiken und Finanzstabilität, wird durch eine makroprudenzielle Perspektive auf das Finanzsystem erweitert bzw. in Frage gestellt (siehe dazu das wichtige Positionspapier von: Crockett 2000). Kauffmann und Scott (2003, 371) definieren systemisches Risiko als »the risk or probability of breakdowns in an entire system, as opposed to individual parts or components, and is evidenced by comovements (correlation) among most or all the parts.«<sup>80</sup> Dabei muss ein systemisches Risiko nicht zwangsläufig durch einen großen, externen Schock ausgelöst werden,<sup>81</sup> sondern ist häufig die Folge von unkontrollierten oder unkontrollierbaren Kettenreaktionen. »[S]ystemic risk is the risk of a chain reaction of falling interconnected dominos« (Kaufman, zitiert in: Kaufman und Scott 2003, 372). Zu solchen Vorgängen kann es etwa kommen, wenn gehäufte Kreditausfälle einer Bank dazu führen, dass diese ihre Kredite an eine andere Bank nicht mehr zurückbezahlen kann, die deshalb ihre Zahlungen nicht mehr leisten kann usw. Ein sich auf diese Weise dominoartig ausbreitender Kreditausfall ist allerdings nur ein besonderer Fall für sich

---

80 Die Annahme einer Korrelation zwischen den Teilen eines ökonomischen Systems ist ein wichtiges Unterscheidungsmerkmal von Theorien systemischer Risiken. Schließlich wird in vielen Risikomodellen, die auf der Hypothese Effizienten Marktfunktionierens basieren, davon ausgegangen, dass es gerade keine Korrelation zwischen unterschiedlichen Positionen auf dem Markt gibt. Statistisch gesprochen liegt eine reine Zufallsverteilung – *randomness* – vor. Das wiederum ist gleichbedeutend mit einem Markt im Gleichgewicht. Korrelation zwischen unterschiedlichen Positionen ist demgegenüber eine Abweichung von dieser »Normalität« der Märkte.

81 Häufig wird die Kategorie des systemischen Risikos daher auch mit der des endogenen Risikos in Verbindung gebracht. Siehe hierzu: Danielsson, Shin und Zigrand (2012).

ausbreitende Stockungen in vernetzten Zahlungssystemen und Störungen der Liquidität. Die Kernoperation und die Funktion des Finanzsystems ist die Gewährleistung fortlaufenden Geldflusses. Gerät diese Funktion ins Stocken, ist schnell eine katastrophenhafte Situation erreicht. Das Bild der fallenden Dominosteine ist insofern schief, als es eher Phänomene der Unterbrechung, des Stoppens der Zahlungsoperationen sind, die eine Krise darstellen.<sup>82</sup>

Erst in der Folge der jüngsten Finanzkrise, bei der insbesondere in Folge der Lehman-Pleite die hohe Vernetzung des Finanzsektors als Quelle von Gefahren sichtbar wurde, hat das Konzept des systemischen Risikos größere Bedeutsamkeit bei der Regulation des Finanzmarktes bekommen. Dabei wurde nicht nur auf bisherige ökonomische Theorien zurückgegriffen, sondern vermehrt Inspiration in anderen Wissensfeldern gesucht – nicht nur, weil die wirtschaftswissenschaftliche *doxa* zu wenig Anschlusspunkte für die Analyse systemischer Risiken gegeben hat, sondern weil sie zudem im Verdacht steht, mit ihren eigenen Modellen derartige Risiken geradezu heraufbeschworen zu haben. So wurden etwa die Grundannahmen der *Efficient Market Hypothesis* (EMH) und deren Vertrauen in die gaußsche Normalverteilung von dem Händler und Bestsellerautor Nassim Taleb (2007) und dem Mathematiker Benoît Mandelbrot (Mandelbrot und Hudson 2006) kritisiert (siehe auch: Mandelbrot und Taleb 2010). Während die Ereignisse der Finanzkrise von EMH-basierten Modellen als extrem unwahrscheinliche *tail events* (an den äußersten Enden der Normalverteilung) angesehen werden mussten, könnten Finanzmodelle mit einer sogenannten Levi-Verteilung bessere Ergebnisse liefern, weil sie die Wahrscheinlichkeit katastrophischer Ereignisse nicht wie Normalverteilungen marginalisieren.

Ein anderes Verständnis über die Wahrscheinlichkeit bzw. die relative Normalität von Finanzkatastrophen sollte über die Theorie der »normal accidents« von Charles Perrow erreicht werden (Palmer und Maher 2010). Der Finanzmarkt erscheint hier als unglaublich komplexes und eng gekoppeltes System, das trotz – oder gerade wegen – einer Vielzahl hoch elaborierter Modelle nicht mehr von Menschen überblickt und schon gar nicht zentral gesteuert werden kann. Die Analogisierung des Finanzmarkts mit hoch-technischen Systemen, für die Perrows *Normal Accident Theory* ausgelegt war, erscheint deshalb so plausibel, weil der verstärkte Einsatz von

---

<sup>82</sup> Die Zentralität des Problems der Liquidität bei den jüngsten Versuchen zur Rettung und Regulierung des Finanzmarktes zeigt vor allem Paul Langley (2014).

Technik, Computern, automatischen Handelsmechanismen etc. eine neue Qualität der Unbeherrschbarkeit erzeugt hat. Enge Kopplungen des Finanzsystems wirken auch deshalb so gefährlich, weil sie in elektronischen Handelsformen materialisiert und automatisiert sind und deshalb tatsächlich wie eine Kettenreaktion abzulaufen scheinen, der Menschen nur hilflos zuschauen können, sofern sich die Prozesse denn überhaupt noch in wahrnehmbaren Zeitabschnitten ereignen (MacKenzie 2011). Gleichwohl ist die Anwendbarkeit der *Normal Accident Theory* auf Finanzkrisen keineswegs unumstritten. Schließlich hat diese Theorie die Tendenz, Verantwortung für Krisen auf systemische Ursachen abzuwälzen.<sup>83</sup>

Neben Mathematik und Katastrophenforschung ist die Biologie – insbesondere die Ökologie und Epidemiologie – eine dritte Inspirationsquelle für das Denken systemischer Risiken auf Finanzmärkten. Mit ihrem in der Zeitschrift *Nature* veröffentlichten Aufsatz *Systemic Risk in Banking Ecosystems* sorgten etwa der Chefökonom der Bank of England und der Ökologieprofessor Robert May für Aufsehen (Haldane und May 2011). Sie wenden sich darin gegen Vorstellungen von Stabilität, die durch größere Vernetzung der Systemkomponenten erreicht würde. Während man in der Ökologie geglaubt habe, dass eine größere Artenvielfalt und damit eine höhere Vernetzung innerhalb der Nahrungskette das Gleichgewicht und die Stabilität im Ökosystem steigert, glaube man auf dem Finanzmarkt, dass eine größere Diversifikation das Gleichgewicht eines Portfolios und letztlich auch das des Finanzsystems steigert. Beide Annahmen sind den Autoren zufolge falsch. Ab einem bestimmten Punkt erhöht größere Diversität die Abhängigkeiten zwischen den Systemkomponenten und damit auch die Wahrscheinlichkeit von Systemzusammenbrüchen, da schon der Ausfall einiger weniger Komponenten kaskadenartige Folgewirkungen haben kann. Während sich diese Erkenntnis in der Ökologie allerdings bereits durchgesetzt habe, glaube man in der Ökonomie fälschlicherweise immer noch an die Tugenden der Diversifikation und hänge immer noch an Idealen des Gleichgewichts. Anleihen bei der Epidemiologie (Cookson, Tett und Cook 2009, Haldane 2009) betonen ähnliche Zusammenhänge. Finanzkrisen können sich gerade durch die dichte Verma-

---

83 So hat Charles Perrow (2010) selbst ihre Anwendung auf die jüngste Krise explizit abgelehnt, weil ein entscheidendes Kriterium im Fall der Finanzkrise nicht erfüllt gewesen sei: alle Akteure versuchen, die Katastrophe zu vermeiden. Weil aber einige Finanzinstitutionen gezielt auf die Krise spekuliert und dann von dieser profitiert haben, ließe sich die Annahme einer »normalen Katastrophe« nicht halten.

schung des Finanzsystems schneller ausbreiten. Problematisch sind dabei besonders sogenannte *superspreaders*, die auf Grund ihrer Größe oder Stellung im Netzwerk besonders viele Finanzinstitutionen »infizieren« können, sobald sie in die Krise geraten.

Diese Anleihen bei diversen Theorien drücken weniger eine neue, kohärente Theorie- bzw. Modellbildung für den Finanzmarkt aus als vielmehr eine Suchbewegung, die vor allem versucht, die Defizite bisheriger Annahmen zu adressieren. Gemeinsam ist diesen Ansätzen allerdings ein Angriff auf das hegemoniale Denken der Normalität bzw. die normative Ordnung der Finanzökonomie. Sowohl die statistische Normalität der Normalverteilung als auch klassische Vorstellungen von Gleichgewicht werden kritisiert (siehe dazu auch: Folkers 2014, 95–99). Katastrophen werden nicht mehr als unwahrscheinliche Ausnahmen marginalisiert, sondern als normale Erscheinungen von Systemen betrachtet, denen mit Maßnahmen begegnet werden muss, die einer anderen normativen Logik folgen.

Aber nicht nur in der Fachdebatte, auch in der als Folge der Finanzkrise aufgelegten Bankenregulierung Basel III (BIS 2010) spielt »systemisches Risiko« eine zentrale Rolle. Während der Vorgänger Basel II aus dem Jahr 2004 nur Marktrisiken (durch Preisschwankungen), Kreditrisiken bzw. Kreditausfallrisiken sowie operationelle, also den eigenen Geschäftsprozess betreffende, Risiken berücksichtigte (BIS 2004), adressiert Basel III explizit »systemic risks arising from the interconnectedness of banks and other financial institutions« (BIS 2010).<sup>84</sup> Entsprechend wimmelt es von Bezugnahmen auf »banking systems« (BIS 2010), »excessive interconnectedness« (BIS 2010, 7) und »transmission channels« (BIS 2010, 2). Die komplexen Vernetzungen des Finanzsystems sind nicht nur problematisch, weil sie die schnelle Ausbreitung von Krisendynamiken bewirken, sondern auch wegen ihrer Opazität, die nicht nur die Krisenanfälligkeit des Finanzsystems weiter erhöht, sondern zudem regulatorische Gegenmaßnahmen bisweilen unmöglich macht. So problematisiert ein Dokument des Bundesfinanzministeriums:

»In den vergangenen Jahrzehnten hat die Komplexität finanzwirtschaftlicher Produkte extrem zugenommen [...]. Die Höhe und Verteilung der eingegangenen Risiken waren nicht nur für die Aufsicht, sondern auch für die Finanzmarktakteure

---

<sup>84</sup> Bei den Baseler Regularien handelt es sich um Eigenkapitalvorschriften des Baseler Ausschusses für Bankenaufsicht, einem Zusammenschluss der wichtigsten Zentralbanken mit Sitz in der Bank für Internationalen Zahlungsausgleich in Basel.

selbst immer schwerer einzuschätzen. Gerade die US-amerikanische Subprime-Krise und die daraus resultierende Bankenkrise nach dem Zusammenbruch der US-Bank Lehman Brothers haben belegt, dass Ratingagenturen die Risiken komplexer Finanzprodukte zu spät erkannt haben. Die Aufsicht konnte die Gefahren für die Stabilität der Finanzmärkte nicht rechtzeitig erfassen und keine wirkungsvolle Regulierung durchsetzen.« (BMF 2013b)

Aber trotz der massiven Problematisierung der internen Beschaffenheit des Finanzsystems ist dessen Bedeutsamkeit für Wirtschaft und Gesellschaft im Zuge der Krise eher noch stärker betont worden. Schließlich ist der Finanzmarkt auf vielfältige Weise mit der Realwirtschaft verbunden, und genau das macht die Regulation bzw. die »Rettung« des Finanzsystems in den Augen politischer Entscheidungsträger so wichtig. Der Finanzmarkt dürfe nicht zusammenbrechen, weil er eine Reihe vitaler Dienste für die gesamte Ökonomie leiste, insbesondere die Verfügbarmachung von Liquidität in Form von Krediten (Langley 2014, 178). Der Finanzmarkt wirkt hier wie eine Infrastruktur, die einen wesentlichen Rohstoff oder die wesentliche Energiequelle (Geld) in die »Realwirtschaft« pumpt und deshalb nicht zusammenbrechen darf. Selbst Staaten und damit der gesamte öffentliche Sektor sind von der Liquiditätszufuhr durch die Finanzmärkte abhängig. Diese Abhängigkeit ist mit der Euro-Krise bzw. der Staatsschuldenkrise erneut sichtbar geworden, als Länder wie Irland, Portugal, Spanien und Griechenland immer größere Schwierigkeiten bekamen, sich Geld durch Anleihenverkäufe auf dem Finanzmarkt zu beschaffen und mit Finanzhilfen der EU und des IWF vor der »Insolvenz« gerettet werden mussten. Auch im Fall dieser Krisen wurden »Ansteckungseffekte auf andere Länder der Eurozone« (BMF 2013a) befürchtet. Zudem wurde eine Ausbreitung der Vertrauenskrise befürchtet, in welche die betreffenden Staaten beispielsweise durch schlechte Kreditratings geraten sind, die wiederum die Zinsen für Staatsanleihen in die Höhe treiben (Langenohl 2015). In diesem Sinne ist also auch der Finanzsektor ein vitales System: eine für die Gesellschaft lebenswichtige Infrastruktur, die zugleich von teils intrinsischen und deshalb systemischen Risiken bedroht wird.

#### 2.4.5. Problemtransfer im Sicherheitsdispositiv

In allen diskutierten Feldern – Infrastruktur, Lebensmittelsicherheit, Seuchenkontrolle, Logistik, nationale Sicherheit, Finanzmarkt und Ökonomie – lassen sich sehr ähnliche Gefahrenwahrnehmungen feststellen. Stets geht



es um Gefährdungen, die von Komplexität und einer bisweilen »exzessiven Interkonnektivität« (BIS 2010, 7) ausgehen: die Verbindungen der Waren- bzw. Lebensmittelketten im Bereich Logistik und Lebensmittelsicherheit, die Abhängigkeiten innerhalb der Netzwerke der Infrastruktur, die Verflechtungen innerhalb des Finanzsystems. Diese Gefahren und Verwundbarkeiten sind jeweils zwar nicht vollkommen neu, erhalten aber in jüngerer Zeit eine gesteigerte Aufmerksamkeit unter Sicherheitsexpert\_innen, politischen Entscheidungsträger\_innen und in einer breiteren Öffentlichkeit. Die beachtliche Konjunktur des Sicherheitsproblems systemisches Risiko wird dabei durch die selbstverstärkende Resonanz zwischen den unterschiedlichen Bereichen zusätzlich begünstigt. Die Problematisierung ansteckender Gefährdungen wirkt ihrerseits hoch ansteckend. So kommt es zu einem regen Austausch von Konzepten und Metaphern, analytischen Verfahren und Techniken in und zwischen den Feldern. Das liegt zunächst einmal daran, dass viele Bereiche tatsächlich eng miteinander verzahnt sind: Infrastruktur und Logistik, Logistik und Lebensmittelproduktion, der Finanzmarkt, die Realwirtschaft und die Staatshaushalte etc. Genau deshalb lassen sich diese Felder auch als interdependente Systeme verstehen, die jeweils kritische bzw. vitale Dienste für die anderen leisten: ohne Geld bzw. Liquidität keine Produktion substanzieller Güter, ohne funktionsfähige Logistik und Lieferketten keine Verteilung dieser Güter, ohne Verkehrs- und Informationsinfrastruktur keine Logistik, ohne Energieinfrastruktur keine Informationsinfrastruktur, keine Produktion, kein funktionierendes Gesundheitswesen oder Finanzwesen, und ohne eine gesunde Bevölkerung, die auf ein funktionierendes Gesundheitssystem angewiesen ist, keine Aufrechterhaltung all dieser Infrastrukturen usw. usf. Dabei besteht keine klare Hierarchie zwischen den unterschiedlichen Bereichen, sondern eher eine wechselseitige Angewiesenheit. Und genau darin besteht die grundlegende Annahme bei der Sicherung vitaler Systeme: Die Gesellschaft besteht aus einer Reihe interdependenter Systeme, die aufeinander angewiesen sind und zur Aufrechterhaltung des Funktionierens des *system of systems* abgesichert werden müssen.

Tatsächlich werden aus einer solchen Logik heraus regulatorische Schnittfelder geschaffen, die explizite Verbindungen zwischen unterschiedlichen Bereichen herstellen. Auf die Frage, ob und warum Banken Kritische Infrastrukturen seien, erhielt ich in einem Expertinneninterview die Antwort: »Absolut Kritisch. Systemrelevante Banken sage ich nur.« (Interview 1) Gleichwohl gibt es keine übergeordnete Regulierungsinstanz,

die für sich beanspruchen könnte, die Sicherung vitaler Systeme aus einem Guss zu organisieren. Vielmehr existieren die Verbindungen im Modus dispositivhafter Streuung ohne übergeordnete Instanz.

Aber welche Mechanismen ermöglichen und begünstigen die Resonanzen zwischen den Bereichen? Was fördert den regen Transfer analoger Problematisierungen? Die Emergenz eines Dispositivs ergibt sich aus Affinitäten und Anschlussfähigkeiten zwischen den unterschiedlichen Bereichen sowie durch Rückkopplungen, die zu Stabilisierungen zunächst nur sporadischer Verbindungen führen. Eine erste Annäherung an das Phänomen der Ausbreitung analoger Problematisierungen bieten Rückgriffe auf Konzepte der Epistemologie. So lässt sich mit Blick auf Kuhns (1976) Wissenschaftstheorie feststellen, dass bestimmte Modelle zur Analyse systemischer Gefährdungen in jüngerer Zeit einen paradigmatischen Wert über ihr jeweiliges Gebiet hinaus erhalten haben. Kuhn (1976, 68–78) hatte argumentiert, dass sich wissenschaftliche Paradigmen nicht deshalb ausbreiten, weil die Forscher\_innen Regeln folgen, sondern weil sie sich an den als beispielhaft angesehenen Stilen anderer Wissenschaftler\_innen orientieren. Übertragen auf das Sicherheitsdispositiv lässt sich argumentieren, dass sich Sicherheitsexpert\_innen an den als beispielhaft angesehenen Problematisierungen anderer Sicherheitsexpert\_innen orientieren. Es geht also nicht unbedingt darum, dass Akteure formale Vorgehensweisen oder Bestimmungen übernehmen, sondern eine »Familienähnlichkeit«<sup>85</sup> der Probleme in anderen Feldern mit den eigenen Schwierigkeiten feststellen. Begünstigt wird dies dadurch, dass die analytische Einheit »System« ohnehin eine »trading zone« (Galison 1996) darstellt, die die Kompatibilitätswahrscheinlichkeit bzw. den Anschlusswert disparater Forschungsfelder erhöht. Teilweise wird der Transfer von einem Feld in das andere von konkreten Expert\_innen oder »Grenzgänger\_innen« realisiert, die in anderen Feldern »epistemologische Hindernisse« (Bachelard 1974, 170ff.) identifizieren, die in ihrer eigenen Disziplin bereits überwunden sind. Ein Beispiel dafür ist der Biologe Robert May, der mit Andrew Haldane über die Finanzkrise geschrieben hat: »The more I hear about financial economics, the more I am struck by its similarity to ecology in the 1960s.« (May zitiert nach: Cookson, Tett und Cook 2009, Haldane 2009)

---

85 Kuhn (1976, 70f.) bezieht sich explizit auf das Konzept der Familienähnlichkeiten bei Wittgenstein, der ebenfalls argumentiert hatte, dass die Fähigkeit, die Ähnlichkeit einer Gruppe von Sachverhalten (etwa Stühlen) zu erkennen, auf der intuitiven Fähigkeit basiert, Analogien zu erkennen.

Die Akzeptanz eines alternativen Paradigmas steigt zudem, wenn durch das Paradigma nicht nur andere Beschreibungen eines bestimmten Sachverhalts (in diesem Fall einer Krise oder Katastrophe) möglich werden, sondern wenn das alternative Paradigma auch in Aussicht stellen kann, systematische Leerstellen oder blinde Flecken vorherrschender Modelle zu beseitigen. Ein Paradigmenwechsel, so argumentierte schon Kuhn (1976, 79–109), ereignet sich nämlich zumeist dann, wenn hartnäckige Anomalien auftreten, die auf der Grundlage bestehender Theorien nicht erklärt werden können. Derartige Anomalien können in den Verwerfungen während der Finanzkrise gesehen werden, die die meisten Risikomodelle eigentlich für geradezu unmöglich gehalten hatten. So bemerkte ein Händler damals frustriert: »Events that models only predicted would happen once in 10.000 years happened every day for three days.« (Mathew Rotham zitiert nach: Blackburn 2008, 99) Besonders nachhaltig kann eine solche Argumentation verfangen, wenn zusätzlich gezeigt werden kann, dass die falschen Annahmen nicht nur ein angemessenes Verständnis der Risiken verhindert haben, sondern Risiken durch die Annahmen und ihre Umsetzung in operativen Modellen überhaupt erst erzeugt wurden. Gerade in der Analyse der Finanzkrise wurden nicht nur die epistemologischen Annahmen, sondern auch die performativen Effekte von Finanzmodellen kritisiert – mitunter, wie bei Cookson, Tett und Cook (2009), unter expliziter Bezugnahme auf die *performing markets*-Literatur der *Social Studies of Finance* eines Donald MacKenzie (2006).<sup>86</sup>

Jenseits dieser epistemischen Transferleistungen lassen sich strategische Bezugnahmen auf andere Bereiche ausmachen, die ebenfalls zur Ausbreitung einer bestimmten Sicherheitslogik beitragen. Die Bezugnahme auf bereits durchgesetzte Regulationen in anderen Bereichen erhöht die Plausibilität für intendierte Maßnahmen. So berichtete mir eine Mitarbeiterin im BBK mit Zuständigkeit für Kritische Infrastrukturen über den Sinn von Bezugnahmen auf Regulation in anderen Bereichen:

---

86 In seinem weit über die sozialwissenschaftliche Diskussion hinaus berühmt gewordenen Buch *An Engine not a Camera* hatte MacKenzie im Anschluss an Michel Callon (1998) argumentiert, dass die moderne Finanztheorie Marktgeschehen nicht nur abbildet, sondern performativ hervorbringt. Dabei hat er auch auf die Möglichkeit der »counterperformativity« (MacKenzie 2004, 306) hingewiesen, bei der Finanzmodelle das Gegenteil dessen bewirken, was sie voraussagen.

»Im Basis-Schutzkonzept,<sup>87</sup> das ja relativ früh – 2005 – entstanden ist, haben wir mangels anderer Überzeugungsmechanismen eben beispielsweise auf das Aktiengesetz zurückgegriffen oder auch damals auf Basel II, jetzt wäre es Basel III, bzw. auf das Kreditwirtschaftsgesetz. Oder die so genannte MaRisk, die für die Banken von der BaFin<sup>88</sup> hier erstellt wird, zumindest Anleitungen im Bereich des Risikomanagements Banken. Grund war der: auch Überzeugungsarbeit, Sensibilisierungsarbeit.« (Interview 1)

Dabei geht es den Akteuren nicht primär um die Verbreitung einer bestimmten Sicherheitsrationalität. Vielmehr adressieren sie lokale Hindernisse und Widerstände, schaffen damit aber zugleich die »kapillaren« Verbindungswege, über die sich eine bestimmte Machttechnologie ausweiten kann. Sie verfolgen dabei bewusst ihre Interessen in einer strategischen oder taktischen Absicht. Dennoch ist die Emergenz des Dispositivs der Resilienz nicht auf ihre Strategien zurückzuführen, weil sich dieses nur über die Verkettungen bildet und damit ein Effekt ist, der von niemandem intendiert und bewerkstelligt werden kann.

»Die Machtbeziehungen sind gleichzeitig intentional und nicht-subjektiv. [...] Die Rationalität der Macht ist die Rationalität von Taktiken [...], die sich miteinander verketten, einander gegenseitig hervorrufen und ausbreiten, anderswo ihre Stütze und Bedingung finden und schließlich zu Gesamtdispositiven führen: auch da ist die Logik noch vollkommen klar, können Absichten entschlüsselt werden – und dennoch kommt es vor, daß niemand sie entworfen hat und kaum jemand sie formuliert: impliziter Charakter der großen anonymen Strategien, die, nahezu stumm, geschwätzige Taktiken koordinieren« (Foucault 1977, 116).

## 2.5. *Norm*: Resilienz als Antwort auf systemische Gefährdung

Wenn Sicherheit in der reibungslosen Funktion von Systemen besteht, vitale Systeme also zum zentralen Schutzobjekt des Sicherheitsdispositivs geworden sind, diese Systeme aber zugleich ein intrinsisches Gefährdungspotenzial – systemisches Risiko – aufweisen, dann müssen Sicherheitstech-

---

<sup>87</sup> Gemeint ist: BMI, BBK und BKA (2005).

<sup>88</sup> MaRisk steht für »Mindestanforderungen an das Risikomanagement« für Banken, die von der Bundesanstalt für Bankenaufsicht (BaFin) erstellt und kontrolliert werden. Dabei handelt es sich um Konkretisierungen von internationalen Regulierungen – wie den Baseler Eigenkapitalvorschriften – oder von nationalen Regelwerken wie dem Kreditwesengesetz.

nologien versuchen, dieses Gefährdungspotenzial zu reduzieren. Techniken, die bloß darauf zielen, externe Gefahrenquellen abzuhalten, reichen nicht mehr aus, weil auch kleinste und niemals gänzlich abwendbare Störquellen systeminterne Dynamiken in Gang setzen können, die zu Katastrophen eskalieren können. Demgegenüber bietet die Arbeit am und im System einen Ansatzpunkt für dessen Sicherung im Angesicht unbestimmter Gefährdung. Negativ formuliert werden solche am System ansetzende Sicherheitsmaßnahmen – etwa die Auflösung zu enger systemischer Kopplungen – als Verwundbarkeitsreduktion gefasst. Gerade in Bezug auf die Sicherheit von vitalen Systemen wird jedoch häufig auch positiv von der Steigerung der Resilienz gesprochen, um die Gesellschaft und ihre Systeme »widerstandsfähiger und krisenfester (resilienter)« (ZÖS 2008, 44) zu machen.

Resilienz hat hier einen interessanten Doppelstatus. Einerseits findet sich eine Reihe von Sicherheitstechnologien, die sinnvoll als Maßnahmen zur Erhöhung systemischer Resilienz beschreibbar sind. Resilienz ist insofern eine *Technologie* zur Kontrolle systemischer Risiken und zur Regierung der Katastrophe. Zugleich kann in Resilienz aber auch ein *telos*, ein neues normative Leitbild der Sicherheit gesehen werden. Resilienz steht nicht nur für Mittel zur Erhöhung der Sicherheit, sondern ebenso für ein alternatives Sicherheitsverständnis. Sicherheit ist diesem Verständnis zufolge weniger ein Zustand der Abwesenheit von Gefahr, sondern vor allem ein Prozess der erfolgreichen Reaktion auf und der ständigen Anpassung an eine sich ständig verändernde Gefahrenumwelt. Es ist diese doppelte Bedeutung von Resilienz als Sicherheitstechnologie, die nicht nur Instrumente für ein gegebenes Ziel liefert, sondern zugleich eine Verschiebung der Zielvorgabe bewirkt, welche die Schlüsselrolle von »Resilienz« im kontemporären Sicherheitsdispositiv konstituiert.

In den Debatten der *Critical Security Studies* und der *Studies of Governmentality* finden sich sehr unterschiedliche Einschätzungen über das Konzept und die Praktiken der Resilienz. Während einige Autor\_innen in der Resilienz eine Alternative zum »Big Brother State« sehen (Lentzos und Rose 2009, 243), erkennen andere in Resilienz die Strategie eines verantwortungslosen Neoliberalismus, der nicht mehr bereit ist, für die Sicherheit seiner Bürger zu sorgen (Amin 2013, Joseph 2013), oder gar einen »neoliberalen Katastrophismus«, der Zerstörungen und ökonomische Ungleichgewichte als schöpferisch-kreative Momente bewusst in Kauf nimmt (Cooper und Walker 2011, Cooper 2011). Das Problem dieser häu-

fig allzu pauschalen Einschätzungen über Laster und Tugenden der Resilienz besteht darin, dass hier jeweils nur eine spezifische Artikulation der Resilienz in einem spezifischen Zusammenhang in den Blick genommen wird. Was Resilienz in der gegenwärtigen Ökologie der Sicherheit jedoch vor allem kennzeichnet, ist ihre unscharfe Definition und Offenheit für unterschiedlichste Applikationen. Nur deshalb konnte Resilienz, wie Stefan Kaufmann (2012) argumentiert, zum »boundary object« werden, das flexibel in unterschiedlichen Feldern der Sicherheitspolitik wirksam wird.

Um in dieser Arbeit zu einer differenzierteren Einschätzung zu gelangen, möchte ich im Folgenden unterschiedliche Varianten und Strategien der Resilienz beleuchten. Zunächst werde ich kurz auf die Genese des Konzepts in der Systemökologie eingehen, um zu zeigen, welche epistemischen und normativen Denkweisen mit Resilienz verknüpft sind (2.5.1.). Sodann möchte ich zeigen, wie sich dieses normative Leitbild der Resilienz aktuell in unterschiedlichen Maßnahmen materialisiert und dadurch zur eigenständigen Sicherheitstechnologie wird. Hierbei lässt sich zwischen dem Vorhalten von Notfallreserven und operativen Ressourcen zur Notfallbewältigung (2.5.2.) und Maßnahmen zur Neuausrichtung der Architektur oder Struktur der Systeme (2.5.3.) unterscheiden. Zudem lässt sich ein Verständnis von Resilienz als evolutionäre Adaptivität identifizieren, das eine Abkehr von der Zielvorstellung der Sicherheit als Zustand der Gefahrlosigkeit impliziert (2.5.4.). Ich werde dabei zeigen, dass diese drei Varianten der Resilienz (Vorhaltung von Ressourcen, Veränderung des Systemdesigns, Adaptivität) in verschiedensten Bereichen – von der Finanzwirtschaft bis zur Seuchenbekämpfung – in Anschlag gebracht werden. Schließlich werde ich im Rückblick auf die seit dem 11. September getroffenen Maßnahmen zur Regierung der Katastrophe nachzeichnen, dass ein neues Sicherheitsdispositiv, das Dispositiv der Resilienz, entstanden ist (2.5.5.).

### 2.5.1. Von der Normalität zur Normativität: Resilienz bei Holling

Zu Recht wird der Biologe Crawford Holling immer wieder als maßgeblicher Wegbereiter für die Ausarbeitung des Konzepts systemischer Resilienz genannt (Cooper und Walker 2011, Kaufmann 2012, Nelson 2014).<sup>89</sup>

---

<sup>89</sup> Gewiss ließen sich weitere Vorläufer für ein Denken der Resilienz finden. So gibt es eine Reihe von Kontexten – von der Materialforschung bis zur Traumapsychologie –, in de-

Bereits in den frühen 1970er Jahren hatte er begonnen, die Bedingungen für die Integrität und Kontinuität von Ökosystemen mit dem Begriff der Resilienz zu beschreiben. Als Vertreter der Systemökologie unterscheidet sich sein Ansatz vor allem von populationsökologischen Perspektiven (Lindseth 2011). Holling hat sich nämlich nicht primär mit der Konstanz und Quantität von Populationsbeständen befasst. Ihm ging es vielmehr um die schiere Existenz einer Art oder eines Ökosystems:

»Individuals die, populations disappear, and species become extinct. That is one view of the world. But another view of the world concentrates not so much on presence or absence as upon the numbers of organisms and the degree of constancy of their numbers.« (Holling 1973, 1)

Sein Ansatz unterscheidet sich damit vom Denken der Normalität, das laut Foucault (2004, 88ff.) typisch für das im 19. Jahrhundert entstandene Sicherheitsdispositiv war. Schließlich bezogen sich das Denken des Normalen und die Technologien der Normalisierung im 19. Jahrhundert zentral auf die Figur der Bevölkerung. Anders als bei der Normalisierung geht es bei Resilienz nun aber nicht mehr um vornehmlich quantitative Fragen der Häufigkeit, der relativen Distanz zum Mittelwert, der erwartbaren Wiederholung eines Verhaltens etc. Entscheidend sind vielmehr die Relationen eines Systems, dessen grundlegende Strukturmerkmale. »But if we are dealing with a system profoundly affected by changes external to it, and continually confronted by the unexpected, the constancy of its behavior becomes less important than the persistence of its relationships.« (Holling 1973, 1) Dieser Fokus auf die Persistenz der Relationen eines Systems führte Holling zu seiner Bestimmung von Resilienz als »measure of the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables.« (Holling 1973, 14) Resilienz ist also ein Maß für die Beständigkeit, Widerstandsfähigkeit und Toleranz eines Systems gegenüber externen Ereignissen, die Fähigkeit, trotz Störungen und Unregelmäßigkeit bestehen zu bleiben. Mit »Beständigkeit« ist dabei gerade kein Gleichbleiben – etwa von Bestandszahlen – gemeint, sondern die Fähigkeit, sich an Irritationen anzupassen und im besten Fall sogar von ihnen zu »lernen«. Resilienz verbindet, wie Holling (2001, 399) später formulieren sollte, »learning with

---

nen sich das Konzept relativ unabhängig von Holling entwickelt hat. Zudem lassen sich andere Denkformen identifizieren, die, ohne den Begriff zu verwenden, große Ähnlichkeiten mit dem Konzept der Resilienz aufweisen.

continuity.« Anders als es die Etymologie des Wortes (*resilieri* ist das lateinische Wort für »zurückprallen«) oder das häufig bemühte Bild des Stehaufmännchens zur Veranschaulichung des Konzepts nahelegen würden, ist Resilienz bei Holling gerade nicht die Fähigkeit eines Systems, nach einem Schock zum *status quo ante* zurückzukehren, sondern die Fähigkeit, durch Transformationen bestehen zu bleiben. Es geht nicht um die Rückkehr zum Gleichgewicht, sondern um einen Entwicklungs- und Anpassungsprozess.

Den dynamischen Aspekt der Widerstandskraft von Ökosystemen betont Holling auch mit seiner Unterscheidung zwischen Resilienz und Stabilität. Letztere steht für die »ability of a system to return to an equilibrium state after a temporary disturbance; the more rapidly it returns and the less it fluctuates, the more stable it would be« (Holling 1973, 14). Gegen die Stabilitätsperspektive argumentiert Holling, dass es in einem komplexen Ökosystem nicht nur einen, sondern mehrere mögliche Gleichgewichtspunkte bzw. »multistable states« (Holling 1996, 38) gibt. Auch größere Störungen – zum Beispiel Waldbrände, Schädlingsbefall – sind zwar aus einer Stabilitätsperspektive schädlich, können der Resilienz des Systems jedoch zuträglich sein, wenn dadurch beispielsweise die Diversität des Baumbestandes eines Waldes erhöht wird (Holling 1973, 15f.). Die Selbstheilungskräfte eines Systems bestehen folglich vor allem darin, dass es in Auseinandersetzungen mit der Umwelt neue Normen entwickeln kann.<sup>90</sup> Resilienz weist damit mehr Ähnlichkeiten mit dem von Georges Canguilhem geprägten Konzept der »biologischen Normativität«<sup>91</sup> – das

---

90 Damit geht Resilienz über Homöostase hinaus. Homöostase bezeichnet schließlich lediglich die Mechanismen, die es einem Organismus oder System ermöglichen, zu einem Gleichgewicht bzw. präferierten Sollwert zurückzukehren. Das Konzept der Homöostase wurde bereits im 19. Jahrhundert durch den Biologen Claude Bernard geprägt, auch wenn er diesen Begriff noch nicht verwendete (siehe dazu: Canguilhem 1979, 101–106).

91 Im Kern von Canguilhems Konzept der biologischen Normativität steht die Auffassung, dass das »Leben den Bedingungen gegenüber, unter denen es möglich ist, nicht indifferent bleibt, daß es vielmehr Polarität und damit eine unbewusste Wertsetzung enthält, mit anderen Worten, daß das Leben letztlich eine normative Aktivität ist. In der Philosophie versteht man unter *normativ* jedes Urteil, das ein Faktum von einer Norm her wertet oder qualifiziert; dieses Urteilen aber wird eigentlich jenem anderen untergeordnet, welches die Normen setzt. In seiner vollen Bedeutung heißt *normativ*: das Normen Setzende. In genau diesem Sinne sollte man unserer Ansicht nach auch von einer biologischen Normativität sprechen.« (Canguilhem 1977, 82) Ähnlich gelagert ist das Konzept der Metastabilität von Canguilhems Schüler Gilbert Simondon (1992, 302), der den »metastable states« vom »stable equilibrium« unterschieden hatte.



kreative Setzen von Normen – auf als mit der Normalität statistischer Durchschnittswerte, Normalverteilungen und Gleichgewichtszustände, an der sich laut Foucault die Sicherheitsdispositive seit dem 19. Jahrhundert orientiert haben. Das eigentliche Problem besteht aus dieser Perspektive dann auch nicht im Ungleichgewicht oder der Abweichung von der Norm, sondern im Zugrundegehen des Systems.

Holling weist die Stabilitätsperspektive aber nicht nur aus wissenschaftlichen Gründen zurück. Vor allem richtet er sich gegen die seiner Meinung nach fatalen Effekte der Orientierung an Stabilität im Umweltmanagement. Stabilität ist für ihn kein angemessenes Konzept für Ökolog\_innen, sondern eher das Leitbild von Ingenieur\_innen, weshalb er später »Stabilität« auch als »engineering resilience« (Holling 1996) bezeichnet hat. Die Stabilitätsorientierung der »engineering resilience« legt der Natur eine ihr fremde normative Ordnung auf, die sich nicht am Erhalt und der Selbstregulationsfähigkeit des Systems selbst, sondern nur auf einen sozialen und ökonomischen Planungshorizont bezieht. Dazu werden zum Beispiel Monokulturen angelegt, weil es so leichter ist, konstante Bestandszahlen beizubehalten. Kurzfristig kann diese Strategie Erfolg haben und die Stabilität des Systems erhöhen. Langfristig wird das System allerdings verwundbarer gegenüber externen Schocks. Die Resilienz schwindet gerade mit der Produktion wachsender Stabilität. »Short-term success in stabilizing production leads to long-term surprise« (Holling 1996, 37). Aus der Perspektive der Norm der Resilienz führt der planerische Eifer, der sich an einem technischen Optimum orientiert statt an den »multistable states« (Holling 1996, 38) der Natur selbst, zu adversen Effekten.

Holling fordert gleichwohl nicht, die Natur sich selbst zu überlassen. Er fordert einen anderen Managementansatz, der nicht nur den augenblicklichen Normen, sondern der normsetzenden Aktivität der Natur, also der Resilienz, Rechnung trägt. Statt technischem Planungseifer, der sich den »myth[s] of manageability« (Holling zitiert nach: Wildavsky 1988, 82) hingibt, empfiehlt Holling einen »management approach based on resilience«. Dieser Management-Ansatz entfernt sich auch von der Wissensordnung planerischer Idealvorstellungen. Weil die Zukunft stets ungewiss sei, dürfe man nicht vom falschen Ideal der »sufficient knowledge« ausgehen, sondern müsse im Wissen um das eigene Nicht-Wissen – in »recognition of our ignorance« (Holling 1973, 21) – handeln.

Mit seiner Konzeption der Resilienz hat Holling also nicht nur in das wissenschaftliche Feld der Ökologie wirken wollen, sondern immer auch

politische Absichten verfolgt. Im Namen der Selbstregulationsfähigkeit ökologischer Systeme formuliert Holling eine Kritik an technischer Planung, Stabilitätsdenken und der Überschätzung des Wissens über die Zukunft. Er kritisiert die immer noch zu große Künstlichkeit von Stabilitätsnormen und weist auf die Grenzen des Wissens hin: Weder weiß man genau über Schockereignisse in der Zukunft Bescheid, noch kann man genau wissen, zu welchen Anpassungsleistungen das System imstande ist. Und schließlich betont er die perversen Effekte einer Planung, die die natürlichen normativen Ordnungen und die Grenzen des Wissens nicht ausreichend beachtet. Das Konzept der Resilienz transportiert damit sowohl eine neue konzeptuelle Norm für die Regulation von ökologischen (und bald auch technischen, ökonomischen und sozialen) Systemen als auch einen Maßstab der Kritik an bisherigem Sicherheitshandeln. Diese Kritik weist interessante Parallelen zur (neo)liberalen Kritik an staatlicher, zentraler Planung auf: am zuviel Regieren der Wirtschaft, an den »Präventionen des Wissens« (Hayek 1989) und den perversen Effekten von »künstlichen« Eingriffen in das selbstregulierende Marktgeschehen.<sup>92</sup> Insofern ist die immer wieder – von Kritiker\_innen wie auch Sympathisant\_innen der Norm der Resilienz – festgestellte Analogie von ökologischem Resilienzdenken und neoliberaler Wirtschaftstheorie (Wildavsky 1988, 79, Cooper und Walker 2011) durchaus zutreffend. Darüber darf allerdings nicht die Spezifik und Eigenlogik der Einsätze der ökologischen und der neoliberalen Kritik des Regierens übersehen werden. Denn trotz analoger Motive und ähnlicher Angriffspunkte verfolgen etwa die ökologische Kritik Hollings und die neoliberale Kritik Hayeks ganz unterschiedliche Ziele: einmal Umweltschutz, einmal freies Wirtschaften. Es ist daher zu pauschal, Holling vorschnell als »neoliberal« abzutun. Nicht zuletzt, weil dadurch die Offenheit und die kritischen Potenziale seines Resilienzkonzepts übersehen würden.<sup>93</sup>

---

92 An anderer Stelle habe ich im Anschluss an Foucault argumentiert, dass der Neoliberalismus in einer langen Tradition epistemischer und technischer Kritik der Regierung steht (Folkers 2016, 12–17). Allerdings stehen ebenso progressive Kritiker technokratischer Regierungsweisen – etwa aus der Frauen- und Alternativbewegung – in dieser Traditionslinie. Im Folgenden – insbesondere in den Kapiteln 3.2.1., 3.3.2. und 3.3.2. – werde ich die Ähnlichkeiten und Differenzen von ökologischer und neoliberaler Kritik weiter beleuchten.

93 So hat Sara Nelson (2014) überzeugend argumentiert, dass das Resilienzkonzept nicht per se neoliberal ist, sondern lediglich einer »neoliberal counterrevolution« zum Opfer

Hollings Resilienzkonzept ist aber nicht nur an bestimmte Kritiken des Regierens und der Sicherheit anschlussfähig, sondern vor allem an Debatten und Sicherheitsbemühungen in einer Vielzahl gesellschaftlicher Bereiche. Sein systemtheoretischer Ansatz ermöglicht den relativ einfachen Transfer des Resilienzkonzepts in den Bereich der Reaktion auf systemische Risiken. Heute spricht man auch im Finanzwesen und bei der Infrastruktursicherung<sup>94</sup> von Resilienz. Resilienz ist dadurch zum »boundary object« im Sicherheitsdispositiv geworden. Daran war nicht zuletzt Holling selbst beteiligt, der immer wieder auf die Übertragbarkeit seines Konzepts auf komplexe soziale und ökonomische Systeme hingewiesen hat (siehe etwa: Holling 2001). Zugleich ist die Tatsache, dass Holling bereits 1996 seine Unterscheidung von Stabilität und Resilienz zugunsten der Unterscheidung von *engineering resilience* und *ecological resilience* aufgegeben hat, ein Hinweis darauf, dass der Erfolg seines Konzepts auch Interpretationen Raum gegeben hat, die nicht in seinem Sinne waren. Wenn ein Konzept durch unterschiedliche Bereiche und Anwendungsbereiche »wandert«, bleibt es nicht unverändert. Mittlerweile findet sich eine Vielzahl von Artikulationen, Spielarten und Technologien der Resilienz, die das Regieren von Katastrophen und systemischen Risiken in unterschiedlichen Bereichen anleiten.

### 2.5.2. Reserven, Puffer, Redundanzen: Resilienz durch Vorratshaltung

In eine erste Gruppe von Maßnahmen der Resilienzsteigerung lassen sich Vorbereitungsstrategien gruppieren, bei denen schützende Ressourcen für mögliche und nicht gänzlich vermeidbare Notfälle vorgehalten und aufgebaut werden. Gewiss hat diese Strategie nicht erst auf die Emergenz eines elaborierten Resilienzverständnisses warten müssen. Schließlich wissen wir schon aus den Josef-Erzählungen der Bibel, dass das Anlegen von Vorräten hilft, um Krisenzeiten zu überstehen. Allerdings sind die »Ressourcen«, die heute angehäuft werden, und auch die Strategien und Rationalitäten der Lagerhaltung andere als im Ägypten des Alten Testaments. Zudem kommt der alten Technik der Lagerhaltung bei Technologien der Resilienz eine

---

gefallen sei. Anstatt Resilienz pauschal zu kritisieren, fordert sie, Resilienz wieder als »critical tool« gegen diese Konterrevolution in Stellung zu bringen.

94 In Kapitel 3.3.2. werde ich auf die Ausarbeitung des Resilienzkonzepts im Kontext der Problematik der Energiesicherheit durch Amory Lovins und Hunter Lovins Anfang der 1980er Jahre eingehen.

neue Rolle zu, insofern sie die Operationen eines abstrakten Systems aufrechterhalten soll und nicht vorrangig Nahrung für eine hungernde Bevölkerung vorhält.<sup>95</sup> Damals wie heute gilt jedoch: Sicherheit ist immer auch eine Frage der Reserve, der verfügbaren Ressourcen und Materialien. Das Anlegen von Notfallreserven ist stets ein Vorsorgehandeln, was schon durch die Etymologie des deutschen Wortes Vorrat verbürgt ist. Vorrat kommt vom mittelalterlichen Vor-bedacht und ist insofern eine Materialisierung der Vorausschau und Vorsorge. Die Sicherungsfunktion von Lagerbeständen liegt letztlich darin, dass sie Beständigkeit in unbeständigen Zeiten gewährleisten können. Michel Serres argumentiert entsprechend, dass Vorratshalden Orte darstellen, an denen die Zeit geradezu eingefroren ist.

»What do we stockpile, squirrel-like? Power, before using it: dry-cell and storage batteries; dams. Money: bank accounts, insurance, capital. Codes: libraries, computer memory, data banks. Food: cold rooms for meat or fruit, grain silos, dark cellars. Sperm, oocytes, embryos. Time does not always flow. We can find or excavate places where it has frozen.« (Serres 2008b, 179)

Die gefrorene Zeitlichkeit der Lagerbestände ist damit geradezu das Gegenbild zur Flüssigkeit sozio-technischer Operationen, die es zu sichern gilt. Damit sind Konflikte zwischen der sichernden Funktion von gefrorenen und damit der Zirkulation entzogenen Beständen und flüssigen, aber gleichzeitig störanfälligen Prozessen geradezu vorprogrammiert.

Redundante Ressourcen können dabei je nach Feld Notstromaggregate (bei der Sicherung der Infrastruktur),<sup>96</sup> Eigenkapitalpuffer (im Finanzsektor), Arzneimittel (bei der Seuchenkontrolle) oder Mikrofilme (beim Schutz von Kulturgut)<sup>97</sup> sein. Derartige Vorkehrungen werden natürlich nicht nur im Hinblick auf systemische Risiken getroffen. Aber sie werden hier besonders bedeutsam. Denn im Falle vitaler Systeme soll durch diese Vorhaltungsmaßnahmen sowohl ein eingetretener Schaden abgefedert als auch dessen weitere Ausbreitung verhindert werden. Entsprechende Redundan-

---

95 Tatsächlich hält die Bundesrepublik aber auch Lebensmittel für den Kriegs- und Katastrophenfall vor. »In der ›Bundesreserve Getreide‹ lagern Getreide, wie Weizen und Hafer, sowie in der ›Zivilen Notfallreserve‹ Reis, Hülsenfrüchte, Vollmilchpulver und Kondensmilch.« (TAB 2011, 216f.)

96 Ausführlicher gehe ich auf Notstromversorgungssysteme und die besondere Rolle von Vorratshaltung bei der Sicherung des Stromsystems in Kapitel 3.3.5 ein.

97 Zum Schutz von Kulturgut durch die sogenannte »Sicherungsverfilmung« siehe: BBK (2010e).

zen können damit unmittelbar als Notfallreserven, aber gleichzeitig auch als Brandmauern oder *shock absorber* verstanden werden, wie ich sogleich anhand der drei Bereiche Schutz Kritischer Infrastrukturen, Finanzmarkt-sicherung und Seuchenkontrolle zeigen werde.

Die Logik der Resilienzsteigerung durch den Aufbau zusätzlicher Kapazitäten bzw. »effiziente[r] Redundanzen« (BMI 2009, 10) für den Notfall findet sich vor allem im Bereich des *Schutzes Kritischer Infrastrukturen*. Vorkhaltung von strategischen Ölreserven zum Schutz der Energieversorgung, die durch das Erdölbevorratungsgesetz geregelt ist (TAB 2011, 25), Notstromaggregate zur Gewährleistung der Elektrizitätsversorgung bei Stromausfällen (BBK 2008b) und Datensicherung durch *backup* bei kritischen Informationsinfrastrukturen (BMI 2005, 16) sollen ebenso wie Ausweichstandorte von Organisationen wie Banken, Versicherungen und staatlichen Behörden (BSI 2008, 112)<sup>98</sup> oder ein weitverzweigtes Schienen- und Straßennetz verhindern, dass der Ausfall vitaler Infrastruktursysteme und Versorgungsströme zur Katastrophe wird. Infrastrukturen sind »matter that enable the movement of other matter« (Larkin 2013, 329). Als Systeme sind Infrastrukturen also nur dann operationsfähig, wenn beide Arten von *matter* ausreichend und für den Krisenfall redundant vorhanden sind: sowohl die materiellen Strukturen als auch die durch sie zirkulierten Dinge. Reserven bestehen dabei idealerweise sowohl im Hinblick auf die Netze der Zirkulation – Straßen, Pipelines, Stromnetze etc. – als auch auf die Reserven bei den Gütern, Materialien, Rohstoffen und Informationen. Eine resiliente Infrastruktur umfasst sowohl Netze der Zirkulation als auch Orte, an denen Reserven versammelt werden und auf Abruf bereit stehen. Speicher, Lager und Server (die *stocks*) sind ebenso wichtig wie Netze, Kabel und Schienen, die die *flows* ermöglichen. Damit ständig alles im Fluss sein kann, muss der Zirkulation immer auch etwas entzogen und gespeichert werden.

Aber auch bei der *Sicherung des Finanzsystems* gegen systemische Risiken geht es darum, ein angemessenes Verhältnis von Zirkulation und Reserve zu etablieren. Das zirkulierende und vorzuhaltende Gut ist hier verfügbares Kapital. Das wurde während der Finanzkrise deutlich, als zunächst die US-amerikanische Bank Lehmann Brothers zahlungsunfähig wurde. Lehmanns Zahlungsunfähigkeit führte zum Ausfall von Zahlungen, die bei anderen Banken zu Buche schlugen. Verunsicherung breitete sich aus, was zum

---

<sup>98</sup> Zur Frage der Ausweichstandorte im sogenannten *Business Continuity Management* siehe Kapitel 4.

kompletten Zusammenbruch des Interbankkredithandels führte. Diese »Kreditklemme« – Banken liehen sich untereinander kein Geld mehr – manifestierte dann endgültig die Finanzkrise, die nicht nur eine Krise war, weil sie zu Verlusten führte, sondern weil sie kurzfristig das Operieren des Finanzsystems unterbrochen hatte und damit einen zentralen Faktor der ökonomischen Autopoiesis nachhaltig beschädigte (Arnoldi 2009, Esposito 2011, Folkers 2013a). Die Stockung des weitverzweigten Zahlungsflusses, die Gerinnung oder Austrocknung eines Systems, das im Kern ein kontinuierliches Strömen ist, führte zur Katastrophe. Anders als bei einem Atomreaktorunfall kann der finanzielle *meltdown* nicht durch eine abrupte Unterbrechung der Operationskette aufgehalten werden, weil genau diese Unterbrechung den eigentlichen Katastrophenfall darstellt. »Liquiditätsprobleme«, so bemerkte schon Luhmann (2003, 190), stellen in einem auf fortlaufende Zahlungen angewiesenen System die »Katastrophenschwelle« dar; und zwar nicht nur für eine einzelne Bank, sondern für das Finanzsystem als solches. Deshalb bestand die Reaktion der Zentralbanken und Staaten auf die Finanzkrise darin, mit Liquiditätsinjektionen die Flüssigkeit des Finanzsystems wiederherzustellen (Langley 2014, 36–59). Die Kreditklemme sollte aufgelöst werden, indem so lange Geld durch die vertrockneten Kanäle des Finanzsystems gespült wurde, bis die Zahlungen wieder von alleine flossen.

Die während der Finanzkrise aufgetauchten Unterbrechungen haben ein bisher in dieser Schärfe noch nicht bekanntes Problem sichtbar werden lassen. Bis zur Krise wurde davon ausgegangen, dass solvente Banken immer auch liquide Banken sind, weil sie sich stets Zahlungsmittel auf den Kreditmärkten besorgen können. Die Engpässe auf den Kreditmärkten, die durch Verluste während der *subprime*-Immobilienkrise und schwindendes Vertrauen zwischen den Banken entstanden sind, haben jedoch dafür gesorgt, dass auch Banken mit genügend Eigenkapital an den Rand der Zahlungsunfähigkeit gerieten.

»During the early liquidity phase of the financial crisis starting in 2007, many banks – despite meeting existing capital requirements – experienced difficulties because they did not prudently manage their liquidity. [...] The rapid reversal in market conditions showed how quickly liquidity can dry up and also how long it can take to come back.« (BIS 2014, 5)

Diese Verwicklungen haben den Unterschied zwischen Solvenz und Liquidität sichtbar gemacht und als zwei regulatorische Problembereiche konstituiert (siehe dazu: Langley 2014, 36–59; 102–123). Liquiditätsprobleme

stellen dabei eine besonders verwickelte Version der auch in Infrastruktursystemen beobachtbaren *stock* und *flow*-Problematik dar. Es geht hier nämlich nicht nur um das prinzipielle Vorhandensein von Reserven (ausreichend Eigenkapital in beliebiger Form bzw. Solvenz), sondern um deren augenblickliche Verfügbarkeit und damit gleichsam um deren Aggregatzustand: *frozen assets* – also gebundenes Kapital – nützt nichts, wenn *liquid assets* benötigt werden, um fällige Verbindlichkeiten zu bedienen. Um das Problem der Liquidität zu adressieren, wurde in der Folge der Finanzkrise vor allem eine neue Regelung von der Bank für Internationalen Zahlungsausgleich in Basel im Rahmen der sogenannten Basel III-Regeln verabschiedet: die *Liquidity Coverage Ratio* (LCR) (BIS 2013). Das LCR zielt darauf, die »short-term resilience« der Banken zu erhöhen. Dafür sollen die Banken stets einen »adequate stock of unencumbered high-quality liquid assets« vorhalten, der verfügbar ist, um ein »30 calendar day liquidity stress scenario« (BIS 2013, 7) überbrücken zu können und damit so etwas wie eine Notstromversorgung für Banken darstellt.

Aber auch das Problem der Insolvenz von Banken und deren Schockwirkung für das Finanzsystem haben neue Regulationsbemühungen auf den Plan gerufen. So wurden die Eigenkapitalvorschriften für Banken im Regulationswerk Basel III<sup>99</sup> und daraufhin schrittweise ebenfalls auf nationaler bzw. europäischer Ebene noch einmal verschärft. Durch Vorhaltung von mehr Eigenkapital der Banken soll ein Puffer gebildet werden, der die Kapazität von Banken erhöhen soll, nicht nur kurzfristige Zahlungsverpflichtungen leisten zu können, sondern auch massive Verluste zu absorbieren, ohne insolvent zu werden. Bereits Basel I und Basel II regelten Verpflichtungen für die Vorhaltung von Eigenkapital bei Banken. Basel III stellt demgegenüber eine Erweiterung dar, weil bei der Berechnung des notwendigen Eigenkapitals *systemische Risiken* einbezogen werden und der makroprudenzielle Regulierungsanspruch stärker akzentuiert wird.

»To address the market failures revealed by the crisis, the Committee is introducing a number of fundamental reforms to the international regulatory framework. The reforms strengthen bank-level, or microprudential regulation, which will help raise the resilience of the individual banking institutions to periods of stress. The reforms also have a macroprudential focus, addressing system-wide risks that can

---

<sup>99</sup> Basel III wird das Maßnahmenpaket genannt, das in Reaktion auf die Finanzkrise von der Bank für Internationalen Zahlungsausgleich mit Sitz im schweizerischen Basel entwickelt wurde. Die 2010 fertiggestellte vorläufige Endfassung des Berichts ist durch die EU in der *Capital Requirements Directive* (CRD) umgesetzt worden.

build up across the banking sector as well as the procyclical amplification of these risks over time. Clearly these micro and macroprudential approaches to supervision are interrelated, as greater resilience at the individual level reduces the risk of system-wide shocks.« (BIS 2010, 2)

Der Schutz einzelner Banken ist die Voraussetzung dafür, dass Krisen sich nicht zu systemischen Zusammenbrüchen ausweiten. Das Eigenkapital ist dabei eine Versicherung dafür, dass eine Bank auch im Fall massiver Verluste weiterhin operationsfähig bzw. »am Leben« bleibt.

Im Zuge von Finanzkrise und Bankenrettung hat vor allem ein Problem die Agenda der Finanzregulatoren bestimmt: die Risiken, die von sogenannten »systemrelevanten Banken« ausgehen, häufig auch als *too big to fail*-Problem adressiert. Systemrelevante Banken werden mit einem doppelten Risiko in Verbindung gebracht. So heißt es in einem Bericht des im Zuge der Finanzkrise bei der Bank für Internationalen Zahlungsausgleich in Basel geschaffenen Financial Stability Board (FSB):

»This report recommends a policy framework for addressing the systemic and moral hazard risks associated with *systemically important financial institutions* (SIFIs) whose disorderly failure, because of their size, complexity and systemic interconnectedness, would cause significant disruption to the wider financial system and economic activity.« (FSB 2010, 1)

Von systemrelevanten Banken gehen erstens systemische Risiken aus, weil sich ihr Zusammenbruch »ansteckend« auf den Rest des Finanzsystems auswirken könnte. Dabei geht es nicht nur um ihre Größe, sondern auch um den Grad ihrer Vernetzung. Deswegen wird auch von »too complex« oder »too interconnected to fail« (Bafin 2013, 31) gesprochen. Das FSB schlägt daher vor, für SIFIS noch strengere Eigenkapitalregelungen als die durch Basel III für alle Banken vorgesehenen zu treffen, um deren »loss absorbency« (FSB 2010, 2) zu erhöhen. Seit 2011 werden vom FSB Listen mit den als global systemrelevant eingeschätzten Banken herausgegeben, die sich bis 2016 einen zusätzlichen Eigenkapitalpuffer zulegen müssen. Mittlerweile werden vom *Financial Stability Board* insgesamt 28 Banken und neun Versicherungen (in Deutschland die Deutsche Bank und die Allianzversicherung) als global systemrelevant eingestuft. Diese Maßnahmen zur Sicherung systemrelevanter Banken gehen über die Logik der vorbereiteten Vorhaltung von Ressourcen hinaus. Adressiert wird zusätzlich das Problem des *node failures*: der Ausfall eines zentralen Knotenpunkts des Finanzsystems, der gravierende Schäden für das gesamte Netz mit sich bringen würde.



Während der *europäischen Staatsschuldenkrise* ab dem Jahr 2010 hatten plötzlich auch Staaten mit denselben Problemen zu kämpfen, die auch am Beginn der Finanzkrise standen. Die Geldbeschaffung auf den Kapitalmärkten gestaltete sich für besonders verschuldete Eurostaaten, allen voran Griechenland, zunehmend schwierig. Das ist durchaus bemerkenswert. Denn auch wenn es historisch immer wieder zu Staatsschuldenkrisen gekommen ist, so stehen Staatsschulden traditionell doch unter einem anderen Vorzeichen als Schulden privater Akteure. Souveräne Staaten genießen nämlich für gewöhnlich einen besonderen Vertrauensvorschuss – einen »sovereign trust« (Langenohl 2015, 75), so dass ihre Bonität nicht in der gleichen Weise wie die privater Akteure hinterfragt wird (siehe dazu auch: Boy 2015). Andreas Langenohl (2015) hat gezeigt, wie dieser *sovereign trust* im Zuge der Neuverteilung fiskalischer Souveränität durch die Gründung der Europäischen Währungsunion und dann im Zuge der Eurokrise immer weiter erodierte. Staaten wurden zunehmend wie andere ökonomische Akteure beobachtet, bewertet und entsprechend bei schlechten Kreditratings mit hohen Zinsen bestraft. Das hat wiederum die Geldbeschaffung so erschwert, dass sich die Möglichkeit von Staatsbankrotten, die weitere schwerwiegende ökonomische Schockwirkungen zur Folge haben würden, am Horizont abzeichnete. Statt weiter auf den *sovereign trust* zu setzen, sollte jetzt die Kollateralisierung der Staaten vorangetrieben werden. Für die drohende Katastrophe eines Staatsbankrotts sollten also vorbereitende Maßnahmen in Form von Ausfallsicherungen geschaffen werden.

Der »Euro Rettungsschirm« ist durch seine Symbolik – wie ein Regenschirm schützt er vor schlechtem Wetter – zur Ikone einer bestimmten Politik der Vorbereitung geworden. Offiziell wurden nur die Sofortmaßnahmen zur Rettung von akut in die Krise geratenen Eurostaaten als »Rettungsschirm« bezeichnet und auch hier wurde der entsprechende Rettungsfonds lieber *European Financial Stability Facility* (EFSF) genannt. Wohl auch, um den Eindruck reiner Krisenmanagementpolitik zu zerstreuen, wurde der dauerhafte europäische Krisenmechanismus dann schließlich *Europäischer Stabilitätsmechanismus* bzw. *European Stability Mechanism* (ESM) genannt. An seiner Funktion als Notfallplan, für den spezielle Notfallreserven (ein Rettungsfonds) vorgehalten werden, lässt allerdings selbst das Bundesfinanzministerium, das in dieser Hinsicht für gewöhnlich sehr zurückhaltend ist, keinen Zweifel:

»[D]ie Euro-Länder [haben] mit dem Europäischen Stabilitätsmechanismus einen permanenten Schutz- und Notfallmechanismus eingerichtet, der im Vorhinein ein bekanntes, ausgereiftes Instrumentarium zur Bewältigung von Staatsschuldenkrisen im Euroraum bereithält. Ein solches Instrumentarium ist selbst bei optimaler Vorsorge gegen derartige Krisen notwendig, um für alle Eventualitäten gerüstet zu sein und die Währungsunion vor Erschütterungen durch Schwierigkeiten einzelner Mitgliedstaaten zu schützen.« (BMF 2013a)

Letztlich handelt es sich bei allen Instrumenten des ESM um finanzielle Zuwendungen im Dienste kriselnder Euroländer: Darlehen, Finanzhilfen und Rekapitalisierungen von wichtigen Finanzinstitutionen, Anleiheaufkäufe und vorsorgliche Finanzhilfen (siehe dazu: BMF 2013a). Das Ziel dabei ist es, die Zahlungsunfähigkeit und damit den Ausfall des Systems Staat bzw. öffentlicher Haushalt zu verhindern. Außerdem geht es darum, Kreditausfälle bei Gläubigern zu verhindern und damit die Schockwirkungen einer Staatspleite zu reduzieren. Nicht zuletzt geht es bei der Euro-Rettung aber auch darum, das Vertrauen in die verschuldeten Länder auf den Finanzmärkten zu stärken (Langenohl 2015, 81–86). Das ist nicht nur eine versteckte Funktion, sondern explizites Ziel der Strategien. Andreas Langenohl (2015, 81) zitiert Wolfgang Schäuble mit den Worten: »The key issue for the euro zone is the trust of the financial markets«. Das Vorhalten von Ressourcen zur Kreditsicherung (*collateral*) dient hier nicht zuletzt zur Prävention des Erschöpfens der sozialen Ressource Vertrauen. Vorbereitende Maßnahmen – der Aufbau von Ausfallsicherungen – werden hier also vor allem getroffen, um vorsorglich zu verhindern, dass diese Maßnahmen überhaupt in Anschlag gebracht werden müssen.

Die Vertrauenssicherung ist offiziell auch der Grund, warum die Inanspruchnahme von Mitteln aus dem ESM an eine Reihe von Konditionen gebunden ist. Jedes Land, das Hilfe aus dem ESM bezieht, muss sich im Gegenzug zu noch strikteren Sparmaßnahmen verpflichten, als durch die verschärfte »haushaltspolitische Überwachung der EU« (BMF 2013c), den *Fiscal Compact*, ohnehin schon durchgesetzt werden.<sup>100</sup> Das Vertrauen in die verschuldeten Länder soll also durch ein striktes haushaltspolitisches Kontrollregime erhöht werden, das letztlich auf eine Politik der Austerität hin-

---

100 Die wohl wichtigste Maßnahme aus diesem Paket der haushaltspolitischen Überwachung ist die Verpflichtung für Eurostaaten, eine »Schuldenbremse« in ihren jeweiligen Landesverfassungen zu verankern. In Deutschland wurde die Schuldenbremse bereits im Grundgesetz verankert und erlaubt Ausnahmen nur bei schweren Katastrophen und gravierenden ökonomischen oder Finanzkrisen (siehe zu diesen Ausnahmen: Kapitel 2.1.3.).

ausläuft. Damit vermischen sich beim ESM Strukturanpassungsmaßnahmen mit Maßnahmen zur Verhinderung eines Systemausfalls. Paradoxerweise unterminiert aber letztlich diese fiskalische Kontrolle – einmal abgesehen von den gesamtwirtschaftlichen Folgen für Wachstum und öffentliche Wohlfahrt – die Wirksamkeit des *sovereign trust* und verstärkt so letztlich das Problem – den Vertrauensverlust –, auf das es reagiert. Es scheint, als habe man es hier mit der »Wiederauffüllung eines Dispositivs« (Foucault 1978) zu tun, bei dem das proklamierte Ziel – die Wiederherstellung der Bonität eines souveränen Staates – letztlich umschlägt in eine kleinliche Überwachung von Staaten, in den neoliberalen Traum eines »ständigen ökonomischen Tribunal[s] [...] mit der Absicht, das Handeln der Regierung in streng ökonomischen und marktbezogenen Begriffen zu beurteilen.« (Foucault 2006, 342)

Auch auf dem Gebiet der *Seuchenkontrolle* kommt der Vorhaltung von Ressourcen zur Vorbereitung auf den Ernstfall eine entscheidende Bedeutung zu. Die Seuchenkontrolle basiert wesentlich auf einer Reihe von Infrastrukturen, die geschützt, gewahrt und aufgebaut werden müssen: Infrastrukturen der Überwachung (Fearnley 2008), der Arzneimittelbevorratung (Elbe, Roemer-Mahler und Long 2014) sowie der Versorgung von Infizierten. Immer stärker stehen diese Kritischen Infrastrukturen selbst und nicht mehr (nur) die Bevölkerung im Fokus der Aufmerksamkeit der Seuchenkontrolle (Lakoff 2008). Idealerweise kann sich auf eine Pandemie durch Entwicklung und Vorhaltung entsprechender Impfstoffe vorbereitet werden. Impfen schützt schließlich nicht nur die jeweils geimpfte Person, sondern reduziert auf der Ebene der Bevölkerung auch die weitere Ausbreitung der Krankheit. Ein zentrales Problem der Seuchenkontrolle besteht allerdings darin, dass die genaue Art des Virus zumeist im Vorhinein nicht bekannt ist, insofern *drift*- und *shift*-Phänomene zur schnellen Transformation der Erreger beitragen. »Die Ungewissheit, welcher Erreger die nächste Pandemie auslösen könnte, macht es auch derzeit unmöglich, erregerspezifische Impfstoffe im Vorhinein zu entwickeln.« (BBK 2007a, 4) Es wird davon ausgegangen, dass es nach Ausbruch einer Pandemie etwa sechs Monate dauert, bis ein entsprechender Impfstoff zur Verfügung steht (siehe: BBK 2007a, 17). Deshalb wird auf eine »staatliche Bevorratung antiviraler Arzneimittel« (BMG und RKI 2007, 5), sogenannter Neuraminidasehemmer, gesetzt, die die Ausbreitung der Krankheit eindämmen, bis ein Impfstoff verfügbar ist. Der nationale Pandemieplan,

der in Deutschland im Jahr 2005 infolge einer Reihe von Aufrufen der WHO zur Entwicklung nationaler Pläne beschlossen wurde, bemerkt:

»Der Typ, Subtyp oder Stamm eines zukünftigen pandemischen Influenzavirus kann nicht vorhergesagt werden. Die Vorbereitungen von Bund und Ländern zielen daher darauf ab, die Zeitspanne bis zur Verfügbarkeit wirksamer Impfstoffe zu verkürzen.« (BMG und RKI 2007)

Hier wird deutlich, dass die Sicherheitsbemühungen gegen Bedrohungen mit rasanter Ausbreitungsdynamik nicht nur im Davor oder Danach stattfinden, sondern vor allem im kritischen Dazwischen oder Währenddessen bzw. Intervall der Katastrophe (zum Konzept des Intervalls der Katastrophe siehe: Adey und Anderson 2011).<sup>101</sup> Wie schon bei den Maßnahmen zur Stabilisierung des Finanzsystems und der Eurozone geht es darum, frühzeitig zu intervenieren, damit die »Katastrophenschwelle« nicht überschritten wird. Im Fall der Seuchenkontrolle soll deshalb ein ausgefeiltes Überwachungssystem die Entstehung einer Epidemie bzw. Pandemie anzeigen, um möglichst schnell und gleichsam noch auf der Ebene der Emergenz der Gefahr intervenieren zu können. Melinda Cooper (2006) bezeichnet diesen Interventionsmodus daher als »preempting emergence«. Brian Massumi (2009) hat bemerkt, dass der Katastrophenschutz nicht nur auf der Ebene bereits konstituierter und abgrenzbarer Gefahren (*natura naturata*) operiert, sondern bereits auf der Ebene ihrer Entstehung (*natura naturans*). Die gegenwärtige Sicherheitspolitik sei deshalb nicht nur eine Biomacht, sondern eine Ontomacht (Massumi 2010b). Auf dem Finanzmarkt heißt das vor allem: die Ausbreitung eindämmen und den Zerstörungsradius einschränken. So soll der ESM die Ausbreitung der Eurokrise von der Peripherie (Griechenland, Irland, Portugal) auf das Zentrum (Deutschland, Frankreich) der Eurozone aufhalten. Die Regulation der Finanzwirtschaft soll die Ausbreitung auf die Realwirtschaft verhindern. »The objective of the reforms is to improve the banking sector's ability to absorb shocks arising from financial and economic stress, whatever the source, thus reducing the risk of spillover from the financial sector to the real economy.« (BIS 2010, 1) Der Bankensektor soll als »shock absorber« fungieren und nicht als »transmitter of risk to the financial system and broader economy« (BIS 2010, 5).

Der Versuch, die Katastrophe auf der Ebene ihrer Entfaltung aufzuhalten oder zumindest einzudämmen, bestimmt natürlich auch alle Maß-

---

101 Ausführlicher werde ich in Exkurs III auf diese temporale Logik der Resilienz eingehen.

nahmen des operativen Katastrophenschutzes und des Krisenmanagements wie Feuerwehr, medizinische Versorgung, Hilfsorganisationen, Technisches Hilfswerk usw. Diese Vorbereitungsmaßnahmen auf die Katastrophe durch Kapazitäten bei Ersthelfer\_innen und Rettungsorganisationen werden häufig unter die Kategorie der »operationellen Resilienz« (Cooper und Walker 2011, 152) gruppiert.<sup>102</sup> Auch hier kommt der Vorhaltung und dem schnellen Zugriff auf Ressourcen eine zentrale Rolle zu, um die Resilienz des vitalen Systems der Notfallhilfe und des Rettungswesens zu stärken. Dafür sind im Rahmen der *Neuen Strategie zum Schutz der Bevölkerung* Kapazitäten wie Hubschrauber, die analytische Task Force und die ABC-Abwehr eingerichtet worden. Allerdings kommt auch viel alltäglichen und banaler erscheinenden Ressourcen eine »vitale« Rolle zu, die im Notfall über Leben und Tod entscheiden kann: Blutkonserven, Medikamente, Verbandszeug, Krankenhausbetten etc. Am Beispiel der zusätzlichen Krankenhausbetten, die von Katastrophenschützern zwar gefordert, aufgrund des Kostendrucks im Gesundheitssystem allerdings nicht angeschafft werden, wurde bereits auf die Schwierigkeiten hingewiesen, die der Vorhaltung von Ressourcen zur Erhöhung der Resilienz von Systemen häufig im Wege stehen (siehe Kapitel 2.1.3.). Die »Effektivität« des Katastrophenmanagements steht hier im Widerspruch zur ökonomischen »Effizienz« von Systemen.

Ähnlich werden auch die neuen Eigenkapitalvorschriften als große Bürden für den Finanzsektor angesehen. Schließlich müssen sich die Banken aufgrund der Vorschriften Kapital beschaffen, das der Zirkulation und damit auch dem Kreislauf der Verwertung entzogen wird. Das geht gegen den Strich einer Investmentkultur, die immer stärker durch die Aufnahme von Schulden im großen Stil einen Hebel erzeugt hat, der selbst geringste Gewinnmargen zu großen Profiten machen kann. Prinzipiell ist die Vorhaltung von Ressourcen für den Notfall – ob es sich nun um Krankenhausbetten, Eigenkapital, große Lagerbestände etc. handelt – eine kostspielige Angelegenheit. Bemühungen um Optimierung der Effizienz – ob durch Sparzwang öffentlicher Haushalte, durch die *just-in-time*-Revolution in der Industrieproduktion und Logistik (Cowen 2010) oder die systematische Berechnung der »Kosten« von Regulierungsvorhaben auf dem Finanzmarkt (Thiemann und Aldegwy 2015) – haben deshalb in den

---

<sup>102</sup> Auf diese Dimension der Resilienz bzw. der *preparedness* gehe ich vor allem in Kapitel 2.2. sowie in Kapitel 4.2. zum *Business Continuity Management* als Krisenmanagementtechnik ein.

vergangenen Jahrzehnten auch zu einem massiven Abbau derartiger Pufferkapazitäten geführt. Immer mehr gesellschaftliche Systeme sind dadurch auf immer schnellere Dauerzirkulation angewiesen und gegenüber Unterbrechungen in einer Weise verwundbar, wie es lange wohl nur von militärischen Operationen bekannt war. Häufig sind es also weniger technische Entwicklungen,<sup>103</sup> sondern ökonomische, die ein System gefährden und zugleich die Sicherheitsvorkehrungen für diese Systeme schwierig und kostspielig werden lassen. Selbst wenn man zugesteht, dass die Dienste bestimmter Systeme kritisch im Sinne von vital oder lebensnotwendig sind, so impliziert dies keineswegs zwangsläufig, dass es sich dabei auch um besonders verwundbare Systeme handeln muss. Häufig ist dies nur der Fall, weil es teuer wäre, bestimmte Sicherheitsvorkehrungen zu implementieren oder Redundanzen aufzubauen.

### 2.5.3. Resilienz durch Gestaltung der Systemarchitektur

Wenn die systemische Gefährdung aus »exzessiver Interkonnektivität« (BIS 2010, 7) und undurchschaubarer Komplexität heraus entsteht, dann läge es eigentlich nahe, zur Reduktion der Verwundbarkeit einige Verbindungen aufzulösen oder sie zumindest übersichtlicher zu gestalten. Es müssten – wie sich in Anschluss an Charles Perrow (1987, 95–140) formulieren ließe – enge Kopplungen und hohe Komplexität vermieden werden. Das hieße also, das Design von Systemen bzw. die Architektur der Netzwerke vitaler Systeme zu verändern. Schließlich ist Vernetzung nicht gleich Vernetzung. Es gibt unterschiedliche Arten von Netzwerken oder Netzwerktopologien, die mehr oder weniger tolerant auf Störungen und den Ausfall einiger Netzknoten reagieren.<sup>104</sup> Probleme bereiten immer wieder sogenannte *single points of failure*, deren Ausfall zu Stockungen der Ströme und zum Zusammenbruch des Netzwerks führt. Vor allem in der Logistik gibt es viele Bemühungen, solche Punkte zu vermeiden – was den glatten Raum der Weltmeere und Ozeane immer schon zur logistischen Heterotopie gemacht hat: eine glatte Oberfläche, auf der geschmeidiges und flexibles *re-*

---

103 Wie ich in den Kapiteln 3.3.3. bis 3.3.5. zeigen werde, schränken im Fall des Stromsystems tatsächlich technische Faktoren die Möglichkeiten zur Vorhaltung von gespeicherten Stromkapazitäten ein.

104 Gerade diese Technologie der Resilienzsteigerung ist schon bei Holling und dessen Betonung der Bedeutung der relationalen Eigenschaften eines Systems für dessen relative Widerstandskraft angelegt.

*routing* möglich ist (Virilio 1980, 52ff., Deleuze und Guattari 1997, 533f., Mitchell 2011, 36ff.). Beispiele für Versuche, durch eine veränderte Systemarchitektur die Verwundbarkeiten von Systemen zu reduzieren, lassen sich auf dem Finanzmarkt, aber auch in den Bereichen des Infrastrukturschutzes und der Lebensmittelsicherheit finden.

Auch wenn die Verschärfung der Eigenkapital- und Liquiditätsrichtlinien fraglos das wichtigste Instrument zur Bekämpfung systemischer Finanzmarktrisiken ist, findet sich ebenfalls eine Reihe von Initiativen, die undurchschaubare Verflechtungen zwischen Banken transparenter gestalten und damit sicherer machen sollen. Das betrifft insbesondere den sogenannten *over the counter*-Handel, also den außerbörslichen Handel, der direkt zwischen den Marktteilnehmern abläuft und für Regulatoren vollkommen undurchsichtig geworden ist. Mit einem grundsätzlichen Eingriff in die bisher nicht regulierte und wild-wuchernde Finanzinfrastruktur sollen diese Geschäfte künftig in geordnete »Bahnen« gelenkt werden. Derivatgeschäfte sollen künftig über sogenannte *clearing*-Stellen laufen, die exzessive Vernetzungen reduzieren und zudem für Regulatoren durchsichtiger machen sollen (siehe dazu: BMF 2013b).

Die 2012 von der EU verabschiedeten *European Market Infrastructure Regulations* haben also tatsächlich einen Eingriff in die Architektur des Finanzsystems vorgenommen und damit die Finanzmarktinfrastruktur zum expliziten *matter of concern* werden lassen.

»The recent financial crisis demonstrated the potential for contagion arising from the interconnectedness of significant market participants and the limited transparency of counterparty relationships. Robust financial infrastructures make an essential contribution to financial stability by reducing what could otherwise be a major source of systemic risk. At the same time, authorities must take steps to ensure that a core or critical financial infrastructure does not itself become a source of systemic risk.« (FSB 2010, 8)

Diese Logik der Identifizierung Kritischer Infrastrukturen des Finanzsystems bzw. auch innerhalb einer Finanzinstitution ist auch für die geplante bessere Überwachung und Abwicklung von Banken entscheidend. Denn erst wenn die Verbindungslinien zwischen den Banken transparent genug sind, können sie von Regulatoren so überwacht werden, dass gezielte Eingriffe überhaupt möglich sind. Sogenannte »Banktestamente« sollen regeln, was nach der Insolvenz einer Bank geschieht und wie trotz der Insolvenz einer systemwichtigen Bank systemische Risiken vermieden werden können. Die Metapher des Organspendeausweises wäre ebenso treffend gewe-

sen, weil es im Kern darum geht, wie die vitalen Funktionen der Bank auch nach deren Insolvenz weiter operabel gehalten werden können, indem sie von der Abwicklungsmasse isoliert werden. »The report sets out recommendations for improving the authorities' ability to resolve such institutions in an orderly manner, without exposing tax-payers to loss, while maintaining continuity of their vital economic functions.« (FSB 2010, 1) Hier wird die Logik vitaler Systeme weiter getrieben, indem nicht mehr eine komplette Institution, sondern lediglich einzelne Funktionen der Institution als lebenswichtig beschrieben werden (zu einem ähnlichen Vorgang in der US-amerikanischen Bankenregulierung siehe auch: Langley 2014, 178).

Gegen die überbordende Komplexität und zum Problem gewordene Größe von Systemkomponenten (*too big to fail*) wird immer wieder der Wunsch nach kleineren und übersichtlicheren Strukturen, gleichsam nach »Entnetzung« (Stäheli 2013) artikuliert; ein Wunsch, bei dem es häufig nicht nur um unmittelbare Sicherheitsgewinne geht, sondern auch um eine grundsätzlich andere Lebensform. Gegen die unübersichtlichen, ausbeuterischen und zudem gefährlichen *Lebensmittelketten* etwa setzt eine ökologische Kritik und Praxis schon lange auf lokale Lebensmittelproduktion und -distribution. Ganz ohne hoheitliche Regulation hat sich mittlerweile eine alternative Lebensmittelinfrastruktur vom Bioladen über den Erzeugermarkt bis zum *farm-to-table*-Restaurant entwickelt, die ein gewachsenes Bedürfnis nach Einfachheit und Sicherheit befriedigen soll. Zahlreiche Zertifizierungsinitiativen sollen nachverfolgbar machen, wo ein Produkt herkommt und wie es produziert wurde. Gegen verwundbare *Stromnetze* – *brittle power* – haben die ebenfalls in enger Verbindung mit der Alternativkultur stehenden Autoren Hunter und Amory Lovins (Lovins und Lovins 1982) ab den späten 1970er Jahren einen *soft energy path* empfohlen, der auf dezentrale Versorgernetze statt auf zentralisierte Energieproduktion und -distribution setzt.<sup>105</sup> Heute werden Konzepte zur dezentralen Infrastrukturentwicklung entwickelt, die eine Abkehr vom modernen Infrastrukturideal (Graham und Marvin 2001) und seinen großen, zentral geplanten Infrastrukturprojekten implizieren, die weit über grün-alternative Projekte hinausgehen und zur nationalen Sicherheitsstrategie aufgestiegen sind (siehe dazu Kapitel 3). Auch Charles Perrow hat mit der Losung *shrink the targets* für ein Umdenken in der US-amerikanischen Sicherheitspolitik plä-

---

105 Siehe dazu ausführlich Kapitel 3.3.2.



diert, die seiner Meinung nach zu sehr auf die *preemption* von terroristischen Attacken fokussiert. »Instead of focusing only on preventing disasters and coping with their aftermath – which we must continue to do – we should reduce the size of vulnerable targets.« (Perrow 2011, 1) Es gelte deshalb, gefährliche Konzentrationen in den Bereichen Energie, Bevölkerung und politischer und ökonomischer Macht aufzulösen. Ein Konzern wie Walmart, der in den USA ein riesiges Einzelhandel- und Logistikimperium aufgebaut hat, ist für Perrow ein Beispiel für eine ökonomische Machtkonzentration, die gefährliche »single-point dependencies« (Perrow 2011, 301) erzeugt. Ausgerechnet in der Allianz-Studie werden derartige Abhängigkeiten als »monopoly risks« bezeichnet, die etwa durch den gleichzeitigen Ausfall von Infrastrukturen aufgrund eines Fehlers in einer Software entstehen können, die von mehreren Betreibern genutzt wird (Allianz 2008, 47). Ausgerechnet, denn immerhin ist die Allianz als systemrelevante Versicherung selbst ein allzu großes Ziel, ein Netzknoten, der ein dem *monopoly risk* zumindest vergleichbares Risiko darstellen dürfte.

Das zeigt, wie schwer die Strategie kleiner Ziele umzusetzen ist, weil die Auflösung von gesellschaftlich gewachsener, aber bisweilen wild-wuchernder Komplexität auf mächtige Interessen stößt. Es ginge hier schließlich um die Auflösung oder gar Zerschlagung von sehr mächtigen Konzernen. Deshalb verwundert es kaum, dass die »systemrelevanten Banken« bislang eben nicht aufgelöst und in kleinere Einheiten zerlegt wurden. Auch wenn eine solche Auflösung von allzu großen Banken eigentlich eine durchaus folgerichtige Maßnahme gewesen wäre, um die *systemic risks* von Banken zu beseitigen, die *too big to fail* sind.

Es geht aber nicht nur um Macht und ökonomische Interessen, sondern auch um die Selbstverständlichkeiten einer liberalen, vernetzten und mobilen Lebensweise. Das zeigt sich besonders deutlich am Fall der Seuchenkontrolle. Zwar wäre die Einschränkung des Reiseverkehrs ein mögliches, wenngleich wohl nicht besonders effektives, Mittel der Seuchenkontrolle, aber zugleich wäre es kaum möglich, für einen solchen Schritt Zustimmung zu erhalten. Im nationalen Pandemieplan heißt es dazu: »Die Wirksamkeit von verkehrsbeschränkenden Maßnahmen ist umstritten, selbst wenn einschneidende Maßnahmen wie Grenzsicherungen oder Flugverbote ergriffen würden.« (BMG und RKI 2007, 10) Entsprechend verlegt man sich auf die Information und die Kontrolle bzw. das *screening* der Reisenden und versucht, erkrankte Personen herauszufiltern und zu behandeln. Anstatt Grenzen zu schließen wird versucht, die Grenze zu

einer Schleuse zu machen, die die Ausbreitung der Pandemie eindämmt (Opitz 2015).

#### 2.5.4. Evolutionäre Resilienz und die Kritik der Sicherheit

Machtvolle Interessen wie auch die Verpflichtung auf liberale Freiheit und Freizügigkeit begrenzen die Reichweite und Effektivität des Sicherheitsdispositivs. Es gibt aber eine weitere Begrenzung der Sicherheit, bei der die Sicherheit nicht einfach in einem Zielkonflikt mit einem anderen Gut oder Interesse steht, sondern auf eine interne Grenze stößt. Denn häufig gehen Gefährdungen, und zwar gerade solche, die ihren Grund in der wachsenden Komplexität der Gesellschaft haben, auch von den Sicherheitsbemühungen selbst aus. So werden hoch- und großtechnische Systeme zwar in ihrem normalen Funktionieren immer verlässlicher. Die im Normalfall erhöhte Sicherheit wird in vielen Fällen aber durch eine erhöhte Verwundbarkeit im Katastrophenfall erkaufte. Das sogenannte »Verletzlichkeitsparadoxon« drückt diese Eigenschaft *großtechnischer Infrastruktursysteme* aus.

»Gesellschaften reagieren im Laufe ihrer technologischen Entwicklung auf Störungen vor allem der auf hoch entwickelten Technologien basierenden Infrastrukturen deutlich sensibler, da sie sehr hohe Sicherheitsstandards und eine hohe Versorgungssicherheit gewohnt sind. Dieser Umstand, dass sich mit zunehmender Robustheit und geringerer Störanfälligkeit ein durchaus trügerisches Gefühl von Sicherheit entwickelt und die Auswirkungen eines »Dennoch-Störfalls« überproportional hoch sind, wird als Verletzlichkeitsparadoxon bezeichnet: In dem Maße, in dem ein Land in seinen Versorgungsleistungen weniger störanfällig ist, wirkt sich jede Störung umso stärker aus. Dieses Paradoxon wird kontinuierlich verstärkt, indem in nahezu allen gesellschaftlichen Bereichen elektrische beziehungsweise elektronische Geräte, Mess- und Regelungstechnik, Informations- und Kommunikationstechnologien weiter zunehmen und die Abhängigkeit zum Beispiel von der Verfügbarkeit elektrischen Stroms oder aber von Informations- und Kommunikationstechniken weiter wächst.« (BMI 2009, 8)

Häufig sind gerade die angesprochenen Mess- und Regelungstechniken sowie die Informationstechniken eine Reaktion auf technische Sicherheits- oder Kontrollprobleme, die nun ihrerseits zum Problem wird. So hat James Beninger (1986) gezeigt, dass die »Informationsgesellschaft« aus einer Kontrollrevolution hervorgegangen ist, die es ermöglichen sollte, immer komplexere und störanfälligere technische, bürokratische und betriebliche Systeme durch den Einsatz von Informationsverarbeitungssystemen in den

Griff zu bekommen. Heute sind die digitalen Kontrolltechniken aber selbst zur schwer kontrollierbaren Risikoquelle geworden. Vielleicht verdeutlicht das nichts so sehr, wie das jüngere Phänomen von Cyberangriffen durch sogenannte *botnets*, bei denen vernetzte Alltagsgeräte wie Babyphone und intelligente Kühlschränke zu einer digitalen Störmada zusammengeschlossen werden, um von Firmen oder Privatleuten Geld zu erpressen oder einfach möglichst großen Schaden anzurichten.<sup>106</sup>

Eine ähnliche Entwicklung findet sich auch im Bereich der *Seuchenkontrolle*. So wird die neue Relevanz der Biosicherheit seit der Jahrtausendwende explizit als Reaktion auf die Erfolge vergangener Kampagnen der öffentlichen Gesundheitsvorsorge, bzw. der Biopolitik der Bevölkerung, verstanden.

»Die Bedeutung der Infektionskrankheiten wird heute [...] weitgehend unterschätzt. Der durch die Verbesserung der Hygiene, die Einführung von Schutzimpfungen und die Entwicklung der Antibiotika seit Beginn dieses Jahrhunderts deutlich rückläufige Trend der Sterblichkeit an übertragbaren Krankheiten ist aber jetzt – weltweit gesehen – gebrochen. [...] Das öffentliche Gesundheitssystem steht heute wachsenden Herausforderungen gegenüber vor allem durch: das Auftreten neuer und die wieder zunehmende Ausbreitung bekannter Infektionskrankheiten (Emerging and resurging diseases) z.T. mit resistenten Stämmen; größere Ausbrüche lebensmittel-assoziiierter Infektionen; den möglichen Ausbruch einer Influenza Pandemie; mögliche bioterroristische Aktivitäten.« (AKNZ 2001, 13)

Insbesondere die multi-resistenten Erreger (MRE) sind ein ungewolltes Nebenprodukt der medizinischen Entwicklung. MRE Keime sind Viren oder Bakterien, die gegen Antibiotika und Virostatika-Medikamente Resistenzen entwickelt haben. Jüngst hat die WHO in ihrem vielbeachteten *Antimicrobial Resistance. Global Report on Surveillance* diese Dialektik des medizinischen Fortschritts so beschrieben:

»For more than 60 years, antibacterial drugs have been regarded as the panacea to cure infections [...]. Indeed *the development of each new antibacterial drug has been followed by the detection of resistance to it.* [Hervorhebung A.F.] The development of resistance

---

106 Aufsehererregend war hier vor allem der weltweite Netzangriff im November 2016, der Großkonzerne wie die Telekom, Netflix, PayPal, Amazon und Twitter sowie allein in Deutschland 900.000 Internetanschlüsse betroffen hat (BSI 2017, 7). Eine ähnliche Dialektik der digitalen Kontrolltechniken zeigt sich auch in Bezug auf den Einsatz von digitalen Technologien (*smart grids* und *smart meter*) im Bereich der Stromversorgung, die die volatile Einspeisung erneuerbarer Energien steuern sollen, gleichzeitig aber auch Hackerangriffe auf das Stromsystem zum katastrophischen Risiko haben werden lassen. Siehe dazu: 3.3.4. sowie 3.3.5.

is a normal evolutionary process for microorganisms, but it accelerated by the selective pressure exerted by widespread use of antibacterial drugs.« (WHO 2014, 1)

Antibiotika werden also nicht mehr unumschränkt als Panazee (Allheilmittel) verstanden, sondern als ambivalentes Pharmakon (Gift und Medizin gleichzeitig) wahrgenommen (siehe zu dieser Entwicklung auch: Landecker 2016). Die Erreger sind nämlich ihrerseits resilient und können sich neuen Situationen anpassen.

Die »Lebensmittel-assoziierten« Infektionen, die als weitere Ursache für eine »Rückkehr der Seuchen« betrachtet werden, sind zwar nicht die direkte Folge eines medizinischen, aber doch eines biopolitischen Entwicklungsschritts. Die industrialisierte Landwirtschaft hat einen bisher nie gekannten Schutz vor Hungersnöten mit sich gebracht. Der Nahrungsmangel, einst »Heimsuchung auf seiten der Bevölkerungen, Katastrophe, Krise [...] auf seiten der Regierung« (Foucault 2004, 54), ist in westlichen Gesellschaften verschwunden. Heute gibt es ein Überangebot von Lebensmitteln, das aber zugleich neue Gefährdungen in Form von Lebensmittelkrisen aller Art hervorbringt.

»Moderne Lebensmittelverarbeitung, internationaler Handel und ausgefeilte Logistik machen es möglich: Essen zu jeder Zeit, bei jeder Gelegenheit und immer wenn es uns gerade passt. [...] Nur: Wer blickt da noch durch, bei der Menge an Lebensmitteln? Globale Märkte, internationale Warenströme und schnelllebige Produktions- und Konsummuster bergen neue Risiken und erfordern neue Strategien der Lebensmittelsicherheit.« (BMELV 2013, 6)

Diese Ambivalenzen und Paradoxien in der Infrastrukturentwicklung, der öffentlichen Gesundheitsvorsorge und der Lebensmittelproduktion deuten jeweils auf ein Problematisch-Werden klassischer Bio- und Technopolitiken der Moderne hin. Das höchst erfolgreiche biopolitische Dispositiv aus Hygiene, Impfungen und Antibiotika, das ab dem 19. Jahrhundert zunächst alle westlichen Staaten ergriffen hatte, ist ebenso fragwürdig geworden wie die Lebensmittelproduktion und die in Deutschland unter dem Begriff der Daseinsvorsorge (siehe dazu Kapitel 3.1.) bekannte staatliche Infrastrukturpolitik, die der gesamten Bevölkerung einen sicheren Zugang zu »vitalen« Dienstleistungen wie Wasser, Strom oder Verkehr ermöglicht hat.

Sind es in den Bereichen Ernährung, Infrastruktur und Gesundheitsvorsorge Sicherheitstechniken, die bereits im 19. und spätestens seit der ersten Hälfte des 20. Jahrhunderts entwickelt wurden und die heute prob-

lematisch geworden sind, so werden gegenwärtig im Finanzsektor Sicherheits- bzw. Risikoregulationstechniken hinterfragt, die mitunter wesentlichen jüngeren Datums sind. Fast zeitgleich mit der Rettung der Banken unter der Maßgabe des *too big to fail* ist bereits auf die perversen Effekte dieser Strategie hingewiesen worden: Weil die Banken sich ihrer Bedeutung bewusst seien, bestehe die Gefahr, dass sie sich auf einen *government bail out* verlassen und ihre Risikovorsorge weiter vernachlässigen. So kommt die Figur des *moral hazard* ins Spiel, die sonst Phänomene wie etwa mangelnde Gesundheitsvorsorge bei Krankenversicherten oder ein vermeintliches Ausruhen in der »sozialen Hängematte« bei Sozialversicherten beschreiben soll (für einen kritischen Blick auf diese Artikulation des *moral hazard* siehe: Stone 2002). Schnell ist das Programm zur Bankenrettung umgeschlagen in eine Politik der Reduzierung von »*moral hazards posed by systemically important financial institutions*« (FSB 2010). Die Kategorie des *moral hazard* erlaubt es dabei, eine Technologie der Sicherheit – den *bail out* gemäß der Rationalität des »*too big to fail*« – als Sicherheitsproblem kenntlich zu machen.

Darüber hinaus kam es als Folge der Finanzkrise aber auch zu einer grundsätzlichen Infragestellung des Sicherheitsregimes auf den Finanzmärkten. So wurde die Finanzkrise gerade in der soziologischen Literatur immer wieder als Paradoxie der Sicherheit bzw. des Risikomanagements thematisiert und theoretisiert: aus einer Perspektive der reflexiven Moderne als »unintendierter Nebeneffekt« des *financial engineering* (Arnoldi 2009), systemtheoretisch als Wendung der projizierten Zukunft gegen die Gegenwart (Esposito 2011) oder poststrukturalistisch als Ironie der Normalisierung bzw. Autoimmunität (Folkers 2013a). Aber auch den Expert\_innen, Händler\_innen, Analyst\_innen und Regulationsinstanzen des Finanzsektors sind die perversen Effekte der Sicherheit aufgefallen. Eine besondere Rolle nimmt dabei sicherlich Andrew Haldane ein, mittlerweile Chefökonom der Bank of England, der in einer Reihe von Reden, Artikeln und Interventionen auf die Schwachstellen der gängigen Annahmen des Risikomanagements aufmerksam gemacht und zu einem grundlegenden Neudenken des Finanzmarktes aufgefordert hat. Dabei diente ihm gerade der Bezug auf die Rationalität der Resilienz dazu, ein verfehltes Sicherheitsdenken der klassischen finanziellen Risikoregulationsmodelle sichtbar zu machen. Haldane, dem gewiss keine fundamentale Ablehnung des Finanzwesens nachgesagt werden kann, hat dabei immer wieder auf die Verschlingung von Regulation und Produktion von Risiko auf dem Finanz-

markt aufmerksam gemacht (zu Haldane aus sozialwissenschaftlicher Perspektive siehe: Erturk et al. 2011, Cooper 2011, Tellmann 2015). Keineswegs – so Haldane – dürfe man den populären Diagnosen glauben, die suggerieren, dass die Finanzkrise auf ein moralisches Defizit der Akteure – auf Gier, Verantwortungslosigkeit, »Zockermentalität« etc. – zurückzuführen sei.

»In the 1987 film Wall Street, the financial sector mantra was greed is good. The stock market crash of the same year put paid to that doctrine, at least temporarily. By the early part of this century, both the circumstances and the individuals had changed. So too had the mantra. It had become the rather gentler »diversification is desirable.« (Haldane 2009, 3)

Nun hat das Risikomanagementverfahren der Diversifikation tatsächlich zu großen Fortschritten in der Kontrolle von Risiken beigetragen. Allerdings wurde es immer nur aus der Perspektive einer einzelnen Institution aus betrachtet und den Effekten dieser Verfahren auf der Ebene des Gesamtsystems zu wenig Aufmerksamkeit zuteil.

»From an individual firm perspective, these strategies indeed looked like sensible attempts to purge risk through diversification [...]. Viewed across the system as a whole, however, it is clear now that these strategies generated the opposite result [...]. Securitisation increased the dimensionality, and thus complexity, of the financial network. Nodes grew in size and interconnections between them multiplied. The financial cat's cradle became dense and opaque. [...] In short, diversification strategies by individual firms generated heightened uncertainty across the system as a whole.« (Haldane 2009, 4)

An dieser Stelle wird die Gemeinsamkeit des Ökologen Robert May und des Ökonomen Andrew Haldane verständlich. Wie May in der Ökologie geht auch Haldane für die Ökonomie davon aus, dass größere Diversität bzw. Diversifizierung und Vernetztheit die Stabilität bzw. Resilienz eines Systems nicht zwangsläufig erhöht, sondern ab einem bestimmten Umschlagspunkt anfällig für katastrophische Zusammenbrüche macht. Eine Perspektive, die mittlerweile in der Rede von »exzessiver Interkonnektivität« auch von dem entscheidenden Regulationswerk Basel III geteilt wird.

Haldane leugnet gleichwohl nicht vollkommen den stabilisierenden Charakter der Diversifizierung. Zwar können viele der auf dem Finanzmarkt zum Einsatz kommenden Risikomanagements- und Diversifikationstechniken tatsächlich Krisen verhindern oder eindämmen, indem sie eine risikoneutralisierende Wirkung auf die Märkte ausüben. Allerdings ist diese Eigenschaft zweischneidig. An einem bestimmten Punkt – der soge-

nannte *tipping point* – kann der sichernde, risikoneutralisierende und normalisierende Effekt in sein Gegenteil umschlagen.

»In a nutshell, interconnected networks exhibit a knife-edge, or tipping point, property. Within a certain range, connections serve as a shock-absorber. The system acts as mutual insurance device with disturbances dispersed and dissipated. Connectivity engenders robustness. Risk-sharing – diversification – prevails. But beyond a certain range the system can flip the wrong side of the knife-edge. Interconnections serve as shock amplifiers, not dampeners, as losses cascade. The system acts not as a mutual insurance device but as a mutual incendiary device. Risk-spreading – fragility – prevails.« (Haldane 2009, 9)

Für Haldane ist das Netzwerk, die komplexe heterarchische Risikoregulationspraxis auf dem Finanzmarkt beides: eine Technik der Sicherheit und ein Faktor katastrophaler Gefährdung. Die »Topology of the financial network« (Haldane 2009, 3) ist zugleich – aber nicht gleichzeitig – sowohl Sicherungsnetz als auch Ansteckungszusammenhang. Denn dasselbe adaptive bzw. selbstregulative System, ja, dieselben Regulierungsmechanismen können sich auf unterschiedliche Weise auswirken. Das Konzept des *tipping point* bezeichnet dabei das Umkippen der Selbstregulation von Homöostase in »Durchdrehen« (Bateson 1983, 619) und macht zugleich das Dilemma der Architekten sicherer Systeme sichtbar. Denn wenn das moderne *financial engineering* zumindest in Normalfällen tatsächlich mehr Sicherheit schafft, dann lassen sich diese Techniken nicht einfach abschaffen, wie es bisweilen gefordert wird, ohne zugleich auf ihre Vorzüge und sichernden Effekte verzichten zu müssen.

Auch wenn Resilienz auf den Finanzmärkten bisweilen eine leere Worthülse sein mag, so steckt doch in einer Perspektive wie der von Haldane jede Menge Zündstoff und vielleicht sogar eine neue normative Ordnung der Sicherheitsstrategien auf dem Finanzmarkt. Das beginnt beim Disziplinwechsel: Nicht mehr die Physik, die spätestens mit dem Aufkommen neoklassischer Gleichgewichtstheorien Ende des 19. Jahrhunderts die Ökonomie dominierte (Mirowski 1989), sondern die Biologie ist jetzt der Stichwortgeber für ökonomisches Denken. Besonders die auch von Haldane inszenierte Gegenüberstellung der Theorie effizienter Märkte und einer alternativen, »ökologischen« Markttheorie zeigt die potenzielle Radikalität des Paradigmas der Resilienz. Märkte sind demnach keine effizienten Maschinen, die sich ingenieurmäßig programmieren lassen, sondern komplexe adaptive Systeme, die zwar für Steuerungsimpulse sensibel sind, aber diese auf eigenlogische und letztlich unvorhersehbare Weise verar-

beiten. Ein ökologisches Modell der ökologischen Resilienz eignet sich nicht als »engine« (MacKenzie 2006) für ein *financial engineering*.<sup>107</sup> Schon Holling (1996) hatte mit seinem Konzept der Resilienz die »performativen« bzw. perversen Effekte von ingenieurmäßigen Planungsvorhaben kritisiert und zwischen einer ökologischen, gleichsam »natürlichen«, und einer ingenieurmäßigen, »künstlichen« Resilienz unterschieden. Anders als die Normalitäts- und Gleichgewichtsannahmen der Theorie Effizienter Märkte (siehe dazu: Folkers 2014, 95–97) kann die normative Ordnung der Resilienz nämlich nicht mehr von einer optimalen Norm oder optimalen Verteilung ausgehen, die es erlaubt, Risiken auszuschalten und dabei zugleich den Gewinn zu maximieren. Vielmehr steht Resilienz dafür, dass ein System wechselnde Gleichgewichtszustände durchlaufen kann.

Während die Normalisierung laut Foucault noch versucht, empirische Normalitäten aufzufinden, die als »optimal für ein gegebenes soziales Funktionieren angesehen« (Foucault 2004, 18f.) werden, ist das Auffinden einer optimalen Norm gemäß einer strengen Auslegung der Resilienz unmöglich.<sup>108</sup> Schließlich muss davon ausgegangen werden, dass sich die empirischen Normalitäten eigenlogisch verändern und ständig neuen Bedingungen anpassen. Es gibt also weder eine präskriptive noch eine deskriptive empirische Norm, die zum Leitmaß für die Sicherheit eines Systems herangezogen werden kann. Resilienz ist hier vielleicht nicht das Gegenteil, aber zumindest der Gegenspieler der Effizienz und der Suche nach exakt berechenbaren »optimalen« Zuständen. In Hollings Worten:

---

107 Donald MacKenzie (2006) hat mit der These, die moderne Finanztheorie sei ein »engine not a camera« sowohl die Perspektive des in den *Social Studies of Finance* (SSF) ungemein populär gewordenen *performing markets*-Ansatz beschrieben als auch darauf hingewiesen, dass wesentliche Protagonisten der Finanztheorie diese Sichtweise geteilt haben. So stammt der Vergleich der Finanztheorie mit einem Motor des Finanzwesens von Milton Friedmann. Die jüngere Kritik an den perversen Effekten des *financial engineering* stellt also nicht nur einzelne Theorien, sondern einen ganzen Theorietypus und -ethos in Frage: die Finanztheorie als *financial engineering*, als maßgebliches Praxiswissen für Marktakteure. Das hat Konsequenzen für den sozialwissenschaftlichen *performing markets*-Ansatz, die innerhalb der SSF noch nicht gezogen wurden.

108 Wie Matthias Thiemann und Mohamed Aldegwy (2015) zeigen, versucht der ökonomische Mainstream immer noch, politische Regulationen des Finanzmarkts unter Effizienzgesichtspunkten quantitativ zu analysieren, um die optimale Regulationspraxis zu ermitteln. Unter Resilienzgesichtspunkten wäre das nicht nur wenig sinnvoll, sondern geradezu schädlich, weil so wieder ein »künstliches« Optimum anvisiert wird. Letztlich könnte Resilienz auch dazu beitragen, die quantitative Fixierung der Ökonomie in die Schranken zu weisen. Noch scheint allerdings das Festhalten an alten epistemischen Gewohnheiten vorherrschend zu sein.



»Attention shifts [...] to the qualitative and to questions of existence or not.« (Holling 1973, 1) »[E]volution like a game, but a distinctive one in which the only payoff is to stay in the game. Therefore, a major strategy selected is not one maximizing either efficiency or a particular reward, but one which allows flexibility above all else.« (Holling 1973, 18) Resilienz ist hier keine Norm, sondern ein Potenzial, das sich erst nach Krisen oder Katastrophenereignissen auf niemals gänzlich vorhersehbare Weise realisiert. Resilienz ist eine komplexen, adaptiven Systemen eigene »Normativität« (Canguilhem 1977, 82). Insofern ähnelt Resilienz der Prozesslogik der Evolution. Sie ist kein Zustand, sondern ein Prozess der evolutionären Anpassung an eine sich ständig verändernde Gefahrenumwelt – ein Prozess, der, weil sich diese Gefahrenumwelt ständig verändert, unabschließbar ist.<sup>109</sup> In diesem Sinne lässt sich eine Bemerkung in der *Nationalen Strategie zum Schutz Kritischer Infrastrukturen* des Bundesinnenministeriums verstehen, in der gefordert wird: »Das bisherige Sicherheitsdenken muss sich zu einer neuen »Risikokultur« transformieren.« (BMI 2009, 9) Gerade in dieser evolutionären Auslegung der Resilienz liegt ihr kritisches und reflexives Potenzial. Es ist so nämlich möglich, überzogene Erwartungen an Sicherheit zu hinterfragen und die Pathologien, die durch das Festhalten an diesen Erwartungen in die Welt kommen, zu benennen. Insofern ist Resilienz mehr als eine Reihe von Technologien der Sicherheit wie das Vorhalten von Redundanzen und robustes Systemdesign. Resilienz führt zugleich einen veränderten *telos* der Sicherheit ein und kann so nicht nur auf Sicherheitsprobleme reagieren, sondern auch Probleme mit der Sicherheit zur Sprache bringen.

Aber auch wenn Resilienz Reflexivität ermöglicht, ist sie doch keine »reflexive solution« (Beck und Lau 2005, 531). Resilienz ist weniger eine »Lösung« als eine Rationalität zur Problematisierung und Kritik von Sicherheitsansprüchen. Sie erlaubt keine Überwindung der Paradoxien der zweiten Moderne, sondern führt zu einer anderen Prozessierung von Problemen. Zudem hat die evolutionäre Artikulation von Resilienz aber auch eine ganz und gar nicht reflexive Schlagseite. Resilienz kann nämlich

---

109 Darin liegt eine Ähnlichkeit zu Luhmanns Postulat in *Ökologische Kommunikation*, dass sich die Gesellschaft, also ihre einzelnen Subsysteme, nur evolutionär auf ökologische Gefährdungen einstellen können (siehe insbesondere: Luhmann 2008, 22–26). Allerdings ist diese Evolution im Falle der Resilienz sicherheit zu einem expliziten politischen Projekt geworden und kann nicht mehr wie bei Luhmann als stumme Eigenlogik sozialer Systeme verstanden werden.

auch als Strategie eingesetzt werden, um Sicherheitsansprüche der Bevölkerung abzuwehren (das betonen: Amin 2013, Joseph 2013). Schließlich können eben nicht alle Gefahren im Vorhinein abgesehen und verhindert werden. Vielmehr kann man immer nur nachträglich aus ihnen lernen. Deshalb kann unter Bezugnahme auf die Rationalität der Resilienz auch das Scheitern von Sicherheitsmaßnahmen zur Legitimationsgrundlage einer beständigen Ausweitung und Intensivierung der Sicherheit beitragen.<sup>110</sup> Das Eingeständnis, dass es keine hundertprozentige Sicherheit gibt, impliziert schließlich, dass man stets noch sicherer sein könnte, stets mehr für die Resilienz der Systeme im Angesicht einer sich ständig verändernden Gefahrenumwelt machen kann und muss. Darin liegt der spezifische »Modus der Unabschließbarkeit« (Bröckling 2012, 103) der Resilienz. Sowohl als Technologie wie als *telos* der Sicherheit ist Resilienz polyvalent. Nur die Untersuchung konkreter Fälle erlaubt Aussagen über die faktischen Effekte dieser neuen Rationalität der Sicherheit.

#### 2.5.5. Das Sicherheitsdispositiv der Resilienz

In den fünfzehn Jahren seit dem 11. September 2001 sind eine Vielzahl von Strategien entwickelt, Maßnahmen getroffen, Gesetze verabschiedet und Institutionen geschaffen worden, die einer neuen sicherheitspolitischen Orientierung in Deutschland Gestalt gegeben haben. Unter dem Eindruck der Terrorakte des 11. September und des Elbehochwassers 2002 hat die Innenministerkonferenz (IMK) 2002 die *Neue Strategie zum Schutz der Bevölkerung* beschlossen, die die Blaupause für die Rejustierung bestehender institutioneller Arrangements und Einrichtungen zur Regierung katastrophischer Risiken auf Bundes- und Landesebene gewesen ist. Der sichtbarste institutionelle Ausdruck der »neuen Strategie« auf Bundesebene war die Einrichtung des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK). Beim BBK wurde auch das Gemeinsame Lage- und Meldezentrum (GMLZ) eingerichtet, das deutsche Notfall-Informationssystem deNIS II aufgebaut sowie eine Reihe weiterer Maßnahmen initiiert. 2004 wurde ebenfalls der zuvor vom Robert Koch-Institut erstellte *Nationale Pandemieplan* von der Gesundheitsministerkonferenz zur Veröffentli-

---

<sup>110</sup> Auf diese Schlagseite der evolutionären Resilienz werde ich ausführlicher in Kapitel 4.4.1. sowie in Exkurs III mit Bezug auf das *Business Continuity Management* in Banken eingehen.

chung freigegeben, 2005 dann der *Nationale Plan zum Schutz der Informationsinfrastruktur* vom Bundesinnenministerium beschlossen, dessen Umsetzung das ebenfalls beim Bundesinnenministerium ansässige Bundesamt für Sicherheit in der Informationstechnik (BSI) überwacht. 2008 hat das Bundeskabinett die *Deutsche Anpassungsstrategie an den Klimawandel* (DAS) aufgelegt, die wichtige Implikationen für den Bevölkerungsschutz hat.<sup>111</sup> 2009 wurde vom Bundestag das Zivilschutzgesetz reformiert und dabei in *Zivilschutz und Katastrophenhilfegesetz* umbenannt. Im selben Jahr hat das Bundesinnenministerium zudem die *Nationale Strategie zum Schutz Kritischer Infrastrukturen* beschlossen. Die Finanzkrise ab 2007 war Auslöser für eine Reihe von Reformen zur Regulierung des Finanzmarktes, die häufig von internationalen oder transnationalen Körperschaften beschlossen wurden, aber auch unmittelbare Auswirkungen auf die Bundesrepublik hatten bzw. auf nationaler Ebene umgesetzt wurden. 2010 kam es zur Veröffentlichung des Bankregulierungsstandards Basel III, der seit 2013 gültig ist und bis 2018 vollständig umgesetzt sein soll. Ebenfalls im Jahr 2010 wurde das *European Systemic Risk Board* bei der europäischen Zentralbank (EZB) eingerichtet, das eine makroprudenzielle Bankenüberwachung zur Verhinderung oder Eindämmung systemischer Risiken in Europa leisten soll. 2011 hat das bei der Bank für Internationalen Zahlungsausgleich in Basel tätige *Financial Stability Board* (FSB) zum ersten Mal eine Liste mit global systemrelevanten Banken (*Global Systemically Important Financial Institutions*, kurz GSIFs) herausgegeben, die seither jährlich erneuert wird. Ein Jahr später wurde dann von der EU die *European Market Infrastructure Regulation* (EMIR) verabschiedet. In Reaktion auf die Eurokrise ist im Jahr 2010 zunächst der temporäre Euroschutzschirm gespannt worden (EFSF), der 2012 vom *Europäischen Stabilitätsmechanismus* (ESM) abgelöst wurde. 2011 wurde vom Bundeskabinett eine neue Cybersicherheitsstrategie verabschiedet sowie das nationale Cyberabwehrzentrum und ein Cybersicherheitsrat eingesetzt. 2015 folgte dann das IT-Sicherheitsgesetz, das insbesondere Betreiber Kritischer Infrastrukturen verpflichtet, verstärkte Maßnahmen zum Schutz ihrer Informationstechnik und somit der davon abhängenden Infrastrukturdienstleistungen vorzunehmen. Zusammengefasst ergibt sich eine ganze Batterie von Regierungsinitiativen, verstreut über eine Vielzahl gesellschaftlicher Felder und verteilt auf etliche Institutionen und Hoheitsgebiete.

---

111 Siehe dazu Kapitel 3.2.3.

Diese Maßnahmen sind zwar nicht das Ergebnis einer konzertierten Aktion, gehören aber dennoch zusammen. Das Prinzip ihrer Zusammengehörigkeit, das Netz, das die vielen Elemente verbindet und ihnen eine gemeinsame Ausrichtung gibt, ist das Sicherheitsdispositiv der Resilienz, das sich auf die Regierung der Katastrophe und die Kontrolle systemischer Risiken konzentriert. Von anderen Sicherheitsdispositiven – etwa der Souveränität oder der Normalisierung – ist dieses Dispositiv dadurch abgrenzbar, dass die Elemente (Institutionen, Gesetze, sozio-technische Vorrichtungen etc.), die das Dispositiv bilden, eigenen, analogen Problematisierungen folgen und von wiederkehrenden Technologien der Sicherheit getragen sind. Diese Ähnlichkeiten lassen sich entlang der vier Dimensionen kenntlich machen, die hier die Analyse des Dispositivs angeleitet haben: Zeit (1), Raum (2), Objekt (3) und Norm (4). Charakteristisch für das untersuchte Dispositiv ist dabei zunächst die *zeitliche Ausrichtung* wesentlicher Interventionsstrategien, nämlich die Vorbereitung auf ebenso unwahrscheinliche wie unvermeidliche Bedrohungen. Vorbereitung bzw. *preparedness* bildet eine genuine »attitude [...] of prudence« (Ewald 2002, 297), die in so unterschiedlichen politischen Strategien wie der *Neuen Strategie zum Schutz der Bevölkerung* und der Eurostabilisierung durch den ESM zum Tragen kommt (1).<sup>112</sup>

Das *räumliche Operationsfeld* des Sicherheitsdispositivs ist das »Milieu der Zirkulationen« (Foucault 2004, 42). Im nationalen Pandemieplan, aber auch in der *European Market Infrastructure Regulation* (EMIR) sollen Anschlüsse gesichert und Ströme kanalisiert werden und zugleich gefährliche Zirkulationen unterbunden und Überflutungen vermieden werden. Das nationale Territorium wird dafür in eine Reihe von »Risikozone[n]« zerlegt, um eine effizientere Allokation vorbereitender Sicherheitsressourcen zu ermöglichen (2).<sup>113</sup> Ferner gibt es geteilte *Sicherheitsprobleme und Schutzobjekte*, wobei hier zwei Gruppen unterschieden werden können: die Bevölkerung

---

112 Wie bereits erwähnt, operiert die Regierung der Katastrophe nicht nur durch Vorbereitung im Davor, sondern auch im Dazwischen und Danach. Die Betonung der Vorbereitung ist in dem bisher untersuchten Material dennoch so charakteristisch, dass ich hier vor allem darauf abstelle. Insbesondere im Kapitel 4 werde ich mich eingehender mit der zeitlichen Ordnung der Resilienzsicherheit im Dazwischen und Danach beschäftigen. Siehe dazu vor allem: Exkurs III.

113 Die Konzentration auf das Milieu der Zirkulationen war allerdings auch schon für das Sicherheitsdispositiv der Normalisierung kennzeichnend. Im Kapitel 3 werde ich genauer zeigen, wie sich die Morphologie des Milieus der Sicherheit im Verlauf des 20. Jahrhunderts geändert hat (siehe insbesondere die Systematisierung in Exkurs II).

und die Katastrophe sowie das System und das systemische Risiko. So soll eine Reihe von Maßnahmen die Bevölkerung vor *singulären Katastropheneignissen* schützen. Gleichzeitig richtet sich eine Reihe von Initiativen eher darauf, die Verwundbarkeit von »vitalen Systemen« gegenüber komplexen Ereignisverkettungen – *systemischen Risiken* – zu reduzieren (am deutlichsten erkennbar in den Strategien zum Schutz der Infrastruktur und des Finanz- bzw. Währungssystems). Dabei lässt sich für Deutschland seit Ende des ersten Jahrzehnts des neuen Jahrtausends eine Akzentverschiebung hin zur stärkeren Betonung des Problems systemischer Risiken, des Schutzobjekts vitaler Systeme und der Sicherheitsstrategie der Verwundbarkeitsreduktion beobachten. Die Systeme gelten dabei einerseits als vital für das Funktionieren der Gesellschaft und das Leben der Bevölkerung, andererseits aufgrund ihres endogenen Risikos aber auch als gefährlich und figurieren deshalb sowohl als Schutzobjekt wie als Gefährdungszusammenhang im Sicherheitsdispositiv (3). Schließlich orientiert sich das Dispositiv an der normativen Ordnung der Resilienz – in der *Nationalen Strategie zum Schutz Kritischer Infrastrukturen* wird ebenso wie in der Bankenregulierung Basel III versucht, robuste Systeme zu designen, die auch unter Stress nicht kollabieren. Resilienz ist dabei sowohl Technologie als auch *telos* der Sicherheit. Als Technologie der Sicherheit umfasst Resilienz Maßnahmen zum Aufbau von (redundanten) Ressourcen für den Notfall – von Eigenkapital bis zu Blutkonserven und Notstromaggregaten – ebenso wie Maßnahmen, die durch verändertes Systemdesign bestehende Verwundbarkeiten reduzieren wollen (die Maßnahmen reichen hier von der *European Market Infrastructure Regulation* bis hin zu lokaler Distribution von Lebensmitteln). Schließlich lässt sich der Aufbau von Kapazitäten des Krisenmanagements und der schnellen Reaktion auf Katastrophen durch Ersthelfer als operationelle Resilienz verstehen. Als veränderter *telos* der Sicherheit betont Resilienz die Notwendigkeit der evolutionären Anpassung von Systemen an neue Gefahrensituationen und Herausforderungen und steht damit für eine Abkehr der Vorstellung von Sicherheit als Zustand der Gefahrlosigkeit (4). Aufgrund dieser Doppelrolle als *telos* und Technologie, als normative Ordnung, die eine Reihe von konkreten Interventionsstrategien vorgibt, werde ich das herausgearbeitete Dispositiv als Sicherheitsdispositiv der Resilienz bezeichnen.<sup>114</sup>

---

114 Anders als der von Stephen Collier und Andrew Lakoff (2015) vorgeschlagene Begriff der *vital systems security* zur Bezeichnung kontemporärer Konfigurationen der Regierung der Katastrophe hat der Begriff Sicherheitsdispositiv der Resilienz den Vorteil, dass

Um diese vier Koordinaten – Zeit, Raum, Objekt, Norm – spannt sich das Resilienzdispositiv auf. Sie erlauben es, die Ähnlichkeit zwischen Maßnahmen zu erkennen, die scheinbar auf ganz verschiedene Probleme reagieren und verschiedene Effekte zeitigen. Darin liegt die einheitliche »strategische Ausrichtung« des Dispositivs, die gleichwohl ohne Strategen auskommt (siehe: Foucault 1978, 132). Es gibt keinen Akteur, keine Institution, keine zentrale Instanz, die im Hintergrund die Fäden zieht und die Maßnahmen des Dispositivs steuert. In diesem Sinne ist der Begriff des Dispositivs ein heuristisches Hilfsmittel, um die Gemeinsamkeiten verstreuter Entwicklungen zu bezeichnen. Das Dispositiv ist ein operativer Begriff, ein Werkzeug, das die Wirklichkeit auf eine bestimmte Weise zuschneidet, um einen aufschlussreichen Blick auf die betrachteten Phänomene zu erlauben. Gleichwohl hat das Dispositiv auch eine faktische Wirksamkeit. Es ist nicht nur das, was von einer einheitlichen Logik durchweht ist, es ist auch das Prinzip, das diese einheitliche Logik weiter ausbreitet, ein wirksames Dispersions- und Distributionsprinzip. Die Vorsilbe des Begriffs wird oft übersehen. Es ist ein Dis-positiv, also weder eine Gegebenheit, die einfach so beobachtbar wäre, noch eine bloße epistemische Konstruktion. Das Dis-positiv ist ein nicht positiver, nicht unmittelbar sichtbarer Teil der Wirklichkeit. Etwas, das die Positivitäten, die Gegebenheiten anordnet, verteilt und verbindet.

Zeit	Raum	Objekt	Norm
<i>Vorbereitung</i> für unwahrscheinliche und unvermeidliche Katastrophen	<i>Milieu</i> der Zirkulation, Risikozonen	<i>Bevölkerung</i> (Schutz der Bevölkerung vor Katastrophen) <i>Vitale Systeme</i> (Reduktion der Verwundbarkeit durch systemische Risiken)	<i>Resilienz</i> – operationelle Resilienz – systemische Resilienz (Vorratshaltung, Veränderung des Systemdesigns) – Adaptivität (evolutionäre Resilienz)

Tabelle 3: Die vier Achsen des Sicherheitsdispositivs der Resilienz

damit auch Maßnahmen gemeint sein können, die sich nicht auf Kritische Infrastrukturen und vitale Versorgungssysteme richten. Umgekehrt lassen sich Strategien zur Sicherung vitaler Systeme identifizieren, die nicht der Logik der Resilienz folgen.

## Exkurs zur Gesellschaft: Selbstgefährdung und Selbstbeschreibung

Es ist allzu verführerisch, das Sicherheitsdispositiv der Resilienz auf einen bestimmten Gesellschaftstypus zu beziehen.<sup>115</sup> Ist Resilienz nicht die quasi notwendige Form, die Sicherheit in der »Netzwerkgesellschaft« (Castells 2010) annehmen muss? Ist Resilienz nicht die adäquate Semantik einer globalisierten Gesellschaft, die aus ihrem nationalen Gehäuse herausgetreten ist, einer Gesellschaft, die ihre Autopoiesis zunehmend über globale sozio-technische Netzwerke abwickeln muss und dabei verstärkt aus ihrer Systemumwelt gestört wird? Aus dem Verlauf der Analyse sollte bereits klar geworden sein, dass das Begehren nach gesellschaftstheoretischer Übersicht nicht nur eine Regung des soziologischen Geistes ist. Auch die untersuchten Akteure des Sicherheitsdispositivs selbst nehmen eine gesellschaftstheoretische Beobachterperspektive ein, wenn sie versuchen, die neue Qualität der Gefährdungen sichtbar zu machen und Sicherheitsmaßnahmen zu rechtfertigen. Systemische Risiken – so die Sicherheitsexpert\_innen – betreffen schließlich die »ganze Gesellschaft« (ZöS 2008, 16) und erfordern daher eine »ganzheitliche [...] Betrachtung« (ZöS 2008, 26). Und tatsächlich kann der ultimative Horizont, auf den das Sicherheitsdispositiv sich bezieht – das *system of systems* verstanden als ein interdependenter Zusammenhang sozio-technischer Systeme – als ein spezifisch soziales Imaginäres<sup>116</sup> verstanden werden. Gerade die Problematisierung systeminterner Gefährdungspotenziale scheint ein Katalysator für (gesamt-)gesellschaftliche Selbstbeobachtungen zu sein. »[M]oderne, funktional stark differenzierte Gesellschaften [werden] als Folge des gesellschaftlichen Fortschritts und einer komplexen technischen Vernetztheit zunehmend verwundbar« (Schutzkommission 2011, 130) Die »Gesellschaft« wird sich ihrer selbst im ängstlichen Blick auf katastrophische Zusammenbrüche bewusst: Sie reflektiert sich als Gesellschaft, die sich zunehmend selbst gefährdet.

115 Das Sicherheitsdispositiv soll hier nicht im Sinne einer Diagnose der Gesamtgesellschaft – etwa: »die Resilienzgesellschaft« oder dergleichen – verstanden werden. Dass das Dispositiv wie gezeigt quer durch eine Vielzahl gesellschaftlicher Bereiche wirksam ist, heißt nicht, dass es koextensiv mit einem integralen Gesellschaftskörper ist. Vielmehr ist das Sicherheitsdispositiv nur eine von vielen wirksamen gesellschaftlichen Kräften.

116 Charles Taylor (2004, 2) hat zurecht darauf hingewiesen, dass ein solches soziales Imaginäres mehr ist als eine bloße Ideologie. »The social imaginary is not a set of ideas; rather, it is what enables, through making sense of, the practices of a society.«

Anstatt das Sicherheitsdispositiv in einem größeren gesellschaftlichen Rahmen zu verorten, bietet es sich deshalb an, die gesellschaftstheoretischen Rahmungen des Dispositivs selbst in den Blick zu nehmen, also gleichsam »die Gesellschaft« im Inneren des Dispositivs aufzusuchen.<sup>117</sup> Es ist gewiss kein Zufall, dass befürchtete (Selbst)Gefährdungen spezifische Gesellschaftsbeschreibungen evozieren. Schon Ulrich Beck hatte ja darauf hingewiesen, dass ein zentrales Charakteristikum der Risikogesellschaft darin besteht, dass sie sich selbst als solche versteht. Der Zusammenhang von Reflex (riskante Nebenfolgen gesellschaftlicher Rationalisierung) und Reflexion (auf diese Rationalisierung und ihre Folgen) ist zugleich ein Zusammenhang von selbstgefährdender »Selbstkonfrontation« (Beck in: Ewald 1993, 536) und Selbstbeschreibung. Allerdings hat Beck diesen Zusammenhang fälschlicherweise nur für die zweite Moderne konstatiert und damit einen grundlegenden Zusammenhang von Sicherheit und »Gesellschaft« übersehen, der ein immunologisches Denken des Sozialen notwendig macht. So hat etwa der italienische Philosoph Roberto Esposito jüngst in sozialontologischer Absicht argumentiert, dass jedes Gemeinwesen (*Communitas*) mit dem Problem einer exzessiven wechselseitigen Abhängigkeit und Ausgesetzttheit und damit einer irreduziblen Selbstgefährdung konfrontiert ist, auf die es mit Strategien der »Immunsierung« reagieren muss (Esposito 2004). Das *Paradigma der Immunsierung*, das Esposito (2014) vor allem für die Theoretisierung der Biopolitik produktiv gemacht hat, lässt sich auch für eine Analytik der Sicherheitsdispositive mobilisieren. Gefährdungen regen nämlich zu Selbstbeschreibungen an, so wie das Immunsystem eines Organismus immer dann, wenn es durch eine schädliche Beeinträchtigung provoziert wird, eine Selbstpräsentation erzeugen muss, die es erlaubt, das Eigene vom Eindringenden, das Harmlose vom Gefährlichen zu unterscheiden. Die Selbstbeschreibung im Angesicht der Gefahr hat insofern bereits eine sichernde, selbstvergewissernde Funktion. Allerdings ändert sich je nach Sicherheitsdispositiv die spezifische Art und Weise der wahrgenommen (Selbst)Gefährdung wie auch der Gesellschaftsbeschreibung, die diese Gefährdung in einem größeren Zusammenhang verortet und ihr so einen genuin »sozialen« Sinn gibt. So lässt sich

---

117 Diese Formulierung lehnt sich an Denkfiguren und den Sprachgebrauch von Latour an (siehe etwa: Latour 2007, 299–328, 2014, 542ff.). Die Forderung, gesellschaftliche Selbstbeobachtungen als Teil der Gesellschaft zu verstehen, finden sich sehr prominent freilich auch bei Luhmann (1998b, 866–1149) sowie bei und im Anschluss an Foucault (siehe etwa: Foucault 2001, Donzelot 1991).



unter Einsatz einer angemessenen Portion Stilisierung jedem Sicherheitsdispositiv – Souveränität, Normalisierung, Resilienz – eine spezifische Version der Gesellschaft zuordnen. Damit wird nicht wie bei Esposito ein Beitrag zur Sozialontologie geleistet, sondern vielmehr der historischen Ontologie des Sozialen am Leitfaden der Sicherheit nachgespürt. Darin lässt sich so etwas wie eine immunologische Wende des Denkens der Sozialität sehen.

Wie kein Zweiter hat Thomas Hobbes und insbesondere sein *Leviathan* (Hobbes 1966) das Denken souveräner Sicherheit geprägt. Hobbes Konzeption des menschlichen Lebens im Naturzustand, den er bei seinen Zeitgenoss\_innen im Bürgerkrieg vorfand, erblickt in der wechselseitigen Tötbarkeit der Menschen ein intrinsisches Gefährdungspotenzial des Gemeinschaftlichen: Der Mensch ist dem Menschen ein Wolf. Für Hobbes war der Gesellschaftsvertrag, der eine souveräne Macht einsetzt, deshalb der Sicherheitspakt der Wahl. Durch den Gesellschaftsvertrag schließen sich die Bürger\_innen zum Leviathan zusammen und bilden eine souveräne Macht, der sie sich fortan unterwerfen. Sie übertragen ihre Willkürfreiheiten an den Souverän. Dieser nimmt nunmehr das soziale Gewaltpotenzial in seine Hand und monopolisiert es im Staat. Als Gegenleistung für die »Selbstbeschränkung« der Bürger\_innen (die Einschränkung ihrer Freiheit und ihr Gewaltverzicht) sichert der Staat ihre »Selbsterhaltung« (Hobbes 1966, 131), indem er sie voreinander schützt. Die Paradoxie dieses Sicherheitsmodus liegt in der »Ironie der Gewaltrechtfertigung« (Loick 2012, 81–86) der Souveränität.<sup>118</sup> Die Staatssicherheit selbst wird zur Gefahr für Leib, Leben und vor allem die Freiheit der Individuen. Damit perpetuiert das staatliche Gewaltmonopol nur die nagende Angst der Menschen im Naturzustand und damit das affektive Band der Gesellschaftsmitglieder.

Bei der Evolution zum Vorsorgestaat (Ewald 1993) und der biopolitischen Bevölkerungssicherheit wurde ebenfalls ein intrinsischer Zusammenhang zwischen einer bestimmten Gruppe von Risiken und einem bestimmten Sein des Sozialen hergestellt. Hier geriet zunächst eine bestimmte Rationalität der Sicherheit – individuelle Haftung – an ihre Grenzen, als immer mehr statistische Evidenzen den genuin sozialen Charakter von Risiken wie Arbeitsunfällen, Arbeitslosigkeit und Armut deutlich machten.

---

118 Ähnlich identifiziert auch Roberto Esposito (2014, 359) in Hobbes' Theorie der Souveränität einen »Rest an Gewalt, den das immunitäre Dispositiv nicht vermitteln kann, da er von ihm selbst hervorgebracht wird.«

Die Kategorie der »sozialen Risiken« (Ewald 1993, 414) geht bereits von der Tatsache gesellschaftlicher Selbstgefährdung aus. »Das Soziale« erscheint als ein Zusammenhang allseitiger Gefährdung. Risiko und Gefährdung sind nicht nur eine Begleiterscheinung, sondern geradezu die Substanz der Gesellschaft.

»Wenn also die Gesellschaft mit Risiken einhergeht, dann nicht nur, weil unsere Gesellschaften gefährlicher geworden sind, sondern weil das, was wir als »Gesellschaft« bezeichnen, nur als Subjekt oder Grundlage von Risiken Sinn hat, die damit zu sozialen Risiken werden.« (Ewald 1993, 467)

Die bedrohliche Interdependenz des Sozialen, die phänomenhaft in der sozialen Verelendung der Industriearbeiter\_innen und den Ansteckungsgefahren urbaner Bevölkerungszusammenballungen erschien, wurde von der soziologischen Theorie auf einen organischen Sozialzusammenhang bezogen, der insofern als distinkt sozial angesehen werden konnte, als er nur aus »sozialen Tatbeständen« zusammengesetzt war. Jetzt erst war die Gesellschaft der Soziologie intelligibel geworden und hatte die politische Gemeinschaft der durch Vertrag vereinigten Individuen als wesentliche soziale Ontologie der Sicherheit abgelöst. Die genuin soziale Interdependenz der Gefährdung erheischt Solidarität für die von »sozialen Risiken« (Ewald 1993, 414) in Mitleidenschaft Gezogenen. Emile Durkheim (1988) mit seiner Theorie der organischen Solidarität, die einem arbeitsteiligen Kollektiv angemessen ist, kann deshalb – wie François Ewald (1993, 462) argumentiert – als der Soziologe des Vorsorgestaats verstanden werden (siehe auch: Donzelot 1988, 401). Der »Solidaritätsvertrag« (Ewald 1993, 449), dessen Kern das mächtige technische Instrument der Sozialversicherung ausmachte, konstituierte einen biopolitischen Sicherheitsmodus. Auch das normalisierende Sicherheitsdispositiv wurde von links wie von rechts für seine Pathologien und Paradoxien kritisiert. Gerade neoliberale Kritiker\_innen haben immer wieder auf die perversen Effekte des Wohlfahrtsstaats hingewiesen, der seine Rezipient\_innen entweder gar nicht erreiche oder sie abhängig und dadurch umso verwundbarer mache (zu dieser Kritik siehe unter anderem: Hirschman 1991, 27–34, Cruikshank 1999).

Die »Gesellschaft« des Sicherheitsdispositivs der Resilienz ist nicht mehr das Soziale der frühen Soziologie, sondern eher ein postsoziales<sup>119</sup>

---

119 Zum Konzept des Postsozialen siehe auch: Knorr Cetina und Bruegger (2004).

Gefüge Latour'schen Typs.<sup>120</sup> Das Netzwerk bzw. das vernetzte System ersetzt das Denkmodell des Organismus. Nicht mehr funktionale Arbeitsteilung oder ein Gesellschaftsvertrag, sondern technische, informatorische, räumliche, zeitliche etc. Anschlüsse stiften das Band des Gemeinsamen. »Der Leviathan ist ein Geflecht von Netzen« (Latour 2008, 159). Eine vernetzte und komplexe Bedrohung – das Terrornetzwerk – wird durch die netzförmigen Verwundbarkeitsstrukturen noch verstärkt – systemisches Risiko. Deswegen müssen die Schutzressourcen und Techniken ebenso Sicherheitsnetze bilden: von der Strategie »verteilter Sicherheit« über die resiliente Architektur von Computernetzen (Internet) bis hin zum vernetzten, heterarchischen Risikomanagement auf den Finanzmärkten (zur Proliferation des Netzdenkens in der gegenwärtigen Sicherheitspolitik siehe: de Goede 2012). Die Gesellschaft ist kein organisches Ganzes mehr, sondern ein ebenso zerfasertes und dezentriertes wie ultra-interdependentes Geflecht. Die Elemente dieses Netzwerkes sind nicht nur sozial. Sie setzen sich zusammen aus Menschen und Tieren, natürlichen Elementen, Prozessen und Agentien, technischen Artefakten und Programmen, es sind »Hybride, Mischwesen zwischen Natur und Kultur« (Latour 2008, 19) bzw. »Cyborgs« – Mischwesen zwischen Organismus und Maschine (Haraway 1987). Entlang der Lebensmittelkette versammeln sich Pflanzen, Tiere, Chemikalien, Keime, industrielle Produktionsverfahren, Medikamente und menschliche Produzent\_innen und Konsument\_innen. Die Übertragungswege der Pandemie durchqueren Flughäfen und Klimaanlage,

---

120 Diese Einschätzung mag auf den ersten Blick verwundern. Hat sich Latour nicht stets gegen jede Form der umfassenden Gesellschaftsbeschreibung – egal ob es sich dabei um den großen Leviathan (Callon und Latour 2006) handelt, oder um ein Soziales, das sich nur durch Soziales erklären lasse (Latour 2007, 13) – verwehrt? Gewiss, aber spätestens seit er sich vorgenommen hat, das Soziale »neu zu versammeln« (Latour 2007), blitzt bei Latour immer wieder eine ganz bestimmte Version der Gesellschaft auf, die sich sinnvoll auf die Selbstbeschreibung der *vital systems security* beziehen lässt. In einem gemeinsam mit Ulrich Beck geführten Interview hat Latour jüngst gefordert, nach einem neuen Leviathan zu suchen. »In Abwandlung der Hobbschen Theorie befinden wir uns in einem neuen Naturzustand. In einem Krieg aller gegen alle, in dem die Protagonisten nicht nur Wölfe und Schafe sind, sondern auch Thunfisch und Kohlendioxid, der Meeresspiegel, Wurzelknöllchen oder Algen. Das Problem ist, dass dieser Naturzustand, anders als bei Hobbes, nicht in der grauen Vorzeit liegt – er ist unsere Gegenwart. Wir erkennen, dass wir ein zivilisiertes Gemeinwesen nur schrittweise bauen können. Und auf diese Weise nach einem neuen Leviathan suchen, der mit Gaia fertig wird.« (Beck und Latour 2014) Sven Optiz (2016) hat in seiner scharfsinnigen Analyse der Latour'schen Kosmopolitik gezeigt, dass dessen Suche nach einem neuen Leviathan von einer spezifischen Katastrophenerfahrung – der globalen Erwärmung – ausgeht.

Krankenhäuser und Massenveranstaltungen, Menschen und Vögel. Infrastrukturen vereinen technische Elemente (Kabel, Straßen, Brücken, Schienen, Stromleitungen, Materiallager, Logistikzentren etc.) und soziale Elemente (Standards, Normen, organisatorische Routinen), die sich wechselseitig produzieren und stabilisieren. Sie ermöglichen soziale Vollzüge (Mobilität, Informationsübermittlung) und werden umgekehrt durch soziale Konventionen (Vereinheitlichung von Anschlussnormen) ermöglicht. Sie etablieren einen spezifischen, regulierten Bezug zur Natur (als Bestand, also als ständig verfügbare Ressource (Heidegger 2004, 20f.), bzw. als Umwelt großtechnischer Systeme (Hughes 1987, 53f.)) und werden zugleich vom unregulierten Rest und regulatorischen *spillover* (von Stürmen, Fluten, Erdbeben etc.) bedroht. Schließlich ist der Mensch Teil von infrastrukturellen Gefügen, aber nicht deren souveräner Bediener, sondern nur ein Element. Wie es in einem Bericht des BBK zu Kritischen Infrastrukturen heißt: »Nicht zuletzt der Mensch selbst ist wesentlicher Bestandteil eines Infrastruktursystems, z.B. in der Systemsteuerung oder als Wartungspersonal« (BBK-Städtetag 2010, 24) In einem erweiterten Sinne wird die Gesellschaft von den Sicherheitsexpert\_innen als Ökologie interdependenter Infrastrukturnetze, vitaler Systeme, gedacht. Die Gesellschaft ist das *system of systems*. Zwar sind die einzelnen Systeme durchaus spezialisierte Funktionssysteme. Aber insofern davon ausgegangen wird, dass sie wechselseitig füreinander systemwichtige Leistungen erbringen, kommt zugleich ein Ganzes in den Blick, das ansonsten in Subsysteme, Lebensformen, Sprachspiele, Professionen oder isolierte Individuen zerfasert scheint.

Die gesellschaftstheoretischen Rahmungen der Sicherheitsexpert\_innen sind ein zentraler Gegenstand der vorliegenden Analytik. Denn der Blick auf die »Gesellschaft« oder das *system of systems* ist selbst ein wesentlicher Mechanismus der Ausweitung der entsprechenden Sicherheitstechniken. Sicherheitsexperten entwerfen damit gleichsam eine Landkarte ihres potenziellen Betätigungsfeldes, auf dem sie sich selbst als »obligatorische Passagepunkte« (Callon 2006b, 149) einzeichnen und sich dadurch unentbehrlich machen können. Sie machen das sichtbar, was sie beherrschen und kontrollieren wollen, und bewirken so im Erfolgsfall die Ausweitung der Netze der Sicherheit.

Die postsoziale Kondition der Gesellschaft vitaler Systeme würde es eigentlich verbieten, dass der Sicherheitspakt nur zwischen den Mitgliedern eines politischen Gemeinwesens oder einer rein sozialen Gesellschaft geschlossen wird. Vielmehr wäre auch so etwas wie ein »Naturvertrag«

(Serres 1994) notwendig, der einer Kosmopolitik Gestalt gegeben könnte, die nicht nur wie bei Beck (2008, 94–129; 285–333) die soziale Weltgemeinschaft, sondern im Sinne Latours auch »Wurzelknöllchen und Algen« (Beck und Latour 2014) beinhaltet und so gleichsam ein planetarisches Kollektiv auf den Plan ruft, das zu ganz neuen Formen cyborgianischer Solidarität finden müsste.<sup>121</sup> Wie eine solche Kosmopolitik aussehen könnte, was ein Naturvertrag konkret beinhalten würde und wie sich dieser aushandeln lässt, ist noch nicht vollständig abzusehen.

	Souveränität	Normalisierung	Resilienz
Gesellschaft	Politischer Körper – Leviathan	Sozialer Körper – Organismus	Sozio-technisch-ökologisches Netzwerk, <i>system of systems</i>
Paradigmatische Gefahr	Bürgerkrieg	Soziales Elend, Arbeitsunfall	Katastrophischer Systemzusammenbruch
Art der Selbstgefährdung	Der Mensch ist dem Menschen ein Wolf	Soziale Interdependenz durch Arbeitsteilung, Ansteckung durch urbane Bevölkerungsdichte	Interdependenz komplexer Systeme, Fortsetzung von Störung und Unterbrechung, Ansteckung durch globale Vernetzung
Paradigmatischer Denker des Sozialen	Hobbes	Durkheim	Latour
Vertragswerk	Gesellschaftsvertrag	Solidaritätsvertrag	Kosmopolitischer Naturvertrag?
Sicherheitsmodus	Ausübung souveräner Macht, Staatssicherheit	Normalisierung, soziale Sicherheit bzw. Bevölkerungssicherheit	Resilienz, Sicherung vitaler Systeme
Paradoxie bzw. Kritik der Sicherheit	Staat bzw. souveräne Macht wird selbst zur Gefahr und perpetuiert Angst und Gewalt	Wohlfahrtsstaatlicher Paternalismus, Rezipient_innen des Sozialstaates werden abhängig und verwundbar	Vernetzung etabliert vitale Versorgungskanäle, aber auch Übertragungswege für (systemische) Gefährdung

*Tabelle 4: Die Gesellschaften der Sicherheitsdispositive*

<sup>121</sup> Isabell Stengers (2008, 153–185) hat zuerst ein Konzept der Kosmopolitik für Menschen und Nicht-Menschen in die Diskussion gebracht.

---

Was sich in der Analyse hingegen deutlich abzeichnet, ist, dass nicht mehr Souveränität oder Solidarität, sondern Resilienz als fortgesetzte Funktionstüchtigkeit der Systeme die wesentliche Lösung des neuen Sicherheitsdispositivs geworden ist. Sicherheit als Resilienz lässt sich gerade nicht mehr – wie bei Hobbes – durch Isolierung und Trennung der Mitglieder des Kollektivs erreichen. Es geht nicht mehr darum, ein bissiges Wolfsrudel auseinander zu treiben, sondern ein hoch-komplexes Infrastruktursystem zu errichten und zu warten. Es müssen gerade die Anschlüsse, Vernetzungen und Konnektivitäten des Systems bzw. zwischen den Systemen gesichert werden, ohne dabei gefährliche Übertragungswege für ausufernde Katastrophen zu erzeugen. Darin liegt die potenzielle Paradoxie der Sicherung des Kollektivs vitaler Systeme im Sinne des Resilienzdispositivs: die Vernetzung etabliert vitale Übertragungskanäle, die ihrerseits stets neue Störungs- und Katastrophenpotenziale erzeugen können.

### 3. Der Schutz vitaler (Öko)systeme

Vitale Systeme sind zum zentralen Problemkomplex des Sicherheitsdispositivs der Resilienz aufgestiegen. Wie in den vorausgegangenen Kapiteln gezeigt werden konnte, gelten sie als entscheidendes Schutzobjekt, weil das Funktionieren der Gesellschaft und das (Über)leben der Bevölkerung von ihnen abhängen. Sie gelten gleichzeitig aber auch als Gefährdungszusammenhang, weil sie selbst aufgrund ihrer internen Komplexität und Interdependenz ein intrinsisches Gefährdungspotenzial – systemisches Risiko – darstellen. Schließlich eröffnen sie ein Interventionsfeld für die Regierung der Katastrophe. Technologien zur Steigerung der systemischen Resilienz – Aufbau von Redundanzen, Veränderung des Systemdesigns – erlauben es, sich bereits in der Gegenwart auf eine unbestimmte, zukünftige Gefahr einzustellen. Während im vorherigen Kapitel vor allem herausgearbeitet wurde, *dass* vitale Systeme einen zentralen Problemkomplex im Sicherheitsdispositiv der Resilienz darstellen, vertieft dieses Kapitel die Untersuchung, indem es nachzeichnet, *wie* es zu dieser Entwicklung gekommen ist. Es fragt nach den historischen Entstehungszusammenhängen der gegenwärtigen sicherheitspolitischen Besorgnis um Kritische Infrastrukturen und vitale Versorgungsleistungen und verfolgt die Transformationen und Akzentverschiebungen dieser Sorge im Verlauf des 20. Jahrhunderts bis in unsere Gegenwart. Damit leistet die Arbeit einen Beitrag zur Erforschung der Versorgungssicherheit – eine in der sozialwissenschaftlichen Diskussion häufig vernachlässigte Dimension moderner biopolitischer Sicherheit, die gleichwohl zentral für das Verständnis der Funktionsweise des Sicherheitsdispositivs der Resilienz ist. Um den spezifischen Gehalt von Versorgungssicherheit zu bezeichnen, den ich in diesem Kapitel geltend machen werde, verwende ich den Begriff »Biopolitik vitaler Systeme«. Im Unterschied zur Biopolitik der Bevölkerung zielt die Biopolitik vitaler Systeme

nicht unmittelbar auf den Körper des Einzelnen oder der Gattung,<sup>122</sup> sondern auf die Gewährleistungen der technischen und ökologischen Bedingungen des Lebens.

Eine Reihe von Krisen und Systemzusammenbrüchen kann als Wegbereiter der modernen Problematik der Versorgungssicherheit und der temporären Biopolitik vitaler Systeme angesehen werden: die Verwüstungen der Infrastruktur und die Verwundbarkeit der Zivilbevölkerung im Ersten und Zweiten Weltkrieg, die Bedrohungen des Kalten Krieges, die disruptiven Effekte der Ölkrise von 1973 für die Wirtschaft und das öffentliche Leben westlicher Industriestaaten sowie das Bewusstwerden einer Vielzahl ökologischer Gefahren seit den 1970er Jahren. Auf ihre je spezifische Weise haben all diese Krisen und Systemzusammenbrüche sowie die Problematisierungen, die auf sie folgten, die für gewöhnlich im Hintergrund bleibenden sozio-technisch-natürlichen Voraussetzungen sozialer Vollzüge sowie die materiellen Bedingungen des Lebens der Bevölkerung in den Vordergrund gerückt. Sie haben die »immer schon« gegebene, aber zumeist implizit bleibende Angewiesenheit des Lebens auf technische, soziale und natürliche Strukturen jenseits seiner selbst explizit gemacht. These dieses Kapitels ist, dass dieser Explikationsprozess das Feld einer Biopolitik vitaler Systeme eröffnete bzw. ent- und ausfaltete, in welcher Lebenssicherung vor allem als Sicherung des Anschlusses an Systeme vollzogen werden muss.

Explizit wird so die Angewiesenheit des Lebens auf die Technosphäre der Infrastruktur. Durch das Kritisch-Werden der Infrastruktur ändert diese zumeist schweigende materielle Grundlage der Gesellschaft<sup>123</sup> ihren

---

122 Der Körper des Einzelnen und der »Gattungskörper« bilden Foucault (1977, 166) zufolge die beiden Pole der Biopolitik. Dabei spricht er manchmal von der »Bio-politik der Bevölkerung« (Foucault 1977, 166), um exklusiv den auf den Gattungskörper zentrierten Pol zu beschreiben. Hier verwende ich Biopolitik der Bevölkerung der Einfachheit halber in einem allgemeineren Sinn, nämlich in Abgrenzung zur Biopolitik vitaler Systeme. Klarerweise gilt für das Verhältnis von Biopolitik der Bevölkerung und Biopolitik vitaler Systeme dasselbe, was Foucault bereits in Bezug auf die Zweipoligkeit bemerkt hatte: sie bilden »keine Gegensätze«, sondern sind »durch ein Bündel von Zwischenbeziehungen verbunden [...]« (Foucault 1977, 166).

123 Infrastruktur heißt dem Wortsinn nach das Darunterliegende oder Unterbau. In jüngerer Zeit sind Infrastrukturen in der Geographie (Graham und Marvin 2001, Gandy 2004, McFarlane und Rutherford 2008), Anthropologie (Anand 2011, Larkin 2013), Soziologie (Mukerji 2010) und in den *Science and Technology Studies* (Star 1999, Bowker und Star 2000, Edwards 2003) zu einem wichtigen Thema geworden. Auch hier wird argumentiert, dass Infrastrukturen gleichsam die Grundlage der Gesellschaft darstellen, indem sie Men-



Modus und wird zur vielbesprochenen Zielscheibe der Machtausübung und des Sicherheitsdispositivs. Die Gesellschaft selbst bzw. zumindest ihre Sicherheitsexpert\_innen beginnen, Infrastruktur als »critical foundations« (PCCP 1997) wahrzunehmen, die geschützt werden muss, um das Leben der Bevölkerung und die Operationen von Ökonomie und Gesellschaft zu sichern.

Das Heraustreten vitaler Systeme aus dem Hintergrund auf die Bühne der Sicherheitspolitik betrifft aber nicht nur Kritische Infrastruktursysteme, sondern auch Ökosysteme. Wie ich zeigen möchte, sind nicht nur die Technosphäre, sondern auch Atmosphären und die Biosphäre zum Gegenstand der Biopolitik vitaler Systeme und des Sicherheitsdispositivs der Resilienz geworden. Auch sie gelten als vital für das Überleben nicht nur der nationalen Bevölkerung, sondern der menschlichen Gattung als solcher. Diese Dimension gegenwärtiger Sicherheitstechnologien wurde in den Debattenbeiträgen zur *vital systems security* bisher kaum beachtet (für wichtige Ansätze siehe allerdings: Braun und Wakefield 2014b, Braun 2014). Dabei kann die Analyse der Technologien der Sicherung vitaler Ökosysteme die Debatten um die Regierung der Katastrophe entscheidend bereichern. Erstens lässt sich so zeigen, dass die Rationalitäten des Umweltschutzes bzw. der *environmental security* (zu diesem Konzept siehe: Corry 2014, Dalby 2017) das Sicherheitsdispositiv der Resilienz entscheidend beeinflussen. Nicht nur, weil sie »die Umwelt« zum Schutzobjekt erklären, sondern auch, weil – wie ich nachzeichnen werde – genuin ökologische Sicherheitsstrategien Eingang in das Dispositiv finden. Nicht zufällig kommt das Konzept der Resilienz selbst aus dem Bereich der Ökosystemforschung. Zweitens steht das Aufkommen dieser ökologischen Sicherheitsrationalität für ein Problematisch- bzw. Reflexiv-Werden klassischer

---

sehen über räumliche und zeitliche Distanzen hinweg miteinander verbinden und somit die Netze der Gesellschaft ausweiten und auf Dauer stellen (Latour 1990, 2008, 159ff.). Zwar übernimmt die vorliegende Arbeit zentrale Einsichten dieser Beschäftigung mit Infrastruktur, zugleich verschiebt sie jedoch den Fokus der Analyse. Statt eines infrastrukturellen Fundamentalismus bzw. »infrastructuralism« (Sahlins 2010), der Infrastruktur an die programmatische Stelle setzt, die zuvor von der »sozialen Struktur« okkupiert war, richtet die Arbeit ihre Aufmerksamkeit auf die politischen Einsätze der Infrastruktursicherung, indem sie den Rationalitäten nachspürt, innerhalb derer Infrastrukturen als Technologien und Zielscheiben der Macht funktionieren. Sie verschreibt sich damit einem Forschungsprogramm, das sich am besten als Technopolitik beschreiben lässt (zu Debattenbeiträgen, die eine solche technopolitische Analysestrategie verfolgen siehe: Barry 2001, Mitchell 2002, Schnitzler 2008, Edwards und Hecht 2010, Collier 2011, Opitz und Tellmann 2015a, Folkers 2017c).

Politiken des Infrastrukturschutzes. Große Infrastrukturprojekte, denen lange Zeit ein entscheidender Beitrag für die Sicherung des Menschen *vor* der Natur zuerkannt wurde, werden von ökologischen Kritiker\_innen zunehmend als Gefährdungszusammenhang *für* die Natur betrachtet. Im Zuge dieses Reflexiv-werdens wird aber nicht einfach nur *die* Natur gegen *die* Technik ausgespielt, sondern die Unterscheidung von Natur und Technik selbst wird porös. Insofern lassen sich in Infrastruktur einerseits und Ökosystemen andererseits auch nicht einfach zwei separate Schutzziele ausmachen. Vielmehr ist, wie zu zeigen sein wird, die gegenwärtige Biopolitik vitaler Systeme von der Verschränkung von Bio- und Technosphäre gekennzeichnet.

Während im vorherigen Kapitel vor allem die Rekonstruktion der Technologien des Resilienzdispositivs und die Isomorphien zwischen unterschiedlichen Bereichen der Sicherheitspolitik im Vordergrund standen, geht es hier stärker als zuvor um die komplexe Topologie divergierender Sicherheitsstrategien, die sich bisweilen ergänzen und Wahlverwandtschaften miteinander aufweisen, sich bisweilen aber auch scharf widersprechen. Das Dispositiv der Resilienz operiert in einem komplexen Spannungsfeld unterschiedlicher Sicherheitsansprüche. Es versammelt eine Vielzahl von Akteuren mit häufig sehr widersprüchlichen Zielen und Interessen. Um die Emergenz dieses Spannungsfelds zu verstehen, ist das folgende Kapitel nicht nur gegenwartsanalytisch, sondern auch historisch angelegt und macht die Entwicklung des Sicherheitsdispositivs als Folge unterschiedlicher Kritiken der Sicherheit verständlich.

Das Kapitel nimmt drei historische Übergänge in den Blick: von der Daseinsvorsorge zum Schutz Kritischer Infrastruktur, von der »großen« zur »grünen Infrastruktur«, vom Atomstaat zur Energiewende. Dadurch lassen sich exemplarische Themen und Problemverschiebungen der Sicherung vitaler Systeme beleuchten. Die Analyse der genannten Übergänge bildet weniger eine Geschichte definitiver historischer Brüche. Vielmehr möchte ich mit dem Blick auf diese Übergänge exemplarisch Einsicht in zentrale Verlaufsmuster und Aktzentverschiebungen der Biopolitik vitaler Systeme herstellen. Zunächst gehe ich auf die deutsche Tradition des Infrastrukturschutzes ein, indem ich die Entstehung und Ausarbeitung des Konzepts der »Daseinsvorsorge« beim Juristen Ernst Forsthoff untersuche. Das Paradigma der Daseinsvorsorge, das in der noch jungen Bundesrepublik zunächst zu großer Bedeutung gelangte, wurde in den 1990er Jahren im Zuge der Liberalisierung der Infrastrukturen zunehmend durch

das Paradigma der »Gewährleistungsverantwortung« an den Rand gedrängt. Diese Transformation prägt auch die Politiken zum Schutz Kritischer Infrastrukturen (3.1.). Während in Kapitel 3.1. das juridische Prinzip der Daseinsvorsorge und die neoliberale Kritik an staatlichen Infrastrukturmonopolen untersucht werden, steht im nächsten Kapitel das »Vorsorgeprinzip« und die ökologische Kritik an großen Infrastrukturprojekten im Vordergrund. Das Kapitel zeichnet nach, wie umweltpolitische Problematiken auf dem Radar der Sicherheits- und Vorsorgepolitik erscheinen konnten und wie durch diese ökologischen Sensibilitäten sowohl große Infrastrukturprojekte wie auch die klassische Sicherheitspolitik der Daseinsvorsorge in die Kritik geraten sind (3.2.). Schließlich widme ich mich dem Problemkomplex der Energiesicherheit. Hier überschneiden sich die Themen der vorherigen Kapitel, weil im Feld der Energiepolitik sowohl ökologische Sicherheitsanliegen als auch Infrastrukturschutz von zentraler Bedeutung sind und nicht selten in Konflikt miteinander geraten. An diesem konkreten Feld möchte ich deutlich machen, wie kompliziert es ist, den multiplen Ansprüchen auf Sicherheit in der gegenwärtigen Gesellschaft gerecht zu werden (3.3.). Das Kapitel schließt mit Überlegungen darüber, wie sich das Konzept der Biopolitik in Anbetracht der hier skizzierten Entwicklung der *vital systems security* konzipieren und erweitern lässt. Ich plädiere für einen Analyserahmen, der gerade nicht nur die »politics of life itself« (Rose 2007), sondern auch die »Politik des Lebens jenseits seiner selbst« in den Blick nimmt. Nicht der Körper – egal ob der des Individuums, der Gattung oder der molekulare Körper genetischer Codes – stellt die zentrale Interventionsoberfläche der Biopolitik dar, sondern die Umwelt oder das Milieu (Exkurs II).

### 3.1. Von der Daseinsvorsorge zum Schutz Kritischer Infrastruktur

Erst vor dem Hintergrund der langen Tradition der Versorgungssicherheit wird verständlich, warum der Ausfall oder die Störung wichtiger Funktions- und Leistungssysteme zum entscheidenden Problembereich des Sicherheitsdispositivs der Resilienz geworden ist. In diesem Kapitel werde ich zunächst Problematisierungen und politische Projekte analysieren, die dazu beigetragen haben, dass die Technosphäre der Infrastruktur zum

Gegenstand der Sicherheitsbesorgnis geworden ist. Ich werde also die sich wandelnden Problemkonstellationen beleuchten, die der Techno-Biopolitik vitaler Infrastruktursysteme im Verlauf des 20. Jahrhunderts ihre je spezifische Gestalt gegeben haben: von der Daseinsvorsorge zum Schutz Kritischer Infrastrukturen.

Im Vorwort des BBK-Jahresberichts 2006 betonte der damalige Innenminister Wolfgang Schäuble, Katastrophenschutz gehöre zum »Kernbereich staatlicher Daseinsvorsorge« (BBK 2007b, 2). Äußerungen wie diese unterstreichen die anhaltende Bedeutung des Konzepts der Daseinsvorsorge für die deutsche Politik und insbesondere für das Selbstverständnis des Bevölkerungs- und Infrastrukturschutzes. »Daseinsvorsorge« fungiert dabei zumeist als unbestimmter Rechtsbegriff, um den Aufgabenbereich staatlichen bzw. kommunalen Handelns zu bezeichnen, der sich mit der Versorgung der Bevölkerung mit Diensten befasst, die wir heute »infrastrukturell« nennen würden:<sup>124</sup> Strom, Müllbeseitigung, Wasser, Telekommunikation etc. Trotz oder gerade wegen seiner Unbestimmtheit ist der Begriff der Daseinsvorsorge ungemein anschlussfähig. Staatliche ebenso wie zivilgesellschaftliche Akteure können sich bis heute auf den Begriff berufen, der 1938 mit Blick auf den nationalsozialistischen Staat von dem Juristen Ernst Forsthoff geprägt wurde.

Die anhaltende Konjunktur des Begriffs sollte allerdings nicht darüber hinwegtäuschen, wie grundlegend sich Bedeutung und Praxis der Daseinsvorsorge gewandelt haben. Denn das, was einmal staatliche bzw. kommunale Daseinsvorsorge war, wurde im Zuge der jüngsten Liberalisierungs- und Europäisierungsschübe gewissermaßen entkernt. Diese Entwicklung bedingt unverkennbar auch die sicherheitspolitischen Programmatiken des Bevölkerungsschutzes und insbesondere des Schutzes Kritischer Infrastrukturen. So heißt es im selben Jahresbericht:

»Insbesondere vor dem Hintergrund der Privatisierung vormals staatlicher beziehungsweise öffentlicher Infrastruktur-Einrichtungen der Daseinsvorsorge, wie Post, Telekommunikation, Bahn und Gesundheit, wird Sicherheit zunehmend auf mehrere Schultern verteilt.« (BBK 2007b, 24)

Die Sicherung von zentralen Versorgungsleistungen ist heute nicht mehr bloß Aufgabe des Staates, sondern ebenso privater Unternehmen. Infra-

---

124 Der Begriff »Infrastruktur« hat sich erst nach dem Zweiten Weltkrieg ausgehend von Bemühungen der NATO, ihre militärischen Strukturen aufeinander abzustimmen, eingebürgert (siehe: Laak 1999, 280f., NATO 2001).

struktursicherung wird dadurch neu verteilt. Und auch die Problematisierung und Gestaltung der Infrastruktursicherheit hat sich verändert. Beim Schutz Kritischer Infrastrukturen geht es neben der Abhängigkeit der Bevölkerung von Dienstleistungen zunehmend auch um die Interdependenz, also die wechselseitige Abhängigkeit von Infrastrukturen untereinander. Diese Interdependenz erzeugt wie bereits gezeigt systemische Gefährdungen, die durch eine Reduktion endogener Gefährdungspotenziale und den Aufbau systemischer Resilienz adressiert werden sollen.

Trotz dieser historischen Diskontinuitäten lassen sich bereits in Forsthoffs Schriften zur Daseinsvorsorge aus den 1930er Jahren die Konturen der gegenwärtigen Biopolitik vitaler Systeme erkennen. So hatte er bereits die »lebenswichtige Angewiesenheit« der Bevölkerung auf infrastrukturelle Versorgungsleistungen betont – und damit ein Motiv geprägt, das in gegenwärtigen Problematisierungen Kritischer Infrastrukturen wiederkehrt. Das Problem des Infrastrukturschutzes berührt den »Kernbereich« der Biopolitik in technologischen, industriellen Gesellschaften, in denen die Erhaltung und Steigerung des Lebens immer stärker von technischen Faktoren abhängig ist (Collier 2011) und in diesem Sinne als »bio-technico-political« (Rabinow 1995, 8) verstanden werden muss.<sup>125</sup>

Im Folgenden werde ich zunächst auf die Entwicklung des Konzepts der Daseinsvorsorge bei Ernst Forsthoff eingehen (3.1.1). Schon im Werk Forsthoffs hat das Konzept viele Wendungen genommen, welche die politischen Bedingungen reflektieren, innerhalb derer Forsthoff der Politik der Daseinsvorsorge Geltung verschaffen wollte. Erst in der BRD hat das Konzept die Wirkmächtigkeit entfaltet, die sich Forsthoff ursprünglich vom Nationalsozialismus erhofft hatte. Wie ich zeigen werde, hat sich der daseinsvorsorgende Staat mit der Liberalisierung der Infrastruktur und dem neuen, neoliberalen Leitbild des »schlanken Staates« in jüngerer Zeit jedoch immer stärker zum nur noch »gewährleistenden Staat« gewandelt

---

125 In der Biopolitikdebatte wird der Zusammenhang von Technik und Leben zumeist nur über das Thema der Biotechnologie verhandelt. In diesem Sinne spricht etwa Donna Haraway (1997, 12) von der Fortentwicklung der Biomacht zur Technobiomacht seit dem Zweiten Weltkrieg mit Aufstieg der Veränderungen der Lebenswissenschaften und Biotechnologien, die die neue Figur des »Lebens selbst« (Rose 2007, Haraway 1997, 12) hervorbringt. Hier möchte ich auf eine andere und bereits deutlich früher einsetzende Problematisierung des Zusammenhangs von Leben und Technik eingehen, die Haraways Periodisierung in Frage stellt. Das soll es auch erlauben, die Fokussierung der Biopolitikdebatte auf das Leben selbst in Richtung einer Politik des Lebens jenseits seiner selbst zu erweitern (siehe dazu auch Exkurs II).

(3.1.2). Die Programmatik zum Schutz Kritischer Infrastruktur – so werde ich schließlich argumentieren – ist in diesem Sinne eher ein »Kernbereich staatlicher Gewährleistungsverantwortung« als staatlicher Daseinsvorsorge. Was gleichwohl erhalten bleibt, ist die schon bei Forsthoff prominente Betonung der »Vitalität« der Daseinsvorsorge. Allerdings geht es jetzt nicht mehr nur um die Lebenswichtigkeit der Infrastruktur für die Bevölkerung, sondern zunehmend um deren Bedeutung für die Funktion interdependenter vitaler Systeme (3.1.3).

### 3.1.1. Die Vorsorgemaschine in der Vitalsphäre: Daseinsvorsorge bei Ernst Forsthoff

»Ein [...] wesentliches Merkmal der Technik ist ihre Affinität zur Macht.«  
(Forsthoff 1971, 34)

»Die Macht liegt nunmehr in den Infrastrukturen dieser Welt.«  
(Comité Invisible 2015, 80)

Ernst Forsthoff ist gewiss nicht der Erste, der staatliche Vorsorgebemühungen für infrastrukturelle Dienste eingefordert hat. Vielmehr lassen sich seine Interventionen in einer längeren Geschichte biopolitischer Interventionen verorten. Zunächst sind da die frühneuzeitlichen Entwicklungen des Polizeywesens, das anders als die heutige Polizei nicht nur die öffentliche Ordnung und die Bekämpfung von Kriminalität im Sinne hatte, sondern sich in einem umfassenden Sinne um die »Materialität der Existenz und der Koexistenz der Menschen [...], die materiellen Details des Tauschs und des Verkehrs [...] [und um die] Probleme der Gesundheit, der Straßen, der Märkte, des Getreides, der Verkehrswege« (Foucault 2004, 486f.) gekümmert hat, um so die »Kraft des Staates« zu steigern (siehe zur Policy insgesamt: Foucault 2004, 449–519). Ebenso lässt sich an Interventionen auf der Ebene des »Milieus« denken, mit denen im frühen 19. Jahrhundert die Hoffnung verbunden war, die in den industrialisierten Städten aufbrechenden »sozialen Fragen« zu beheben (Rabinow 1995, Foucault 2003). Was Forsthoff den damals noch vereinzelt und verstreut staatlichen Vorsorgebemühungen hinzugefügt hat, ist ein Begriff, der bis heute ein wesentlicher Bezugspunkt politischer Debatten ist: »Daseinsvorsorge«. Im Rahmen der Entwicklung dieses Begriffs hat Forsthoff eine eindrucksvolle Problembeschreibung der Lebensbedeutsamkeit von Infrastrukturen für

moderne, urbane Gesellschaften geliefert. Seine ebenso emphatische wie klare Herausarbeitung des vitalen Charakters von Technik und Infrastruktur in der industriellen Gesellschaft lässt sich mobilisieren, um die Verwobenheit der Bio- und Technopolitik der Sicherheit zu theoretisieren. In einem doppelten Sinne – als historisch wirkmächtiger Denker und als Denker der historischen Wirklichkeit – ist Forsthoff hier von Interesse.

Forsthoff studierte Rechts- und Staatswissenschaft, unter anderem bei Carl Schmitt. 1933 veröffentlichte Forsthoff sein Buch *Der Totale Staat*, das in vielerlei Hinsicht als »Bewerbungsschrift für die Nationalsozialisten« (Kaube 2002, 34) gelesen werden kann. Mit der Bezeichnung »totaler Staat« zielte Forsthoff gleichwohl nicht auf das, was nach 1945 als Totalitarismus bezeichnet werden sollte. Der »totale« Staat war für ihn vielmehr der Gegenentwurf zum liberalen Minimalstaat; ein Staat, der sich gerade nicht zurücknimmt, sondern – durchaus im Sinne der deutschen Polizei- und Staatswissenschaft des 18. Jahrhunderts – sein Betätigungsfeld erweitert. Diese Konzentration auf den Staat lehnten die Nationalsozialisten als »Etatismus« ab (siehe: Kersten 2005, 549). Schließlich wollte Forsthoff die Partei dem Staat unterordnen und nicht den Staat zur Beute der Parteiherrschaft machen.<sup>126</sup> Das zeigte sich auch in seiner Schrift *Die Verwaltung als Leistungsträger* von 1938, in der er erstmals das folgenreiche Konzept der Daseinsvorsorge entwickelte. Die Verwaltung, auf die Forsthoff in dieser Schrift zielte, sollte nämlich gegenüber der Spitze des Staates und dem »Führer« eine relative Autonomie genießen und technokratisch kontrolliert statt dezisionistisch vorgehen. Forsthoff – und das unterscheidet ihn von

---

126 Forsthoff wird später seine eigene »Theorie« des Totalitarismus entwickeln, die diesen auf die Ursupation des Staates durch die Partei zurückführt, und seine Rede vom »totalen Staat« als »schief, wenn nicht falsch« kritisieren: »Aber der Totalitarismus, der ein Prinzip ist – alles, was innerhalb der Staatsgrenzen geschieht, ist hoheitlich zu regeln und der totalen Herrschaft zuzurechnen – ist nicht Sache des Staates gewesen, nicht einmal in Zeiten des Absolutismus. Ein solches Prinzip ist mit dem Wesen des Staates als eines Garanten von Recht und Ordnung unvereinbar. Total kann nur eine Partei sein, die sich zur Volksbewegung ausgeweitet hat. Zum totalen Staat kommt es nur dann, wenn es einer solchen totalen Bewegung gelingt, sich des Staates zu bemächtigen und ihn für ihre Zwecke zu instrumentalisieren. Der totale Staat ist eine auf Missbrauch beruhende Entartung des Staates.« (Forsthoff, 1971: 54) Tatsächlich argumentieren Franz Neumann (1984) und auch Foucault (2006, 173ff.) ganz ähnlich: nicht der Staat, sondern die Partei kennzeichnet die Regierungsweise des Nationalsozialismus. Dass Forsthoff bei den Nazi-Funktionär\_innen gleichsam abgeblitzt ist – er erhielt in den vierziger Jahren ein Berufsverbot durch die Gestapo –, macht seine reaktionären und offen antisemitischen Positionen freilich nicht weniger problematisch.

seinem Lehrer Carl Schmitt – war ein Denker der Bürokratie, der legalen Herrschaft, und nicht des »Führers«, der charismatischen Herrschaft.<sup>127</sup>

Forsthoffs Problem in *Die Verwaltung als Leistungsträger* ist ein rechtliches. Der Problemhintergrund ist jedoch ein gesellschaftlicher. Das verleiht seinem Text einen geradezu soziologischen Einschlag. Seiner eigenen Disziplin wirft der Jurist eine unzureichende Reflexion über die Rolle der Verwaltung im modernen Staat vor. Die juristische Reflexion sei nämlich immer noch im liberalen Rechtsparadigma mit seiner klaren Gegenüberstellung von öffentlichem Recht und Privatrecht gefangen. Dabei haben sich – und hier beginnt Forsthoffs soziologische Problematisierung – die gesellschaftlichen Verhältnisse seit der Entstehung des liberalen Rechtsstaats so massiv gewandelt, dass diesem die gesellschaftliche Grundlage entzogen wurde. »Die Feststellung ist erlaubt, daß sich die rechtsstaatliche Ideologie einem sozialen Bilde zugeordnet hat, das nur bis Mitte des vorigen Jahrhunderts Realitätswert besaß.« (Forsthoff 1938, 4) Das »soziale Bild«, das Forsthoff für seine Gegenwart entwirft, nimmt seinen Ausgang von einer Reihe allgemeiner und durchaus gängiger Beschreibungen industrieller Gesellschaften in den 1930er Jahren. Forsthoff weist auf Phänomene wie Bevölkerungswachstum und Verstädterung hin und ruft – mit Bezug auf Ortega y Gasset (siehe: Forsthoff 1938, 4) – den Topos der Massengesellschaft bzw. der »massentümlichen Lebensform« (Forsthoff 1938, 7) auf. Seine entscheidende Pointe liegt aber in einer sozialvitalräumlichen bzw. rechtsräumlichen Überlegung. Wie für seinen Lehrer Carl Schmitt (2011, 13–20) ist das Recht für ihn nämlich eine »Einheit von Ordnung und Ortung«. Anders als Schmitt interessiert sich Forsthoff aber nicht so sehr für den geopolitischen »Nomos der Erde«, sondern für die immer poröser werdenden Grenzen zwischen öffentlichem Raum und Privatsphäre. Forsthoff unterscheidet zwischen dem beherrschten und dem effektiven Lebensraum des Menschen (Forsthoff 1938, 4). Der beherrschte Lebensraum ist der Bereich, über den der Mensch autonom verfügen kann und der ihm »eine Summe von Lebensgütern« liefert, die »eine vergleichsweise gesicherte Lebensbasis darstellen« (Forsthoff 1938, 5). Die Beispiele für solche beherrschten Räume – »[D]er Hof, der Acker,

---

127 Mit explizitem Bezug auf Max Weber bemerkt Forsthoff in *Die Verwaltung als Leistungsträger*: »Innerhalb fester Instanzenzüge hat das Charisma keinen Ort. Wer diese Organisationen der Daseinsvorsorge in die Hand bekommen will, muß einen Rechtstitel vorweisen, der ihm den Eintritt in die Befehlsgewalt gestattet, das heißt, er muss die Legalität für sich haben.« (Forsthoff 1938, 9)



der ihm gehört, das Haus, in dem er lebt.« (Forsthoff 1938, 4) – verweisen auf eine Welt, die bereits zu Forsthoffs Zeiten im Verschwinden begriffen war. So ist denn auch Forsthoffs These, dass die Domäne des beherrschten Lebensraumes im Verhältnis zum Einzugsbereich des effektiven Raumes schrumpft.

»Der effektive Raum ist derjenige, in dem sich das Leben, über den beherrschten Raum hinaus, tatsächlich vollzieht. Die industriell-technische Entwicklung des 19. und 20. Jahrhunderts hat es nun mit sich gebracht, dass sich der effektive Lebensraum vermöge der Ausbildung des modernen Verkehrswesens außerordentlich vergrößert hat und auch jetzt noch in der Zunahme begriffen ist, während der beherrschte Lebensraum sich stark verringerte [...]. Die zur Minimalisierung gehende Verengung des beherrschten Lebensraumes kennzeichnet die städtische, zumal die großstädtische Lebensweise.« (Forsthoff 1938, 4f.)<sup>128</sup>

Aus dieser Verringerung des beherrschten Lebensraums ergibt sich für Forsthoff eine neue, radikale Bedürftigkeit des modernen »Daseins«, das die Bedingungen seiner Existenz nicht mehr in der eigenen Hand hat. Das macht die große Masse der Bevölkerung »appropriationsbedürftig«, angewiesen auf Güter und Leistungen, die von anderen – Staaten und großen Unternehmen – bereitgestellt werden, kurz: angewiesen auf Daseinsvorsorge: »Diejenigen Veranstaltungen, welche zur Befriedigung des Appropriationsbedürfnisses getroffen werden, bezeichne ich als Daseinsvorsorge.« (Forsthoff 1938, 6). Daseinsvorsorge erbringt »Leistungen, auf welche der in die modernen massentümlichen Lebensformen verwiesene Mensch lebensnotwendig angewiesen ist.« (Forsthoff 1938, 7). Beispiele hierfür sind die »Versorgung mit Wasser, Gas und Elektrizität [...] die Bereitstellung der Verkehrsmittel jeder Art, die Post, Telephonie und Telegraphie, die hygienische Sicherung« (Forsthoff 1938, 7).

---

128 Forsthoffs Begriff des beherrschten Lebensraums wirkt wie eine Übersetzung des lateinischen Rechtsinstituts und Raumbegriffs des *dominium*: die Sphäre uneingeschränkter Souveränität des »Hausherren« über seine Güter, wozu unter anderem seine Frau, Kinder und Sklaven gehörten. Zugleich hatte das Konzept des *dominium* großen Einfluss auf das bürgerlich-liberale Eigentumsrecht (siehe: Kautzer 2007), das eine zentrale Angriffsfläche von Forsthoffs Intervention darstellt. Während Schmitt zeigen wollte, dass das moderne nationale Territorium von neuen Großraumordnungen unterhöhlt wird, versuchte Forsthoff also nachzuweisen, dass die bürgerliche Privatsphäre von der neuen Realität des effektiven Lebensraums so systematisch durchzogen wird, dass das bürgerliche Recht seine räumliche Grundlage verloren hat. Siehe dazu ausführlicher Folkers (2017c).

Forsthoff unterscheidet zwischen unterschiedlichen historischen Regimen der Daseinsvorsorge. Im 18. Jahrhundert war die individuelle Daseinsvorsorge dominant, die ab dem 19. Jahrhundert von einer kollektiven Daseinsvorsorge (zum Beispiel von Arbeiter\_innenvereinen) supplementiert wurde. Aber erst seit dem 20. Jahrhundert und insbesondere mit dem Aufkommen des Nationalsozialismus habe sich eine staatlich-politische Daseinsvorsorge entwickelt (Forsthoff 1938, 6). Paradigmatisch dafür galt Forsthoff ausgerechnet die »Leistungs- (Lieferungs-) Pflicht« des 1935 erlassenen »Energiewirtschaftsgesetzes« (Forsthoff 1938, 49). Das Gesetz war bis 1998 nahezu unverändert auch in der BRD gültig. Sein Ziel, die »Energieversorgung so sicher und billig wie möglich« zu gewährleisten, ist auch heute noch zentraler Grundsatz des mittlerweile erweiterten Energiewirtschaftsgesetzes. Für dieses Ziel sollten »schädliche Auswirkungen des Wettbewerbs« durch »öffentlichen Einfluss« und Förderung von »Verbundwirtschaft« (EnWG 1935) verhindert werden, wie es in der Vorrede zum Gesetzestext von 1935 hieß. Konkret führte das zu einer Dezentralisierung der Energieversorgung und zur Einrichtung von Gebietsmonopolen für die damals vorherrschenden Energieversorger. Diese Regelungen passen in eine Zeit, in der Synergieeffekte durch die Schaffung »gebündelter«, vertikal-integrierter Versorgungsunternehmen entstehen sollen (zur integrierten Infrastrukturentwicklung siehe: Graham und Marvin 2001).<sup>129</sup> Entsprechend finden sich regulatorische Maßnahmen, die zentrale Punkte des EnWG bereits vor der Machtergreifung der Nazis antizipiert haben. So wurde bereits im sogenannten »Elektrofrieden« von 1908 Gebietsvorherrschaften zwischen AEG und RWE festgelegt (Eckardt, Meinerzhagen und Jochimsen 1985, 25). Allerdings stand das Gesetz auch im Zusammenhang mit den seit der Machtergreifung der Nazis betriebenen Kriegsvorbereitungen. So hat der damalige Reichswirtschaftsminister Hjalmar Schacht die Regelung auch als »Gesetz zur Wehrhaftmachung der deutschen Industrie« (zitiert in: Eckardt, Meinerzhagen und Jochimsen 1985, 18f.) bezeichnet. Tatsächlich sollte die Dezentralisierung der Stromversorgung nämlich vor allem verhindern, dass es durch feindliche Luftangriffe schnell zu großflächigen Versorgungsenpässen kommt.<sup>130</sup>

---

129 Siehe dazu ausführlicher den folgenden Abschnitt 3.1.2.

130 »So wurde die Industrie im ersten Vierjahresplan schon 1933 aufgefordert, innerhalb von vier Jahren kriegsfähig zu sein. Dafür wurden eine weitgehend autarke Energiewirtschaft und eine Großraumverbundwirtschaft als Voraussetzung angesehen. Diese Verbundwirtschaft hatte die Aufgabe, kriegsfähige Produktionsanlagen mitein-

Forsthoff hob am Energiewirtschaftsgesetz allerdings weniger seine »Kriegswichtigkeit« als seine »Lebenswichtigkeit« hervor. Wichtig für seine Argumentation war vor allem, dass die Energiebetriebe nicht nur formell dazu verpflichtet wurden, der gesamten Bevölkerung Strom zukommen zu lassen, sondern dass die Regierung auch »materiell auf die Versorgungsbedingungen Einfluss nehmen« (Gesetzestext EnWG zitiert nach: Forsthoff 1938, 34) können sollte. Ähnliche Regelungen forderte Forsthoff auch für andere Infrastrukturdienste. Diese staatliche, politische Daseinsvorsorge erschien ihm notwendig, weil die infrastrukturelle Ausweitung des effektiven Lebensraumes traditionelle Aufteilungen von öffentlich und privat auflöste, wodurch ein neuer biopolitischer Bezugsraum entstand. Forsthoff hätte gewiss Giorgio Agamben zugestimmt, der feststellt:

»Jeder Versuch den politischen Raum des Abendlandes neu zu denken, muß von dem klaren Bewußtsein ausgehen, daß wir von der klassischen Unterscheidung von *zōé* und *bíos*, zwischen privatem Leben und politischer Existenz, zwischen dem Menschen als einfachem Lebewesen, das seinen Ort im Haus hat, und dem Menschen als politischem Subjekt, das seinen Ort im Staat hat, nichts mehr wissen.« (Agamben 2002, 197)

Noch bei seinen intimsten körperlichen Bedürfnissen (man denke etwa an den Gang zur Toilette) ist der moderne Mensch an die öffentlichen Netze der Infrastruktur angeschlossen. Die eigene Wohnung bzw. das Haus ist im wahrsten Sinne des Wortes eine »Maschine zum Wohnen« (Le Corbusier) geworden, weil sie nur durch ihren Anschluss an die Infrastruktur überhaupt bewohnbar wird. Deswegen wird die Vorsorge für ein »Dasein« notwendig, in dem nacktes Leben (*zōé*) und politische Existenz (*bíos*) in einer Zone der Ununterscheidbarkeit existieren. Diese Zone ist für Forsthoff jedoch nicht, wie für Agamben, das Lager, sondern vielmehr der »effektive Lebensraum« vitaler Infrastrukturnetze.

Der Begriff der Daseinsvorsorge ist schillernd und hat nicht zuletzt auch eine philosophische Resonanz. Der Existenzphilosoph Karl Jaspers (1999, 54) sprach nur wenige Jahre vor Forsthoff pejorativ von der »Daseinsfürsorge«. Und überhaupt lässt die Kombination von »Dasein« und »Sorge« an die deutsche Existenzphilosophie denken, deren prominenteste Ausprägung bekanntlich Martin Heideggers Daseinsanalytik darstellt. Zwar ist existentialistisches Pathos auch Forsthoff keineswegs fremd,

---

ander zu vernetzen, so daß bei der Zerstörung einer Leitung oder eines Kraftwerks die Energie aus noch intakten Quellen über unversehrt gebliebene Drähte herangeführt werden konnte.« (Eckardt, Meinerzhagen und Jochimsen 1985, 29)

aber letztlich scheint wichtiger für seine Überlegungen das Konzept der »Vorsorge« aus der Hegel'schen Rechtsphilosophie (Hegel 1970, 346) zu sein, vermittelt über den Hegelianer Lorenz von Stein, auf den Forsthoff mehrere Male affirmativ Bezug nimmt (etwa: 1938, 14). So hatte Hegel in der Polizei (in einem umfassenden, der Polizeiwissenschaft des 18. Jahrhunderts entsprechenden Sinn) das Organ erblickt, das eine angemessene »Vorsorge gegen die in jenen Systemen [der bürgerlichen Gesellschaft, A.F.] zurückbleibende Zufälligkeit« (Hegel 1970, 346) leisten kann. Schon bei Hegel finden sich also Überlegungen, die einen Vorsorgestaat antizipieren, der die Sicherheit seiner Bürger gegenüber den Kontingenzen bzw. Risiken der modernen Lebensform gewährleisten muss. Zudem argumentiert auch Hegel, dass die Bedürftigkeit des Menschen aus dessen Deterritorialisierung, also dem Verlust seines »angestammten« Raumes, entsteht. Der in der Moderne aus traditionellen und familialen Banden gelöste Mensch muss nunmehr auf dem fremden Boden der bürgerlichen Gesellschaft sein Leben bestreiten.

»Die bürgerliche Gesellschaft [...] substituiert [...] statt der äußeren unorganischen Natur und des väterlichen Bodens, in welchem der Einzelne seine Subsistenz hatte, den ihrigen und unterwirft das Bestehen der ganzen Familie selbst, der Abhängigkeit von ihr, der Zufälligkeit. So ist das Individuum Sohn der bürgerlichen Gesellschaft geworden, die ebensowohl Ansprüche an ihn, als er Recht auf sie hat.« (Hegel, 1970: 386)

Entsprechend hat die »polizeiliche Aufsicht und Vorsorge [...] für Straßenbeleuchtung, Brückenbau, Taxation der täglichen Bedürfnisse sowie für die Gesundheit Sorge zu tragen.« (Hegel, 1970: 384). Hegel und Forsthoff verbindet jenseits dieser Details eine grundsätzliche Ablehnung des liberalen Rechts- und Staatsverständnisses. Beide lehnen ein nur abstraktes bzw. formelles Recht ab und sind der Ansicht, dass die formellen Regelungen von einem starken Staat materialisiert werden müssen. Dafür bedarf jede Rechtsordnung jedoch eines materiellen Unterbaus, einer Infrastruktur.

Aber nicht nur die Bezüge, die Forsthoff mit seiner Begriffswahl herstellt, sondern auch die, die er zurückweist, sind aufschlussreich. Daseinsvorsorge steht nämlich vor allem im Kontrast zur Sozialfürsorge (Forsthoff 1938, 5).<sup>131</sup> Gilt letztere für »individuelle [...] Notlage[n]«

131 Dabei ist sich Forsthoff im Klaren, welches historische Sorgeregime der moderne Staat aufgreift und fortsetzt: die christliche *caritas*. In *Der totale Staat* sieht er die Aufnahme der christlichen Sorge in den modernen, staatlichen Sicherheitsapparat noch kritisch: »Der Apparaturstaat ist ein Staat ohne Gehalte, und wo sich ihm Gehalte aufdrängen, wo er

(Forsthoff 1938, 47), ist erstere von einer auf Grund der sozialen Stellung zustande kommenden Notsituationen unabhängig. »Auch der sozial verhältnismäßig Hochgestellte [...] ist auf die [...] Leistungen der Daseinsvorsorge [...] angewiesen.« (Forsthoff 1938, 47). Die Risiken, vor denen die Daseinsvorsorge schützen soll, betreffen unabhängig von »Stand und Klasse« die gesamte Bevölkerung; sie sind, um mit Ulrich Beck (1986, 48) zu sprechen, »demokratisch«. Das Soziale mit seinen Klassen, Interessengegensätzen und unterschiedlichen Verwundbarkeiten wird ersetzt durch das biopolitische Risikokollektiv »Dasein«. Die technischen Netze und vitalen Leistungen der Daseinsvorsorge halten dieses Kollektiv zusammen und sichern es – setzen es gleichzeitig aber auch einer bisher ungekannten Gefährdung aus und konstituieren so ein neues soziales Imaginäres. »Damit ist auch die lebenswichtige Verviesenheit des Einzelnen auf die Funktionen der Daseinsvorsorge zum Inhalt jenes politischen Bewusstseins der Verbundenheit geworden, welches die politische Gemeinschaft konstituiert.« (Forsthoff 1938, 19). Obwohl Forsthoff völkisches Vokabular nicht fremd war, konstruiert er die »politische Gemeinschaft« hier nicht als biologisch bestimmte Volksgemeinschaft oder »Rasse«. Zusammengehalten wird sie nicht durch das Blut, das durch ihre Adern fließt, sondern durch die »Leistungen der Daseinsvorsorge« – Wasser, Strom, Gas, Verkehr –, die durch die Netze der nationalen Infrastruktur zirkulieren. Nicht der Boden des Vaterlandes, sondern der »effektive Raum« als sozio-techni-

---

den Versuch macht, sie in sich aufzunehmen, da zerstört er sie, er nimmt ihnen ihr spezifisches Wesen, indem er sie auflöst in seine Normierungen und Berechenbarkeiten. Hans Freyer hat in seiner auch heute noch sehr bemerkenswerten Schrift »Revolution von Rechts« darauf hingewiesen, wie dieser Staat in seiner Sozialgesetzgebung und -verwaltung die Substanz des Sozialen, die christliche Caritas, zerstörte und aus Liebe Gesetz, aus Christentum Politik, aus freiwilliger Handreichung das einklagbare Recht machte, eine Wohltätigkeit mit Kartotheke, eine Liebe mit Instanzenentzug.« (zitiert nach: Ronellenfitsch 2004, 60) Später kam Forsthoff zu einer anderen, positiveren Einschätzung der Rolle des staatlichen Sicherheitsapparats. In einem Vortrag zum Anlass einer Kant-Feier bemerkte er 1941: »Die Daseinsvorsorge, in der Begegnung von Mensch zu Mensch ein Akt der Caritas, wird hier (im öffentlichen Raum) zum Akt der Gerechtigkeit, einer Gerechtigkeit, die in der kantischen Rechtslehre und ihrer Unterscheidung von Moralität und Legalität keinen Platz hat.« (Forsthoff 1941, 87) Hier wird erneut Forsthoffs Nähe zum Hegel'schen Rechtsdenken sichtbar. Daseinsvorsorge gehört in die Sphäre der Sittlichkeit (also jenseits von Moralität und abstraktem Recht). Auch Hegel hatte einen ähnlichen Übergang von der *caritas* zur staatlich-polizeilichen Vorsorge diagnostiziert: »Das Zufällige des Almosens, der Stiftungen, wie des Lampenbrennens bei Heiligenbildern usf., wird ergänzt durch öffentliche Armenanstalten, Krankenhäuser, Straßenbeleuchtung usw.« (Hegel 1970, 388)

sches »Milieu der Zirkulation« (Foucault 2004, 40f.) ist der »Lebensraum« dieser politischen Gemeinschaft.<sup>132</sup>

Gleichzeitig finden sich diese biopolitischen Überlegungen aufs Engste verbunden mit technopolitischen. Denn die lebenswichtige Verwiesenheit auf die Dienste der Daseinsvorsorge macht es notwendig, dass sich die Politik der Technik bemächtigt. Dafür muss die historisch vom Liberalismus überlieferte »Verdinglichung« der Politik aufgebrochen werden.

»Diese Kapitulation des Menschen vor den Dingen [...] überdauerte die Grenzziehung, welche die neuere Philosophie der naturwissenschaftlichen Begriffsbildung zuteil werden ließ, und die Scheidung von Naturwissenschaften und Geisteswissenschaften [...]. Erst in der Nachkriegszeit, als der Mensch begründeten Anlaß hatte, sich als Gefangener der Dinge zu fühlen, begann seine Auflehnung, sein Ringen um die Wiedererlangung des Primates.« (Forsthoff 1938, 17)

Daseinsvorsorge erfordert also eine »Verwaltung der Dinge«,<sup>133</sup> die zugleich eine Regierung über das Leben ist. Denn um zu leben, bedarf es der vitalen Dinge des Daseins, für die der Staat Vorsorge leisten muss. Durch seinen Zugriff auf Rohstoffe und Technik verfügt der Staat nämlich über eine bisher nicht gekannte »Verankerung in der Vitalsphäre der Bevölkerung« (Forsthoff 1971, 79). Er erhält »infrastrukturelle« (Mann 1984) oder »logistische Macht« (Mukerji 2010),<sup>134</sup> die es ihm gestattet, in Bereiche des

132 Hierin unterscheidet sich Forsthoffs Denken des Lebensraums auch grundsätzlich von dem geodeterministischen Lebensraumdenken von Friedrich Ratzel (zum Ratzel'schen Lebensraumdenken, siehe: Lemke 2007a, 24f., Abrahamsson 2013). Während bei Ratzel ein »natürlicher« Raum die Möglichkeiten zur Entfaltung der Zivilisation vorgibt, ermöglicht der sozio-technische Raum bei Forsthoff erst das Natürliche, nämlich das Leben der Bevölkerung.

133 Forsthoff hegte für Henri de Saint-Simon, der die Formel von der »administration du chose« geprägt hatte, große Bewunderung (Forsthoff 1971, 36ff.).

134 Michael Mann und Chandra Mukerji verfolgen mit ihren Konzepten der infrastrukturellen bzw. logistischen Macht ähnliche Ziele. Beiden geht es um die Etablierung eines alternativen Paradigmas der Macht, das sich von strategischer bzw. despotischer Machtausübung, die durch List, Täuschung oder Gewalt auf den Willen von Menschen einwirkt, unterscheidet. Während Mann dabei allerdings eher ein marxistisches Verständnis von infrastruktureller Macht eigen ist, bei dem es vor allem um die Frage geht, in wessen Händen die infrastrukturellen Machtmittel sind, betont Mukerji die relative Eigenständigkeit der Machtlogistiken. Diese erzeugen eine gebaute Umwelt, die einen spezifischen Möglichkeitshorizont der in ihnen lebenden Kollektive aufspannt. Des Weiteren geht es beiden um die Frage, wie es möglich war, dass staatliche Macht nicht mehr nur lokal und sporadisch, sondern systematisch über ein gesamtes Territorium ausgeübt werden kann. Entsprechend fokussieren beide auf den Einsatzzentrum logistischer bzw. infrastruktureller Macht in der frühen Neuzeit mit dem

(gesellschaftlichen) Lebens vorzudringen, die selbst den despotischsten Mächten bisher verschlossen waren. Zugleich ist infrastrukturelle Macht aber auch Biomacht, die Macht über das Leben der Bevölkerung ausübt, indem sie dieses ermöglicht, erhält und erweitert. Gerade diese Kombination aus Bio- und Technomacht erzeugt den ungeheuren und unheimlichen Machtzuwachs des Staates.

»[Der] absolute Polizeistaat konnte zwar das berufliche Leben reglementieren, er konnte Kant tadeln, Schiller zensurieren und die Verbreitung deterministischer Lehren verbieten, er konnte gewiß bis in die Einzelheiten bestimmen, *wie* gelebt werden sollte. Aber die Vorsorge dafür, *daß* überhaupt gelebt werden kann, lag nicht annähernd in gleichem Umfang bei ihm, wie heute. Insofern ist die Abhängigkeit des Menschen vom Staate im 19. und 20. Jahrhundert viel intensiver geworden, als sie es je in den vergangenen Jahrhunderten gewesen ist.« (Forsthoff 1938, 8, Hervorhebung im Original)

Die Kehrseite davon, dass der Staat zunehmend dafür sorgt, dass *überhaupt gelebt werden kann*, dass also die Biomacht das »Leben in ihre Hand nimmt« (Foucault 1977, 163), ist ein wachsendes nekropolitische Potenzial.<sup>135</sup> In ein weitverzweigtes und voraussetzungsvolles technologisches Milieu (den effektiven Lebensraum) eingebettet, wird das individuelle Dasein zum nackten Leben, das ohne seine technologische Nabelschnur und staatliche Vorsorge in einer Zone infrastruktureller Entkopplung dem Tod überlassen ist.<sup>136</sup> Unter techno-biopolitischen Bedingungen heißt »Leben machen« Anschlüsse herstellen und »Sterben lassen« den Stecker ziehen.

---

Aufkommen absolutistischer Territorialstaaten. Bei Forsthoff lässt sich sehen, wie sich die Problematik logistisch-infrastruktureller Macht im Rahmen der Biopolitik des 20. Jahrhunderts transformiert hat. Sie ist nicht mehr nur die Macht über ein Territorium, sondern die Macht zum und über das Leben: Biomacht.

135 »Aber diese ungeheure Todesmacht kann sich zum Teil gerade deswegen mit solchem Elan und Zynismus über alle Grenzen ausdehnen, weil sie ja nur das Komplement einer positiven Lebensmacht darstellt, die das Leben in ihre Hand nimmt, um es zu steigern und zu vervielfältigen, um es im einzelnen zu kontrollieren und im gesamten zu regulieren.« (Foucault 1977, 163). Biomacht beinhaltet also für Foucault sowohl das lebensfördernde »Leben machen« als auch das »Sterben lassen« (Foucault 2001, 282). Achille Mbembe (2003) hat den Begriff der Nekropolitik eingeführt, um damit die Kehrseite der lebensfördernden Biopolitik zu bezeichnen. Dabei versteht er Angriffe auf die infrastrukturelle Lebensgrundlage der Bevölkerung in gegenwärtigen militärischen Konflikten explizit als nekropolitisch (siehe: Mbembe 2003, 29).

136 Ich verwende den Begriff der »Zone infrastruktureller Entkopplung« wie Nadine Marquardt (2017) in Anlehnung an Castel (2000) und Barry (2006), um eine techniksociologische Sensibilität in der Soziologie der Exklusion bzw. umgekehrt eine exklusionssoziologische Sensibilität in der Techniksoziologie zu evokieren. Giorgio Agamben

Schon dieses gleichsam passive Tötungspotenzial des daseinsvorsorgenden (und das heißt für Forsthoff: nationalsozialistischen) Staates lässt erschauern. Aber auch die aktive »Nekropolitik« (Mbembe 2003) der Nazis – sowohl der biopolitische Krieg zur Erschließung von »Lebensraum« als auch die nationalsozialistische Vernichtungspolitik – war nur durch die »Funktionen der Daseinsvorsorge« (Autobahnen, Schienennetze, industrielle Produktion) möglich, die den deutschen »Volksgenossen« ihr Leben ermöglichen und sichern sollten. Die nationalsozialistische Vernichtungspolitik hat Forsthoff nicht antizipiert. Die biopolitische Kriegsführung<sup>137</sup> zur Erweiterung des Lebensraumes verstand er jedoch explizit als Bestandteil der Daseinsvorsorge:

»Denn es ist gerade eine entscheidende Folgewirkung der massentümlichen Lebensformen und der Beengtheit des völkischen Lebensraums, daß die Daseinsvorsorge, der Kampf ganzer Völker (nicht um imperialistische Ziele, sondern) um die Lebensbehauptung des Volkes selbst sowohl wie jedes einzelnen Volksgenossen als solche zu dem eigentlichen Politikum geworden ist, während jedenfalls die außenpolitischen Kämpfe der früheren Jahrhunderte im wesentlichen auf der Basis einer gesicherten Existenzgrundlage ausgetragen wurden.« (Forsthoff 1938, 12)

Die fatalen Implikationen der Politik der Daseinsvorsorge sind in Forsthoffs Text *Die Verwaltung als Leistungsträger* präsent und werden durch Publikationsort und -datum – Deutschland im Jahr 1938 – in der Rückschau noch unterstrichen. Kurz vor Beginn der Mobilmachung zum »totalen Krieg« schreibt Forsthoff hier über die materiellen, technischen und räumlichen Bedingungen dieser Mobilmachung und deren »vitale« Konsequenzen.

---

berührt in seinen eindringlichen Beschreibungen der Fälle »nackten Lebens« durchaus die technische Dimension der Biopolitik des nackten Lebens. Zur Figur der Ultrakomatosen bemerkt er korrekterweise: »Ihr Leben wird allein durch die Wirkungen der Reanimationstechniken auf der Basis einer juristischen Entscheidung erhalten« (Agamben 2002, 195). Letztlich theoretisiert Agamben aber nur die rechtliche Logik der Verbannung und nicht deren technologische und infrastrukturelle Dimension. Ich gehe hier davon aus, dass ein nacktes Leben dadurch produziert wird, dass man es von seinen umwelthaften Lebensbedingungen abschneidet. Das nackte Leben existiert nicht erst und hat dann noch eine Umwelt, sondern Leben ist immer schon Leben-in-Umwelten, so dass die Reduzierung auf ein nacktes Leben einen deprivativen Akt darstellt.

137 Zur Logik biopolitischer Kriegsführung bemerkt Foucault (1977, 163): »Kriege werden nicht mehr im Namen eines Souveräns geführt, der zu verteidigen ist, sondern im Namen der Existenz aller. Man stellt ganze Völker auf, damit sie sich im Namen der Notwendigkeit ihres Lebens gegenseitig umbringen. Die Massaker sind vital geworden.«



Dass Forsthoffs Konzept der Daseinsvorsorge dennoch bis heute überlebt hat und mittlerweile auch von linksliberalen und kommunitaristischen Initiativen als Losung verwendet werden kann, liegt wohl daran, dass seine Problemdiagnose des liberalen Rechtsdenkens eine Reihe von schwer abweisbaren Punkten enthält. Sowohl Hobbes als auch der Liberalismus waren prinzipiell davon ausgegangen, dass der Einzelne die Befriedigung seiner Lebensbedürfnisse autonom regeln kann. »Der bürgerliche Typus ist bestimmt durch die Sicherheit und Gewißheit, mit der er sich innerhalb der gesellschaftlichen Zustände geborgen weiß: jeder hat für sein eigenes Wohl zu sorgen.« (Forsthoff 1938, 44). Dem Staat kommt dann nur noch die Aufgabe zu, den Einzelnen vor den Angriffen Anderer und äußerer Feinde zu schützen, wie das Recht zugleich vor den Übergriffen des Staates schützen soll, so dass der Staat nicht nur öffentliche Sicherheit, sondern auch Rechtssicherheit bzw. Rechtsschutz garantieren muss. Öffentliche Sicherheit als substantielle, staatlich-biopolitische Sorgeleistung war lange Zeit nicht Teil des liberalen Sicherheitsdenkens und wurde daher zunächst nur kompensatorisch von der kirchlich-karitativen Wohlfahrtspflege übernommen. Die materiellen Bedingungen eines solchen Sicherheitsverständnisses haben sich unzweifelhaft aufgelöst, weil der Einzelne stets auf Teilhabe an Leistungen angewiesen ist, über die er prinzipiell nicht selber verfügen kann. Das »Problem der Teilhabe« (Forsthoff 1938, 15ff.) kann innerhalb der liberalen Rechtsdogmatik, die auf Rechtssicherheit und individuelle Freiheitsverbürgung abgestellt hat, nicht adäquat gestellt werden.

Selbst liberale Denker können kaum die Augen vor den Veränderungen verschließen, die durch die industrialisierte, technologische Gesellschaft ausgelöst wurden. Mit seinem Lösungsangebot, wie er es im Jahr 1938 formuliert hat, verlässt Forsthoff allerdings gänzlich die liberale Problematik der Sicherheit. Forsthoffs Konzept der Daseinsvorsorge ist in diesem Sinne nicht nur illiberal (Opitz 2008), seine Konzeption ist vielmehr antiliberal. Er will Freiheit durch Sicherheit ersetzen und nicht »nur« die Freiheit, notfalls mit freiheitsentziehenden Mitteln, sichern. »An dieser Stelle wird klar, daß eine rechtlich gesicherte Teilhabe an der Daseinsvorsorge, funktionell betrachtet, eine Art von Ersatz für jene überholten Sicherungen bietet, welche die Grundrechte in sich beschlossen.« (Forsthoff 1938, 46) Indem Forsthoff die Sicherung der Daseinsvorsorge gegen die Freiheit der Grundrechte ausspielt, reinszeniert er den Hobbes'schen *trade-off* von Freiheit und Sicherheit unter Bedingungen der industriellen Gesellschaft und biopolitischer Staatlichkeit.

Forsthoff ist von dieser Position später abgerückt. Bereits 1941, möglicherweise unter dem Eindruck eines ihm gegenüber verhängten Lehrverbots, hat er der Freiheit eine größere Rolle im Vorsorgestaat zuerkannt. »Nun plädiert Forsthoff [...] zum ersten Mal dafür, dass die staatliche Daseinsvorsorge der Persönlichkeit des Einzelnen angemessen sein muss.« (Kersten 2005, 55). In den 1950er Jahren gestattet sich Forsthoff sogar Überlegungen, die in Richtung einer Demokratisierung bzw. kommunaler Selbstverwaltung der Daseinsvorsorge gehen (Kersten 2005, 559). Allerdings hat er nie davon abgesehen, einen Gegensatz zwischen rechtsstaatlicher Sicherung der Freiheit und vorsorgestaatlicher Sicherung der Teilhabe und Existenz zu erkennen.

»Die rechtsstaatliche Verfassung ist nach ihrer Logik und Struktur auf die Gewährleistung von Freiheit, genauer auf die Sicherung der Gewißheit der gesetzmäßigen Freiheit angelegt. Diesen Zweck erfüllt sie optimal. Freiheit bedeutet Distanz des Einzelnen zum Staat. Hinsichtlich der Daseinsvorsorge ist jedoch das Interesse des Einzelnen genau gegenläufig: es geht auf die gesicherte Teilhabe an Leistungen.« (Forsthoff 1971, 78)

Neben dieser autoritären Grundhaltung ist er aber auch seinem Interesse für die politischen und rechtlichen Folgen der fortschreitenden Entwicklung der Technik treu geblieben. So argumentierte er in *Der Staat in der Industriegesellschaft* von 1971, dass Fragen der Technik bzw. »der technischen Realisation« heute vordringlicher seien als die soziale Frage (Probleme »der sozialen Realisation«), insofern letztere weitgehend gelöst sei. Vor allem Themenbereiche des Umweltschutzes und der Wahrung der Integrität der menschlichen Natur angesichts fortschreitender Möglichkeiten der Humangenetik trieben ihn nun um, denn ebenso wie im Fall der vitalen Infrastrukturdienste gehe es auch hier um Fragen des Lebens und Überlebens und damit um »mehr als die Freiheit«:

»Es geht um mehr als die Freiheit. Es geht angesichts der Expansion der Technik [...] – um den Schutz der Umwelt gegen die Zerstörung durch die Industrie und schließlich um die Integrität des Menschen selbst, nachdem dieser zum Gegenstand genetischer Forschung geworden ist.« (Forsthoff 1971, 25)

Auch Umweltschutz und Schutz des menschlichen Lebens selbst sind damit für Forsthoff Aufgaben der Daseinsvorsorge, verstanden als Sicherung des Existenziellen und Vitalen. Die Sicherung des Lebens ist der Sinn, das beständige *telos* der Daseinsvorsorge. Durch die anhaltende Fortent-

wicklung der Technik, die die Bedingungen des Lebens grundsätzlich verändert, bekommt die Daseinsvorsorge also eine expansive Dynamik.

In Debatten der *Critical Security Studies* hat sich mittlerweile der Eindruck verfestigt, dass der gegenwärtige Topos »Schutz Kritischer Infrastrukturen« seine Genealogie primär in militär-strategischen Überlegungen hat (Galison 2001, Dunn Cavelti 2008, Collier und Lakoff 2008, Graham 2011). Diese genealogische Abstammungslinie kann kaum bestritten werden. In dem Maße, in dem Logistik im zwanzigsten Jahrhundert zum entscheidenden Faktor in der Kriegsführung aufgestiegen ist (DeLanda 1991, 105ff.), wurde auch der Schutz heimischer Infrastrukturen zur zentralen Herausforderung militärischer Sicherheitsstrategien: sowohl um die Fortsetzung der industriell gewordenen Kriegsführung zu gewährleisten als auch um die Zivilbevölkerung zu schützen, die immer stärker in die biopolitische Kriegsführung involviert wurde. Gleichzeitig wird mit diesem Fokus auf das Militär häufig ausgeblendet, dass die Sicherung von Infrastrukturleistungen auch unabhängig von den Entwicklungen im Bereich der Kriegsführung im 20. Jahrhundert ein Gegenstand biopolitischer Sicherheitsprogramme geworden ist. Infrastrukturentwicklung und deren Sicherung sind spätestens seit dem 19. Jahrhundert ein zentraler Problembereich der »sozialen Moderne« (Rabinow 1995). Sie sind zu Gegenständen einer Politik geworden, die Hegel Vorsorge und Forsthoff Daseinsvorsorge genannt hat. Zu etwa der gleichen Zeit, in der Forsthoff das Konzept der Daseinsvorsorge ausarbeitete, ist in den USA die Politik des New Deal entstanden, die ebenfalls durch die staatliche Förderung großer Infrastrukturprojekte – sogenannte *public works* – den Wohlstand der Bevölkerung sichern wollte. Infrastrukturen sind dadurch Gegenstände einer sorgenden Sicherheitspolitik – der Versorgungssicherheit – ebenso wie eines souverän-militärischen Sicherheitsapparats geworden. Das Charakteristische der Problematisierungen und Strategien des frühen 20. Jahrhunderts ist wohl, dass beide Pole – souveräne Sicherheit und biopolitische Sicherheit – im Feld des Infrastrukturschutzes und der Kriegsführung artikuliert werden. Genauso wie Forsthoffs Konzept der Daseinsvorsorge auch mit Blick auf die Vorbereitungen zum »totalen Krieg« Nazideutschlands formuliert wurde, haben sich die ökonomischen Expert\_innen des New Deal in die Militärstrategien der USA während des Zweiten Weltkriegs gegen Nazideutschland eingebracht (Collier und Lakoff 2015, 28).<sup>138</sup> Diese dop-

---

138 Als die USA 1942 in den Weltkrieg in Europa eintraten, haben vor allem die Luftstreitkräfte Wirtschaftsplaner\_innen des New Deal in ihre Überlegungen zum *strategic bombing*

pelte – souverän-militärische und biopolitisch-wohlfahrtsstaatliche – Genealogie unterstreicht die Ambivalenz staatlichen Infrastrukturschutzes; eine Ambivalenz, die bis heute in Strategien zum Schutz Kritischer Infrastrukturen fortlebt. Es geht beim Schutz Kritischer Infrastrukturen eben nicht nur um nationale Sicherheit gegenüber Terroranschlägen oder Cyberangriffen, sondern ebenso um die (Minderung der) Folgen der Privatisierung für die Grundversorgung der Bevölkerung.

### 3.1.2. Von der Daseinsvorsorge zum Gewährleistungsstaat

Im nationalsozialistischen Staat sah Forsthoff die vielversprechendsten Ansätze für eine Politik der Daseinsvorsorge. Aber erst in der Bundesrepublik sollte sein Begriff Eingang in den Sprachegebrauch politischer Entscheidungsträger\_innen finden. Vor allem durch sein während der Zeit seines Lehrverbots im Nationalsozialismus geschriebenes *Lehrbuch des Verwaltungsrechts* (Forsthoff 1950), das kurz nach dem Krieg erschien, wurde »Daseinsvorsorge« zu einem zentralen Rechtsbegriff der Bundesrepublik. Forsthoffs Konzept der Daseinsvorsorge konnte auch deshalb so wirkmächtig werden, weil sich seine politischen Forderungen so vortrefflich ins »integrierte Infrastrukturideal« einpassten, das Stephen Graham und Simon Marvin (2001, 37–89) zufolge die Infrastrukturentwicklung in westlichen

---

einbezogen, um gezielter zentrale Knotenpunkte der deutschen Infrastruktur identifizieren zu können. Dabei zeigte sich vor allem die Treibstoffversorgung als neuralgischer Punkt der deutschen Industrie und Kriegsführung. Schließlich war es für Nazideutschland seit Kriegsbeginn schwer, Treibstoff zu beziehen. Die gezielte Zerstörung von Hydrierwerken in Deutschland, in denen Kohle zu flüssigem Kraftstoff verarbeitet wurde, sowie von Erdölförderinfrastrukturen der Achsenmächte in Rumänien, haben die Kriegsfähigkeit Deutschlands faktisch unmöglich gemacht. Albert Speer (1969, 357), damals Reichsminister für Rüstung und Kriegsproduktion, bemerkte in seinen *Erinnerungen* später: »Die chemischen Werke hatten sich als überaus bombenempfindlich erwiesen [...] [So] wurde der technische Krieg entschieden.« Ebenfalls bemerkt Speer, dass Hitler ab 1945 befohlen habe, die industrielle Infrastruktur zu zerstören, um dem »deutschen Volk« seine Lebensbedingungen zu entziehen (Speer 1969, 447f., Foucault 2001, 308) Nach dem Krieg war es vor allem der Morgenthau-Plan, der den Abbau der Kriegsfähigkeit Deutschlands durch industriell-infrastrukturelle Abrüstung vorsah. Der Marshall-Plan zum Wiederaufbau Deutschlands und Europas setzte kurze Zeit später bereits ein anderes infrastrukturelles Sicherheitsprojekt in Kraft: Europa sollte infrastrukturell so integriert und verkoppelt werden, dass Kriege zwischen den europäischen Nationen schon technisch-materiell nicht mehr möglich wären (siehe: Laak 2012, Opitz und Tellmann 2015a).

Industriestaaten im Zeitraum von 1850 bis 1960 anleitete. Forsthoffs Problembeschreibung und Konzept konnten so leicht verfangen, weil sie eine Reihe von Praktiken und Projekten ebenso rahmten wie befeuerten, die ohnehin im Gang waren. Forsthoff hat die Vorsorgepolitik weder erfunden noch bloß reflektiert, sondern verstreute Praktiken mit dem Begriff der Daseinsvorsorge versammelt.

Vom »integrierten Infrastrukturideal« sprechen Simon und Marvin zunächst aufgrund des ingenieurmäßigen Leitbildes moderner Infrastrukturentwicklung seit Ende des 19. Jahrhunderts. Planung und Entwicklung der Infrastruktur sollten gleichsam aus einem Guss erfolgen. Unterschiedliche Infrastrukturnetze wurden technisch aufeinander abgestimmt und miteinander verbunden.<sup>139</sup> Die moderne Infrastrukturentwicklung sollte nicht mehr sporadisch vorgehen, sondern unterschiedliche technische Elemente zu einem »technischen Ensemble« (Simondon 2012, 47ff.) verbinden. Entsprechend hat die Technikentwicklung des 20. Jahrhunderts, die mit der Elektrifizierung und der Digitalisierung gleich zwei umfassende Innovationssprünge erlebt hat, zunächst den charakteristischen Typus des »system-builders« (Hughes 1987, 52) und wenig später auch ein spezifisches, technisches Systemdenken hervorgebracht (Hughes 2004, 77–109), das bisweilen unter dem Begriff der Kybernetik firmiert. Zugleich ist »Integration« aber nicht nur ein technisches, sondern auch ein sozialpolitisches Ideal der Infrastrukturentwicklung. Infrastruktur wirkte gleichsam als gesellschaftliches »Integrationsmedium« (Laak 2001, 370), indem sie »erschließt, verbindet, verknüpft, vernetzt und integriert« und damit »zugleich Voraussetzung und Ergebnis von Interaktion zwischen räumlichen, zeitlichen und sozialen Schichten« (Laak 2001, 370) ist. Eine rationale Stadtplanung und die entsprechende technokratische Ideologie von Planer\_innen und Architekt\_innen wie Robert Moses oder Le Corbusier gehören für Graham und Marvin daher ebenso zum integrierten Infrastrukturideal wie eine auf Massenkonsumption im Privathaushalt ausgelegte Wirtschaftsordnung und eine über das gesamte nationale Territorium ausgerollte, integrierte und integrierende Infrastrukturplanung (siehe: Graham und Marvin 2001, 43). Dadurch wurde das Staatsgebiet infrastrukturell territorialisiert und für die Ausübung der »infrastrukturellen Macht« (Mann 1984) des Zentralstaates erschlossen.

---

139 Im deutschen Sprachraum wird häufig von Verbundwirtschaft gesprochen. So auch im Energiewirtschaftsgesetz der Nazis von 1935.

Der deutlichste Ausdruck dieses räumlichen Ideals der integrierten Infrastrukturplanung in der Bundesrepublik bestand in der grundgesetzlich verankerten Verpflichtung zur »Schaffung einheitlicher Lebensverhältnisse« (GG, Artikel 72, 2, seit 1994 heißt es nur noch abgeschwächt »Gleichwertigkeit der Lebensverhältnisse«) innerhalb des deutschen Staatsgebietes. Alle Bürger der Bundesrepublik sollten demnach Zugang zu den gleichen Leistungen der Daseinsvorsorge erhalten. Der Staat sah es als seine Aufgabe an, infrastrukturelle Netze auch in ländlichen Regionen auszubauen, um »unterschiedlich entwickelte Räume an ein gleichmäßig hohes Wohlstandsniveau heranzuführen« (Neu 2009b, 11). Zwar ist die Daseinsvorsorge vornehmlich eine kommunale Aufgabe – man spricht teilweise auch von »kommunaler Leistungsverwaltung« (Matzerath 1991). Aber der politische Horizont ist das nationale Territorium, das nunmehr jedoch nach Vorbild der Stadt angelegt wurde. Es kam zur Urbanisierung des Territoriums. So wurde die

»Einebnung des Stadt-Land-Gegensatzes [ein] bewußt angestrebtes Ziel, wobei im Vordergrund des politischen Interesses die Verhältnisse des flachen Landes stehen. Das bedeutet letztlich, daß »Urbanisierung« nicht mehr lediglich ein Prozeß innergesellschaftlicher Veränderung ist, sondern daß sie nunmehr Gegenstand und Ziel staatlicher Politik geworden ist« (Matzerath 1991, 23).

Zudem konnte und sollte der Bundesstaat die Infrastrukturentwicklung auf kommunaler Ebene mit zentral geplanten Maßnahmen flankieren. Ein wesentliches Instrument dieses Projektes waren nicht nur Gesetze, die – ähnlich wie das von Forsthoff besprochene Energiewirtschaftsgesetz – bestimmte Leistungs- und Lieferungsverpflichtungen festlegten, sondern vor allem eine Reihe staatlicher und halbstaatlicher Infrastrukturbetreiber. Die bekanntesten Beispiele hierfür sind sicherlich die Staatsbetriebe Post und Bahn. Auf kommunaler Ebene kamen eine ganze Reihe weiterer Infrastrukturdienste wie Müllentsorgung und Wasserversorgung hinzu. Häufig hatte man, bzw. hat man es teilweise bis heute, mit einem »Mischwesen aus Staat und Industrie« (Kersten 2005, 561) zu tun, etwa im Energiesektor, der von wenigen großen, monopolartigen Unternehmen dominiert und vom Staat massiv reguliert und subventioniert wurde.

Graham und Marvin zufolge verlor das integrierte Infrastrukturideal seit den 1960er Jahren langsam an Integrationskraft – und mit ihm, so können wir hinzufügen, das Konzept der Daseinsvorsorge in seiner bundesrepublikanischen Nachkriegsausprägung. Neue sozioökonomische Rahmenbedingungen (Neoliberalisierung und Postfordismus), sozial-

räumliche Transformationen (Globalisierung) und technische Innovationen (Digitalisierung) bewirkten diese Veränderung ebenso wie eine Reihe von Kritiken am integrierten Infrastrukturideal (Graham und Marvin 2001, 90–136). Sowohl seine mangelnde Verwirklichung als auch sein androzentrischer und westlicher Bias, aber auch die ökologischen Kosten moderner Großtechnologie wurden in den Neuen Sozialen Bewegungen immer wieder Ziel von Protesten, die zu einer Infragestellung einer Reihe technopolitischer Selbstverständlichkeiten westlicher Gesellschaften führten. Im Ergebnis führte diese Kritik gemeinsam mit den sozioökonomischen, technischen und räumlichen Veränderung dazu, dass das oft zur *black box* erstarrte Paket »integrierter Infrastruktur« wieder aufgeschnürt und »neu versammelt« wurde. Graham und Marvin (2001) bringen diese Prozesse auf den Begriff des »splintering urbanism«. Die vormals integrierte und zentrierte Infrastruktur zersplittert in neue sozio-technische und sozialräumliche Arrangements, was zum Abschied von »politischer Integration« als »Telos der Infrastruktur« (Laak 2001, 391) führt.

Diese Transformationen veränderten natürlich auch die Ausgangsbedingungen der Politik der Infrastruktur in Deutschland. Will man die Prozesse verstehen, die zur Veränderung der Daseinsvorsorge in der BRD beigetragen und veränderte Ausgangsbedingungen für die Infrastruktursicherung erzeugt haben, dann muss man den Blick auf die miteinander verschränkten Entwicklungen der Liberalisierung, der Europäisierung und des demographischen Wandels lenken. Zusammengenommen führten diese Prozesse zu einem neuen Leitbild der Infrastrukturpolitik, das mit dem Konzept der Daseinsvorsorge nicht mehr angemessen erfasst werden kann.

Die Liberalisierung der Infrastruktur ist mehr als die *Privatisierung* bzw. Teilprivatisierung staatlicher Betriebe (Mayntz 2009). Jenseits von Besitzverhältnissen haben sich nämlich vor allem die rechtlichen und ökonomischen Rahmenbedingungen für Infrastrukturbetreiber verändert. Die mit der Privatisierung einhergehende Deregulierung in Bereichen wie Telekommunikation und Schienenverkehr etwa hat erlaubt, dass die ehemaligen Staatsbetriebe wie Bahn und Post *Konkurrenz* durch andere Unternehmen bekommen können. Dadurch sind – insbesondere im Bereich der Telekommunikation – umkämpfte Märkte für infrastrukturelle Leistungen entstanden. Außerdem bestand im sogenannten *unbundling* ein weiterer Teil der Infrastrukturliberalisierung. *Unbundling* bzw. Entflechtung heißt, dass unterschiedliche Infrastrukturleistungen nicht mehr vom gleichen Betreiber

erbracht werden, sondern auf verschiedene Unternehmen aufgeteilt werden. Ein Beispiel wäre die Produktion, Transmission und Distribution von Strom; Dienste, die heute – zumindest formell – von unterschiedlichen Betrieben (Stromkonzernen und Netzbetreibern) erbracht werden. Dadurch wird die Durchgriffsmacht staatlicher Betriebe bzw. monopolistischer Großunternehmen geschwächt und – idealerweise – Verbraucher\_innen, die nun zwischen unterschiedlichen Anbietern auswählen können, gestärkt. Zugleich werden aber auch Kapazitäten zur zentralen Steuerung, Kontrolle und Sicherung von Infrastrukturleistungen vermindert.

Europa ist spätestens seit der Gründung der Montanunion 1951 immer auch, wenn nicht sogar vornehmlich, ein infrastrukturelles Integrationsprojekt gewesen (Opitz und Tellmann 2015a). Die forcierte Koordinierung von Politik und Ökonomie seit der Gründung der EU hat diesen Trend verstärkt. Heute ist Europa in vielerlei Hinsicht die maßgebliche »technical zone« (Barry 2006), in der die EU einheitliche »connection standards« (Barry 2006, 240) für die europaweite Interoperabilität der Infrastruktur vorgibt. Damit hat der transnationale Netzwerkraum Europas in vielerlei Hinsicht den Nationalcontainer als maßgeblichen Horizont für die Entfaltung der Infrastruktur abgelöst. Dabei findet weit mehr statt als nur ein sogenanntes *rescaling*, ein bloßer Wechsel des Größenmaßstabs. Es etabliert sich auch eine neue Idee davon, was die infrastrukturelle Integration dieses Raumes beinhalten soll und kann. So zeigt der Jurist Jens Kersten, dass in der EU ein neues rechtliches Leitbild entstanden ist, das sich vom bundesdeutschen Ideal der »Einheitlichkeit der Lebensverhältnisse« verabschiedet hat. Stattdessen wird »wirtschaftlicher, sozialer und territorialer Zusammenhalt« (Kersten 2008, 5) angestrebt: »Ziel der Netzpolitik ist also nicht, die Differenzen zwischen europäischen Zentren und Peripherien [...] einzuebnen. Vielmehr sollen die Zentren und die Peripherien angemessen verbunden werden.« (Kersten 2008, 5) Angestrebt wird eine »territoriale Kohäsion«, die das Entstehen von »entnetzten« Inseln vermeiden soll (Opitz und Tellmann 2015a, 182).

Schließlich wird auch der demographische Wandel immer wieder als Grund für die Veränderung der Daseinsvorsorge angeführt (Neu 2009c). In schrumpfenden Regionen, etwa in einigen Gebieten Ostdeutschlands, wird es immer schwieriger, das gleiche infrastrukturelle Serviceniveau zu gewährleisten, das in den dicht besiedelten Metropolregionen vorherrscht. Im Zuge dieser Veränderungen hat sich ein neues Paradigma infrastruktu-



reller Vorsorge entwickelt, das der »Gewährleistungsverantwortung« bzw. »Mindestgewährleistung« (Kersten 2008). »Infrastruktur ist nicht mehr die Vorleistung einer geräuschlosen staatlichen ›Vorsorgemaschine« (Kersten 2008, 3), weil der Staat die technischen Mittel dazu aus der Hand gegeben hat. Vielmehr will der Staat nur noch die Verantwortung dafür übernehmen, dass gewisse Dienste überhaupt zur Verfügung stehen. Der »Gewährleistungsstaat« ersetzt den Staat umfassender Daseinsvorsorge: »Der Staat [...] zieht sich Stück für Stück aus der Leistungserbringung zurück und stellt sicher, dass vormals staatliche Dienstleistungen nun durch andere (private) Anbieter erbracht werden.« (Neu 2009b, 12f.)

Zudem hat sich auch die räumliche Grundlage der Infrastrukturpolitik verändert: von der Topographie des Territoriums zur Topologie des Netzwerkes. Die Netze der Infrastruktur sollen nicht länger das gesamte nationale Territorium gleichmäßig durchwirken und integrieren, sondern transnationale Räume – wie die EU als technische Zone – »vernetzen«. »Territoriale Ungleichheit« (Neu 2009a) muss dabei in Kauf genommen werden. Lediglich technopolitische Exklusion in einem topologischen Sinn, also das Entstehen von »Zonen infrastruktureller Entkopplung« (Marquardt 2017), muss vermieden werden: Verhinderung von Ausschluss durch Anschluss.<sup>140</sup>

Diese doppelte sozioökonomische und sozialräumliche Deterritorialisierung hat die Ausübungsbedingungen und Modi infrastruktureller bzw. logistischer Macht fundamental verändert – mit entscheidenden Auswirkungen auf die Politik der Versorgungssicherheit. War bei Mann und Mukerji noch die Vorstellung, dass diese Infrastrukturen und Logistik es einem Zentralstaat ermöglichen, politische Macht über ein nationales Territorium gleichsam »auf Distanz« auszuüben, fällt in der neuen Kons-

140 Die Netz- oder Linienförmigkeit gehört gewiss zum Wesen der Infrastruktur, weshalb die Vorstellung einer vollkommenen infrastrukturellen Erschließung immer schon phantasmatisch ist (Latour 2008, 159). Das integrierte Ideal war eben genau das: ein Ideal, das nicht Wirklichkeit geworden ist, aber dennoch wirksam war. Ob eine territoriale oder topologische Matrix die Infrastrukturentwicklung anleitet, macht einen Unterschied, der sich selbst noch in Details wie schlechtem Handyempfang in ländlichen Regionen zeigen kann. Diesen Unterschied kann ein »topological approach« (Harvey 2012, 76) zur Analyse von Infrastruktur bzw. das Festhalten am Netzwerk als grundlegender Beschreibungssprache allzu leicht aus den Augen verlieren. Stattdessen wäre es sinnvoller, von einem »becoming topological« (Lury, Parisi und Terranova 2012) infrastruktureller Macht auszugehen, in deren Rahmen das »nationale Territorium« in dem Maße deterritorialisert wird, wie es gleichzeitig zu einer Reterritorialisierung »transnationaler Netzwerke« kommt.

tellation sowohl die Zentralstellung des Staates als auch die räumliche Grundlage des nationalen Territoriums weg. Die infrastrukturelle Macht ist jetzt auf eine Vielzahl von Infrastrukturbetreibern verteilt und verstreut sich über Netzwerke transnationaler Reichweite. Der Staat ist zwar nicht bedeutungslos geworden, aber er steht weniger im Zentrum der infrastrukturellen Macht als vielmehr begleitend an ihrer Seite. Er übt nicht alleine Macht aus, sondern versucht vor allem zu überwachen und zu »gewährleisten«, dass es zu keinem Missbrauch logistischer Macht kommt. Der Leviathan ist nicht mehr das souveräne Zentrum der Macht und Garant der Sicherheit, sondern Teil eines »Geflecht[s] von Netzen« (Latour 2008, 159).

### 3.1.3. Kritische Infrastruktur: Versorgungssicherheit im Gewährleistungsstaat

Der Übergang zwischen den Paradigmen der Daseinsvorsorge und der Gewährleistungsverantwortung ist fließend. Auch die Daseinsvorsorge wurde häufig über gesetzliche Verpflichtungen privater Infrastrukturbetreiber gesichert. Nur in einigen Fällen erfolgte sie unmittelbar durch staatliche Betriebe. Zudem ist der Staat bis heute in einer Reihe von ehemaligen Staatsunternehmen Mehrheitsaktionär und besetzt zentrale Posten in der Unternehmensführung. Vielfach sind die Zuständigkeiten, Einflussmöglichkeiten und Besitzverhältnisse für die Infrastrukturen ähnlich verwickelt und unübersichtlich wie ihre technischen Netze. Aber auch wenn die substanziellen Leistungen der Daseinsvorsorge nach wie vor von einem »Mischwesen aus Staat und Industrie« bereitgestellt werden, wie schon Forsthoff in den 1970er Jahren diagnostizierte, so macht es doch einen Unterschied, ob dieses Mischwesen als »Stamokap« (staatsmonopolistischer Kapitalismus) oder als »PPP« (Privat Public Partnership) aufgefasst wird.

Das Gewährleistungsparadigma hat sich auch im Bevölkerungsschutz und insbesondere im Schutz Kritischer Infrastrukturen durchgesetzt. Zwar wird in der *Nationalen Strategie zum Schutz Kritischer Infrastrukturen* die »Gewährleistung des Schutzes der Kritischen Infrastrukturen als Kernaufgabe staatlicher Sicherheitsvorsorge« (BMI 2009, 3, Hervorhebung A.F.) verstanden. Zugleich aber wird bemerkt, dass mit dem Trend zur Privatisierung der Infrastruktur

»auch die Verantwortung für die Sicherheit, Zuverlässigkeit und Verfügbarkeit dieser Infrastrukturen zunehmend in private, zumindest aber geteilte Verantwortung über[geht]. Staatliche Aufgaben [...] bewegen sich damit vorrangig im Rahmen einer Gewährleistung, allenfalls der Sicherstellung der Versorgung in Krisenzeiten« (BMI 2009, 6).

Der Paradigmenwechsel zum Gewährleistungsstaat ist also kein stummer Prozess, der nur von Sozialwissenschaftler\_innen diagnostiziert wird, sondern eine explizite Ausgangsbedingung des Regierens und der Infrastruktursicherung der Gegenwart, wie auch in meinen Interviews im BBK zu Fragen des Schutzes Kritischer Infrastrukturen deutlich wurde.

»Also früher ist man davon ausgegangen, in den 1950er, 1960er, 1970er Jahren, dass der Staat [...] für eine allumfassende Daseinsvorsorge verantwortlich war. Für die Versorgung der Bevölkerung mit sämtlichen Gütern und Dienstleistungen, die sie brauchen. Das heißt, der Staat der Daseinsvorsorge war tatsächlich auch immer die staatliche Aktivität. [...] Der Gewährleistungsstaat rückt von diesem Konzept etwas ab, indem er sagt: Ja, Daseinsvorsorge ist immer noch wichtig. (Auch wenn wir nicht genau wissen, was alles dazu gehört) [*spricht Klammern aus*]. Aber wir müssen es nicht selber machen, wir müssen nur dafür Sorge tragen, dass die Güter und Dienstleistungen da sind. Aber ich bin nicht mehr der Staat der Daseinsvorsorge, der alles selber macht. Sondern ich privatisiere auch und stehe in vielen Teilen als Garant zur Verfügung.« (Interview 1)

Das Ideal der Daseinsvorsorge ist keineswegs verschwunden, tritt aber verstärkt in Konkurrenz zu Idealen wie Wettbewerb und Wirtschaftlichkeit. Infrastruktursicherung muss deshalb unterschiedlichen und im Zweifel auch widersprüchlichen Interessen gerecht werden. Der Schutz Kritischer Infrastrukturen »leistet damit für Unternehmen einen Beitrag zur Wertschöpfung sowie zur Einhaltung bestehender rechtlicher Bestimmungen und unterstützt Behörden im Rahmen ihrer Daseinsvorsorge« (BMI 2011). »Vernetzte Sicherheit« im Bereich des Infrastrukturschutzes heißt: »Zusammenarbeit von Staat und Wirtschaft in etablierten Sicherheitspartnerschaften« (BMI 2009, 6). Nicht nur Hilfsorganisationen wie das Rote Kreuz oder die DLRG, sondern etwa auch Die Bahn, IBM, Vattenfall oder die Commerzbank sind die wesentlichen Partnerunternehmen der staatlichen Sicherheitspolitik.<sup>141</sup> Das BBK ist ein »Netzknoten« zwischen Unter-

141 Siehe dazu etwa die Liste der beteiligten Unternehmen an den Broschüren des Innenministeriums zum Schutz Kritischer Infrastruktur: BMI, BBK und BKA (2005, 1), BMI (2011, 2).

nehmen und Staat und soll »Kooperationen zwischen Behörden und Unternehmen auf[...]bauen« (BMI, BBK und BKA 2005, 28).

Was genau verändert sich durch die Liberalisierung der Infrastruktur und durch die neu entstanden Sicherheitspartnerschaften? Auf den ersten Blick scheint die Privatisierung, De-Monopolisierung und Entflechtung der Infrastruktur den Bemühungen zur Bekämpfung systemischer Gefährdungen entgegenzukommen. Nicht nur lässt sich die Notwendigkeit zur privat-öffentlichen Kooperation gut mit dem Paradigma »vernetzter Sicherheit« vereinbaren. Zudem scheint die Entflechtung der Infrastruktur im Zuge ihrer Liberalisierung das Potenzial zu haben, gefährliche Vernetzung, »exzessive Interkonnektivität« (BIS 2010, 7) und »Monopolrisiken« (Allianz 2008, 47) zu reduzieren, die mit dem Auftreten systemischer Risiken in Verbindung gebracht werden (siehe Kapitel 2.4.). Pauschale Aussagen verbieten sich zwar, weil die Liberalisierungsprozesse je nach Bereich höchst unterschiedlich verlaufen sind und nicht immer ein klarer Trend zur Entflechtung zu verzeichnen ist.<sup>142</sup> Allerdings lassen sich eine Reihe von technischen, räumlichen, organisatorischen und ökonomischen Gegen-trends identifizieren, die die scheinbar einfache Rechnung »splintering urbanism« (Graham und Marvin 2001) = »distributed preparedness« (Collier und Lakoff 2008), also die Idee einer Erhöhung systemischer Resilienz durch verstreutes Systemdesign, durchkreuzen.

Veränderte technische Bedingungen haben die Vernetzung der Infrastruktur prinzipiell erhöht. Das betrifft insbesondere die Stromversorgung und die Digitalisierung (BMI, BBK und BKA 2005, 5, BMI 2011, 9).

»Zahlreiche Kritische Infrastrukturen, die in der Vergangenheit physisch und logisch getrennte Systeme darstellten, sind inzwischen durch technologischen Fortschritt mit anderen Infrastrukturen vernetzt. Dies gilt insbesondere in Hinblick auf Energieversorgung, Informationstechnologie und Telekommunikation.« (BBK 2009c, 25)

Zudem hat die Liberalisierung auf europäischer Ebene zur Entstehung transnationaler Infrastrukturnetze beigetragen und damit räumliche Abhängigkeiten erhöht. Mit der Ausbreitung von transnationalen Märkten für Dienste wie Strom und Telekommunikation hat sich auch die transnatio-

---

142 So lässt sich etwa die Aufhebung des Trennbanksystems in den 1990er Jahren in den USA, die immer wieder mitverantwortlich für die Finanzkrise 2008 gemacht wird, als genauer Gegenteil zur Entflechtung verstehen. Auch in Deutschland sind die Entflechtung der Infrastrukturen und das Ende von Monopolstrukturen häufig allenfalls formal vollzogen.

nale Vernetzung der entsprechenden Infrastrukturen verstärkt. Neben intensiver technischer entsteht also auch eine extensive räumliche Vernetzung zwischen Infrastrukturen. Das hat die Europäische Union auf den Plan gerufen, die zu einem wesentlichen Motor der Bemühungen zum Schutz Kritischer Infrastrukturen geworden ist. Bereits 2005 legte die Kommission ein *Grünbuch* zum Schutz Kritischer Infrastruktur auf (EU 2005). Unmittelbarer Anlass waren zwar die Terroranschläge auf Verkehrsinfrastrukturen in London und Madrid, aber es waren gerade die durch die Liberalisierung der Infrastruktur veränderten Rahmenbedingungen, die dem *Grünbuch* zufolge gemeinsame Anstrengungen der Mitgliedstaaten auf europäischer Ebene notwendig machten.

»Die Beschädigung oder der Ausfall einer Infrastruktureinrichtung in einem Mitgliedstaat kann sich negativ auf andere Mitgliedstaaten und die europäische Wirtschaft auswirken. Dies wird umso wahrscheinlicher, als mit den neuen Technologien (z.B. Internet) und der Liberalisierung der Märkte (z.B. der Gas- und Strommärkte) zahlreiche Infrastrukturen in größere Netze eingebunden werden. In diesem Fall ist der Schutz nicht stärker als das schwächste Glied in der Kette der Schutzmaßnahmen. Ein einheitliches Schutzniveau ist daher erforderlich.« (EU 2005, 5)

Für »Kritische EU-Infrastrukturen«, die besonders in den Bereichen Verkehr und Energie liegen und bei deren Ausfall mehr als nur ein Mitgliedstaat betroffen wäre (EU 2006, 4, 2008, 8), werden verstärkte Sicherheitsbemühungen, insbesondere bei der Koordination zwischen den Mitgliedstaaten, vorgesehen.

Teils können die Entflechtung der Infrastrukturen und die Konkurrenz zwischen unterschiedlichen Anbietern aber auch organisationale Schwierigkeiten bedeuten. Häufig führt das *umbündling* der Infrastruktur nämlich nicht zu einer substanziellen, sondern nur zu einer organisatorischen Entflechtung und Zersiedelung von Verantwortlichkeitsstrukturen (zu unterschiedlichen Formen der Entflechtung siehe: Graham und Marvin 2001, 97). Die Opazität der Infrastrukturen erhöht sich, wenn niemand mehr einen Überblick über das gesamte Bündel eines Infrastrukturdienstes – etwa der Stromversorgung (siehe dazu ausführlich Kapitel 3.3.3. in dieser Arbeit) – hat. Die so entstehende Intransparenz kann wiederum die Vulnerabilität von Infrastrukturen erhöhen (BBK 2009c, 60). Dabei liegt diese Intransparenz nicht nur in der technischen Komplexität der Systeme, sondern auch in deren sozioökonomischer Organisationsstruktur.

Schließlich sind es die veränderten ökonomischen Rahmenbedingungen, die immer wieder für eine Verschlechterung oder zumindest ein Problematisch-Werden der Infrastruktursicherheit verantwortlich gemacht werden.

»Veränderungen im Marktgeschehen, wie sie etwa durch die Liberalisierung der Märkte und die Privatisierung ehemals staatlicher Infrastrukturbetriebe stattfinden, können das Sicherheitsniveau und die Investitionen in Sicherheitsmaßnahmen beeinflussen. Die Wettbewerbssituation und der damit verbundene Preisdruck schaffen Rahmenbedingungen, in denen sicherheitsrelevante Vorkehrungen wie etwa redundante Systeme oder andere Sicherheitspuffer reduziert werden. Die Anforderungen von Regelwerken werden zwar weitgehend eingehalten. Immer genauere Berechnungsverfahren ermöglichen jedoch, Spielräume weiter auszunutzen und Sicherheitspuffer zu reduzieren. Diese Puffer können dann insbesondere in Krisensituationen fehlen.« (BMI 2011, 9)

Gerade die veränderten kalkulativen Rationalitäten eines liberalisierten Infrastrukturbetriebs – seine »Berechnungsverfahren« – gelten dabei sowohl für staatliche als auch private Anbieter von Infrastrukturen. Wenn nicht mehr die Effektivität bei der Gewährleistung sicherer Infrastrukturen (substanzielle Rationalität), sondern die Effizienz des ökonomischen Mitteleinsatzes, das Verhältnis von Kosten und Nutzen von Sicherheitsmaßnahmen, ausschlaggebend ist (formelle Rationalität), dann wird es schwer, Sicherheitsmaßnahmen wie redundante Infrastrukturkomponenten oder »Puffer« aufrecht zu erhalten. Eine zentrale Strategie zur Erhöhung systemischer Resilienz – die Vorhaltung redundanter Ressourcen – gerät damit unter Druck.

Diese räumlichen, technischen, organisatorischen und ökonomischen Trends machen die Liberalisierung der Infrastruktur auch in den Augen des Bevölkerungsschutzes zu einem Problem:

»Ein weiterer Punkt ist auch noch die Privatisierung vieler Infrastruktur-Dienstleistungen, die ja seit Anfang der 1990er Jahre zunehmend mehr um sich griff, die am Anfang ja völlig unproblematisch durchgeführt wurde. Man hat sich ja auch keinerlei Gedanken darüber gemacht, was passiert, wenn wir die Bahn nicht mehr steuern können, was passiert, wenn wir der Post keine Weisungen mehr geben können. Und so nach und nach, als dann die ersten Probleme auftraten, gerade auch im Bereich der Bahn-Infrastruktur, hat man sich überlegt, wie bekommen wir das Pferd, das wir losgelassen haben durch die Privatisierung, eben doch noch so gezügelt, dass die Leistung noch bereitstehen kann. Im juristischen Bereich hat sich in diesem Zusammenhang eben auch der Begriff der Gewährleistungsverantwortung oder des Gewährleistungsstaates etabliert. [...] Dass man die Wirkungen der

Privatisierung nicht mehr so ganz schleifen lassen wollte, sondern dass man dann dachte, irgendetwas müssen wir doch noch tun und sehen, dass wir die Infrastrukturen, die wir dann in die ›Freiheit‹ [*spricht Anführungszeichen aus*] entlassen, auch in gewisser Weise noch ein bisschen steuern können.« (Interview 1)

Die »neuen Bedrohungen« durch Phänomene wie Terrorismus und Klimawandel sind nur die eine Seite, die Gefahrenseite, auf die der Schutz Kritischer Infrastrukturen antwortet. Neue staatliche Bemühungen zur Sicherung der Infrastruktur sind ebenso Reaktionen auf Sicherheitslücken, die von der Liberalisierung selbst gerissen wurden. Zwar kann der Staat die entstandenen Risse im Geflecht infrastruktureller Versorgungsdienste nicht aus eigener Kraft kitten. Bemühungen zum Schutz Kritischer Infrastrukturen sollen jedoch zumindest dafür sorgen, dass besonders wichtige »Knotenpunkte« (BMI 2011, 10) nicht beschädigt werden, um die Kohäsion und Integrität des Gesamtnetzes zu wahren. In dieser Hinsicht steht das »kritisch« in der Kritischen Infrastruktur für »neuralgische Punkte« im Infrastrukturnetz, die ebenso funktionswichtig wie verwundbar sind und »deren Beeinträchtigung zu weitreichenden Ausfällen oder Schäden führen« (BMI 2011, 43) würde.

Als kritisch werden bestimmte Infrastrukturen aber auch verstanden, weil ihre Leistungen besonders wichtig sind und sie deshalb zentrale Schutzobjekte darstellen. Häufig ist in diesem Zusammenhang auch von »vitalen« Infrastrukturen (EU 2005, 2) die Rede. Damit wird erneut der Zusammenhang von technischen Netzen und Leben aufgerufen, der schon für Forsthoffs Konzept der Daseinsvorsorge so zentral war. Diese Problematisierung von Infrastrukturen, in der sich bio- und technopolitische Aspekte vereinen, scheint in den Programmen zum Schutz Kritischer bzw. vitaler Infrastrukturen wieder »aufzuleben«. Metaphern, die eine »Vitalität« der Infrastrukturen betonen, finden sich zuhauf. Immer wieder ist die Rede von Infrastrukturen als »Lebensadern« (BMI 2009) oder »Nervensystem« (BMI 2005, 3). Infrastrukturen, so sollen derartige Redewendungen wohl verdeutlichen, sind »lebenswichtig« (BMI 2009, 7) bzw. »überlebenswichtig« (BBK 2009c, 17). Bedeutsam ist diese Lebenswichtigkeit unter anderem, weil sie eine rechtliche Grundlage für bundesstaatliche Eingriffe in Infrastrukturen darstellt. Das Bundeskriminalamt etwa kann im Zusammenhang mit Infrastrukturstörungen ermitteln, wenn »sicherheitsempfindliche Stellen von lebenswichtigen Einrichtungen [betroffen sind], bei deren Ausfall oder Zerstörung eine erhebliche Bedrohung für die Gesundheit von Menschen zu befürchten ist« (BMI, BBK und BKA 2005, 28).

Infrastrukturschutz ist zunächst ein Werkzeug zum Schutz der Bevölkerung. Es geht um den »Schutz menschlichen Lebens durch Reduzierung der Verwundbarkeit Kritischer Infrastrukturen« (BMI, BBK und BKA 2005, 7). Die Infrastrukturen werden geschützt »in order to contribute to the protection of people« (EU 2008, 77). Der Schutz der Infrastrukturen »dient also mittelbar auch dem Schutz der Bevölkerung« (BBK 2009c, 20). Die Rede von der »Vitalität« und »Lebenswichtigkeit« von Infrastrukturen unterstreicht die Bedeutung, ja vielleicht sogar Zentralstellung der »Biologitimität« (Fassin 2012, 249)<sup>143</sup> im deutschen Katastrophenschutz. Zentrales Schutzgut ist das Leben der Bevölkerung, während die Infrastrukturen nur ein Mittel bzw. eine Interventionsoberfläche darstellen, um die Sicherheit der Bevölkerung zu gewährleisten.

Das Motiv der Abhängigkeit, das sich hier zeigt, war schon bei Forsthoff präsent. Auch er hat immer wieder die »lebenswichtige Verwiesenheit des Einzelnen« (Forsthoff 1938, 19) auf infrastrukturelle Dienstleistungen betont. Es ist das Motiv der »Interdependenz«, das die gegenwärtige Problematisierung der Infrastruktur von älteren bio-technopolitischen Sicherheitsrationalitäten unterscheidet. Eine Interdependenz Kritischer Infrastrukturen besteht, wenn ihre Dienste füreinander funktionswichtig, also kritisch oder vital sind. Es besteht dann nicht mehr nur eine einseitige Abhängigkeit der Bevölkerung von der Infrastruktur, sondern auch eine wechselseitige Abhängigkeit zwischen den Infrastruktursystemen (zu den Begriffen Abhängigkeit und Interdependenz aus Sicht des Infrastrukturschutzes siehe: BBK 2009c, 21ff.). Die Betonung solcher Interdependenzen impliziert eine »systemische« Perspektive. Mit dem Blick auf Interdependenzen verschiebt sich also die Valenz dessen, was »vital« an Infrastrukturen ist. Infrastrukturen gelten dann nämlich als Systeme, die füreinander »vital« und auch deshalb besonders schutzbedürftig sind. Kritikalität besteht nicht mehr primär in der Lebens-, sondern in der Systemwichtigkeit von Infrastrukturen. Der ultimative Horizont ist das »Gesamtsystem« bzw. das *system of systems*. »Infrastrukturen gelten dann als »kritisch«, wenn sie für die Funktionsfähigkeit moderner Gesellschaften von wichtiger Bedeutung sind und ihr Ausfall oder ihre Beeinträchtigung nachhaltige Störungen im Gesamtsystem zur Folge hat.« (BMI 2009, 5) »Vital« sind demnach insbesondere »systemkritische« Infrastrukturen: »Eine Infra-

143 »I have proposed the term »biogitimicy« for this recognition of life as the highest of all values« (Fassin 2012, 249) Diese »idea of human life as the highest good« ist laut Fassin (2012, 249) erst in der Moderne zum Durchbruch gekommen.



struktur besitzt vor allem dann eine *systemische Kritikalität*, wenn sie aufgrund ihrer strukturellen, funktionellen und technischen Positionierung im Gesamtsystem der Infrastrukturbereiche von hoher interdependenter Relevanz ist.« (BMI 2009, 5)

Gerade die »technischen Basisinfrastrukturen« (Energie, Verkehr, Wasser sowie Informations- und Kommunikationstechnologie) sind kritisch für das Leben der Systeme, weil »sozioökonomische Dienstleistungsinfrastrukturen« (Gesundheit, Ernährung, Rettungswesen, politische Institutionen, Finanz- und Versicherungswesen, Medien und Kultur) von ihnen abhängig sind (Vgl. BMI, 2009: 5). In dieser Aufteilung zwischen technischer Basisinfrastruktur und sozioökonomischen Dienstleistungsinfrastrukturen werden Infrastrukturdienste noch gemäß einer Funktionshierarchie unterschieden (siehe dazu: BBK 2009c, 22f.). Häufig wird jedoch auch eine radikalere, gewissermaßen heterarchische Form der Interdependenz unterstellt, durch die alle Infrastrukturen füreinander vital werden.

Durch das Motiv systemischer Interdependenz verschwindet die biopolitische Ausrichtung des Katastrophen- und Infrastrukturschutzes nicht, modifiziert sich jedoch entscheidend. Man hat es jetzt eher mit einer Biopolitik vitaler Systeme als einer Biopolitik der Bevölkerung zu tun (zu dieser Unterscheidung siehe: Collier und Lakoff 2015). Es geht nicht mehr unmittelbar um den Schutz des Lebens. Im Vordergrund steht zunächst einmal die Resilienz vitaler Systeme. Bemühungen zur Steigerung der Resilienz werden notwendig, weil – wie gesehen – Infrastrukturen auf Grund ihrer Interdependenz nicht nur für die Bevölkerung, sondern ebenso für einander vital sind und damit ein wesentliches Schutzobjekt wie auch einen Gefährdungszusammenhang im Sicherheitsdispositiv der Resilienz darstellen. Gewiss spielt menschliches Leben in der Biopolitik vitaler Systeme weiterhin eine gewichtige Rolle. Allerdings drängt sich der Verdacht auf, dass die Aufrechterhaltung des Infrastruktursystems zu einem Zweck an sich geworden ist. Menschliches Leben ist dann nicht mehr oberstes Schutzgut, sondern lediglich »Komponente« der Infrastruktur. »Zudem ist ihre Funktion auch immer durch eine menschliche Komponente geprägt, denn Infrastrukturanlagen werden von Menschen gesteuert, überwacht und gewartet.« (BBK 2009c, 23) Der Staat versteht sich dann weniger als Schutzinstanz des Lebens bzw. Hirte der Bevölkerung, sondern immer stärker als Steuermann der Systeme.<sup>144</sup>

---

144 Foucault unterscheidet zwei semantische Hauptströmungen im abendländischen Regierungsdanken, die aus der jüdisch-christlichen Tradition stammende Hirtenmetapher und

»Der Staat kooperiert partnerschaftlich mit anderen öffentlichen und privaten Akteuren bei der Erarbeitung von Analysen und Schutzkonzeptionen. Er steuert primär moderierend, nötigenfalls normierend, die Maßnahmen zur Sicherung und zur Sicherstellung des Gesamtsystems sowie der Systemabläufe.« (BMI 2009, 2)

Leben der Bevölkerung und Funktion der vitalen Systeme sind die zentralen Legitimationsmuster und Verständnisprinzipien der Initiativen für den Schutz Kritischer Infrastrukturen – aber nicht die einzigen. Das betrifft einerseits die Wertordnungen der einzelnen vitalen Systeme, die natürlich implizit mitgemeint sind, wenn es um den Schutz des »Gesamtsystems« geht. Zudem werden häufig »volkswirtschaftliche Schäden« (BMI 2009, 7) als Grund für die Schutznotwendigkeit von Infrastrukturen ins Feld geführt. Allein durch die besondere Stellung der Privatwirtschaft sind ökonomische Denkmuster in den Rationalitäten des Infrastrukturschutzes fest verankert. Daneben spielen auch Fragen der Staatsräson eine Rolle. Wenn es heißt, dass Störungen der Kritischen Infrastrukturen »Vertrauensverluste in die politische Führung einer Gesellschaft bewirken können« (BMI 2009, 7), dann erklingt darin ein Echo des klassischen Hobbes'schen Sicherheitspaktes, bei dem die souveräne Macht nur so lange legitim bleibt, wie es ihr gelingt, die Sicherheit ihrer Bürger zu gewährleisten.

Diese Vielzahl von sich überkreuzenden Rationalitätsformen, die den Schutz kritischer Infrastrukturen informieren – souveräne Sicherheit, biopolitische Bevölkerungssicherheit und Sicherheit vitaler Systeme – erzeugen eine Polyvalenz der »Kritikalität« bzw. »Vitalität« der Infrastruktur. Es ist nicht nur unklar, wo die »neuralgischen« Punkte innerhalb eines Infrastrukturnetzes liegen, sondern vor allem auch, in Bezug worauf eine Infrastruktur »kritisch« ist: die staatliche Souveränität, das Leben der Bevölkerung oder die Funktion vitaler Systeme. Diese Polyvalenz führt zu einer charakteristischen Unbestimmtheit der Programmatiken des Schutzes Kritischer Infrastrukturen. In der »offiziellen Definition« heißt es nur:

»Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchti-

---

die in der griechisch-römischen Tradition vorherrschende Steuermannmetaphorik (Foucault 2004, 173–200). In einer späteren Vorlesung wird Foucault die Steuerungsmetaphorik der Regierung mit der Kybernetik in Verbindung bringen (Foucault 2009b, 310f.). Auch Michel Serres (1994, 38) hat auf eine Konjunktur des kybernetischen Steuermannedenkens in der Regierungskunst der Gegenwart hingewiesen: »So muss der Fürst, einst Hirte von Tieren, Pilot oder Kybernetiker werden, jedenfalls also Physiker« (Serres 1994, 38).

gung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.« (BMI 2009, 3)

Die Unschärfe dieser Definition wird durchaus gesehen: »Das ist eine sehr, sehr weite und sehr offene Definition, die einerseits natürlich Raum für Interpretationen auf jeder Ebene lässt, auf der anderen Seite natürlich wenig griffig ist, was uns auch immer wieder um die Ohren gehauen wird.« (Interview 1)

Die Unbestimmtheit des Konzepts erlaubt größere Flexibilität im Angesicht einer ebenso unbestimmten und offenen Zukunft. Zudem erlaubt die Offenheit der Kritikalitätskriterien den staatlichen Infrastrukturschützer\_innen auch einen großen Interpretationsspielraum, um private Infrastrukturbetreiber in die Pflicht zu nehmen. Wie eine solche Verpflichtung genau bewerkstelligt werden kann, ist allerdings selbst nicht Teil der Programmatik zum Schutz Kritischer Infrastrukturen. Zwar gibt es eine Reihe von konkreten gesetzlichen Verpflichtungen und Qualitätsstandards für bestimmte Infrastrukturdienste. Diese sind jedoch häufig nicht direkt auf Fragen der Notfallsicherheit bezogen.<sup>145</sup> Rechtlich geregelt ist nur, dass der Staat im »Ausnahmefall« die Infrastrukturleistungen zur Verfügung stellen müsste, obwohl unklar ist, wie und ob er das überhaupt könnte.<sup>146</sup> Konkrete rechtliche »Anknüpfungspunkte« (BMI, BBK und BKA 2005, 6) für das Sicherheitsparadigma der Kritischen Infrastrukturen sind also noch rar. Immer wieder finden sich Hinweise auf Paragraph 91, Absatz 2 des Aktiengesetzes, das Vorgaben für das Risikomanagement von Aktiengesellschaften macht. Zudem wird auf regulatorische Entwicklungen im Bank- und Versicherungsbereich hingewiesen. So wird auf die Eigenkapitalregelungen Basel II hingewiesen, in der die Banken zur Beachtung von »operationellen Risiken« (BMI 2011, 11) aufgefordert werden. Verweise finden sich auch auf das europäische Versicherungsrecht Solvency II (BMI 2011, 11). Die Suche nach »Anknüpfungspunkten« unterstreicht die Notwendigkeit für den Schutz Kritischer Infrastrukturen, bei anderen, verwandten

145 Eine Ausnahme stellen die Regelungen des IT-Sicherheitsgesetzes dar, die – zumindest für den Bereich der IT-Sicherheit – konkrete Verpflichtungen für Betreiber Kritischer Infrastrukturen vorsehen.

146 In einem Interview, das ich im BBK in der Abteilung für den Schutz Kritischer Infrastrukturen geführt habe, hieß es zu dieser Frage: »Rein theoretisch müsste er dann auch im Ausnahmefall einspringen, wenn sich keiner mehr auf dem Markt findet, der diese Aufgaben wahrnimmt [...]. Wobei es dazu nicht in allen Fällen Regelungen gibt. [...] Das ist noch nicht bis zum Letzten ausgereizt, um es vorsichtig zu sagen. [...] Da gibt es noch Lücken.« (Interview 1)

Sicherheitslogiken gewissermaßen »andocken« zu müssen, um erfolgreich zu sein. Offenbar bietet das Feld des Finanz- und Versicherungswesens besonders viele Anknüpfungspunkte, weil der Umgang mit Risiken hier eine besonders elaborierte Tradition hat (siehe dazu ausführlich Kapitel 4.3.).

Aber auch wenn es nur wenige rechtliche Anknüpfungspunkte gibt, so etabliert der Schutz Kritischer Infrastrukturen doch ein Paradigma für die Sicherung sozio-technischer Versorgungsdienste, das nicht nur an das Sicherheitsdispositiv der Resilienz andockt, das sich in jüngerer Zeit um katastrophische und vor allem systemische Risiken gebildet hat, sondern gleichzeitig auch an das Paradigma des »Gewährleistungsstaates«. Ähnlichkeiten zum Paradigma der Gewährleistungsverantwortung gibt es zunächst in räumlicher Hinsicht: Das operative Raumschema des Schutzes Kritischer Infrastrukturen ist nicht mehr das gänzlich erschlossene nationale Territorium, sondern die Netzwerktopologie der Infrastruktur, die besonders verwundbare, also kritische oder neuralgische Punkte enthält, die geschützt werden müssen, um einen Zusammenbruch des infrastrukturellen Gesamtsystems zu verhindern. Nicht flächendeckender Service, sondern Verhinderung eines systemischen Kollapses ist das angestrebte Ziel. Zudem sieht auch der Schutz Kritischer Infrastrukturen nur eine sehr begrenzte staatliche Handlungskompetenz vor. Der Staat wirkt im Normalfall lediglich koordinierend – als »Netznoten« der »vernetzten Sicherheit«. Als substanzieller Akteur kann (bzw. muss) er nur in äußersten Notfällen, in infrastrukturellen Katastrophen eben, auftreten. Kurz: Der Staat muss existenziell wichtige Infrastrukturleistungen auch im Angesicht von Katastrophen gewährleisten, aus eigener Kraft erbringen kann er sie aber nicht. Zudem ist der Staat selbst Teil des Gewebes Kritischer Infrastrukturen und kann daher nicht mehr souverän seine »Vorsorgemaschinen« (Kaube 2002) überblicken, sondern muss lernen, sich selber als Teil eines fragilen, interdependenten Netzes, als Staat am Draht, zu beobachten. Der Staat ist kein allmächtiger »Metaverteiler« (Latour 2014, 633) mehr, der über dem Geschehen steht, den unterschiedlichen Bestandteilen des Gemeinwesens seine Funktionen zuteilt und die Versorgungsströme zwischen diesen Teilen steuert, sondern selbst Teil einer flachen Landschaft vernetzter Beziehungen.

Mit dieser Orientierung am Notfall geht auch einher, dass der Schutz Kritischer Infrastrukturen weniger für eine Biopolitik des guten Lebens, sondern vielmehr für eine Biopolitik des Überlebens steht. Kritische Infra-

strukturen sind vor allem solche Versorgungsleistungen, die »(über)lebenswichtig« sind. Die »systemische« Lesart der »Vitalität« der Infrastruktur, nach der vitale Systeme wechselseitig voneinander abhängig sind und deshalb dauerhaft funktionsfähig sein müssen, um einen Systemzusammenbruch zu verhindern, deutet in zwei Richtungen über diese Biopolitik des nackten Lebens hinaus. In einem Fall kann sie zu einer selbstreferenziell-funktionalistischen Logik führen, wo die Systeme gleichsam um ihrer selbst willen aufrecht erhalten werden müssen. Im anderen Fall erlaubt sie die Erweiterung der Infrastruktursicherung über das unmittelbar »Lebensnotwendige« hinaus. Welche Richtung genau eingeschlagen wird, ist gegenwärtig noch nicht abzusehen. Die Programme zum Schutz Kritischer Infrastrukturen sind strategisch offen und können von unterschiedlicher Seite interpretiert werden. Es deutet letztlich nichts darauf hin, dass die »Biogegitimität« des Bevölkerungsschutzes schlicht durch die »Cyberlegitimität« des Infrastrukturschutzes ersetzt würde.

### 3.2. Von der großen zur grünen Infrastruktur?

Wie im vorhergehenden Kapitel gezeigt, markiert das Projekt der Daseinsvorsorge einen wesentlichen Entwicklungsschritt des techno-biopolitischen Sicherheitsprojekts des Infrastrukturschutzes in Deutschland. Der Politik der Daseinsvorsorge ging es historisch zunächst darum, die von Infrastrukturleistungen abhängige Bevölkerung an die für sie lebenswichtigen Versorgungsströme anzuschließen. Zeitgenössische Projekte zum Schutz Kritischer Infrastruktur sorgen sich demgegenüber nicht nur um die Abhängigkeit der Bevölkerung von Versorgungsleistungen, sondern vornehmlich um die Interdependenz der Infrastrukturen untereinander.

In diesem Kapitel werde ich auf eine weitere Verschiebung der Biopolitik vitaler Systeme im 20. Jahrhundert eingehen, durch die auch Ökosysteme zum Gegenstand der Sicherheitsbesorgnis geworden sind. Das verstärkte Auftreten von ökologischen Fragen als Probleme biopolitischer Sicherheitstechnologien seit den 1970er Jahren hat weniger die *endogenen* Gefährdungspotenziale großtechnischer Systeme, sondern vielmehr deren *Externalitäten*<sup>147</sup> auf die politische Agenda gesetzt: die negativen

---

147 Ich verwende den Begriff der Externalitäten hier nicht lediglich im ökonomischen Sinne, wo Externalitäten vor allem unbeabsichtigte Kosten und Nutzen ökonomischer Prozes-

Folgewirkungen moderner Infrastrukturprojekte für die natürliche Umwelt, das Klima sowie die Sicherheit und Gesundheit von Mensch und Tier. Die wesentlichen Instrumente der Sicherheit in der Daseinsvorsorge – der Ausbau und die Absicherung infrastruktureller Netze – wurden gerade in der Folge von Technikkatastrophen verstärkt als Quelle von Gefahren wahrgenommen. Mit den Ökologiebewegungen,<sup>148</sup> die sich häufig als Reaktion auf solche Katastrophen gebildet haben, ist eine neue Form der Kritik auf die historische Bühne getreten, die »Risiko« zu einem zentralen kritischen Instrument gemacht hat, um die zu wenig beachteten Effekte moderner Technikentwicklung zu problematisieren. Zunächst konnte so eine Reihe von Selbstgefährdungstendenzen der technologischen Moderne bewusst gemacht werden. Zudem wurde aber auch ein neuer Gegenstand der Sicherheit erschlossen, ein neues Objekt, das es zu schützen gilt: die Natur bzw. die Umwelt. Heute geht es bei Bemühungen zur Regierung der Katastrophe nicht mehr nur um Naturgefahren, sondern ebenso um Gefahren für die Natur. Und es wird davon ausgegangen, dass ökologische Sicherheit und menschliche Sicherheit, Umweltschutz und Bevölkerungsschutz im Rahmen eines erweiterten Sicherheitsverständnisses zusammengehören. Die Gefährdung und Zerstörung natürlicher Lebensgrundlagen hat nämlich die vitalen »Dienstleistungen« der Umwelt für die Bevölkerung sichtbar werden lassen, so dass Ökosysteme zu Gegenständen der Biopolitik vitaler Systeme geworden sind.

In diesem Kapitel werde ich diese vielfältigen Verschiebungen des Sicherheitsverständnisses durch ökologische Problematisierungen anhand einer Reihe exemplarischer Themen betrachten, die zugleich sichtbar machen, wie die Erweiterung der Biopolitik vitaler Systeme bestehende Sicherheitstechnologien kompliziert. Zunächst werde ich auf die Entstehung des Vorsorgeprinzips im deutschen Umweltrecht eingehen, um zu zeigen,

---

se für dritte Parteien bezeichnen. Vielmehr geht es mir allgemeiner um Folgewirkungen moderner Infrastrukturen für die »Natur« bzw. die »Umwelt«. Dabei werde ich argumentieren, dass diese Bereiche als Gegenstand von Sicherheitstechnologien erst als Folge ihrer Beeinträchtigung, also als Folge von Externalitäten, in Erscheinung treten. Siehe auch die Verwendung von Externalitäten bei Latour (2001a, 288). Für eine soziologische Theorie der Externalisierung siehe auch: Lessenich (2016).

148 Ich spreche hier bewusst von »Ökologiebewegungen« im Plural, um den heterogenen Charakter des Umwelt-Aktivismus zu betonen. Nicht alle dieser Bewegungen waren gleichermaßen an der Kritik und Fortentwicklung des Sicherheitsdispositivs beteiligt und nur selten zielten ihre Einsätze bewusst auf Sicherheit im engeren Sinne. Vielmehr konnte gerade ihr quer zu klassischen sicherheitspolitischen Agenden stehender Ansatz zu einer Modifikation von Sicherheitsproblemen und Technologien beitragen.

wie sich die Tradition der deutschen Vorsorgepolitik auf die neuen ökologischen Probleme eingestellt hat. Das Vorsorgeprinzip steht für die rechtliche Institutionalisierung eines reflexiven Umgangs mit Nicht-Wissen im Angesicht komplexer und potenziell schwerwiegender Umweltschäden durch den Einfluss menschlicher Technik. Zugleich wird durch dieses Rechtsprinzip die Vorsorgezone gegenüber der Politik der Daseinsvorsorge von sozio-technischen Systemen auf Ökosysteme ausgeweitet. Ausgeweitet hat sich aber auch die Funktion des Vorsorgeprinzips selbst. Heute ist das *precautionary principle* nicht nur in der Umweltpolitik, sondern etwa auch in der Anti-Terrorpolitik operativ und dadurch zu einer eigenständigen Rationalität der Sicherheit geworden, die auf vielfältige Weise mit Sicherheitstechnologien wie Vorbereitung und Resilienz interagiert (3.2.1.). Sodann werde ich auf den Fall der techno-hydraulischen Bearbeitung von Flutrisiken und ihrer ökologischen Kritik eingehen. An diesem geradezu paradigmatisch gewordenen Fall kann gezeigt werden, wie die »grüne« Kritik an der »großen Infrastruktur« die Paradoxien infrastruktureller Sicherheit zur Sprache gebracht und einen alternativen, ökologischen Hochwasserschutz vorgeschlagen hat, der Katastrophen- und Naturschutz zusammenbringen soll (3.2.2.). Anschließend werde ich auf das Schnittfeld von Klimawandelanpassung und (infrastrukturellem) Bevölkerungsschutz eingehen. Der Klimawandel ist gegenwärtig der zentrale politische Schauplatz, auf dem die Selbstgefährdungstendenzen technologischer Gesellschaften sicht- und kritisierbar geworden sind. Das Projekt der Klimawandelanpassung in einer infrastrukturell hochkomplexen Gesellschaft erzeugt dabei eine noch komplexere Sicherheitsproblematik. Nicht nur verursacht die industrielle Entwicklung den Klimawandel. Zudem wird eine industriell-infrastrukturelle Gesellschaft als besonders verwundbar durch die Folgen des Klimawandels angesehen. Darüber hinaus kann am Fall der Klimawandelanpassung eine besonders aufschlussreiche Interaktion zwischen den Sicherheitstechnologien der Vorsorge, der Vorbereitung und der Resilienz studiert werden (3.2.3.). Jüngere Anstrengungen, die Natur selbst als Infrastruktur zu beschreiben und zu gestalten, sind ein deutlicher Ausdruck für die Abkehr von der technologischen Infrastrukturpolitik vergangener Dekaden. Zum einen wird die sogenannte grüne Infrastruktur als zu schützendes, vitales System wie auch als Sicherheitstechnik mobilisiert. Zum anderen ist das Erdsystem als planetarisches »life support system« im Zeitalter des Anthropozäns zu einem neuen Gegenstand der Politik geworden (3.3.4.).

### 3.2.1. Ausweitung der Vorsorgezone: Die Genese des *precautionary principle*

Das Vorsorgeprinzip bzw. *precautionary principle* ist mittlerweile weltweit eines der meist diskutierten Politikkonzepte zum Umgang mit ungewissen und schwerwiegenden Risiken. Es leitet globale Umweltpolitik ebenso an wie Maßnahmen im Krieg gegen den Terror, es sorgt für Verstimmungen in internationalen Handelsabkommen zwischen den USA und Europa, es wird entschieden verteidigt, aber auch scharf attackiert. Beim Vorsorgeprinzip handelt es sich um ein deutsches Exportprodukt. Kaum ein Text zum Vorsorgeprinzip kommt ohne Verweis auf seine Herkunft aus dem deutschen Umweltrecht aus (siehe etwa: Sunstein 2007, 29, Aradau und Munster 2011, 41). Nur selten wird allerdings der politische Problemhorizont beleuchtet, in dem das Vorsorgeprinzip entstanden ist (Boehmer-Christiansen 1994), oder gar der Zusammenhang zur Tradition des deutschen Vorsorgerechts hergestellt. Der Begriff der Vorsorge ist, wie im vorangegangenen Kapitel gezeigt, bereits durch Forsthoffs und Hegels Konzepte der Vorsorge für das Dasein in die deutsche Rechtstradition eingegangen. Bereits hier war »Vorsorge« eine Technik gegen »zurückbleibende Zufälligkeit« (Hegel 1970, 346), also Risiken im weitesten Sinne. Forsthoff hat die umweltpolitische Relevanz der Vorsorge bereits antizipiert, als er in *Der Staat in der Industriegesellschaft* die Bedeutung des Staates bei der »Vorsorge für die Reinhaltung der Luft und der Gewässer« (Forsthoff 1971, 26) ebenso betonte wie den Umstand, dass Vorsorge nunmehr »im Weltmaßstab« (Forsthoff 1971, 27) zu erfolgen habe. Drei Jahre nach Erscheinen seines Buches sollte es dann soweit sein. 1974 wurde ein Gesetz für die »Reinhaltung der Luft« – das Bundesimmissionschutzgesetz (BImSchG) – verabschiedet (BImSchG 1974). Die sozialliberale Koalition unter Willy Brandt löste damit das bereits 1969 formulierte Wahlversprechen »Blauer Himmel über der Ruhr« ein. Gerade die Menschen in industriellen Ballungsräumen sollten vor den Emissionen der Industrie geschützt werden, die, wie durch wissenschaftliche Studien immer deutlicher wurde, die Gesundheit der Bevölkerung massiv beeinträchtigten. Der lange Titel des Gesetzes »zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche Vorgänge« zeigt bereits an, dass es nicht nur um Luftreinheit ging, sondern um den Schutz eines umfassenden atmosphärischen Milieus, das durch allerlei Schadstoffe – von Lärm bis zu Vibrationen – verunreinigt werden kann. Schon der Bezugsbereich des BImSchG ist interessant, denn das Gesetz hat es mit rechtlich höchst schwierigen, ja unfassbaren



Rechtsmaterien, nämlich sogenannten Imponderabilien zu tun. Als Imponderabilien werden traditionell solche Rechtsmaterien bezeichnet, die nicht von sich aus zu Boden fallen und deshalb als unbeherrschbar bzw. rechtlich nur schwer zu regulieren angesehen werden. Diese Problematik hat mit dem wachsenden Wissen um schädliche Immissionen neue Dringlichkeit erfahren. Dadurch sind auch imponderable Materien justiziabel geworden (BImSchG 1974).

Das BImSchG orientierte sich weitgehend am *Clean Air Act*, der in den USA bereits 1970 verabschiedet wurde. Die eigentliche rechtliche Innovation war jedoch die Verankerung des Vorsorgeprinzips im Gesetz, wodurch das BImSchG das erste Vorsorgegesetz wurde (Boehmer-Christiansen 1994, 36, UBA 2001, 14, Sanden 2006, 257). Vorsorge heißt, wie es das Bundesverfassungsgericht einmal formuliert hat, die Errichtung einer »Sicherheitszone vor der Gefahrenschwelle« (zitiert nach: Sanden 2006, 243). Rechtlich ist dabei ausschlaggebend, dass anders als im Gefahrenabwehrrecht, wo erst gehandelt wird, wenn ein kausaler Gefährdungszusammenhang feststeht, im Vorsorgerecht Sicherheitshandeln auch unter Bedingungen der Ungewissheit erforderlich ist (siehe: Sanden 2006, 244). Vor allem die in den 1980er Jahren geführte Debatte über das Waldsterben, dessen Zusammenhang mit saurem Regen zwar vermutet, aber nicht bewiesen werden konnte, führte zur großen Akzeptanz des Immissionsgesetzes und des dort verankerten Vorsorgeprinzips (Boehmer-Christiansen 1994, 45–47).

Bereits im Verlauf der 1980er Jahre fand das Vorsorgeprinzip Eingang in internationale Abkommen zum Schutz der Nordsee (Ewald 2011, 484). Ebenfalls in den 1980er Jahren wurden im Montrealer Protokoll Vorsorgemaßnahmen zum Schutz der Ozonschicht getroffen (UBA 2001, 15). Zu Beginn der 1990er Jahre schaffte das Vorsorgeprinzip dann den Sprung auf die große Bühne der internationalen Politik mit gleich drei Bezugnahmen in zentralen internationalen Abkommen, konkret in den Maastricht-Verträgen der EU, der in New York beschlossenen Klimarahmenkonvention der Vereinten Nationen und der berühmten Erklärung über Umwelt und Entwicklung von Rio (UBA 2001, 15). In den 2000er Jahren folgen Abkommen über Biosicherheit und Schutz vor chemischen Gefahren (UBA 2001, 15). Das Vorsorgeprinzip ist heute eine im zweifachen Sinne globale Angelegenheit. Einerseits findet es gerade in internationalen Verträgen und Abkommen Beachtung, es ist eine »global form« (Ong und Collier 2005b, 11) der Umwelt- und Sicherheitspolitik. Andererseits ist sein Bezugspunkt

geradezu planetarisch. »An inventory of applications of this principle is beginning to look a bit like the narrative of genesis in the Bible: the principles protects the sea and the ocean, the rivers, the atmosphere, the land, its fauna, and its flora.« (Ewald 2011, 484) Es geht also um nichts weniger als die Gesamtheit der Schöpfung, von der kleinsten Mikrobe, die durch biotechnologische Forschung als Gefahrenstoff freigesetzt werden könnte, bis zur gefährdeten Erdatmosphäre. Gegenüber der Politik der Daseinsvorsorge zeichnet sich das Vorsorgeprinzip durch einen radikal erweiterten Sorgehorizont aus. Zwar geht es auch den Maßnahmen im Rahmen des Vorsorgeprinzips um den Schutz des »effektiven Lebensraums« des modernen Menschen. Aber das Vorsorgeprinzip zielt dabei anders als die Daseinsvorsorge nicht nur auf die Technosphäre vernetzter Infrastruktur, sondern auf die gesamte Biosphäre, nicht nur auf das nationale Territorium oder den vernetzten, infrastrukturellen Raum Europas, sondern auf den gesamten Planeten. Der »effektive Lebensraum« ist nun die Erde und ihre Atmosphäre. Das »Sein«, das geschützt werden muss, ist nicht mehr nur der »massentümliche Mensch«, sondern eben dieses komplexe und verwundbare biosphärisch-ökologische Etwas, das man heute »die Umwelt« nennt. Der Sorgehorizont erweitert sich dabei nicht nur räumlich, sondern auch zeitlich. Ging es für die Daseinsvorsorge noch um den Schutz vor bereits eingetretenen oder um die Vorbeugung von klar erkennbaren Risiken, sind es jetzt weit in der Zukunft liegende und lediglich wahrscheinliche bzw. mögliche Gefährdungen, auf die Vorsorge reagieren soll.

Die Formulierungen des Vorsorgeprinzips in den oben genannten Erklärungen sind zwar auf die je spezifischen Themengebiete zugeschnitten, aber sie ähneln sich dennoch bis in den Wortlaut hinein. Die Formulierung des Vorsorgeprinzips in der Erklärung von Rio hat besondere Berühmtheit erlangt:

»Zum Schutz der Umwelt wenden die Staaten den Vorsorgeansatz entsprechend ihrer Möglichkeiten umfassend an. Angesichts der Gefahr erheblicher oder irreversibler Schäden soll fehlende vollständige wissenschaftliche Gewissheit nicht als Grund dafür dienen, kostenwirksame Maßnahmen zur Verhinderung von Umweltschäden hinauszuzögern.« (Erklärung von Rio, zitiert nach: UBA 2001, 15)

Verhindert werden sollen »ernsthafte und nicht wieder gutzumachende Schäden« (Klimarahmenkonvention, zitiert nach: UBA 2001, 15), besonders problematisch sind deshalb Stoffe, die »langlebig und toxisch sind und zu Bioakkumulation neigen« (Dritte Internationale Konferenz zum Schutz der Nordsee, zitiert nach: UBA 2001, 15). Derartige »Umweltbeeinträchti-

gungen [sollen] mit Vorrang an ihrem Ursprung« (Maastricht Verträge, zitiert nach: UBA 2001, 15) bekämpft werden, auch wenn dieser Ursprung der Gefahr gar nicht mit Gewissheit bekannt ist. Die Vorsorgepolitik ist damit von einem Naturbild geprägt, das die Natur nicht in einem ewigen, quasi zeitlosen Zustand des Gleichgewichts sieht, sondern als bedroht, unwiederbringlich beschädigt zu werden. Zudem wird anders als im Denken der Resilienz nicht auf die Entstehung neuer, stabiler Gleichgewichtszustände spekuliert. Deshalb soll, damit es gar nicht erst zu irreversiblen Schäden kommt, diesen *vorgebeugt* werden. Dafür sollen primär die *Schadensursachen* adressiert werden. So verstanden steht Vorsorge im Gegensatz zur Politik der Vorbereitung, die sich primär auf die Bearbeitung von Folgeschäden konzentriert. Eigentlich vertrackt wird die Vorsorgepolitik allerdings dadurch, dass in den komplexen Wirkungsketten sowie in den langen Zeitreihen Ursache und Wirkung überhaupt nicht so eindeutig festgemacht werden können. »Vorsorge« ist insofern eine Politik unter Bedingungen *wissenschaftlicher Unsicherheit*. Eine Politik, die nicht trotz, sondern wegen Nicht-Wissen zum Handeln oder Handlungsverzicht auffordert und damit eine charakteristische »Politisierung des Nichtwissens« (Wehling 2006, 316) erzeugt.

Die Ungewissheit und das Nicht-Wissen, um die es hier geht, sind keine Phänomene des Noch-Nicht-Wissens. Vielmehr hat man es zumeist mit wissenschaftlich produziertem Nicht-Wissen (Luhmann 1992b, Wehling 2006) zu tun. Das Vorsorgeprinzip ist immer schon auf die historische Situation der »Wissensgesellschaft« bezogen. So fiel seine Entstehung 1974 gewissermaßen mit dem Höhe- und Wendepunkt technokratischen Regierens zusammen. Immer mehr politische Entscheidungen sollten durch klare Vorgaben von Expert\_innen gestützt werden. Zugleich begann das Vertrauen in die Expertokratie bereits zu bröckeln. Demgegenüber lässt sich das Vorsorgeprinzip geradezu als Immunisierung gegenüber zu hohen Anforderungen an die Wissensgrundlage politischer Entscheidungen verstehen. Das Vorsorgeprinzip ist auch eine Verpflichtung darauf, wissenschaftliche Verdachtsmomente ernst zu nehmen und nicht erst auf »Beweise« in Form bereits eingetretener Schadensfälle zu warten. In dieser Hinsicht ist das Vorsorgeprinzip gerade nicht »lähmend«, weil es mögliche technowissenschaftliche Innovationen bremst, sondern es ermächtigt und ermöglicht politisches Handeln (Boehmer-Christiansen 1994). Gerade dadurch ist es ein paradigmatisches »Modell für den Umgang mit wissenschaftlichem Nichtwissen« (Wehling 2006, 278-292).

Gleichwohl wäre es falsch, das Vorsorgeprinzip als *per se* nicht wissensbasiert zu beschreiben, wie gelegentlich mit der Unterscheidung von »risk based« und »precaution based policies« von Teilen der Risikoforschung nahegelegt wird (kritisch dazu: Klinke und Renn 2002, 1074). Vielmehr bekommt Wissenschaft hier, wie François Ewald zurecht bemerkt, eine neue Rolle zugewiesen:

»[W]e are now less interested in the confidence science provides than in the suspicions and doubts it can arouse both about what we know and what we do not know. With precaution, science becomes a principle of challenge. Science becomes a challenge to itself as well as to the many proofs that everyday life should not be the subject of permanent anxiety.« (Ewald 2002, 289)

Heute ist es in Fragen des Umweltschutzes eine Selbstverständlichkeit, dass »die einfache Wissenschaft der linearen, mechanistischen Deutungsansätze [...] um die dynamischen und sich ständig weiter entwickelnden Eigenschaften der Systemwissenschaften ergänzt« (UBA 2001, 2) wird. Wenn Klimawandelskeptiker\_innen heute darauf verweisen, dass die Beweislage für den anthropogenen Charakter der Erderwärmung noch zu unsicher ist, um Maßnahmen einzuleiten, dann haben sie weder die ethisch-politischen Herausforderungen der Vorsorge noch die epistemologischen Veränderungen der Wissenschaften begriffen. Sie hängen einem veralteten Verständnis von Wissenschaft als »sound science« an (Demeritt 2006) und verstehen Wissenschaft als bloße Evidenzfabrik, die klar umrissene Tatsachen gleichsam schlüsselfertig den politischen Entscheidungsträger\_innen zukommen lässt.<sup>149</sup>

Allerdings übersieht Ewald mit seiner Fokussierung auf die epistemologischen Konsequenzen des Vorsorgeprinzips, wie Peter Wehling (2006, 291) zurecht feststellt, die »politische[n] und normative[n] Problemstellungen«, die mit ihm einhergehen. Schließlich läuft das Vorsorgeprinzip geradezu auf eine Politisierung und Ethisierung der Wissenschaft hinaus. Immer dort, wo von einem epistemologischen Standpunkt aus keine Gewiss-

149 Diese Veränderung der Wissenschaften haben in den *Science Studies* lange vor den jüngsten Debatten über ein vermeintlich postfaktisches Zeitalter Diskussionen darüber ausgelöst, worin gegenwärtig noch eine sinnvolle Wissenschaftskritik bestehen kann. Latour (2004) hat in Anbetracht von Kontroversen zwischen Klimawissenschaftler\_innen und Leugner\_innen der globalen Erderwärmung zurecht argumentiert, dass die Rolle der Wissenschaftskritik nicht mehr lediglich in der »Dekonstruktion« von Wahrheitsansprüchen bestehen dürfe. Vielmehr gelte es ein neues, den gegenwärtigen Wissenschaften angemessenes Verständnis von Realität zu entwickeln.

heit erzeugt werden kann, muss die Ethik oder die politische Entscheidung einspringen. Die moralphilosophischen Grundlagen der Vorsorge hat wohl am deutlichsten der Sozialphilosoph Hans Jonas veranschaulicht. Ewald (2002, 291) hat deshalb Jonas zurecht als den Philosophen des Vorsorgeprinzips charakterisiert, obwohl dieser selber sein philosophisches Hauptwerk, das eben nicht »Vorsorgeprinzip«, sondern *Prinzip Verantwortung* (Jonas 1989) heißt, ohne Wissen des sich etwa zeitgleich entwickelnden Vorsorgeprinzips geschrieben hat. Jonas entwirft eine *Ethik für die technologische Zivilisation* – so der Untertitel seines Buches. Seine Ausgangsüberlegung ist, dass die sowohl räumliche als auch zeitliche Erweiterung der Handlungsmacht der technologisch ausgestatteten Menschheit alle bisherige Ethik, die sich stets nur auf das Nahfeld bezogen hat, infrage stellt (Jonas 1989, 15f.). Menschliche Handlungen betreffen unter hochtechnologischen Bedingungen nicht nur die »gesamte Biosphäre des Planeten« (Jonas 1989, 27), die sozio-technischen »Fernwirkungen« (Jonas 1989, 62) affizieren auch »die ferne Zukunft« (Jonas 1989, 28). Schließlich betrifft menschliches Handeln auch den Menschen selbst, der unter Bedingungen von genetischer Anthropotechnik nicht mehr nur *homo faber*, sondern zugleich *homo fabricatus* geworden ist. Die menschliche Natur ist nicht länger nur die Voraussetzung, der Grund der Ethik, sondern zugleich ihre Zielscheibe bzw. »ethische Substanz« (Foucault 1989a, 37).<sup>150</sup> Daraus ergeben sich für Jonas »neue Dimensionen der Verantwortung« (Jonas 1989, 26ff.) – einerseits die Natur, und zwar sowohl die äußere wie auch die Integrität der »inneren« menschlichen Natur, und andererseits die Zukunft bzw. zukünftiges menschliches Leben. Ein neuer ethischer Imperativ drängt sich auf: »Handle so, daß die Wirkungen deiner Handlungen verträglich sind mit der Permanenz echten menschlichen Lebens auf Erden.« (Jonas 1989, 36) Dieser Imperativ hat Spuren hinterlassen. So wie man argumentieren kann, dass der Kant'sche kategorische Imperativ durch die Formel von der unantastbaren Menschenwürde Eingang in Artikel 1 des deutschen Grundgesetzes gefunden hat, lässt sich sagen, dass Jonas' Imperativ in Artikel 20a des Grundgesetzes zum Vorschein kommt, in dem es

---

150 Die Frage der »ethischen Substanz« betrifft »die Art und Weise, in der das Individuum diesen oder jenen Teil seiner selber als Hauptstoff seines moralischen Verhaltens konstituieren soll« (Foucault, 1989: 37). Nikolas Rose (2007, 252–259) hat überzeugend dargelegt, dass im Zeitalter der Politik des Lebens selbst die ethische Substanz nicht mehr nur bestimmte Bereiche »moralischen Verhaltens«, sondern auch die somatische Grundlage des Menschen betrifft.

heißt: »Der Staat schützt auch in Verantwortung für die künftigen Generationen die natürlichen Lebensgrundlagen und die Tiere« (GG, Artikel 20a).

Auch wenn sich Jonas' Imperativ zunächst sehr sinnfällig anhört (allzumal für Ohren, die mit Begriffen wie Nachhaltigkeit und Generationengerechtigkeit groß geworden sind) – jeder Versuch der praktischen Anwendung seiner Ethik erzeugt größte Schwierigkeiten. Jonas selbst betont: »Allerdings wird die Unsicherheit der Zukunftsprojektionen, die für die Prinzipienlehre unschädlich ist, zur empfindlichen Schwäche dort, wo sie die Rolle von Projektionen übernehmen müssen, nämlich in der praktisch-politischen Anwendung.« (Jonas 1989, 68) Schon immer hat die Ungewissheit über die »Wirkungen der Handlungen« große moraltheoretische Schwierigkeiten bereitet. Kant hat sie deshalb »kategorisch« aus seiner anti-konsequenzialistischen Moraltheorie ausgeschlossen. Im Zeitalter der »Fernwirkungen« wird die Einbeziehung der Wirkungen in Maximen für Handlungen ein ungleich drängenderes Problem, an dem sowohl die Kant'sche Deontologie als auch Aristoteles' *phronesis* scheitern (Jonas 1989, 24). Deswegen braucht es, so Jonas, verstärkte wissenschaftliche Anstrengungen, um die »Fernwirkungen« von Handlungen abschätzen zu lernen (Jonas 1989, 62f.). Deutlich wird hier, dass die Moral der Vorsorge nicht nur zu einer Ethisierung der Wissenschaft führt, sondern sich umgekehrt auch die Ethik »epistemologisiert« bzw. verwissenschaftlicht. Dabei transformiert sich beides, Ethik und Wissenschaft. Jonas fordert deshalb das Wissen zur Spekulation auf, zur Neuentdeckung der Fragen der Ontologie, die zugleich ethische Fragen werden.<sup>151</sup> Zudem soll die Wissenschaft, die Fernwirkungen untersucht, von einer »Heuristik der Furcht« (Jonas 1989, 63) flankiert werden, die wissenschaftliche Prognosen anleitet und ihnen Nachdruck verleiht.

Das Vorsorgeprinzip, das aus dem deutschen Umweltrecht in Reaktion auf industrielle Emissionen und ihre negativen Folgen für menschliche Gesundheit und Waldbestand hervorgegangen ist, hat sich mittlerweile als eigenständige Sicherheitsform etabliert und ist zu einer »abstract form« (Lakoff 2007, 254) geworden, die in ganz unterschiedlichen Politikkontexten zum Einsatz kommt. Als Sicherheitstechnologie verstanden ist Vor-

---

151 »[I]n ihren [gemeint ist die Zukunftsethik, A.F.] theoretischen Implikationen ernst genommen, würde [sie] uns nötigen, das erwähnte Umdenken weit auszudehnen über die Lehre vom Handeln, das heißt der Ethik, hinaus in die Lehre vom Sein, das heißt die Metaphysik, voranzutreiben, in der alle Ethik letztlich gegründet sein muß.« (Jonas 1989, 30)

sorge auch nicht nur ein Rechtsprinzip – auch, wenn es dort besonders gravierende Auswirkungen hat (siehe dazu: Opitz 2011). Vielmehr ist die Vorsorge zu einem generellen Handlungskalkül in ungewissen Gefährdungslagen geworden. Im und als Prinzip unterscheidet sich Vorsorge tatsächlich von Vorbereitung, von *preparedness* oder Anpassung (siehe dazu: Anderson 2010, Bröckling 2012). Während Vorsorge dafür steht, eine Gefahr gar nicht erst eintreten zu lassen, geht es bei Vorbereitung und Resilienz darum (unvermeidbare oder zumindest nur sehr schwer abwendbare) Gefährdungen in ihren Auswirkungen abzumildern.

Das Vorsorgeprinzip ist aber auch zu einer »global form« geworden, die in unterschiedlichen Ländern eingesetzt wird. Deshalb macht es – wie Cass Sunstein (2007, 26f.) betont – auch keinen Sinn anzunehmen, dass Vorsorge nur das deutsche oder europäische Sicherheitsdenken kennzeichnet und den USA vollkommen fremd ist. Zwar gibt es handfeste Konflikte zwischen den USA und der EU darüber, ob das Vorsorgeprinzip als Rechtsgrundsatz beispielsweise die Anwendung genmanipulierter Pflanzen einschränken darf (Jasanoff 2000). Gleichzeitig wurde in den USA der Krieg gegen den Terror immer wieder mit Bezug auf das Vorsorgeprinzip bzw. das *precautionary principle* gerechtfertigt (Sunstein 2007, Aradau und Munster 2007). Diese spezifische Ausweitung der Politik der *precaution* hat das Vorsorgeprinzip in den kritischen Sozialwissenschaften in Misskredit gebracht. Gegen allzu vorschnelle Verurteilungen ist es daher gewiss sinnvoll, zwischen unterschiedlichen Tendenzen und Artikulationsformen der *precaution* zu unterscheiden. So unterscheidet Bröckling (2012, 100) zwischen einer »precaution I«, die bei den Umweltschützer\_innen gängig ist und den Akzent auf Handlungsverzicht legt, sowie einer aktivistischen »precaution II«, die drohendes Unheil durch proaktive Maßnahmen abwenden will. Mit einer ähnlichen Stoßrichtung grenzt auch Ben Anderson (2010) *precaution* und *preemption* voneinander ab. Es ist gleichwohl aus zweierlei Gründen schwer, eine »wasserdichte« Trennlinie zwischen *precaution* und *preemption* zu etablieren. Schließlich stellt auch Handlungsverzicht eine Handlung dar und nötigt zu teils massiven proaktiven Maßnahmen. Man denke etwa an die Anstrengungen der Energiewende, die der Verzicht auf fossile Brennstoffe zum vorsorgenden Schutz des Klimas notwendig macht. Aus dieser Perspektive betrachtet ist es schwer von der Hand zu weisen, dass sich einige Züge des im Zusammenhang mit ökologischen Gefahren entstandenen Vorsorgedenkens auch in Maßnahmen zum Krieg gegen den Terror wiederfinden. So lässt sich auch in der US-amerikani-

schen Anti-Terrorpolitik nach dem 11. September eine »Heuristik der Furcht« ausmachen, in der »wissenschaftliche Tatsachen« durch »affektive Fakten« ersetzt wurden, die ihre Ursache in der Zukunft haben. »The felt reality of threat legitimates preemptive action [...]. Any action taken to preempt a threat from emerging into a clear and present danger is legitimated by the affective fact of fear, actual facts aside.« (Massumi 2010a, 54)

Die Politik der Vorsorge durch »preemptive action« fußt aber nicht nur auf einer fragwürdigen Legitimationsgrundlage, sondern setzt auch eine fatale Praxis in Gang. »The most effective way to fight an unspecific threat is to actively contribute to producing it.« (Massumi 2007) Dabei ist Massumi nicht der einzige, der das Vorsorgeprinzip für seine paradoxen Effekte kritisiert, die besonders am Scheitern des Irakkriegs als präemptive Anti-Terrormaßnahme deutlich geworden sind. Auch der US-amerikanische Rechtsphilosoph und Berater von Präsident Obama, Cass Sunstein, kritisiert die Politik der *precaution* für ihre Fundierung in Gesetzen der Angst. Vor allem aber kritisiert er die innere Widersprüchlichkeit des Prinzips:

»In seinen starken Versionen ist das Vorsorgeprinzip inkohärent [...]. Es beansprucht Orientierung zu geben, scheitert aber daran, weil es genau diejenigen Schritte verurteilt, die es fordert. Die Regulierungsmaßnahmen, die das Prinzip verlangt, bringen selbst neue Risiken mit sich. Damit untersagt das Prinzip, was es zugleich fordert.« (Sunstein 2007, 27)

Man muss diese Kritik am Vorsorgeprinzip nicht teilen oder sich rundheraus von dessen sinnvollem Einsatz verabschieden, um auf einen aufschlussreichen Widerspruch im Vorsorgedenken aufmerksam zu werden. Es ist doch seltsam, dass die Philosophie der Vorsorge zwar explizit die Wirkungen und selbst noch die Fernwirkungen von Handlungen in ethische Kalküle einbeziehen möchte und gleichzeitig ausgerechnet den Effekten der *eigenen* Vorsorgehandlungen keine systematische Aufmerksamkeit schenkt. Die Befürworter\_innen der Vorsorge affirmieren die Unhintergebarkeit wissenschaftlicher Ungewissheit und negieren allzu oft die Unhintergebarkeit praktischer Unsicherheit. Auch noch so viele vorsorgende Sicherheitsmaßnahmen können keine vollkommene Sicherheit schaffen, weil sie selbst gefährliche Effekte haben können. Es besteht dann die Gefahr, dass das Festhalten am Ziel vollständiger Sicherheit zu einer unbegrenzten Proliferation von Vorsorgepolitiken führt und dabei zugleich immer neue Risiken erzeugt.



In der Praxis sollen vor allem zwei Konzepte einer solchen überzogenen Vorsorgepraxis entgegenwirken. Einerseits soll die Verhältnismäßigkeit bzw. die »wirtschaftliche Vertretbarkeit« (siehe: Boehmer-Christiansen 1994, 33) von Vorsorgemaßnahmen beachtet werden. Kosten-Nutzen-Kalküle sind eine nahezu obligatorische Prüfungsform bei der Anwendung des Vorsorgeprinzips. Zum anderen wirkt die Kategorie des Restrisikos, die durch das Verfassungsgerichtsurteil zum »Schnellen Brüter« in Kalkar berühmt geworden ist, als Einschränkung der Vorsorgezumutungen.

»Vom Gesetzgeber im Hinblick auf seine Schutzpflicht eine Regelung zu fordern, die mit absoluter Sicherheit Grundrechtsgefährdungen ausschließt, die aus der Zulassung technischer Anlagen und ihrem Betrieb möglicherweise entstehen können, hieße die Grenzen menschlichen Erkenntnisvermögens verkennen und würde weithin jede staatliche Zulassung der Nutzung von Technik verbannen.« (zitiert nach: Sanden 2006, 262)

In diesem Urteilsspruch lässt sich ein anderer Umgang mit dem Problem des Nicht-Wissens erkennen. Ab einer bestimmten Grenze werden Sorgen um unspezifische Gefahren irrational. Restrisiko und Kosten-Nutzen-Erwägungen sind Denk- und Prüfungsformen zur Begrenzung der potenziell unbegrenzten Logik der Vorsorge und immunisieren dadurch gleichsam gegen zu viel Sicherheit, so wie das Vorsorgeprinzip seinerseits gegen eine zu starke Fokussierung auf wissenschaftliche Sicherheit bzw. Gewissheit schützt.<sup>152</sup>

---

152 Natürlich wird das Vorsorgeprinzip auch noch von sehr vielen anderen Faktoren eingeschränkt, etwa von konkurrierenden Rationalitäten der Sicherheit und anderen Prinzipien des Umweltschutzes. Boehmer-Christiansen (1994, 33) identifiziert neben Vorsorge vier weitere Prinzipien der deutschen Umweltpolitik: Verursacherprinzip, Kooperation, wirtschaftliche Vertretbarkeit und Gemeinlast.

### 3.2.2. Deichgrafendämmerung: Kritik hydraulischer Gouvernamentalität

»Prävention will nichts schaffen, sie will verhindern. [...] Ihr politischer Heros wäre weder der Steuermann noch der gute Hirte, weder der Baumeister noch der Gesetzgeber, sondern der Deichgraf.« (Bröckling 2012, 94)

»There are two kinds of levees: those that will fail and those that have failed.«  
(Bridges, zitiert nach: Perrow 2011, 21)

»Das Modell ist großartig – und schreckenerregend. Man baut eine Mauer und das Wasser hinter der Mauer steigt, also erhöht man die Mauer und das Wasser hinter der Mauer steigt weiter und verbreitert sich. Die Lösung eines Problems enthüllt zehn weitere Probleme, und so fort.« (Serres 1981, 269f.)

In der jüngeren Vergangenheit hatten Gesellschaften auf der ganzen Welt mit einem seltsamen Phänomen zu kämpfen: sogenannte Jahrhundertfluten, die sich gleichwohl eher alle zehn denn alle hundert Jahre wiederholten (in Deutschland etwa im Jahr 2004 und 2013). Was war geschehen? Das Leben an und mit Flüssen und deren Überschwemmungen ist zunächst einmal alles andere als eine spezifisch moderne Erfahrung. Vielmehr ist Hochwasser ein ständiger Begleiter der Zivilisation, der schon früh das Aufkommen einer hydraulischen Gouvernamentalität begünstigt hat,<sup>153</sup> die versucht, der Flut Herr zu werden bzw. sie zu kanalisieren. So hat Michel Serres auf die Maßnahmen zur Kontrolle der Flüsse im antiken Ägypten aufmerksam gemacht, wenn er bemerkt:

---

153 Mit der Wendung »hydraulische Gouvernamentalität« spiele ich auf das Konzept des »hydraulic government« von Karl August Wittfogel an. Der Soziologe und Sinologe Wittfogel definierte die hydraulische Regierung folgendermaßen: »I suggest that farming based on large-scale waterworks be designated »hydraulic farming« [...]. I also suggest that a government managing such an agriculture be designated a »hydraulic government«, and a society dominated by it a »hydraulic society.« (Wittfogel 1957, 344). Wittfogel orientierte sich in seinen Studien über die chinesische Gesellschaft stark an Webers (2005, 713f.) Konzept der Wasserbaubürokratie. Vor allem sein Geodeterminismus – hydraulische Gesellschaften entstehen nur unter Bedingungen bestimmter klimatischer Verhältnisse – brachte ihm viel Kritik ein, ebenso wie seine Identifizierung von hydraulischer mit »orientalischer« Gesellschaft. Wenn ich von hydraulischer Regierung oder hydraulischer Gouvernamentalität spreche, dann geht es mir nicht um einen allgemeinen Kulturvergleich. Vielmehr möchte ich damit lediglich auf spezifische Formen der Regierungskunst hinweisen, die sich mit der Regulierung von Flüssen, Wasser und Fluten beschäftigen.

»[der Fluss] kommt nicht, er kommt gewaltig, unerwartet, er überschwemmt, ertränkt, statt zu befruchten. Da ist es besser, ihn zu kanalisieren und zu regulieren, ein Netz von Wasserläufen um den Hauptstrom anzulegen. In Aufschüttungen und Ausschachtungen, Anhäufungen und Senkungen entfaltet sich das ziviltechnische Genie. Rationalisierung des Zufalls oder Normalisierung des Stochastischen.« (Serres 1981, 269)

Bevor die »Rationalisierung des Zufalls« mit dem Aufkommen von Statistik und Wahrscheinlichkeitsrechnung zu einer Wissenschaft werden konnte, war sie bereits eine praktische Fertigkeit im Rahmen der hydraulischen Künste des Regierens, die bis in die Neuzeit tradiert wurde. Machiavelli konnte am Beginn der Renaissance das Wissen um Deichbau und vorausschauende Flutkontrolle bei seiner Leserschaft, den Fürsten, voraussetzen und so seine Lehre von der *fortuna* verdeutlichen:

»Ich vergleiche sie [gemeint ist die *fortuna*, A.F.] mit einem reißenden Strom, der bei Hochwasser das Land überschwemmt, Bäume und Häuser niederreißt, hier Land fortträgt und dort anschwemmt [...]. Obwohl die Dinge so liegen bleibt doch nichts anderes übrig, als daß die Menschen in ruhigen Zeiten durch den Bau von Dämmen und Deichen Vorkehrungen treffen, und zwar derart, dass die steigenden Fluten entweder durch einen Kanal abgeleitet werden oder ihre Wucht gehemmt wird, damit sie nicht so rasend und verheerend wird.« (Machiavelli 1978, 103)

Elemente des »hydraulic government« (Wittfogel 1957, 344) finden sich also gewiss nicht nur im »Orient«. Auch im »Okzident« ist die Hydraulik eine wesentliche Kunst des Regierens. So unterstreicht Chandra Mukerji die Bedeutung des »virtuos management« (Mukerji 2007, 128) von Flüssen, Meer und Land für den französischen Absolutismus und die Entfaltung seiner logistischen Macht. Wiebe Bijker (Bijker 2002, 573) weist darauf hin, dass die bereits im zwölften Jahrhundert entstandenen »water boards« zum Bau und zur Wartung von Deichen die ersten demokratischen Institutionen Hollands waren. Und Leser von Theodor Storms Novelle *Der Schimmelreiter* über den Deichgrafen Hauke Haien wissen ohnehin, dass Deiche »thick with politics« (Bijker 2007) sind.

Was all diese frühen Formen hydraulischer Gouvernementalität jedoch von der Technopolitik der Wasserkontrolle im 20. Jahrhundert unterscheidet, ist ihre Größenordnung und vor allem der technowissenschaftliche Anspruch, mit dem das 20. Jahrhundert die Probleme von Flut und Hochwasser in die Hand genommen hat. Machiavelli identifizierte die Natur noch mit der Glücksgöttin *fortuna*, als ein launisches »Weib« (Machiavelli 1978, 106), so unstet und unberechenbar wie das Wetter oder eben das

Wasser. Zwar konnte man diese zufällig-willkürliche Natur in gewissen Grenzen zähmen, aber man konnte sie nie beherrschen und schon gar nicht konnte die Natur zur Ikone von Regelmäßigkeit und Berechenbarkeit werden. Das wandelte sich mit dem Aufkommen des naturwissenschaftlichen Denkens, das die Natur nicht nur erkennen wollte, sondern immer mehr Instrumente zu ihrer technischen Beherrschung bereitstellte. Im 20. Jahrhundert hat die technokratische Hoffnung auf Erkenn- und Beherrschbarkeit der Natur ihren Höhepunkt erreicht und in großtechnischen Projekten zur Kontrolle des Wassers einen deutlichen Ausdruck gefunden. Staudämme, hydroelektrische Kraftwerke und schließlich gigantische Sturmflutwehre, technische Großprojekte wie der Assuan-Staudamm, der Hoover-Damm oder das Oosterschelde Sturmflutwehr gelten bis heute als sichtbare Ausdrücke eines technischen Willens zur Macht über die Natur, der eine bestimmte Natur überhaupt erst hervorgebracht hat. So argumentiert Timothy Mitchell in Bezug auf den Assuan-Staudamm, dass durch den Bau des Dammes zugleich eine spezifische Form der Natur des Flusses in Kraft gesetzt wurde.

»Nature was not the cause of the changes taking place. It was the outcome. The very scale of the technical and engineering works of the twentieth century produced a new experience of the river [...] as exclusively a force of nature. [...] In manufacturing the dam, the engineers also manufactured nature.« (Mitchell 2002, 35)

Für die planenden Technokraten war die hydraulische Ingenieurskunst das Mittel, um gleich mehrere Probleme auf einmal anzugehen. Durch Begradigung und Eindeichung der Flüsse sollten diese für den Schiffsverkehr ebenso wie für die Energiegewinnung durch Wasserräder erschlossen werden. Staudämme erlaubten eine gewisse Kontrolle über Wasserstände und ermöglichten es zudem, Elektrizität zu generieren. Vor allem sollte die technische Regulierung von Flüssen deren Überflutungen vermeiden, die das Leben an Flüssen stets so unberechenbar gemacht hatte.

Schnell gerieten diese Projekte jedoch in die Kritik. Eine Reihe von technischen und epistemischen Kritiken der wissenschaftlichen Anmaßungen und perversen Effekte der hydraulischen Kontrollprojekte hat geradezu eine Deichgrafendämmerung herbeigeführt, die unsere liquide Postmoderne kennzeichnet. Eine entscheidende Figur dieser Kritik war der US-amerikanische Geograph Gilbert White, der in Reaktion auf die technischen Großprojekte der New Deal-Ära, wie etwa den Hoover Damm, bereits Ende der 1930er Jahre Einwände gegen den technischen Hochwas-

serschutz formulierte (Felgentreff und Dombrowsky 2008, 16, Collier 2014, 277–280). White, der selbst im für Hochwasserschutz und Flussregulierung zuständigen *National Resources Planning Board* beschäftigt war, richtete seine Aufmerksamkeit vor allem auf die »safety risks« (Wildavsky 1988, 48f.), die von Deichen ausgehen. Deiche gewähren zwar eine Sicherheit gegen bestimmte, relativ moderate Flutereignisse, sind aber machtlos gegen Flutgrößereignisse. Gleichzeitig sorgen sie für ein trügerisches Sicherheitsgefühl. Die Gefahr von Überflutungen, die in vielen Regionen seit Jahrhunderten das Alltagsleben prägte und entsprechenden kulturellen Anpassungsformen Vorschub leistete, wird auf Grund der geringeren Frequenz von Hochwasserereignissen vergessen. Hochwassergebiete werden immer dichter besiedelt und die lokale Bevölkerung ist schlechter auf Überflutungen vorbereitet. Deshalb, so konnte White zeigen, sinkt zwar die Wahrscheinlichkeit von Hochwasserereignissen, zugleich nimmt aber deren Schadenssumme insgesamt zu, weil ein Hochwasser schnell katastrophische und sehr kostspielige Schäden hervorruft (siehe: Felgentreff und Dombrowsky 2008, 16). Dieser paradoxe Zusammenhang von fortschreitender Sicherheitstechnik, wachsendem Sicherheitsempfinden und gleichzeitigem Anwachsen der Gefährdung ist weit über das Feld des Hochwasserschutzes als *levée effect* bekannt (siehe etwa: Law 2006, 231). Der Deich ist von einer Sicherheitstechnik zu einem Sicherheitsproblem geworden.

Neben Deichen ist insbesondere die Begradigung bzw. Normalisierung von Flüssen in die Kritik geraten. Nicht nur werden dadurch Ökosysteme zerstört, die sich an und in dem mäandrierenden Flusslauf entwickeln konnten, zudem wird durch die Begradigung und Kanalisierung von Flüssen auch die Gefahr katastrophischer Überflutungen verstärkt. Der Bund Umwelt und Naturschutz Deutschlands (BUND) erläutert in einer wichtigen Studie zum Hochwasserschutz aus dem Jahr 2002:

»Die Begradigung, Kanalisierung und Verbauung unserer Bäche und Flüsse in den letzten zwei Jahrhunderten hat nicht nur wertvolle Lebensräume zerstört, sondern auch die Hochwassergefahr verschärft. Begradigung reduziert die Wassermenge, die vom Flusslauf aufgenommen werden kann. Der Fluss mit Schlingen und Schleifen kann viel mehr Wasser aufnehmen als der verkürzte, begradigte Flusskanal. Die Begradigung führt zu einem schnelleren Abfluss. Die Hochwasserwelle wird schneller, es bleibt weniger Zeit für kurzfristige Hochwasserschutz-Maßnahmen. Das Ergebnis kann auch sein, dass Hochwasserspitzen aus den Nebenflüssen mit der Welle des Hauptflusses zusammentreffen und die Gefahr insgesamt stark erhöhen.« (BUND 2002, 12)

Schließlich wird immer wieder die Reduzierung von Feuchtgebieten kritisiert, die Wasser aufnehmen können. »(W)etlands act like blotting paper. They absorb water fast and release it slowly. If you take them away, then rainfall is delivered much more quickly into the river system. Flooding is more likely.« (Law 2006, 228) Heute sind diese Feuchtgebiete verschwunden und mit ihnen Ökosysteme und Rückhaltebecken, die Überflutungen auffangen können. »Viele Flüsse ähneln heute Kanälen, mit einem Hochwasserdamm an jedem Ufer. Diese Situation ist mit einem nachhaltigen Hochwasserschutz ebenso wenig wie mit den Aufgaben des Naturschutzes vereinbar.« (BUND 2002, 6) Katastrophen- und Naturschutz gehen in den Augen ökologischer Kritiker Hand in Hand. Leidet das eine, dann leidet auch das andere Anliegen einer »ganzheitlichen« Sicherheitspolitik.

Hochwasser wird es immer geben. Technischer Hochwasserschutz kann dieses Problem daher nicht lösen, sondern nur verlagern (Felgentreff und Dombrowsky 2008, 16). Im schlechtesten Fall verschlimmert er sogar das Problem, auf das er reagiert, indem er die Wahrscheinlichkeit von verheerenden katastrophischen Hochwassern erhöht. Die hydrologische Ingenieurskunst, die in vielerlei Hinsicht tatsächlich eine erstaunliche Kontrolle über die Naturkraft des Wassers ermöglicht hat, hat zugleich die »soziale Verwundbarkeit« gegenüber Hochwasserereignissen enorm erhöht. Aus dem Hochwasser, dem regelmäßigen und doch erratischen »Über die Ufer«-Treten von Flüssen, hat die soziotechnische Modifikation der Flussökologien eine ganz spezifische Form der Naturkatastrophe hervorgebracht: das verheerende Jahrhunderthochwasser. Es stehen dann nicht nur ein paar Felder oder Keller unter Wasser, sondern teure Holzböden, Bahnschienen oder toxische Chemiefabriken. Gerade der Schutz gegen das alltägliche »Über die Ufer«-Treten von Flüssen, die Normalisierung und Kanalisierung der Flüsse, lässt die Wahrscheinlichkeit von großen Katastrophen wachsen. »Building bigger levees increases the scope of the inevitable disaster, while it brings in the business and populations who are protected from minor storms but made more vulnerable to major floods and hurricanes.« (Perrow 2011, 40)

Als Gegenmodell gegen den in den Augen seiner Kritiker gescheiterten technischen Hochwasserschutz wird häufig ein »ökologischer Hochwasserschutz« ins Spiel gebracht. Gefordert werden dann etwa die Rückverlagerung von Deichen, der Stopp des Baus von Talsperren, die Revitalisierung von Feuchtgebieten und vor allem ein Stoppen der Versiegelung der Landschaft und weiteren Bebauung von Hochwassergebieten (BUND 2002, 16–

18). Diese Vorschläge stehen für eine Abkehr von einer normalisierend-präventiven Sicherheitstechnologie, die versucht, das Ereignis des Hochwassers zu verhindern. Der Deich, die Flussbegradigung und die künstliche Kanalisierung sind dafür die paradigmatischen Sicherheitstechniken. Ökologischem Hochwasserschutz geht es demgegenüber nicht um die präventive Verhinderung von Hochwasserereignissen *per se*, sondern lediglich um die Vermeidung katastrophischer Jahrhundertfluten. Dafür soll die Verwundbarkeit der Flussökologie und der Bevölkerung gegenüber Hochwassern vermindert werden. Es geht also um eine resiliente Reaktion auf Hochwasser, nicht um deren vorsorgliche Verhinderung. Zum einen sollen vorsorgliche »Speicher« in Form von Rückhaltebecken und Poldern für den Hochwasserfall angelegt werden, die das zusätzliche Wasser aufnehmen können (Resilienz durch Pufferkapazitäten). Zum anderen soll das Flusssystem so »redesigned« werden, dass es nicht durch erhöhte Fließgeschwindigkeit zu erhöhter Hochwassergefahr kommt (Resilienz durch Veränderung der Systemarchitektur). Die veränderte Systemarchitektur soll dabei jedoch gerade nicht technisch-planerisch vollzogen, sondern vielmehr der Natur selbst überlassen werden. Dabei stehen all diese Vorschläge unter der generellen Devise, Flüssen »ihren freien Lauf [zu] lassen« (BUND 2002, 12).

»Ökologischer Hochwasserschutz braucht eine möglichst weitgehende Wiederherstellung des alten Fließgewässerverlaufs und des Fließgewässer-Kontinuums. Die Flüsse und Bäche müssen von ihrem engen Korsett befreit werden [...]. Der Mensch sollte der Natur vertrauen, der Dynamik Raum geben und sie nur an geeigneten Stellen unterstützen. Der Fluss selbst ist der beste Wasserbauer, wenn er Gelegenheit dazu findet. Die Energie und Wucht des Hochwassers sollte sich gefahrlos für den Menschen und frei in der Natur, im Sinne des Ökosystemschutzes, abarbeiten dürfen.« (BUND 2002, 14)

Ökologischer Hochwasserschutz steht also im Gegensatz zu einer technohydraulischen Kontrollvision, die kanalisierte Ströme nach Belieben steuern will. Auch darin ähnelt er dem Leitbild der Resilienz, wie es Crawford Holling entworfen hat, der sich stets von ingenieursmäßigem Planungseifer distanziert hat. Aber auch eine Parallele zu einer anderen Denktradition sticht ins Auge. So erinnern ökologische Forderungen danach, die »Flüsse laufen zu lassen«, an die wirtschaftsliberale Devise des *laissez faire*. Wie in der neoliberalen Kritik des Staates werden bestimmte Wissens- und Planungsansprüche der Regierung kritisiert. Jeweils werden die perversen

Effekte technokratischer Planung und Steuerung offengelegt.<sup>154</sup> Jeweils wird im Namen der »natürlichen« Selbstregulation eine alternative Regierung der Flüsse und Zirkulationen vorgeschlagen. Dem spontanen Strömen von Märkten und Flussnetzen soll der nötige Freiraum gelassen werden – und zwar auch dann, wenn es bisweilen zu Ungleichgewichten oder Überschwemmungen kommt. Dabei muss dieses »Freiraum lassen« jeweils als aktiver Prozess gedacht werden. Ökologische und neoliberale Kritik sind postnaturalistisch,<sup>155</sup> insofern sie davon ausgehen, dass es keine unbeschädigte Natur des Ökonomischen oder Ökologischen gibt, zu der es sich einfach zurückkehren ließe. Flüsse müssen renaturiert, Märkte dereguliert oder sogar neu geschaffen werden. Tatsächlich sind Ökologie und Neoliberalismus entscheidende Bewegungen der technischen und epistemischen Kritik der Regierung in der zweiten Hälfte des 20. Jahrhunderts. Die Familienähnlichkeiten ihrer Kritiken haben es gewiss wahrscheinlicher gemacht, dass Ökologie und Neoliberalismus bisweilen Hand in Hand gehen. Gleichwohl stehen sich beide Bewegungen häufig auch als erbitterte Feinde gegenüber. Es wäre also verkürzt, von den allgemeinen Verwandtschaften zwischen beiden Formen der Kritik auf eine Konvergenz ihrer Ziele und Effekte zu schließen.

In seinem Aufsatz *Neoliberalism and Natural Disaster* hat Stephen Collier die verschlungenen Wege rekonstruiert, die zu einer tatsächlichen Überschneidung von ökologischen und neoliberalen Kritiken der staatlichen Hochwasserkatastrophenvorsorge in den USA geführt haben und in der Forderung nach einer Individualisierung des Flutrisikos gipfelten. In den 1940ern hatten Neoliberale wie August Friedrich Hayek staatliche Hilfe für

---

154 Natürlich ist diese Kritik nicht in allen Teilen des heterogenen Denkkollektivs des Neoliberalismus gleichermaßen ausgeprägt. Allerdings sollte nicht vergessen werden, dass sich viele Neoliberale nie nur für einen »freien« Markt eingesetzt haben, sondern grundsätzlich einer bestimmten technokratischen Mentalität feindlich gegenüberstanden. So hat etwa August Friedrich Hayek (2010) in seinem Buch *Studies on the Abuse and Decline of Reason* eine von Saint-Simon ausgehende Tradition des industriell-planerischen Politikstils angegriffen, weil er darin einen falschen Gebrauch der Vernunft erblickte. Zum Neoliberalismus als Kritik siehe auch: Folkers (2016, 12–17).

155 Foucault (2006, 172–174) argumentiert, dass der Neoliberalismus sich wesentlich durch seine Kritik an der »naturalistischen Naivität« der Marktdoktrinen des 18. Jahrhunderts vom klassischen Liberalismus abhebt. Zwar haben Märkte – einmal etabliert – tatsächlich selbstorganisierende Eigenschaften und sind darin Naturprozessen ähnlich. Allerdings sind sie nicht einfach schlicht gegeben, sondern müssen durch rechtlich-politische Rahmenbedingungen und die Effekte ökonomischer Theorien überhaupt erst geschaffen werden. Den Konstruktivismus der Neoliberalen betont auch (Mirowski 2009).



Flutopfer noch unterstützt, insofern sie diese als »acts of god« ansahen, die der individuellen Verantwortung entzogen sind (Collier 2014, 273). Etwa zur gleichen Zeit zweifelte der Vordenker der amerikanischen Ökologiebewegung Gilbert White die im Rahmen der New Deal-Politik eingeführte staatliche Unterstützung für Flutopfer bereits an, weil sie zusätzliche Anreize schaffe, in Hochwasserregionen zu ziehen (Collier 2014, 274). Whites – und nicht Hayeks – Argumentation griff der neoliberal-orientierte Ökonom John Kurtilla in den 1960er Jahren auf. Er argumentierte, dass die Fluthilfe auf eine versteckte Subvention von Personen, die in Flutregionen ziehen, hinauslaufe und so eine perverse Entwicklung – die Besiedelung von Hochwassergebieten – fördere. Nur eine Individualisierung des Flutrisikos, also eine private Versicherung gegen Flutschäden, könne diese Ungerechtigkeit der versteckten Subventionen ebenso wie die iatrogenen Effekte der staatlichen Flutsicherheitsprogramme beheben (Collier 2014, 282ff.). Solange die Flut als »Naturkatastrophe«, als höhere Gewalt oder »act of god« verstanden wurde, traten also selbst eingefleischte Neoliberale für die staatliche Unterstützung von Hochwasseropfern ein. Erst durch die denaturalisierende Kritik von White öffnete sich das Feld für eine neoliberale Kritik dieser staatlichen Politik.

Trotz dieser Verstrickung von einigen neoliberalen und ökologischen Kritiken kam es nicht zu einer umfassenden Reformierung der Politik der Flutopferentschädigung – weder in den USA noch in Deutschland. Nach der letzten »Jahrhundertflut« im Jahr 2013 waren deutsche Politiker schnell bereit, die Schäden der »Wucht der Natur« (Angela Merkel in: DPA 2013) zu beheben. Bundeskanzlerin Merkel ließ sich sogar zu der Aussage hinreißen: »Angesichts der Tatsache, wofür wir sonst Geld ausgeben, ist dieses Geld gut ausgegebenes Geld« (siehe: Geis und Hildebrandt 2013). Keine Spur also von einer Kritik an den vermeintlichen Pathologien öffentlicher Ausgaben, die von Neoliberalen so nachhaltig vorgebracht wurden. Die ökologische Kritik scheint demgegenüber besser verfangen zu haben. Schließlich wurden zentrale Forderungen und Strategien des ökologischen Hochwasserschutzes – Deichrückverlegung und Wiedergewinnung von natürlichen Rückhalteflächen – im *Nationalen Hochwasserschutzprogramm* berücksichtigt, das in der Folge der Flutkatastrophe 2013 aufgelegt wurde (NHWSP 2014, 4).

### 3.2.3. Zwischen Vorbeugung und Vorbereitung. Anpassungen an die neue Klimanormalität

Das Phänomen zehnjähriger »Jahrhundertfluten« wirft eine ganze Reihe unbequemer Fragen auf. Haben wir es wirklich (noch) mit einer Jahrhundertflut zu tun? Ist die jüngste Häufung extremer Flutereignisse statistisch gesehen noch normal (schließlich können Jahrhundertfluten statistisch gesehen zwei Jahre hintereinander eintreten, wenn sie dann für zweihundert Jahre ausbleiben)? Oder hat sich eine neue Normalität verheerender »Dekadenfluten« eingestellt? Und wenn dem so ist: Ist es zu dieser neuen Normalität gekommen, weil die perversen Effekte der Flutregulation und Flussnormalisierung eine fatale Denormalisierung herbeigeführt haben? Oder hat eine Häufung von extremen Niederschlägen die Pegelstände der Flüsse auf Rekordniveau hochgeschraubt? Und wenn letzteres: Sind diese extremen Phänomene zufällige Kapriolen des Wetters und deshalb »normale« statistische Ausreißer? Oder haben wir es bereits mit den Folgen eines veränderten Klimas zu tun, das neben höheren Temperaturen auch zu einer neuen Normalität des Extremen führt?

Ein möglicher Zusammenhang von Klimawandel und der Häufung von Jahrhundertfluten ist besonders beunruhigend. Gerade Versicherungen bereitet der Klimawandel Kopfzerbrechen, weil sie sich nicht mehr auf historische Daten beziehen können, sondern zukünftige Verläufe komplexer Zusammenhänge antizipieren müssen (siehe: Bundesregierung 2008, 36). Jedes Flutereignis gilt als Hinweis auf eine denormalisierte Zukunft und schraubt deshalb die Wahrscheinlichkeitsschätzungen für mögliche zukünftige Flutereignisse in die Höhe. Aber nicht nur die Zukunft klimabedingter Flutereignisse ist ein Problem. Schon deren Gegenwart stellt politische Routinen im Umgang mit dem Klimawandel in Frage. Plötzlich ist der Klimawandel nicht mehr ein Problem der Zukunft, das man aufhalten muss und damit auf Distanz halten kann, sondern eine Gefahr im Hier und Jetzt. Der Klimawandel ist nicht mehr, um mit Walter Benjamin (1991c, 592) zu sprechen, das »jeweils Bevorstehende, sondern das jeweils Gegebene«. Der Klimawandel ändert dadurch gewissermaßen seinen temporalen Modus, die Art, wie er Gegenwart, Zukunft und Vergangenheit miteinander verkoppelt. Er ist nicht mehr nur eine Zukunft mit Ursachen in Vergangenheit und Gegenwart, sondern wird immer mehr zu einer Zukunft, die bedrohlich auf die Gegenwart zurollt bzw. bereits in ihr angekommen ist. Gerade die deutsche Umweltpolitik wird von solchen Entwicklungen düpiert. Schließlich gibt es einen parteiübergreifenden Kon-

sens, dass »Nachhaltigkeit« und »Vorsorge« die Leitkonzepte der Umweltpolitik sein sollen. Schäden an der Umwelt sollen vorbeugend vermieden werden. Was also macht die Umweltpolitik, wenn sie es nicht mehr mit zukünftigen, sondern gegenwärtigen Problemen zu tun hat? Im Jahr 2008 hat das Bundeskabinett die Deutsche Anpassungsstrategie an den Klimawandel beschlossen (siehe: Bundesregierung 2008) und den Klimawandel damit als gegenwärtige und nicht mehr gänzlich aufzuhaltende Problematik anerkannt. Aber was heißt es, wenn Klimawandelanpassung zu einer sicherheits- und umweltpolitischen Programmatik wird und damit Vorbeugung durch Vorbereitung sowie Nachhaltigkeit durch Resilienz supplementiert werden?

In relevanten politischen Debatten in Deutschland herrscht mittlerweile große Einigkeit darüber, dass der Klimawandel ein Problem mit signifikanten Auswirkungen in der Gegenwart darstellt. Ein obligatorischer Referenzpunkt für diese Auffassung sind die Sachstandsberichte des Intergovernmental Panel on Climate Change (IPCC), und zwar insbesondere der vierte Sachstandsbericht aus dem Jahr 2007 (siehe: IPCC 2007b). Das IPCC mit Sitz in Genf ist eine vom UN-Umweltprogramm UNEP und der Weltorganisation für Meteorologie ins Leben gerufene Institution, deren Aufgabe darin besteht, politische Entscheidungsträger über den Stand der Forschungen zum Klimawandel zu informieren. Dabei forscht das IPCC nicht selbst, sondern fasst die internationalen Forschungsergebnisse der »vast machine« (Edwards 2010) der globalen Klimawissenschaft zusammen und bereitet sie für politische Entscheidungsträger auf. Dem »hybrid science-policy body« (Edwards 2010, 399) IPCC geht es also weniger um Forschungsinnovationen als darum, einen Konsens über den Klimawandel herzustellen und abzusichern. Für die politische Diskussion in Deutschland und Europa war der Bericht von 2007 vor allem deshalb bedeutsam, weil er unterstrichen hat, dass eine signifikante Erderwärmung (um 0,5 bis 0,9 Grad Celsius seit dem 19. Jahrhundert) bereits eingetreten *ist* und deshalb genuine Bemühungen zur Anpassung an den Klimawandel erforderlich sind. Das geht aus den Empfehlungen der Arbeitsgruppe II des IPCC zu *Auswirkungen, Anpassungen und Verwundbarkeiten* (IPCC 2007a) hervor. Zwar hatten sich die Unterzeichner der Klimarahmenkonvention bereits 1992 verpflichtet, Anpassungsmaßnahmen an den Klimawandel vorzunehmen (siehe: Bundesregierung 2008, 5). Aber erst der IPCC-Bericht von 2007 sorgte dafür, dass das Thema Anpassung an den Klimawandel in Deutschland und der EU auch auf die innenpolitische Agenda gesetzt

wurde, während es zuvor nur in der Entwicklungszusammenarbeit Thema war. 2008 verabschiedete zunächst das Bundeskabinett die *Deutsche Anpassungsstrategie an den Klimawandel* (Bundesregierung 2008), 2009 legte die EU ein *Weißbuch Anpassung an den Klimawandel* vor (EU 2009) und 2011 wurde ein vorläufiger *Aktionsplan* (Bundesregierung 2011) zur Klimawandelanpassung vom Bundeskabinett beschlossen. Der Grundkonsens, der sich durch all diese Papiere zieht, ist: »Das Klima ändert sich!« (Bundesregierung 2011, 6) und deshalb gilt: »Anpassung ist notwendig« (UBA 2008).

So sinnfällig diese Schlussfolgerung auf den ersten Blick erscheinen mag – sie birgt doch politischen Sprengstoff. Schließlich kann Anpassung an den Klimawandel als Bruch mit der Vorsorgetradition im deutschen Umweltrecht erscheinen. Tatsächlich wird die Vorsorgeorientierung der deutschen Umweltpolitik in Bezug auf den Klimawandel von offizieller Seite nie in Frage gestellt. Selbst die *Deutsche Anpassungsstrategie* (DAS) verpflichtet sich explizit auf eine »Vorsorgeorientierung« (Bundesregierung 2008, 6). Und eine Studie des Bundesamtes für Katastrophenhilfe und Bevölkerungsschutz (BBK) zu Klimawandelanpassungsmaßnahmen in den Ländern kommt zu dem Ergebnis, dass »der Schwerpunkt der Anstrengungen beim Thema Klimawandel auf dem Klimaschutz liegt« (BBK 2009a, 68). Die Differenz zwischen Klimawandelanpassung und Klimaschutz wird jedoch sehr wohl bemerkt. In einer weiteren Veröffentlichung des BBK zu den »Herausforderungen« des Klimawandels für den Bevölkerungsschutz wird etwa zwischen »Mitigations-Maßnahmen«, um das »Ausmaß der Klimaänderungen [...] zu reduzieren« und »Adaptions-Maßnahmen«, um den »Auswirkungen des erwarteten und nicht mehr vermeidbaren Klimawandels zu begegnen« (BBK 2011, 21) unterschieden. Vermieden werden soll der Eindruck, dass diese Differenz auch einen Konflikt darstellt. In der DAS heißt es programmatisch: »[B]eide Wege – Maßnahmen zur Verringerung der Treibhausgasemissionen und Maßnahmen zur Anpassung an den Klimawandel – [sind] untrennbar miteinander verbunden.« (Bundesregierung 2008, 5) Deshalb ließen sich sogar »Synergien zwischen Naturschutz, Klimaschutz und Anpassung« erzeugen. Ein Beispiel für solche Synergien besteht im Anlegen und in der Pflege von Feuchtgebieten, die sowohl im Dienste der Klimawandelminderung stehen, insofern sie CO<sub>2</sub> binden können, als auch im Dienste der Klimawandelanpassung und des ökologischen Hochwasserschutzes. Deshalb können intelligente »Maßnahmen die Speicherfunktion von Feuchtgebieten für Kohlenstoff sowie deren Pufferfunktion für Folgen von Extremereignissen auf den

Wasserhaushalt nutzen« (Bundesregierung 2008, 26). Gleichwohl wird ebenso eingeräumt, dass sich »Zielkonflikte« zwischen Anpassung und Minderung nicht immer vermeiden ließen. So führe etwa die »Verdichtung von Stadtstrukturen« zu »reduzierte[m] Energieverbrauch«, verstärke aber zugleich den »Stadtklimaeffekt« (Bundesregierung 2008, 49).

Hinter der Betonung der Vereinbarkeit steht tatsächlich mehr als eine Floskel. Vielmehr lässt sich in der Klimapolitik ein Politikfeld beobachten, in dem Vorsorge und Vorbereitung, vorbeugender Schutz und Resilienz als sich wechselseitig ergänzende Sicherheitsstrategien artikuliert werden. Hier spielt das berühmte Zwei Grad-Ziel eine entscheidende Rolle, also das Ziel der Klimapolitik, die Erderwärmung nicht höher als zwei Grad gegenüber dem vorindustriellen Niveau Mitte des 19. Jahrhunderts steigen zu lassen. Die zwei Grad-Grenze wurde bereits 2001 im dritten Sachstandsbericht eingeführt (IPCC 2001, 5). Während bis zu einem Temperaturanstieg von zwei Grad die Effekte der Klimaänderungen noch beherrschbar erscheinen, werden bei einem Anstieg über zwei Grad katastrophale Folgen befürchtet. Zwar ist umstritten, ob die zwei Grad-Grenze tatsächlich ein angemessenes Ziel der Klimapolitik ist und was genau jenseits dieser Schwelle passiert. Allerdings mehren sich die Stimmen in der Klima- und Erdsystemforschung, die nicht bloß kumulative Effekte der Erderwärmung prognostizieren, sondern auch auf die Gefahr von nicht-linearen Effekten und sogenannten *tipping points* im Klimasystem aufmerksam machen. Jenseits bestimmter kritischer Schwellenwerte, bei denen es sich sowohl um Durchschnittstemperaturen handeln kann als auch um die nachhaltige Beschädigung anderer Faktoren des Erdsystems wie Artenvielfalt, Höhe des Meeresspiegels oder den Verlust der Integrität zentraler weltweiter Ökosysteme, kann es zu grundlegenden Veränderungen kommen. Derartige *phase changes*, also das sogenannte Umkippen von Ökosystemen, Strömungsmustern von Meeren und Winden etc. hätten dann Folgen, die kaum zu kontrollieren wären.

Die Debatte um kritische Schwellenwerte, »Toleranzfenster« und »planetarische Leitplanken« hat eine spezifische »Katastrophenschwelle« (Luhmann 2003, 11) in die Politik des Klimaschutzes eingeführt. Besonders einflussreich ist die Theorie der *planetary boundaries*, die von einer Reihe renommierter Umweltwissenschaftler\_innen entwickelt und 2009 in einem Artikel der Zeitschrift *Nature* unter dem vielsagenden Titel *A Safe Operating Space for Humanity* veröffentlicht wurde (Rockström et al. 2009). Zu den Autor\_innen gehörten unter anderem Hans-Joachim Schellnhuber, Leiter

des Potsdam-Instituts für Klimaforschung und der wohl wichtigste wissenschaftliche Berater der Bundesregierung in Fragen des Klimawandels, sowie Paul Crutzen, Nobelpreisträger und »Entdecker« des Ozonlochs. Geleitet wurde die Gruppe von Johann Rockström vom Öko-*think tank* Stockholm Resilience Center, das entscheidend von Hollings Resilienz-Konzept geprägt ist. Die Autor\_innen identifizieren neun planetarische Grenzen: Klimawandel, Biodiversitätsverlust, biochemische Kreisläufe, Übersäuerung der Ozeane, Süßwasserverlust, Landnutzung, Ozonabbau, atmosphärische Aerosole und chemische Belastung (Rockström et al. 2009). Die Idee, die derartige Grenzmarkierungskonzepte anleitet, ist, dass Resilienz nur innerhalb bestimmter Toleranzfenster möglich ist. Klimawandelanpassung, bzw. *evolutionäre Resilienz* als Adaption an eine sich tiefgreifende verändernde Umwelt, kann nach dieser Logik nur dann erfolgreich sein, wenn *Vorsorgepolitik* irreversible Schäden vermeidet, die durch eine Überschreitung ökologischer Katastrophenschwellen eintreten würden.

Diese Logik liegt auch der deutschen Anpassungsstrategie und dem programmatischen Beharren auf der Untrennbarkeit von Mitigation und Adaption zugrunde. So heißt es in der DAS: »Bei der Einhaltung des 2°C-Ziels wird davon ausgegangen, dass die Folgen durch geeignete und rechtzeitige Anpassungsmaßnahmen aufzuhalten sind und schwere Folgen vermieden werden können.« (Bundesregierung 2008, 5) Hans-Joachim Schellnhuber brachte den Zusammenhang klimabezogener Sicherheitsstrategien auf die griffige Formel: »Es geht darum, das Unbeherrschbare zu vermeiden und das Unvermeidbare zu beherrschen.« (Schellnhuber, zitiert in: UBA 2008, 13) Die Programmatik der Klimawandelanpassung impliziert zwar tatsächlich, dass es um die Einstellung auf eine neue Normalität und nicht um Normalisierung im Sinne von Rückführung zu einer alten, idealen Normalität geht. Klimawandelanpassung ist daher eine Form der Resilienzsicherheit. Aber Widerstandsfähigkeit gegenüber einer sich verändernden Umwelt kann nur dann gewährleistet werden, wenn sie bestimmte Grenzen nicht überschreitet und Veränderungen sich nicht so schnell und plötzlich ereignen, dass sehr langwierige Anpassungsprozesse nicht mehr adäquat implementiert werden können.

Die Anpassungsplanungen für die neue Klimanormalität müssen sich daher im Rahmen des »safe operating space for humanity« bewegen. Aber worin besteht diese neue Klimanormalität? Hier beginnen die Schwierigkeiten, weil große wissenschaftliche Ungewissheit über den Grad der be-

reits eingetretenen und vor allem der zu erwartenden Klimaveränderungen herrscht. So sehr der Klimawandel in Deutschland als Faktum anerkannt wird, so deutlich sind die Unsicherheiten über das genaue Ausmaß der Klimaveränderungen. In der deutschen Anpassungsstrategie wird immer wieder auf »Lücken« des Wissens und »Unsicherheiten« (Bundesregierung 2008, 4) hingewiesen. Und auch das IPCC weist stets sehr sorgfältig auf den Grad der Gewissheit seiner Erkenntnisse und Prognosen hin. Es gibt wohl kaum einen Politikbereich, der so wissenschaftsbasiert operiert und zugleich so reflexiv mit seinem Nicht-Wissen umgeht. Zwar sind die Gewissheitsgrade über den anthropogenen Anteil des Klimawandels, welche die Sachstandsberichte des IPCC ausweisen, stetig gestiegen (Edwards 2010, 401f.). Aber schon bei der Beurteilung über den bereits eingetretenen Klimawandel liegen die Einschätzungen zwischen 0,5 und 0,9 Grad Celsius Erwärmung (Edwards 2010, 402). Diese Unsicherheit ist nicht nur epistemischen Gründen geschuldet, wie etwa Uneinigkeit zwischen den tausenden beteiligten Wissenschaftlern, »noisy data« (Edwards 2010, 413–418), Unterschieden zwischen den zugrunde liegenden Klimamodellen etc. Vielmehr ist die Politik selbst ein wesentlicher Unsicherheitsfaktor. Es ist nämlich nicht klar, wie motiviert und erfolgreich die Regierungen bei der Reduzierung der Treibhausgasemissionen sein werden. Auch diese Ungewissheit wird systematisch in die Prognosen etwa des IPCC einbezogen. Typisch sind Diagramme, die unterschiedliche Szenarien für den durchschnittlichen Temperaturanstieg abhängig von den politischen Initiativen zum Klimaschutz abbilden (Edwards 2010, 403). Dabei können mehrere Grad zwischen dem unterem und dem oberen Szenario liegen. Es gibt also nicht nur eine, sondern viele (mögliche) neue Normalitäten.

Eine weitere Schwierigkeit besteht darin, dass es nicht ausreicht, nur die Steigerung der Durchschnittstemperaturen in den Blick zu nehmen. Weltweit ermittelte Durchschnittstemperaturen sagen schließlich wenig über regionale Veränderungen der Temperaturen und noch weniger darüber aus, wann kritische Schwellenwerte erreicht werden (die etwa zum Abschmelzen von Gletschern führen können). Zudem besteht eine stets wiederholte Erkenntnis der Klimawissenschaft darin, dass mit dem Klimawandel die »Intensität und Frequenz« (BBK 2009a, 15) von Extremwetterereignissen zunimmt. Neben einer veränderten Durchschnittstemperatur wird also auch eine erhöhte »Klimavariabilität« (Bundesregierung 2008, 15) erwartet. In dem Sonderreport des IPCC *Managing the Risk of Extreme Events and Disasters to Advance Climate Change Adap-*

tion werden schematisch drei Prognosen möglicher, veränderter Klimanormalitäten abgebildet (IPCC 2012, 5). Eine einfache Verschiebung des Temperaturdurchschnitts würde demnach gleichzeitig zu mehr extrem heißen Tagen führen, eine erhöhte Klimavariabilität hingegen zu mehr kalten und mehr heißen Tagen und eine veränderte Symmetrie der Temperaturverteilung ebenfalls zu mehr heißen Tagen. Jenseits von Temperaturextremen werden Zunahmen auch bei weiteren Wetterextremen erwartet. So wird in Deutschland neben einer Zunahme von Stürmen mit vermehrten Starkniederschlägen (siehe: BBK 2009a, 58) besonders im Winter gerechnet, während die Niederschlagsmengen im Sommer vermutlich zurückgehen werden (BBK 2011, 3).

Zwar sind die vermuteten und bereits eingetretenen Auswirkungen in anderen Teilen der Erde deutlich gravierender als in Deutschland. Aber auch hierzulande werden massive Auswirkungen erwartet auf Felder, die vom Tourismus bis zur Fischerei, von der Forstwirtschaft bis zur Finanzwirtschaft reichen (siehe die Übersicht in: UBA 2008, 7, sowie: Bundesregierung 2008, 16–53): Versicherer sind mit Kosten durch Klimaschäden, Landwirte mit veränderten Wettermustern, der Naturschutz mit einem Rückgang der Artenvielfalt und Fischer mit verändertem Fischbestand konfrontiert. Forstwirte befürchten Waldbrände und in touristischen Regionen muss möglicherweise das Angebot verändert werden, wenn die Sommer wärmer und die Winter schneeärmer werden. Der Großteil der Veränderungen durch den Klimawandel betrifft entweder klassische Themen der Umweltpolitik und des Naturschutzes – wie die Frage der Artenvielfalt – oder wirtschaftspolitische Themen, vor allem in Land- und Forstwirtschaft.

Klimawandelanpassung wird aber auch als genuines Sicherheitsproblem gerahmt und als Themenfeld für den Bevölkerungsschutz in Stellung gebracht. Schon in der DAS wird der Bevölkerungsschutz als »Querschnittsthema« (Bundesregierung 2008, 42–45) der Klimawandelanpassung benannt. Umgekehrt ist der Bevölkerungsschutz aber nicht nur ein Querschnittsthema der Klimawandelanpassung, sondern umgekehrt ist der Klimawandel auch ein Querschnittsthema des Bevölkerungsschutzes. Neben Terrorismus gilt der Klimawandel als ein »Leitszenario, um Entwicklungen in technischen und nichttechnischen Frühwarnsystemen, Hazard- und Risikoanalysen, Neubewertung der Kritikalität von Infrastruktur und Gesundheitsversorgung im Krisenfall voranzutreiben« (BBK 2009a, 40). Der Klimawandel ist, ähnlich wie die Veränderung der weltpolitischen Lage



und die Steigerung der Komplexität und Interdependenz der Gesellschaft, ein allgemeiner Bedrohungszusammenhang, der die Bedeutung eines neuorientierten Bevölkerungsschutzes unterstreicht.

Als spezifisches Problemfeld ist der Klimawandel für den Bevölkerungsschutz vor allem im Hinblick auf mögliche Extremwetterereignisse von Bedeutung. Es versteht sich von selbst, dass auch Bevölkerungsschützer\_innen mehr an den mit dem Klimawandel einhergehenden *peaks* als an den *means* interessiert sind. So ist für den Bevölkerungsschutz besonders interessant, ob Stürme zunehmen oder Niederschlagsmengen, die dann etwa zu vermehrten Hochwasserlagen führen könnten. Dass die Orientierung am Mittelwert nicht ausreicht, zeigt das Extremwetterereignis »Hitze« vielleicht am deutlichsten. So geht mit steigenden Durchschnittstemperaturen, wenn man von einer Normalverteilung der Temperaturen ausgeht, auch eine steigende Anzahl sehr heißer Tage einher (s.o.) (siehe auch: BBK 2009a, 57). Hitze, also Temperaturen über 30 Grad Celsius (siehe: BBK 2011, 14), ist eine in ihrer Gefährlichkeit häufig unterschätzte Naturkatastrophe. So zählt etwa der europäische Hitzesommer 2003 zu den zehn tödlichsten Naturkatastrophen der letzten 30 Jahre weltweit (siehe: BBK 2011, 40). Allein in Deutschland starben an Folgen der Hitze 9355 Menschen (BBK 2009a, 15). Gerade die »verwundbarsten« Teile der Bevölkerung – Alte, Kranke und Kinder, Arbeiter\_innen, die schwere körperliche Arbeit im Freien verrichten müssen etc. – waren besonders von der Hitze betroffen.

Bevölkerungsschutz ist gleichwohl nur ein Feld einer um sich greifenden sicherheitspolitischen Rahmung des Klimawandels. In jüngerer Zeit ist der Klimawandel immer mehr zu einem Problem von geostrategischer Tragweite geworden. Bereits im Jahr 2003 sorgte ein Bericht von Doug Randall und Peter Schwartz (2003) im Auftrag des Pentagon mit dem vielsagenden Titel *An Abrupt Climate Change Scenario and its Implications for United States National Security* für Aufsehen. Seine Drastik erhält der Bericht dadurch, dass nicht nur ein besonders verheerendes Klimaszenario mit vielen fatalen *feedback loops* und *tipping points* zugrunde gelegt wird, sondern zudem gezeigt wird, mit welchen sozialen und politischen Katastrophen die »Naturkatastrophe« des Klimawandels einhergehen könnte.<sup>156</sup> Eine im Tonfall und in den Prognosen zwar etwas gemäßigtere, aber von der Grundidee sehr ähnliche Studie wurde 2007 vom Wissenschaftlichen Beirat

---

156 Siehe zu diesem Bericht auch die Ausführungen von Melinda Cooper (2008, 80f., 90f.).

Globale Umweltveränderungen der Bundesregierung (WGBU) unter dem Titel *Klimawandel als Sicherheitsrisiko* veröffentlicht (WBGU 2007). Prognostiziert wird darin etwa eine Reihe von »Konfliktkonstellationen«, die durch den Klimawandel erzeugt oder verschärft werden (auch wenn die Rede von »Klimakriegen« (Welzer 2010) vermieden wird). Zudem sind etwa wachsende Migrationsbewegungen aus Ländern und Landstrichen zu erwarten, die von den Folgen des Klimawandels verwüstet wurden. Deshalb sei ein »erweitertes Sicherheitsverständnis« (WBGU 2007, 19) notwendig, das die komplexen Interaktionen von Mensch und Umwelt anerkennt und Klimaschutz als Kernanliegen der Sicherheitspolitik versteht. Beachtlich an dem Bericht ist dabei vielleicht weniger der Inhalt, der eine Reihe mittlerweile recht gängiger Topoi der Konfliktforschung aufruft, als vielmehr die berichtende Institution. Durch derartige Problematisierungen kommt es nicht nur zu einer Versicherheitlichung des Klimawandels, sondern umgekehrt auch zu einer Ökologisierung der nationalen Sicherheitspolitik. Geopolitik operiert nicht mehr nur auf einem politischen Terrain, in dem nationale Territorialstaaten und transnationale Machtblöcke miteinander um Vorherrschaft konkurrieren, sondern in einem Milieu bzw. geovitalen Terrain, in dem Veränderungen der natürlichen Lebensgrundlagen politische Veränderungen und Konflikte hervorrufen.<sup>157</sup>

Diese neue Akteurs- und Rationalitätsvielfalt, die sich mittlerweile um den Klimawandel versammelt, bereitet einigen klassischen Umweltschützer\_innen und sozialwissenschaftlichen Kritiker\_innen Sorgen. Sie fürchten eine Militarisierung des Klimawandels, wenn etwa das Pentagon sich des Themas annimmt (siehe etwa: Massumi 2009, 159–161). Auf der anderen Seite besteht Hoffnung, dass sich durch die Versicherheitlichung des Klimawandels auch eine erweiterte Biogegitimität einspielt und etwa Flucht als Folge des Klimawandels als legitimer Grund für die Gewährung von Asyl anerkannt wird.<sup>158</sup> Während die unterschiedlichen – ökonomischen, sicherheitspolitischen, ökologischen etc. – Rahmungen des Klimawandels

---

157 Gerade in der Humangeographie wird in jüngerer Zeit verstärkt über ein erweitertes Verständnis von Geopolitik diskutiert, in dem sich politische und physische Geographien vermischen, siehe: Yusoff (2013), Barry (2013, 31–56), Dalby (2017).

158 Didier Fassin (2012, 249) hat den Begriff der Biogegitimität geprägt, um den Sachverhalt zu fassen, dass in Frankreich Flüchtlinge Anspruch auf Asyl geltend machen können, wenn sie den Nachweis erbringen, dass in ihrem Heimatland keine angemessene medizinische Versorgung für eine vorliegende Krankheit möglich ist. Nicht mehr allein »politische« Verfolgung, sondern existenzielle, biologische Verwundbarkeit wird damit zu einem Kriterium für die Gewährung von Asyl.

ein großes Konfliktpotenzial aufweisen, existieren die differenten Rationalitäten von Anpassung und Schutz meist relativ problemlos neben- oder miteinander. Das heißt zwar nicht, dass es – wie erwähnt – keine konkreten Politikfelder gibt, wo beide Logiken miteinander in Konflikt geraten können. Aber es besteht doch Anlass, im Klimawandel gegenwärtig vor allem ein Politikfeld zu sehen, in dem Vorbeugung und Vorbereitung einander ergänzen und sich in ein übergeordnetes, erweitertes Verständnis von Resilienz einpassen. Anpassungsmaßnahmen an die neue Klimanormalität sind notwendig, können aber nur erfolgreich sein, wenn bestimmte »Leitplanken« nicht überschritten werden. Ins Kalkül treten daher die Ursachen ebenso wie die Auswirkungen, die langfristigen Trends ebenso wie die kurzfristigen Ereignisse, die Veränderungen in den *means* ebenso wie die in den *peaks* – kurz: das Klima ebenso wie das Wetter.

#### 3.2.4. Ökologische *life support systems*: Grüne Infrastruktur und das Erdsystem

Ein zentrales Feld für Maßnahmen zur Klimawandelanpassung sind Infrastrukturen. Schon die Deutsche Anpassungsstrategie (DAS) erwähnt eine Reihe möglicher Folgen des Klimawandels für die bundesdeutschen Infrastrukturen, insbesondere bei der Energieversorgung und im Verkehrswesen (Bundesregierung 2008, 33ff., 37f.). Befürchtet werden Überschwemmungen und hitzebedingte Verformung von Straßen und Schienen (UBA 2011b, 3), aber auch Probleme von Kraftwerken mit dem Kühlwasser und schwer zu regulierende Schwankungen der Produktion von Windstrom durch vermehrte Stürme (siehe: UBA 2011a, 2, 4). Gerade im Katastrophen- und Bevölkerungsschutz konzentriert man sich auf die Feststellung und Reduzierung der Verwundbarkeit Kritischer Infrastrukturen gegenüber dem Klimawandel (BMI 2009, 7, BBK 2011, 44–47).

Die Verwundbarkeit der Infrastrukturen gegenüber Folgen des Klimawandels (insbesondere im Hinblick auf Extremwetterereignisse) ist vielleicht der deutlichste Ausdruck der immer wieder beschworenen Paradoxien der Verwundbarkeit moderner, technisch-infrastruktureller Gesellschaften (BMI 2009, 8, siehe auch: Kapitel 2.5.5.): Die technische Zivilisation gefährdet mit dem Klimawandel nicht nur die Umwelt, sondern sich selbst, und zwar vermittelt über ihre sozio-technischen Strukturen – industrielle Produktion, Verkehr, Energiesysteme etc. –, die wiederum den anthropogenen Klimawandel überhaupt erst erzeugt haben.

Jenseits der Großerzählungen über die Paradoxien der »zweite Moderne« (Beck und Lau 2005) gibt die Herausforderung des Klimawandels für den Infrastrukturschutz aber auch andere Perspektiven auf diese sozio-technischen Netze und deren Verhältnis zur Natur frei. In den interdisziplinären *Social Infrastructure Studies* ist das Verhältnis von Infrastrukturen zur (natürlichen) Umwelt ein etabliertes Thema. Die Umwelt wird durch Infrastrukturen in einer ganz bestimmten Weise erschlossen und verfügbar gemacht (Edwards 2003, 188f.). Dabei wird die Natur in einer für die Moderne charakteristischen Weise hervorgebracht (als berechenbare Größe, als Ressource, als abzuwehrende oder zu regulierende Kraft, als stillschweigend vorausgesetzte Umweltbedingung), wodurch wiederum die für die »moderne Verfassung« (Latour 2008) charakteristische Trennung von Natur und Kultur in Kraft gesetzt wird (Mitchell 2002, 35, Edwards 2003, 189). Heidegger hat diesen Zusammenhang durch seine Konzepte von Gestell und Bestand auf den Begriff gebracht. Das »Gestell« als das Wesen der Technik, der Gesamtzusammenhang der wissenschaftlich-technischen Welt, »entbirgt« und »versammelt« das, was die Griechen *physis* genannt haben, als »Bestand« (Heidegger 2004, 9–40, zum Bestand insbesondere: 20f.). Ähnlich hat Thomas Park Hughes (1987, 53) in seiner Theorie groß-technischer Systeme argumentiert, dass ein technisches System immer auf eine spezifische Umwelt angewiesen ist und diese zugleich als Umwelt mit hervorbringt – etwa auf Öl als Rohstoff für die Stromproduktion. Die »Umwelt« ist in diesem Sinne ein Produkt systemischer Operationen, also der Art und Weise, wie selektiv auf die Umwelt Bezug genommen und zugegriffen wird – man denke etwa die vielfältigen Techniken zur Aufbereitung des Öls in eine verbrennbare Form, die für die Stromproduktion genutzt werden kann. Gleichzeitig wird die Infrastruktur selbst zu einer Art »zweiten«, artifiziellen Umwelt (Edwards 2003, 188f.), zu einem »socio-technical environment« (Rabinow 1995, 320).

Infrastrukturen sind deshalb nicht nur Mittel in einem »Stoffwechselprozess« mit der Natur, sondern eine spezifische Weise der Rahmung der Natur. Diese Rahmungen sind zunächst epistemisch, weil moderne Infrastrukturentwicklung stets die Kräfte der Natur in einem buchstäblichen Sinne in Rechnung stellt: der Wasserdruck, dem ein Damm standhalten muss, die Menge an Rohöl, die durch eine entsprechende Förderanlage zu Tage gefördert werden kann etc. Aber auch in einem unmittelbar-praktischen Sinn rahmt die Infrastruktur die Natur ein: sie kanalisiert Flüsse, hegt die Zirkulation von Energie in *pipelines* und Stromnetzen ein, er-

schließt den Wald als Naherholungsgebiet durch dessen Anschluss ans Straßennetz. Es ist genau diese doppelte rahmende Einhegung der Natur,<sup>159</sup> die *de facto* die Hybridisierung von Natur und Kultur intensiviert, zugleich aber auch die Grenze zwischen sozio-technischen Systemen und natürlichen Umwelten etabliert und befestigt. Wo die Straße endet, beginnt der Wald und damit die Natur. Diese scheinbar feste Grenze wird immer dann flüssig, wenn es zu einer »Überflutung« der technischen Rahmung, zum *overflow of the enframing* kommt. Im Krisenfall ragen die ansonsten eingehegten »Umweltbedingungen« in die Operationen der Infrastrukturen herein und stören sie. Im Extremfall kollabiert die »interne« Grenze zwischen Technik und Natur, zwischen Infrastruktursystem und Umwelt vollkommen. Der Dambruch verwischt die Grenzen zwischen Fluss und Hydrotechnik, die Explosion auf einer *offshore*-Ölplattform lässt die »schwarze Sonne« aus den engen Kanälen der Energieunternehmen ins Meer fließen, in die Körper von Mensch, Flora und Fauna eindringen. Klebrige Gefüge jenseits von Natur und Kultur entstehen. Spätestens jetzt werden die »Externalitäten« industrieller Produktion und infrastruktureller Zirkulation sichtbar und rufen Expert\_innen und Aktivist\_innen auf den Plan, die aber erst durch eine Reihe von epistemischen und praktischen Reinigungstechniken eine »Umwelt« identifizieren können, die sich vor der »Ölpest« und den Folgen der technischen Katastrophe schützen lässt.<sup>160</sup> »Umweltkatastrophen« sind in diesem Sinne immer auch Katastrophen der Unterscheidung von System und Umwelt. Der eingetretene Kontrollverlust lässt die gehegten Grenzen von Natürlichem und Künstlich-Technischem aufbrechen und dadurch auch die Umwelt als Außen der Systeme verschwinden. Aber in dem Maße, in dem die Umwelt als Außen verschwin-

---

159 Ich verwende den Begriff der Rahmung hier im Anschluss an die Arbeiten von Michel Callon (1998a), der sich seinerseits auf Goffmans Rahmenanalyse bezogen hat. Auch für Callon sind Rahmen sowohl kognitive Raster als auch »physical framwork[s]« (Callon 1998a, 249). Allerdings geht es mir hier – anders als Callon und Goffman – nicht nur darum, wie Interaktionen bzw. ökonomische Kalkulationen gerahmt werden, sondern wie die Natur durch Infrastrukturen eingefasst wird. In diesem Sinne schließe ich auch an Heideggers Technikphilosophie und dessen Konzept des Gestells an, das charakteristischerweise im Englischen als *enframing* übersetzt wird (Heidegger 1977, 20f.) und das das herausfordernde Erschließen der Technik bezeichnet. Callon hat anders als Heidegger den Akt der Rahmung stets zusammen mit der Möglichkeit der Überflutung der Rahmung konzipiert und damit die Aufmerksamkeit auf das gerichtet, was jeder Rahmung und technischen Erschließung entgeht.

160 Diese Abläufe hat David Bond (2013) am Fall des »BP oil spills« im Golf von Mexico analysiert.

det, wird sie gleichzeitig als eigenständiger und zu schützender Gegenstand der Regierung sichtbar,<sup>161</sup> der politische Aufmerksamkeit erheischt. »Die Sorge um die Umwelt beginnt in dem Moment, in dem es gerade *keine Umwelt mehr* gibt, jenen Realitätsbereich [...], wo man sich sorglos der Folgen des politischen, industriellen und ökonomischen Lebens entledigen konnte.« (Latour 2001a, 88, Hervorhebung im Original) Deswegen haben gerade Infrastrukturzusammenbrüche immer wieder dafür gesorgt, dass die Umwelt von einer stillen »natürlichen« Lebensgrundlage zu einem laut besprochenem Gegenstand des Sicherheitsdispositivs geworden ist.

In Zuge eines solchen Problematisch-Werdens der Umwelt kann diese offensichtlich immer weniger von der Technik und der Infrastruktur getrennt werden. Stattdessen wird in der Gegenwart immer häufiger die Hybridisierung von Natur und Infrastruktur betont, wodurch es auch zu einer neuen Artikulation von Infrastruktur kommt. Das zeigt sich in einem aufschlussreichen Beispiel aus der Klimawandelanpassung. Bevölkerungsschützer\_innen problematisieren hier unter anderem die Folgen des Klimawandels für das Wasserstraßennetz, das durch zu niedrige Wasserstände in einem trockenen Hitzesommer wie auch durch Überflutung in seiner Funktionstüchtigkeit beeinträchtigt werden kann.

»Also du hast die Wasserstraße, erstmal hast du einen Fluss. Den hast du vielleicht ausgebaut zur Wasserstraße, weil du ihn verkehrstechnisch nutzen willst und hast dann da irgendwie Befestigungen angebracht und Hafenanlagen installiert usw. Die sind aber davon abhängig, dass der Pegel einfach in einem bestimmten Bereich ist. Wenn er zu niedrig ist, funktioniert es nicht, weil man die Schiffe dann nicht mehr voll beladen kann oder gar nicht mehr fahren kann. Und wenn der zu hoch ist, ist es viel zu gefährlich, dann kannst du auch nicht mehr fahren.« (Interview 2)

Die Infrastruktur ist, wie sich hier zeigt, nicht nur auf eine bestimmte Umwelt angewiesen, sondern besteht geradezu aus dieser »Umwelt«. Sie steht der Natur nicht nur gegenüber, sondern ist selbst die Natur. Auf einen ähnlichen Sachverhalt hat der Anthropologe Ashley Carse (2012) in seiner Analyse des Zusammenhangs von Sozio-Technik und Natur des Panamakanals hingewiesen. Auch hier muss der Wasserspiegel des Kanals auf einem bestimmten Level gehalten werden, damit der Schiffsverkehr weiter möglich ist. Dafür werden immer mehr »natürliche« Gegebenheiten im Einzugsgebiet mobilisiert und so um- und ausgebaut, dass sie als Teil

---

161 Zur Umwelt als »new object of politics« und »set of forces and calculations«, also als Gegenstand, Zielscheibe und Interventionsbereich der Regierung siehe: Mitchell (2009, 420), Bond (2013).

der Kanalinfrastruktur operieren. Infrastruktur kann dann nicht mehr als Gesamtheit technischer Elemente verstanden werden, sondern verweist auf eine spezifische Art der Verknüpfung dieser Elemente. »I have argued that infrastructure is not a specific class of artifact, but a process of relationship building.« (Carse 2012, 556) Am Beispiel urbaner Wasserversorgung haben in der Humangeographie auch Matthew Gandy (2004, 2005) und Eric Swyngedouw (2006) die Konzepte des »urban metabolism« bzw. der »cyborg urbanization« entwickelt, mit denen sie die Durchdringung und Hybridisierung von Natur und Technik in infrastrukturellen Settings betonen.

Eine »hybridisierte« und relationale Sicht auf Infrastruktur prägt aber nicht nur theoretische Debatten, sondern auch jüngere Regierungsprogrammatiken. So hat die Europäische Union in den vergangenen Jahren eine Reihe von Initiativen zum Schutz und Ausbau der sogenannten Grünen Infrastruktur (GI) aufgelegt (siehe: EU 2013, 2014), die auch in Deutschland verstärkt aufgegriffen werden sollen. In diesen Initiativen werden Ökosysteme als Infrastrukturen verstanden, deren Ausbau und Schutz nicht nur Natur- und Umweltschutz, sondern auch Schutz vor den Folgen des Klimawandels und Naturkatastrophen verspricht. Der Titel einer Mitteilung der EU-Kommission aus dem Jahr 2013 an eine Reihe anderer EU-Institutionen verweist auf den Kontext, aus dem das Konzept der grünen Infrastruktur erwachsen ist: *Grüne Infrastruktur – Aufwertung des europäischen Naturkapitals* (EU 2013). Mit Konzepten wie »Naturkapital«<sup>162</sup> und dem auch in Texten zur grünen Infrastruktur immer wieder verwendeten Begriff der »Ökosystemdienstleistung« wird versucht, dem Umweltschutz einen größeren Stellenwert zu verschaffen, indem man der Natur einen ökonomischen Wert beimisst. Die Idee ist, dass Ökosysteme eine Reihe von »Diensten« erbringen – die Natur als Leistungsträger. So heißt es im genannten Bericht der EU-Kommission: »Die Nutzen der Natur (Bereitstellung von Nahrungsmitteln, Rohstoffen, sauberem Wasser und sauberer Luft, Klimaregulierung, Hochwasserschutz, Bestäubung und För-

---

162 Das Konzept des Naturkapitals wird häufig mit dem Buch *Small is Beautiful* des Ökonomen Ernst Friedrich Schumacher (2011) in Verbindung gebracht, das 1973 erschienen ist. Prominent kommt es aber auch im 1999 erschienen Buch *Natural Capitalism* (im deutschen mit Öko-Kapitalismus übersetzt) (Hawken, Lovins und Lovins 2013) vor. Die drei Autor\_innen dieser Streitschrift für *Die nächste industrielle Revolution* – so der Untertitel – sind neben Paul Hawken Amory und Hunter Lovins, die mit ihrem *Brittle Power* (Lovins und Lovins 1982) wesentlich zum Transfer des Resilienzkonzepts von der Ökologie in das Systemingenieurswesen beigetragen haben (siehe dazu: Kapitel 3.3.2.).

derung der Erholung) sind für die menschliche Gesellschaft unverzichtbar.« (EU 2013, 2) In dieser Konzeption von grüner Infrastruktur erbringt diese ganz ähnlich wie Kritische Infrastrukturen »lebenswichtige« Dienste – Luft, Wasser, Nahrungsmittel etc. Der Schutz grüner Infrastruktur erscheint hier genauso wie der Schutz Kritischer Infrastrukturen als Sicherung vitaler Systeme. Allerdings würden diese vitalen Dienste zumeist noch als Umweltbedingungen sozioökonomischer Operationen schlicht vorausgesetzt.

»Viele dieser Nutzen, häufig Ökosystemdienstleistungen genannt, werden jedoch in Anspruch genommen, als ob sie unbegrenzt vorhanden wären, und wie Gratisgeschenke behandelt, deren wirklicher Wert nicht gebührend geschätzt wird. Das kann dahin führen, dass Behörden, anstatt Probleme wie Hochwasserschutz auf natürliche Weise zu lösen, auf technische oder »graue« Infrastruktur zurückgreifen.« (EU 2013, 2)

»Grüne Infrastruktur« ist in diesem Sinne eine Kritik an der großen bzw. »grauen« Infrastruktur. Das Konzept der grünen Infrastruktur setzt an den gerade im Zusammenhang mit Bemühungen zum Schutz Kritischer Infrastrukturen sichtbar gewordenen Pathologien und Paradoxien moderner sozio-technischer Netzwerke an. Der Verweis auf den Hochwasserschutz, aus ökologischer Sicht die geradezu lehrbuchhafte Pathologie der hydraulischen Naturbeherrschung, ist gewiss kein Zufall. Grüne Infrastruktur, so die Botschaft, ist wie die Kritische Infrastrukturen in ihrer Integrität zu schützen, birgt aber anders als diese kein zusätzliches Katastrophenpotenzial, sondern wirkt vielmehr ihrerseits sichernd.

Neben Wasserversorgung, Naturschutz und Artenschutz gelten auch der Katastrophenschutz und der Beitrag zur Klimawandelanpassung als zentrale Dienstleistungen grüner Infrastrukturen. Wie im ökologischen Hochwasserschutz wird betont, dass die Renaturierung von Flussläufen, die Rückverlagerung von Deichen oder das Anlegen von Auenwäldern (EU 2013, 5) vor Überflutungen schützt und zudem noch andere »Dienste« erbringt, etwa die Filterung des Wassers (EU 2014, 7). Die grüne Infrastruktur supplementiert hier technische Vorrichtungen wie Kläranlagen, Deiche und Dämme. Auch im Küstenschutz soll die grüne Infrastruktur, hier in Form von mit »Pflanzen bestandene[n] Meereslebensräume[n]« (EU 2014, 12), ihre Dienste leisten, indem sie vor den Folgen



des Anstiegs des Meeresspiegels schützt.<sup>163</sup> Die Bepflanzung von Häusern in Stadtzentren kann den urbanen »Hitzeinseleffekt« reduzieren, der im Zuge des Klimawandels zu einem zunehmenden Problem werden könne (EU 2014, 13). Die grüne Infrastruktur wirkt hier wie eine Klimaanlage, aber ohne die damit verbundenen ökonomischen und ökologischen Kosten. Im Gegenteil: Vielfach verbessere grüne Infrastruktur nicht nur die Klimaresilienz der Gesellschaft, sondern trage gleichzeitig zum Klimaschutz bei.

Grüne Infrastruktur ist dabei nichts, was einfach vorgefunden wird. Ebenso wie die graue Infrastruktur muss sie gezielt angelegt und vernetzt werden. Denn gerade das Fortschreiten von Infrastrukturen wie Straßen- und Schienennetze hat die grüne Infrastruktur zunehmend zerrissen und fragmentiert. Europa als infrastrukturelles Integrationsprojekt (Opitz und Tellmann 2015a) erscheint aus der Perspektive grüner Infrastruktur als »zerschnittener Kontinent« (EU 2014, 5). Eine ganze Batterie von ökologischen Verbindungselementen soll die grüne Infrastruktur Europas wieder vernetzen: Fischleitern, Grüntunnel und -brücken, Trittsteine, Wildbrücken und Ökokorridore schließen Ökosysteme wieder zusammen und ermöglichen Artenwanderung (siehe: EU 2014, 8). Städtische Parks fungieren als »Frischluftschneisen« (EU 2014, 9), die das Zirkulieren der Luft ermöglichen, ähnlich wie Autobahnen den Flüssen des Straßenverkehrs Raum geben. Fernziel dieser Verbindungs- und Verknüpfungsbemühungen ist die Erzeugung eines transeuropäischen grünen Infrastrukturnetzwerkes (EU 2014, 18), das Zusammenschließen von transnationalen Naturräumen wie Flüssen, Gebirgsketten und Wäldern.

»Bislang konzentrierten sich großmaßstäbliche Infrastrukturinitiativen auf die Bereiche Verkehr, Energie und IKT. Durch die Entwicklung eines an den transeuropäischen Netzen (TEN) für die Bereiche der grauen Infrastruktur ausgerichteten gleichwertigen Instruments für grüne Infrastruktur in Europa (TEN-G) würde ein signifikanter Beitrag zur Sicherung der Resilienz und Vitalität bestimmter europäischer Ökosysteme mit Symbolcharakter geleistet« (EU 2013, 11).

Den wichtigsten Symbolcharakter hat dabei sicherlich die sogenannte *Green Belt Initiative*, die versucht, ein ökologisches Netzwerk im ehemaligen

---

163 Bruce Braun und Stephanie Wakefield haben auf ähnliche Bemühungen in New York City hingewiesen (Braun 2014, 58, Braun und Wakefield 2014b). Hier soll »oyster-tech« die Stadt klimaresilient machen. Austernriffe anstatt riesiger Sturmflutwehre sollen Überflutungen der Stadt, wie sie bei *Hurricane Sandy* eingetreten sind, eindämmen.

Grenzstreifen zwischen Ost und West vom »Barentsee zum Schwarzen Meer« (EU 2013, 11) anzulegen.

»Die Initiative will einen der unüberwindbarsten Grenzstreifen in der Geschichte der Menschheit (den Eisernen Vorhang) zu einem »grünen Band« und somit zum Symbol für Eintracht machen und durch Erhaltung und Schutz einiger der eindrucksvollsten und empfindlichsten Landschaften Europas grenzüberschreitende Zusammenarbeit gewährleisten.« (EU 2013, 11)

Plakativer lässt sich der Paradigmenwechsel von der Sicherheit souveräner Staaten (ein undurchlässiger Eiserner Vorhang und tödlicher Grenzstreifen) zur ökologischen Version der Resilienzsicherheit (ein grünes Band, das Europa vernetzt und »vitalisiert«) in der Tat kaum ausdrücken.

Solche gesamteuropäischen Pläne machen nicht zuletzt aber auch auf eine Transformation innerhalb des ökologischen Denkens aufmerksam. In Anspielung auf das Buch *Small is Beautiful* des Ökonomen Ernst Friedrich Schumacher (2011) heißt es in einer Broschüre der EU zur grünen Infrastruktur: »Klein ist schön, aber groß ist besser.« (EU 2014, 9) Die ökologische Kritik der Gegenwart richtet sich in der Tat nicht mehr gegen die Megalomanie großtechnischer Systeme und technokratischer Projekte, sondern gegen deren Paradoxien und Ineffizienz. Nicht die »große«, sondern die »graue« Infrastruktur dient deshalb begrifflich als Abgrenzungsfolie für die ökologische Kritik. Ökologen denken und planen heute ebenfalls groß. Nicht *small is beautiful* sondern *think big* scheint zu ihrer Lösung geworden zu sein. Das nationale Territorium und selbst die transnationalen Netzwerke Europas lassen sie hinter sich. Ihr Maßstab ist der Planet. Der ultimative Horizont des ökologischen Sicherheitsdenkens ist das »Erdsystem«, welches das menschliche Leben erhält und ermöglicht, aber zugleich durch menschliches Handeln gefährdet ist.

Die Erforschung des Erdsystems, also des gesamten Planeten als selbstregulierendes System (*gaia*, wie es bei James Lovelock (2009) heißt), geht auf eine Reihe von wissenschaftlichen Projekten zurück, die – wie es Hans-Joachim Schellnhuber (1999) in einem programmatischen Artikel für die Zeitschrift *Nature* ausdrückte – eine zweite kopernikanische Revolution ausgelöst haben. Die Erde wird jetzt als Makrosystem mit einer Reihe interagierender und interdependenter Untersysteme (Biosphäre, Atmosphäre, Kryosphäre etc.) verstanden und nicht mehr nur als beliebiger Planet im Sonnensystem. Diese Systeme, die sich unter normalen Bedingungen wechselseitig regulieren, sind die Bedingung für (nicht nur) menschliches Leben auf dem Planeten (Lovelock 2000). Die unterschiedlichen Erdsphä-

ren – insbesondere Atmosphäre und Biosphäre (Lovelock und Margulis 1974) – stehen in geradezu symbiotischen Beziehungen zueinander und bilden so zusammengenommen einen »symbiotic planet« (Margulis 1999). Gleichzeitig werden sie vom menschlichen Wirken ebenso nachhaltig wie schädlich beeinflusst. Schon Schellnhuber (1999, C22) hat den menschlichen Faktor, den er als »prometheus« bezeichnet, als Gegenspieler von Lovelocks *gaia* ins Spiel gebracht. Wenig später hat Crutzen (2002) diese Problematisierung in seinem Aufsatz *The Geology of Mankind* noch zugespitzt. Seit Einführung der Dampfmaschine sei der Mensch zum wichtigsten geologischen Faktor des Erdsystems geworden, weshalb die aktuelle erdgeschichtliche Epoche seinen Namen tragen müsse: – Anthropozän. Gerade in dem Moment, in dem der Mensch sich die Erde so vollständig angeeignet hat, ist er existenziell bedroht von den Schäden, die er der Erde zugefügt hat.<sup>164</sup> Die Erde kommt dadurch nicht mehr nur als ausbeutbare und zu beherrschende Natur, sondern als Grundlage des Lebens und zu schützendes Objekt in den Blick: als »planetary life support system« (Young und Steffen 2009).

Im Vordergrund der Erdsystemforschung stehen die Bereiche der Erde, die eine vitale Bedeutung für die Integrität des Erdsystems und die mit diesem aufs Engste verbundene Menschheit haben. Das Potsdam Institut für Klimafolgenforschung (PIK) unter Leitung von Schellnhuber hat dabei in jüngerer Zeit Analysen zu sogenannten *tipping elements*, also Kippelementen im Klimasystem, durchgeführt (Lenton et al. 2008). Die Theorie der Kippelemente schließt an die Theorie der *tipping points* an, nach der ein System an einem bestimmten Punkt plötzlich und irreversibel umkippen kann. Ist ein Schwellenwert überschritten, stellen sich Rückkopplungseffekte ein, die im System einen raschen und irreversiblen Schaden auslösen. Einer dieser teuflischen *feedback*-Prozesse ist die sogenannte Eis-Albedo-Rückkopplung. Sobald eine größere Eisfläche durch die Überschreitung eines bestimmten Temperaturschwellenwerts abgeschmolzen ist und eine darunter liegende Felsformation freigibt, wird weniger Licht reflektiert. Das intensiviert wiederum das Abschmelzen des Eises. Kippele-

---

164 Zur breiten Diskussion um das Anthropozän in den Sozialwissenschaften siehe unter anderem: Chakrabarty (2009), Malm und Hornborg (2014), Haraway (2015). Zumeist wird das Anthropozän dabei als neue Epochenbeschreibung verstanden, das ein neues Verhältnis von Mensch und Natur andeutet. Nur selten wird der Einsatz des Anthropozän-Motivs in Politiken der Sicherheit diskutiert (Dalby 2017).

mente bezeichnen dabei die Systeme, bei denen solche Umschlagsprozesse drohen und die insofern besonders verwundbar sind.

»Kippelemente sind Bestandteile des Erdsystems von überregionaler Größe, die schon durch kleine externe Störungen in einen neuen Zustand versetzt werden können. Diesem Verhalten liegen selbstverstärkende Prozesse zugrunde, die einmal angestoßen auch ohne weiteren externen Einfluss weiterlaufen. Der Übergang nach dem Überschreiten eines systemspezifischen Kippunktes erfolgt in der Regel sprunghaft und ist häufig unumkehrbar. Seine Umweltauswirkungen sind weitreichend und könnten die Lebensgrundlagen vieler Millionen Menschen gefährden.« (PIK 2016)

Die Kippelemente werden in drei Gruppen unterteilt: Eiskörper, Strömungssysteme (Muster der Windzirkulation und Meeresströmungen von beachtlicher Konstanz und Reichweite) sowie Ökosysteme (Wälder, Korallenriffe). Dabei gibt es eine Reihe von Abhängigkeiten und Wechselwirkungen zwischen diesen Systemen. So könnte das Abschmelzen von Dauerfrostböden in Sibirien zur Freisetzung riesiger gefrorener Kohlendioxid-speicher führen, was das Klima zusätzlich belasten würde. Das Umkippen der Regenwälder und der nördlichen Borealwälder hätte wiederum den Effekt, dass weniger Treibhausgase absorbiert werden könnten. Jeweils wären eine schnellere Klimaerwärmung, die Überschreitung weiterer Schwellenwerte und die Gefährdung weiterer Kippelemente die Folge. Die Kippelemente bilden also ein fragiles, interdependentes Netzwerk und werden deshalb auch als »Achillesfersen« des Erdsystems bezeichnet (PIK 2016). Sie bilden gleichsam die Kritische Infrastruktur des Erdsystems und sind ihrerseits das ultimative *system of systems*, die generelle Umwelt, in die alle sozio-technischen »vitalen Systemen« eingebettet sind.

Auf der Ebene des Sicherheitsdispositivs der Resilienz wird somit eine erweiterte Gesamtökologie vitaler Systeme etabliert, die nicht nur aus einem verwobenen Netz Kritischer Infrastrukturen besteht, sondern ebenso aus einem planetarischen Gefüge zusammenhängender Erdsysteme. Damit erreicht die Verschränkung von Techno- und Biosphäre in der Biopolitik vitaler Systeme ihren vorläufigen Höhepunkt. Die Ökosphäre kann immer weniger als Externalität und Störquelle in die technische Systemumwelt abgeschoben werden, sondern durchdringt und ermöglicht die Technosphäre und das Leben der Bevölkerung. Die Gefährdung der natürlichen Lebensgrundlagen hat so die vitalen Ökosysteme – grüne Infrastrukturen und *planetary life support systems* – zum Gegenstand des Sicherheitsdispositivs werden lassen.

### 3.3. Energiesicherheit: Vom Atomstaat zur Energiewende

In den vorangegangenen beiden Abschnitten habe ich die Etablierung und schrittweise Erweiterung der Biopolitik vitaler Systeme skizziert. Zunächst gerieten sozio-technische Infrastruktursysteme in den Fokus staatlicher Sicherheitsbemühungen; bereits seit Mitte des 20. Jahrhunderts im Rahmen der Daseinsvorsorge und dann – am Beginn des 21. Jahrhunderts – in den Strategien zum Schutz Kritischer Infrastrukturen (3.1.). Kritik an den Pathologien hoch-moderner Infrastrukturentwicklung genauso wie die verstärkte Sensibilität für Themen des Umwelt- und Naturschutzes haben etwa seit den 1970er Jahren dazu beigetragen, dass auch Ökosysteme zu einem Schutzobjekt im Sicherheitsdispositiv der Resilienz geworden sind (3.2.). Techno- und Biosphäre verschränken sich dabei auf immer intrikaktere Weise. Diese Verschränkungen führen keineswegs stets zu symbiotischen Koexistenzen, sondern auch zu konfligierenden Ansprüchen an Sicherheit, etwa von technischer Versorgungssicherheit und Umweltschutz, bisweilen auch von Klima- und Naturschutz. Nirgendwo werden diese Verschränkungen und Konflikte sichtbarer als in den vielfältigen Sicherheitsprojekten, die sich um das Themenfeld Energie gebildet haben. In diesen geht es um die Sicherung von Infrastrukturen ebenso wie um Klimaschutz, um geopolitische Sicherheitserwägungen ebenso wie um die Sicherung von Mensch und Umwelt vor den Risiken großtechnischer Energiesysteme.

Das Problem der Energiesicherheit ist allein deshalb schon so komplex, weil es sich historisch immer wieder verschoben hat. Schon seit Beginn des Jahrhunderts wurde sowohl in sozialpolitischen wie militärischen Kontexten die Abhängigkeit der Gesellschaft von verfügbaren Energiequellen problematisiert. Die energetische Versorgungssicherheit ist damit zur Kernaufgabe des staatlichen Infrastrukturschutzes geworden. Seit Anfang der 1970er Jahre hat dann die Ölkrise sowie die Veröffentlichung des Berichts des Club of Rome zu den *Grenzen des Wachstums* (Meadows et al. 1972) eine Erweiterung des Problemfeldes der Energiesicherheit bewirkt. Zum einen erschien die Energieversorgung plötzlich von geopolitischen Risikofaktoren bedroht. Die westlichen Industrienationen sahen sich abhängig von der instabilen politischen Situation der Ölförderstaaten im Nahen Osten. Zum anderen wurde die Begrenztheit fossiler Brennstoffe und damit die Knappheit der Umwelt als Ressource sichtbar (siehe zu beiden Aspekten: Mitchell 2011). In den 1980ern haben dann schwere

Katastrophen wie der Unfall im Kernkraftwerk Three Miles Island (Perrow 1987, 33–94), der GAU in Tschernobyl (Beck 1986, 7–11, Petryna 2002) und die Ölpest durch die gesunkene Exxon Valdez (Clarke 1999, Bond 2013) eine neue Sicherheitsproblematik der Energieversorgung zum Vorschein gebracht. Nicht unter dem Vorzeichen der Knappheit wie in den 1970er Jahren (Mitchell 2009, 418ff.), sondern unter dem der Verwundbarkeit ist die »Umwelt« dadurch zum Gegenstand von Sicherheitstechnologien geworden (Bond 2013, 697). Gegenwärtig rückt in den alten Industrienationen des Westens die Erderwärmung als gravierendste Folgeerscheinung der Energieversorgung in den Fokus der Aufmerksamkeit (siehe etwa: Urry 2011, 48–65, Urry und Tyfield 2014), während in den sich ökonomisch rapide entwickelnden sogenannten Schwellenländern – allen voran in China – die Gesundheitsbeeinträchtigung der Bevölkerung durch die karbonbefeuerte Industrialisierung weiterhin oben auf der Agenda steht (Choy 2011). Seit der Energiewende ist hierzulande zudem das alte Problem der Versorgungssicherheit in neuem Gewand auf die politische Agenda getreten. So werden gegenwärtig verstärkt Fragen rund um die Sicherheit der Strominfrastruktur thematisiert, die durch die Energiewende neuen Belastungen ausgesetzt ist.

In diesem Kapitel möchte ich anhand exemplarischer Themen, Autor\_innen und Problematisierungen die vielfältigen Brennpunkte der Energiesicherheit seit den 1970ern schlaglichtartig beleuchten. Jede Artikulation der Energiesicherheit setzt Rahmungen voraus, die eine Risikoselektion vornehmen (Douglas und Wildavsky 1982) und es erlauben, auf eine Reihe spezifischer Sicherheitsprobleme und Risiken zu fokussieren: etwa geopolitische Instabilitäten, Kernkrafttrisiken, Erderwärmung etc. Diese Rahmungen gehen aus Risikoprognostiken und politischen Erwartungen hervor, sie materialisieren sich aber auch in unterschiedlichen Designs des Energiesystems und bilden so die »physical frameworks« (Callon 1998a, 249) der Energiesicherheit. Die Sichtbarmachung der Externalitäten dieser Rahmungen ist eine immer wieder zu beobachtende Strategie der Kritik an vorherrschenden Strategien der Sicherheit. Derartige Problematisierungen haben immer wieder zu einer historischen Verschiebung sicherheitspolitischer Aufmerksamkeitsfoki beigetragen.<sup>165</sup> In der Folge sind neue

---

165 Hier zeigt sich die Bedeutung der »temporal dimension of the frame«, die Judith Butler (2009, 10) betont hat: »[T]he »frame« does not quite contain what it conveys [...] does not hold anything together in one place, but itself becomes a kind of perpetual breakage,

Technologien der Energieversorgung ebenso wie der Sicherheit entstanden, die dann ihrerseits zu Gegenständen neuer Problematisierungen geworden sind.

Um diese Dynamiken zu analysieren, werde ich im Folgenden zunächst auf die Kritik am sogenannten »Atomstaat« eingehen, die Ende der 1970er Jahre insbesondere mit Robert Jungks gleichnamigem Buch aufkam und die nicht nur vor den Risiken der Atomkraft warnte, sondern auch vor den Risiken einer neuen Atommacht, die gleichsam aus der »Kernschmelze« von Staat, Ökonomie, Wissenschaft und Großtechnik entstanden war (3.3.1.). Sodann werde ich auf die ebenfalls Ende der 1970er und Anfang der 1980er diskutierten Alternativen zum Atomstaat eingehen. Amory Lovins und Hunter Lovins schlugen als Reaktion auf die Ölkrise der 1970er Jahre einen sanften Energiepfad vor, der nicht nur eine umweltschonendere und nachhaltigere, sondern vor allem auch sichere und resiliente Energieversorgung in Aussicht stellte. Nicht zuletzt durch ihre Intervention ist das Konzept der Resilienz von der Systemökologie in den Bereich der technischen Systemplanung migriert (3.3.2.). Von diesem historischen Ausflug aus erfolgt der Übergang in die energiepolitische Gegenwart. Der Fukushima-Schock hat in Deutschland den Atomausstieg beschleunigt und die Energiewende forciert. Energiewende und Atomausstieg haben aber auch neue Sorgen um vornehmlich netzbedingt-systemische Probleme der Versorgungssicherheit erzeugt (3.3.3.). Die eigentliche Katastrophe der Versorgungssicherheit besteht in der Gefahr eines großflächigen und langanhaltenden Stromausfalls, die Politiken zum Bevölkerungsschutz und zum Schutz Kritischer Infrastruktur in Atem hält (3.3.4.). Schließlich gehe ich auf Strategien ein, diese mögliche Katastrophe abzuwenden, indem Resilienz gleichsam ins Stromsystem eingebaut wird (3.3.5.).

---

subject to a temporal logic by which it moves from place to place. [...] What is taken for granted in one instance becomes thematized critically or even incredulously in another.«

### 3.3.1. Der nukleare Notstand: Der Atomstaat als Sicherheitsrisiko

»Die verstärkte Ausbreitung der Kernkraftanlagen muß die Gesellschaft zum Autoritarismus führen. Tatsächlich ist das feste Vertrauen auf die Kernkraft als Hauptenergiequelle nur in einem totalitären Staat möglich.« (Hayes 1979, 86)

»Ich glaube hier haben wir den reinsten, abgeklärtesten Ausdruck einer Staatsphobie [...]. Der Staat und das Atom, eher noch das Atom als der Staat oder der Staat, der nicht besser ist als das Atom, oder der Staat, der das Atom mit sich bringt, oder das Atom, das auf den Staat verweist und ihn notwendigerweise erfordert.« (Foucault 2006, 112 - Vorlesung aus dem Jahr 1979)

Als der Deutsche Bundestag am 30. Juni 2011 – zum zweiten Mal und nunmehr endgültig – mit großer Mehrheit für den Ausstieg aus der Atomenergie votierte, konnte man sich kaum noch vorstellen, wie sehr die Auseinandersetzung über die »zivile Nutzung« der Atomkraft die alte Bundesrepublik einmal gespalten hatte. Mittlerweile herrscht in Deutschland ein erstaunlich einmütiger »Atomkonsens«. Die deutliche Mehrheit im Bundestag wurde von einer breiten Zustimmung für diesen Schritt in der Bevölkerung getragen. Vor dem Hintergrund des GAUs im japanischen Atomkraftwerk von Fukushima nur einige Monate vor der Bundestagsabstimmung konnte der Ausstieg als staatliche Vorsorgemaßnahme angesehen werden, welche die Bürger vor einer niemals gänzlich kontrollierbaren Energie- und Gefahrenquelle schützt.

Dieses Bild vom schützenden Staat hat eine Sichtweise vergessen lassen, die Ende der 1970er Jahre die massiven Auseinandersetzungen zwischen Atomkraftgegner\_innen und –befürworter\_innen befeuerte: die Kritik am Atomstaat. Hier wurde der Staat nicht als Schutzmacht gegen die Gefahren der Atomtechnologie verstanden. Vielmehr wurde im Staat ein Schutzpatron der Atomenergie gesehen.<sup>166</sup> Schließlich hatten staatlich protegierte Forschung, Subventionen und nicht zuletzt staatliche Versicherungen für die Folgekosten eines Unfalls die Nutzung der Atomenergie überhaupt erst möglich gemacht. Zudem wurden gerade die von sehr wenigen Personen an der Spitze des Staates kontrollierten Atombomben als Zeichen der Machtlosigkeit der Bevölkerung gegenüber einer technisch hochgerüsteten Staatsmacht gedeutet. In der Atombombe schienen sich

---

<sup>166</sup> In anderen Ländern wird und wurde das Verhältnis von Staat und Atom freilich stets ganz anders gesehen. Das gilt gerade für den Atomstaat Frankreich. Siehe dazu: Hecht (2009).



die von der Technowissenschaft nutzbar gemachten extremen Kräfte der Materie mit der äußersten (Tötungs)Macht souveräner Staaten zu verbinden. Dadurch, dass er sich die Macht der Materie gefügig gemacht hatte, konnte der Atomstaat also zugleich seine politische Machtfülle enorm steigern.

Eine ganze Reihe von Büchern und Artikeln (Augstein 1977, Lovins 1978, Hayes 1979) – ganz zu schweigen von unzähligen Flugblättern und politischen Streitschriften – thematisierte seit spätestens Ende der 1970er Jahre diese neue historische Gestalt einer Macht, in der sich Wissenschaft und Technik, Technik und Politik, Politik und Ökonomie zu einer einzigen höchstgefährlichen kritischen Masse zusammengeschlossen hatten. Es war vor allem das 1977 erschienene Buch *Der Atomstaat. Vom Fortschritt in die Unmenschlichkeit* des österreichischen Wissenschaftsjournalisten Jungk (1977), das diese neue Figur auf den Begriff brachte und in der deutschsprachigen Öffentlichkeit verankerte.

Robert Jungk wurde 1913 in Berlin geboren. Als Jude und engagierter Kommunist musste er nach der Machtergreifung der Nazis 1933 emigrieren.<sup>167</sup> Nach dem Krieg arbeitete Jungk als Wissenschaftsjournalist und beschäftigte sich in mehreren Publikationen mit der Entwicklung und den Konsequenzen der modernen Atomphysik. In seinem Buch zum Atomstaat klärt Jungk in aller Gründlichkeit über sämtliche Gefahren der Nukleartechnik auf. Er weist auf die Gesundheitsgefahren für Arbeiter\_innen in Atomkraftwerken hin, die sich selber als »Strahlenfutter« beschreiben (Jungk 1977, 1–40). Er geht auf die Gefahren für die Umwelt in der Nähe von Atomkraftwerken ein (Jungk 1977, 22–29). Er beschreibt die Problematik des Atommülls, der für Jahrtausende sicher gelagert werden muss. Er berichtet ausführlich über die Risiken der Proliferation von Atomwaffen (Jungk 1977, 132–181). Und natürlich widmet er viele Seiten der Darstellung tatsächlich eingetretenen Störfällen in Atomkraftwerken und warnt eindringlich vor der Möglichkeit des 1977 noch nicht eingetretenen GAUs, des größten anzunehmenden Unfalls.

Die Kritik des Atomstaats erschöpft sich jedoch nicht in der Aufzählung von Sicherheitsrisiken. Es sind gerade die Risiken der

---

<sup>167</sup> Dieser biographische Umstand ist relevant, weil es einen Zusammenhang von Exilerfahrung und dem Misstrauen gegenüber der Staatsmacht zu geben scheint: »Nun, ich glaube, daß das politische Exil, das politische Dissidententum des 20. Jahrhunderts seinerseits eine beträchtliche Kraft für die Verbreitung dessen war, was man den Antietatismus oder die Staatsphobie nennen könnte.« (Foucault 2006, 113)

Sicherungsbemühungen selbst, also die Nebeneffekte der staatlich-wissenschaftlich-industriellen Versuche zur Kontrolle der Kräfte des Atoms, die Jungk umtreiben. Damit trägt er der Tatsache Rechnung, dass die Risiken der Nukleartechnik auch von ihren Protegées keineswegs unbeachtet geblieben sind. Vermutlich hat keine technologische Entwicklung zuvor je so umfassende Sicherheitsbemühungen angeregt. Schließlich beruht sie darauf, eine ebenso potente wie potenziell gefährliche Naturkraft auf kontrollierte Weise zu entfesseln. Sicherheit gehört geradezu zum Wesen der Atomtechnik und folglich zum Wesen einer Epoche, die sich selbst als Atomzeitalter beschrieben hat.<sup>168</sup> Aber – und hier setzt Jungks Kritik ein – die neuen Sicherheitsmaßnahmen können die Risiken der Atomkraft nicht nur nicht vollkommen ausschalten, sie erzeugen eigenständige Risiken. Denn die Sicherheitstechnologien des Atomstaats verdoppeln gleichsam die Risiken der Nukleartechnologie, indem sie empfindlich in die bürgerlichen Freiheiten der Bevölkerung eingreifen. Allzu oft verkehren sich auf fatale Weise die Prioritäten der Sicherheitspolitik. »Der Schutz der Atomanlagen vor den Bürgern ist den Atombetreibern mindestens so wichtig wie der Schutz der Bürger vor den Atomanlagen.« (Jungk 1977, 87)

Betroffen davon sind zunächst die Akteure des Atomregimes selbst. Im Atomzeitalter sind Wissenschaftler\_innen Teil einer unübersichtlichen Großorganisation geworden, innerhalb derer sie nur ein Zahnrad sind. Gleichzeitig werden Forscher\_innen immer mehr überwacht, weil man fürchtet, dass sie Erkenntnisse der Forschung missbrauchen oder an politische Feinde – Terroristen oder die andere Partei im Kalten Krieg – weitergeben könnten. Dadurch hat sich ein »Kasernenstil« (Jungk 1977, 124) in der Atomforschung eingespielt, der mit dem klassischen Ideal »freier Forschung« wenig gemeinsam hat. Die Mächtigkeit der Wissenschaft steigt also, insofern ihr technisches Wissen unmittelbar zur Ausübung und Legitimation politischer Herrschaft beiträgt. Gleichzeitig schwindet die

---

168 Heidegger hat in *Der Satz vom Grund* in der Intensivierung von technischen Sicherheitsmechanismen ein geradezu metaphysisches Charakteristikum des Atomzeitalters gesehen: »Durch die Freisetzung der riesenhaften Atomenergien wird jetzt [...] die Forschung ihr ganzes Absehen in einem neuen Stil darauf richten, die freigesetzten Naturenergien zu bändigen. Was heißt dies? Es heißt: die Nutzbarkeit der Atomenergie und dem zuvor ihre Berechenbarkeit auf eine Weise sicherstellen, daß diese Sicherstellung ihrerseits ständig das Einschalten neuer Sicherungen herausfordert.« (Heidegger 1957, 202)

kritische, reflexive und aufklärerische Macht und Autonomie einzelner Wissenschaftler\_innen.

Den Arbeiter\_innen in Atomkraftwerken ergeht es nicht besser. Sie werden ebenfalls unter ein Kontrollregime gestellt, das mit Rekurs auf Sicherheitsanforderungen und Sachzwängen der Atomtechnologie gerechtfertigt wird. Sie werden nicht nur auf politische Gesinnung und psychische Eignung überprüft. Auch ihre Rechte in Arbeitskämpfen, vor allem das Streikrecht, wird beschnitten (Jungk 1977, 20ff.): »Alle Räder stehen still, wenn dein starker Arm es will, gelte in der Atomindustrie nicht mehr. Radioaktive Spaltungsprozesse stehen niemals still. Man muß sie über Jahre, Jahrzehnte, Jahrtausende hinweg überwachen.« (Jungk 1977, 22) Weil gerade vom »menschlichen Faktor« (Jungk 1977, 84) bzw. von der »liveware« (Jungk 1977, 78) Störpotenziale in Kernkraftwerken ausgehen, entwickeln sich mit dem »Fortschritt« der Atomtechnik neue Psycho- und Sozialtechniken, die versuchen, einen neuen Menschentypus heranzuziehen, den Jungk (1977, 72) »homo atomicus« nennt. Solche Bestrebungen zur Erzeugung von »homo atomici« betreffen auch die Öffentlichkeit, die mit immer repressiveren Maßnahmen davon abgehalten werden soll, sich der Atomkraft zu widersetzen. Die Notwendigkeit, dauerhaft die Sicherheit von Atomanlagen und den Schutz vor deren gefährlich strahlenden Hinterlassenschaften zu gewährleisten, tendiert zudem zur Konservierung politischer Verhältnisse. Atomenergie macht den »starken Staat in Permanenz« (Jungk 1977, XVI) oder zumindest eine »technische Priesterkaste« zur Bewachung langlebiger atomarer Abfälle« (Lovins 1978, 257)<sup>169</sup> notwendig und verdoppelt damit die »Zukunftskatastrophe« der Atomenergie durch eine Versiegelung des politischen Erwartungshorizonts: entweder Apokalypse oder Atomstaat.

Die bedrohlichste Resonanz zwischen Sicherheitsrisiken und Risiken der Sicherheit befürchtet Jungk bei atomaren Unfällen aller Art, die schnell einen sowohl technischen wie auch politischen Ausnahmezustand, einen nuklearen Notstand hervorrufen.

»Jeder nukleare Zwischenfall wird – so sehen das die heute in den Kernenergie-Staaten bereits ausgearbeiteten Pläne vor – eine Mobilmachung von Polizeieinhei-

---

169 Die Idee zu dieser »technischen Priesterkaste« stammt vom Nuklearphysiker Alvin Weinberg und wurde von Gegner\_innen der Atomkraft immer wieder als Beleg für den Zynismus und das technokratische Ethos der Atomindustrie angeführt (siehe: Lovins 1978, 257).

ten und Streitkräften in einem Umfang nach sich ziehen, wie sie bisher nur in revolutionären Situationen angeordnet wurde.« (Jungk 1977, 174)

Das Umkippen von einem Rechtsstaat in einen Atomstaat droht hierbei nicht nur ein temporäres Ausnahmeereignis zu bleiben, sondern zu einem Dauerzustand zu werden. »Atomindustrie – das bedeutet permanenten Notstand unter Berufung auf permanente Bedrohung.« (Jungk 1977, 196)

Der drohende nukleare Unfall zeitigt noch bevor er eingetreten ist einen sozialen Kollateralschaden. »Die inzwischen recht zahlreichen Studien über den GAU (größter annehmbarer Unfall) lassen außer acht, daß sich ein »GAGU« (größter annehmbarer gesellschaftlicher Unfall) vorbereitet, den der Druck des »Atomstaates« nicht verhindert, sondern täglich fördert.« (Jungk 1977, 200) Die Atomstaatskritik argumentiert also, dass die immensen Risiken, die durch die Weckung der Kräfte des Atoms entstehen, nur dann halbwegs in den Griff zu kriegen sind, wenn ein totalitäres Sicherheitsregime ins Werk gesetzt wird. Entweder wird die Bevölkerung den Risiken der Atomkraft ausgesetzt oder denen des Atomstaats – im schlimmsten Fall beiden.

Aber worin besteht der Ausweg aus dieser düsteren Zukunft? Für Jungk zeigten sich vielversprechende Ansätze vor allem in dem neuen Stil der Bewegungen gegen den Atomstaat. Die Anti-AKW-Bewegung konfrontierte die Übermacht von Staat und Atom, von Technowissenschaft und formierten Wirtschaftsinteressen, nämlich nicht einfach mit einer Gegenmacht, sondern mit einer alternativen Macht. Die Alternativbewegungen »kommen ohne zentrale Führung [...] aus. Nicht der »monolithische Block« symbolisiert ihren Zusammenhalt, sondern der Strom, der viele Quellen in sich aufnimmt und Hindernisse umfließt, auswäscht, überflutet« (Jungk 1977, 202). »Ein ständiger Energiestrom, aus vielen Köpfen und Herzen [...]: Menschliche Schöpferkraft statt Atomkraft.« (Jungk 1977, 209) Wenn Jungk hier eine zentrale gegen eine dezentrale, eine harte gegen eine sanfte Macht stellt, dann bezieht er sich dabei explizit auch auf Amory B. Lovins (1978) Konzept des »sanften Energiepfades« (siehe: Jungk 1977, XII-XIV, 201–211). Lovins ist ein US-amerikanischer Physiker und Umweltaktivist, der Ende der 1970er Jahre durch Publikationen auf sich aufmerksam machte, in denen er sein Konzept eines »sanften Energiepfades« entwarf. Dadurch wurde Lovins zum Stichwortgeber von Umweltaktivist\_innen ebenso wie für die entstehende ökologisch-alternative Wissen-

schaftsszene.<sup>170</sup> Diese Prominenz verdankt sich wohl nicht zuletzt seiner Fähigkeit, die Energiekrise westlicher Industriestaaten scharf zu analysieren und gleichzeitig ein alternatives Energiesystem zu entwerfen, das einen emanzipatorischen Mehrwert in Aussicht stellte. Der Pfad der sanften Energie war für Lovins zugleich ein Pfad zu einer sanfteren Gesellschaft.

Lovins hat aber nicht nur an eine Gegenöffentlichkeit appelliert, sondern ebenso an Entscheidungsträger\_innen in der Regierung. Er hat seine Interventionen stets so platziert, dass sie als Reaktionen auf vorangegangene Krisensituationen verstanden werden konnten. So veröffentlichte er 1977 kurz nach einem langanhaltenden Stromausfall in New York City einen Artikel in der *New York Times* zu *Resilience in Energy Strategy* (Lovins 1977). Schlagartig bekannt wurde er vor allem durch einen Artikel in der renommierten Zeitschrift für Internationale Politik *Foreign Affairs*, in dem er die Energiestrategie der US-Regierung als Folge der Ölkrise kritisierte (Lovins 1976) und der später einen Teil seines 1977 auf Englisch und bereits ein Jahr später auf Deutsch erscheinenden Buches »Sanfte Energie« bilden sollte (Lovins 1978, 62–116). Das »Energieproblem« (Lovins 1978, 33), das im Zuge der Ölkrise von 1973 aufgetreten war, bestehe nicht nur in der Abhängigkeit westlicher Industriestaaten von Ölimporten aus geopolitisch instabilen Weltregionen, sondern habe zudem etliche Strukturprobleme des Energiesystems sichtbar werden lassen (Lovins 1978, 34). Die Reaktion der USA auf diese Krise – verstärkter Einsatz heimischer Kohle, Erschließung von Öl- und Gasvorkommen in der Arktis und *offshore* sowie die Forcierung der Kernenergie – verschlimmere diese Strukturprobleme nur noch weiter (Lovins 1978, 63). Dieser harte Energiepfad sei auch ökonomisch ineffizient, weil er Energieträger einsetze, die einen sehr hohen Einsatz von Kapital benötigen (Lovins 1978, 63) und zugleich nur wenig rentabel sind, weil ein Großteil der hier eingesetzten Primärenergie bei der Verstromung verloren geht (Lovins 1978, 83). Zudem identifiziert Lovins ähnlich wie Jungk eine Reihe von sozio-politischen Nebenwirkungen des harten Energiewegs.<sup>171</sup> Demgegenüber positioniert er den sanften

170 Jungk war dabei einer der ersten, der Lovins Thesen auch in Deutschland in einer breiteren Öffentlichkeit bekannt machte. Aber auch die ungemein einflussreiche Studie *Energiewende. Wachstum und Wohlstand ohne Erdöl und Uran* des Freiburger Öko-Instituts bezieht sich ausgiebig auf Lovins' Unterscheidung von hartem und sanften Energiepfad (Krause, Bossel und Müller-Reißmann 1980).

171 Dabei beschränkt Lovins seine Kritik nicht auf die Atomkraft, sondern adressiert das gesamte Energiesystem, das auf fossilen und atomaren Energieträgern, zentralen Großkraftwerken, riesigen Infrastrukturnetzen und extensivem privaten und kommerziellen

Energiepfad als alternative »technische [...] und soziopolitische [...] Struktur des Energiesystems«, die »anpassungsfähig, geschmeidig, dauerhaft und sozial verträglich« (Lovins 1978, 82) ist. Sanfte Energien sind erneuerbare Energien aus Wind, Wasser und Sonne. Es sind aber nicht nur die Energieträger, die den sanften vom harten Weg unterscheiden. Vielmehr versammelt sich um die neuen Energien ein ganz anderes Energiesystem, das nicht mehr auf zentraler Energieextraktion, -produktion und -distribution über riesige integrierte Infrastruktursysteme sowie auf extensiver Konsumption basiert. Vielmehr soll die Energie lokal und dezentral produziert und an Abnehmer\_innen verteilt werden, die für einen möglichst effizienten Einsatz der Energie ausgerüstet sind. Diese dezentrale Struktur des Energiesystems ermöglicht zugleich größere lokale Autonomie und den Machtverlust einer technokratischen Zentralregierung. Eine veränderte Energiepolitik kann damit zum »Katalysator« für einen umfassenden gesellschaftlichen und kulturellen Wandel werden (Lovins 1978, 113).

Lovins' alternative Energie- und Gesellschaftsvision ist dabei keineswegs revolutionär. Ihm geht es nicht um einen Bruch mit dem Kapitalismus, sondern um die Rückbesinnung auf die klassisch liberalen Werte lokaler Autonomie und der Marktkonkurrenz zwischen diversen Akteuren »auf Augenhöhe«. Seine Kritik richtet sich, ganz im Sinne der (neo)liberalen Kritik am Zuviel-Regieren und an den Anmaßungen epistemischer Souveränität, gegen den Machtzuwachs der Zentralregierung, gegen Monopolbildung und Expertokratie. Deshalb hatte Lovins innerhalb der linksradikalen Anti-AKW-Bewegung auch eine Reihe von Gegner\_innen. So machte etwa Herbert Kitschelt 1984 auf den marktkapitalistischen Bias von Lovins' Argumentation aufmerksam und forderte dazu auf, »dass aufgeklärte Teilnehmer des ökologischen Diskurses aufhören, Lovins zu zitieren« (zitiert nach: Radkau 2011, 458). Lovins' liberale politi-

---

Energieverbrauch basiert. Die Wirkungen dieses Energiesystems auf die »Gesellschaftsstruktur« fasst er an einer Stelle seines Buches folgendermaßen zusammen: »[E]s wurde gesagt, daß der harte Weg eine stark interventionistische zentrale Steuerung erfordert, an herkömmlichen Marktmechanismen vorbeigeht, politische und wirtschaftliche Macht konzentriert, Urbanisierung fördert, [...] Bürokratisierung und Entfremdung verstärkt, [...] in ungleicher Weise Kosten von Nutzen trennt, die Störanfälligkeit des sozialen Systems sowie das Auftreten paramilitärischer Strukturen im Zivilleben vergrößert, bedeutende wirtschaftliche und gesellschaftliche Gefahren heraufbeschwört, gegenwärtige bestehende Tendenzen in Hinsicht auf zentralisierte politische Macht verstärkt, den Untergang föderalistischer Strukturen beschleunigt und eine elitäre Technokratie nährt – sogar erfordert –, deren Handeln die Legitimität demokratischer Regierungsformen aushöhlt.« (Lovins 1978, 245)

sche Vision schien in vielerlei Hinsicht dennoch den Nerv von Teilen der Alternativbewegung zu treffen, die sich eher anarchistisch-libertär als sozialistisch oder kommunistisch verstanden. Die Opposition von zentral-technokratischer Macht versus dezentral-kreativer Alternativmacht schien die Anti-AKW-Proteste besser zu beschreiben als die klassische Opposition von Arbeit und Kapital.<sup>172</sup> Die Technik selbst und nicht mehr nur ihre ungleiche Verteilung als Produktionsmittel war zum zentralen Politikum geworden. Es ging, wie Jungk (1977, 202) formulierte, um »alle Erscheinungsformen und Machteinflüsse der großindustriellen Technologie«. Dabei galt die gesteigerte Aufmerksamkeit für die »politischen Implikationen« der Technik nicht mehr nur dem sozio-politischen Kontext, in dem diese Techniken funktionierten. Zumindest hatten es die kommunistischen Kader der 1968er-Bewegung schwer mit ihrer These, dass die Atomkraft nur als Instrument des Kapitalismus zu kritisieren sei, während es durchaus eine gute kommunistische Kernkraft geben könne (zum Verhältnis von Anti-AKW und 68er Bewegung siehe: Radkau 2011, 226ff.). Vielmehr ging es um die Art und Weise, wie bestimmte Technologien zugleich die politischen Rahmenbedingungen erschaffen, innerhalb derer sie funktionieren. Die Bewegung richtete ihre Aufmerksamkeit zunehmend auf die Politik der Artefakte selbst – ein Thema, das Langdon Winner Anfang der 1980er Jahre auch in die sozialwissenschaftliche Debatte einbrachte (Winner 1980).<sup>173</sup> Man konnte jetzt davon ausgehen, dass es genuin »autoritäre« und »demokratische« Techniken (für diese Unterscheidung siehe bereits: Mumford 1964) gab. In neuen politischen Konfliktkonstellationen ging es eben

---

172 Auch Helga Nowotny bemerkt, dass es bei dem Widerstand gegen die Atomkraft vor allem um die Frage zentraler Macht ging. »Widerstand gegen die Atomkraft [ist] in ihren gesellschaftlichen Strukturen Widerstand gegen die, die den Nutzen von einer weitergehenden wirtschaftlichen und politischen Konzentration und Zentralisierung haben werden. Er richtet sich gegen die ›Groß-Industrie, von der man den Eindruck hat, daß sie mit ›Groß-Regierungen und der ›Groß-Wissenschaft Hand in Hand arbeitet.« (Nowotny zitiert nach: Lovins 1978, 255)

173 1980, deutlich beeinflusst von den Auseinandersetzungen um die Atomkraft, veröffentlichte Langdon Winner seinen mittlerweile zum Klassiker der Wissenschafts- und Technikforschung aufgestiegenen Text *Do Artifacts have Politics?* Winner argumentiert darin, »certain technologies in themselves have political properties« (Winner 1980, 122). Damit richtete er sich gegen die damals weit verbreiteten Thesen, dass erst der soziale Kontext über die politischen Qualitäten von Artefakten Aufschluss gebe. Durchaus schlüssig argumentierte Winner (1980, 122), dass die These »What matters is not technology itself, but the social or economic system in which it is embedded« in der Konsequenz darauf hinauslaufe zu behaupten: »things do not matter at all«. Für eine Kritik an Winner siehe: Woolgar und Cooper (1999), Joerges (1999).

nicht nur um Sicherung gegenüber Risiken, sondern auch um die Abkehr von bestimmten Formen technischer Herrschaft.

### 3.3.2. Atommacht oder *Brittle Power*? Widerstandskräfte im Energiesystem

Was Lovins für die Geschichte des Sicherheitsdispositivs der Resilienz so bedeutsam macht und was seine linksradikalen Kritiker\_innen vermutlich noch mehr empört hätte als sein Liberalismus, ist, dass er zur selben Zeit, als sein Buch zu sanften Energien gerade auf Deutsch erschienen war, gemeinsam mit seiner Frau Hunter Lovins an einem Bericht für den US-amerikanischen Zivilschutz arbeitete. Im Auftrag der Defence Civil Preparedness Agency, die zum Zeitpunkt der Fertigstellung des Berichts bereits in die neu gegründete FEMA (Federal Emergency Management Agency) übergegangen war, legten Lovins und Lovins eine Studie mit dem Titel *Energy Policies for Resilience and National Security* vor, die 1981 unter dem Titel *Brittle Power. Energy Strategy for National Security* (Lovins und Lovins 1982) erschien. In *Brittle Power* haben die Lovins das von Crawford Holling geprägte Resilienzkonzept aus dem Bereich der Systemökologie auf den Infrastrukturschutz angewendet und damit entscheidend zu dessen Ausweitung beigetragen.

Wie in *Sanfte Energie* wird auch in *Brittle Power* die Reaktion der US-Regierung auf die Ölkrise kritisiert, weil ein letztlich zu kleiner Ausschnitt der Verwundbarkeiten des amerikanischen Energiesystems – die Abhängigkeit der Vereinigten Staaten von den Ölimporten aus dem Nahen Osten – adressiert und so die grundlegendere Energiekrise noch verstärkt wurde. »[M]ost investments proposed to replace foreign oil would actually make our energy supplies *more* vulnerable, in other and even less tractable ways.« (Lovins und Lovins 1982, 3, Hervorhebung im Original) Die Lovins kritisierten dabei nicht nur die falsche Lösung, sondern vor allem die zu enge vornehmlich militärische Rahmung des Problems der »energy security«.

»[E]very sword has at least two edges. Thus a purely military conception of national security dangerously neglects [...] the energy vulnerabilities described in this book [...]. [I]f we suppose that the answer to the Arab oil embargo is simply to expand the domestic supply of all forms of energy, we may merely substitute one class of vulnerabilities for another. Defining a problem too narrowly can »solve« the energy problem, for a time, by making it into a problem of insecurity, inflation, climate, nuclear proliferation, inequity, etc. Whether in energy, military, or biological terms, focusing on only one aspect of security at a time ignores the interactions



among all aspects. [...] Where cause-effect relationships are too complex to understand intuitively, attempted solutions can make a problem worse: *the cause of problems is often prior solutions.*« (Lovins und Lovins 1982, 24f., Hervorhebung im Original)

Durch ihre »ganzheitliche, systemische« Sichtweise reproblematisieren die Lovins die Reaktion der US-Regierung auf das Problem der Ölkrise auf eine Weise, die den Gegenstand, die normative Leitvorstellung und die eingesetzten Maßnahmen der Energiesicherheit verändert. Die systemische Sichtweise betrifft dabei zunächst einmal den Gegenstand der Sicherheit. Das Schutzobjekt ist ein komplexer Zusammenhang von unterschiedlichen, aufeinander verweisenden Komponenten, die alle eine spezifische Quelle der Bedrohung bzw. Verwundbarkeit darstellen: gefährliche Materialien (insbesondere Uran und Plutonium), Übertragungswege (Stromleitungen und *pipelines*), entfernte Extraktionsorte von natürlichen Ressourcen (insbesondere solche in instabilen Weltregionen oder in naturräumlich gefährlichen Gegenden, etwa *offshore*), Energieproduktionsanlagen etc. Das Zusammenspiel dieser vielfältigen Systemkomponenten resultiert in bestimmten Eigenschaften des Gesamtsystems, die dieses mehr oder weniger verwundbar bzw. *brittle*, also zerbrechlich machen (siehe: Lovins und Lovins 1982, 19). Die *brittleness* der US-amerikanischen Energieversorgung liegt an einer Systemeigenschaft, die Amory Lovins schon in *Sanfte Energie* aufs Korn genommen hatte: dem Zentralismus. »America's energy vulnerability is an unintended side effect of *the nature and organization of highly centralized technologies.*« (Lovins und Lovins 1982, 2, Hervorhebung im Original) Akribisch arbeiten Amory und Hunter Lovins die Gründe für die Verwundbarkeit zentralisierter Energiesysteme heraus. Wenn sehr große und geographisch eng zusammenhängende Einheiten für die Energieproduktion zuständig sind, kommt es bei deren Ausfall zu weitreichenden Versorgungsengpässen. Zudem muss die Energie sehr lange Wege durch *pipelines* zurücklegen, die ebenso stör- wie sabotageanfällig sind und deren Unterbrechung zu schwerwiegenden Stockungen in der Energieversorgung führen kann. Viele der Komponenten des Energiesystems sind ferner auf eine Weise aneinander gekoppelt, dass Störungen an einem Ort sich durch die Netze des Systems weiträumig fortsetzen und zu Katastrophen eskalieren können. Die »ansteckende« Wirkung der Störung ist großräumig und blitzschnell, weil selten ausreichende materielle und zeitliche Puffer vorhanden sind, die eine Störung abfedern können. Schließlich sind das Energiesystem und viele seiner Komponenten so komplex, dass es schwer ist, im Störfall die Quelle der Störung zu finden und zu beheben (siehe zu diesem Kom-

plex die Übersicht in: Lovins und Lovins 1982, 218). Vor dem Hintergrund dieser Problembeschreibung drängt sich Dezentralisierung als Strategie geradezu auf, um das Energiesystem sicherer und weniger störungsanfällig zu machen (Lovins und Lovins 1982, 215).

Neben der neuen Strategie der Dezentralisierung und dem neuen Gegenstand – das gesamte Energiesystem von der Extraktion bis zur Konsumption – schlagen Lovins und Lovins aber vor allem ein neues normatives Leitbild, ein neuen *telos* der Sicherheit vor: Resilienz. Lovins und Lovins führen »resilience« als Alternative zum gängigen sicherheitstechnischen Leitbild der »reliability« ein (siehe dazu: Lovins und Lovins 1982, 177ff.). *Reliability* versucht einen möglichst störungsfreien Dauerbetrieb der Energiesysteme zu gewährleisten. Dafür werden, unter Zuhilfenahme von Wahrscheinlichkeitsberechnungen, präventive Schutzmaßnahmen gegen mehr oder weniger wahrscheinliche Gefahren getroffen. Resilienz bricht demgegenüber mit der Zielvorstellung der kompletten Störungsfreiheit. *Accidents will happen*. Gerade die enge Fokussierung auf einen erwartbaren Ausschnitt des Gefahrenspektrums vermindert systematisch die Fähigkeit, angemessen auf unerwartete Ereignisse reagieren zu können und senkt damit die Resilienz des Energiesystems (Lovins und Lovins 1982, 180). Das Ziel sollte stattdessen darin bestehen, ein Energiesystem so zu gestalten, dass letztlich niemals ganz zu vermeidende Störungen sich nicht zu Katastrophen auswachsen können. »Falling gracefully« (Lovins und Lovins 1982, 179) ist deshalb die Devise der Resilienz.

Resilienz ist aber nicht nur der Zustand eines Systems – verstanden als relativer Grad von *bounciness* (etwa: Elastizität) bzw. *brittleness* (Zerbrechlichkeit) –, sondern vor allem ein evolutionärer Prozess. Der Zustand ist bloß passive, der Prozess aktive Resilienz (Lovins und Lovins 1982, 181). Gerade ein Energiesystem, das sich im Angesicht von ständig verändernden Umweltbedingungen behaupten muss, braucht aktive Resilienz: Anpassungsfähigkeit, Flexibilität, Lernfähigkeit (Lovins und Lovins 1982, 186). Gerade diese Dimension aktiver Resilienz ist Systemingenieuren aber so fremd, dass Lovins und Lovins sich gezwungen sahen, in der Biologie nach Vorbildern Ausschau zu halten. Ihr biologischer Stichwortgeber ist Crawford S. Holling. Wie bereits gesehen (2.5.1), hat auch Holling immer wieder gegen ein bloß ingenieurmäßiges Verständnis von Resilienz geschrieben. Die Studie von Lovins und Lovins ist vermutlich der erste ernstzunehmende Versuch, das ökologisch-systemische Resilienzkonzept auf einen anderen Bereich als die Biologie zu übertragen (siehe bereits:

Lovins 1977). Ihre Transferleistung ist wohl deshalb so überzeugend gewesen, weil es ihr gelang, auf einer sehr abstrakten Ebene sozio-technische Energiesysteme und biologische Ökosysteme zu analogisieren. Das Energiesystem zeigt wie das Ökosystem *life-like properties*, hat gleichsam eine vitale Materialität, die mit Eigensinn und Spontanität ausgestattet ist. Zugleich wird das Prinzip der Resilienz aber auch so präsentiert, dass es intuitiv nachvollziehbar ist und an den »gesunden Menschenverstand« anschließen kann.

»Just as population biology [...] reveals the value of being fine-grained and heterogeneous in space, so engineering experience shows a corresponding value in dispersion and in redundant, relatively small modules that can substitute for each other [...]. The selective coupling in food webs, where organisms normally depend on each other but can do without their usual diet and cushion the transition with a buffer stock of stored food if need be, is analogous to the optional autonomy of components – like a householder who normally heats with gas but, at a pinch, can switch to the woodstove and the backyard woodpile. The hierarchy of food chains, where (for example) many different kinds of algae provide primary productivity in a pond interchangeably without worrying about what will eat them in turn, is similar to the redundancy of a grid energized by the similar, interchangeable outputs of different energy sources. The biological adaptability of prolific species is analogous to the ability to evolve a technology quickly through the efforts of many participants. And the compromises inherent in any design for resilience – between standardization and diversity, between autonomy and sharing, between narrow efficiency and broad survivability – are as central to engineering as to life itself.« (Lovins und Lovins 1982, 207)

Resilienz ist einfach, intuitiv nachvollziehbar, geradezu natürlich simpel. Gerade deshalb ist das normative Leitbild der Resilienz in der Lage, die hoffnungslos kontraintuitiv-abstrakte Welt der Sicherheitsexpert\_innen und Systemingenieur\_innen, die sich in ihrer selbstgewirkten Komplexität zunehmend verheddert haben, auf die Erde zurückzuholen. Einfach, klein, übersichtlich, dezentral, lokal: so soll das resiliente Energiesystem der Zukunft sein. Es ist so verständlich gebaut, dass nicht nur Physiker\_innen und Systemingenieur\_innen, sondern schon einfache Handwerker\_innen Störungen beheben können (siehe: Lovins und Lovins 1982, 190ff., 213). Damit verspricht Resilienz nicht nur mehr Sicherheit, sondern zugleich auch einen Ausweg aus der entfremdeten Lebensweise der hochtechnischen Zivilisation. Auch wenn *Brittle Power* deutlich zurückhaltender mit

weitreichenden politischen Versprechen ist als *Sanfte Energie*,<sup>174</sup> so stellt auch die Forderung nach einem resilienten Energiesystem einen emanzipatorischen Mehrwert in Aussicht: die Emanzipation aus der Abhängigkeit von entfernten Energiesystemen und detachierten Expert\_innen zugunsten eines dezentralen Energiesystems und dem lokal situierten Wissen der »einfachen Leute«, die ihre einfachen Energiesysteme selbst betreiben können – *power to the people!*

Gerade erneuerbare Energieträger bieten sich für den Aufbau eines solchen resilienten Energiesystems an. Sie operieren über viele verteilte Module und sind durch kurze und robuste Leitungen miteinander verbunden. Fehler können in ihnen schnell erkannt und behoben werden (Lovins und Lovins 1982, 264f.). Sie sind von Natur aus dezentral. Sonne und Wind haben eine natürliche geographische Streuung und kommen nicht nur an wenigen Orten konzentriert vor. Dadurch kann auch die Abhängigkeit von geopolitisch instabilen Regionen mit großen Erdölvorkommen verringert werden (Lovins und Lovins 1982, 276f.). Schließlich sind erneuerbare Energieträger unerschöpflich und reduzieren damit die Verwundbarkeit durch Verknappung von Ressourcen (Lovins und Lovins 1982, 289). Kurz: Erneuerbare Energien sind »inherently resilient energy supplies« (Lovins und Lovins 1982, 264). Das gilt aber natürlich nur so lange, wie die Tugenden erneuerbarer Energien nicht durch die Laster der zentralistischen Energieplanung zunichte gemacht werden. Gigantische Wind- oder Solarparks, von denen durch lange Leitungen Strom an entfernte Orte übertragen werden muss, sollen daher gerade aus Sicherheitsgründen vermieden werden.

*Brittle Power* ist eine Kritik an übersteigerten Ansprüchen von Sicherheit und Expert\_innenwissen und deren pathologischen Effekten und zugleich eine Empfehlung zur Reprogrammierung des Regierens. Ironischerweise konnte die ökologisch-liberale Kritik von Lovins und Lovins vor allem deshalb so wirkmächtig werden, weil sie an Strategien im Inneren eben der »harten Sicherheitsapparate« anschließen konnte, die scheinbar den Zielpunkt der Kritik darstellten. Schließlich waren US-amerikanische Mili-

---

174 So bestreiten die beiden hier – im Gegensatz zu Lovins' »Katalysatorthese« in *Sanfte Energie* – explizit einen Zusammenhang von »sozialer« und »technischer« Dezentralisierung (Lovins und Lovins 1982, 50ff.), während sie an anderer Stelle zugleich vermuten, dass die Sowjetunion auf eine Dezentralisierung ihrer Energieressourcen verzichtet, um den Einfluss der Zentralmacht Moskaus nicht zu gefährden (Lovins und Lovins 1982, 219).

tärstrateg\_innen längst mit den Vorzügen der Dezentralisierung durch die Strategie der »distributed preparedness« (Collier und Lakoff 2008) vertraut (siehe Kapitel 3.1.1.). Die geographische Zerstreuung kriegswichtiger Infrastruktur, um diese gegenüber feindlichen Bombenangriffen weniger verwundbar zu machen, gehörte schließlich bereits zum Kern des »nuclear preparedness apparatus« (Collier und Lakoff 2015, 28) der USA während des Kalten Krieges. Lovins und Lovins waren sich dieser Tradition durchaus bewusst und haben sie gezielt aufgegriffen (Lovins und Lovins 1982, 69f.). Dadurch haben sie die Sicherheitstechnik der Dezentralisierung und die Norm der Resilienz miteinander verbunden und zugleich ökologische und militärische Sicherheitsstrategien zusammengeführt.

Wenn Dezentralisierung heute noch als politisches Versprechen funktioniert, dann eher in einer seltsam staatstragenden Manier, wie etwa beim Zukunftsguru Jeremy Rifkin. Dieser beschreibt in seinem Buch *Dritte Industrielle Revolution* (Rifkin 2011) das revolutionäre Potenzial einer Kombination von neuen Informationstechnologien und dezentralisierten erneuerbaren Energien. Rifkin, der seine Leser\_innen durch Kanzler\_innenämter, Aktionär\_innenversammlungen und schicke Abendessen im kleinen exekutiven Kreis mitschleift und dabei ausführlich über seine guten Kontakte zu zentralen Entscheidungsträger\_innen in Politik und Wirtschaft unterrichtet, wirkt wie ein aus der Rolle fallender Wiedergänger der Atomstaatskritiker\_innen 1970er, wenn er sich einerseits der emanzipatorischen Rhetorik der Alternativbewegung bedient, andererseits aber genau die Akteure von Staat und Kapital adressiert, welche die erklärten Feinde der Alternativbewegung darstellten.

»Die elitären fossilen Energien der ersten beiden industriellen Revolutionen begünstigten vertikale, auf Massenproduktion ausgerichtete Ökonomien und damit die Herausbildung riesiger, zentralisierter Unternehmen [...] Die reichliche Verfügbarkeit von erneuerbaren Energien der Dritten Industriellen Revolution dagegen fördert die Entstehung tausender dezentraler Firmen und kollaborativer Geschäftsbeziehungen, die in Netze eingebettet sind, die eher wie Ökosysteme denn wie Märkte funktionieren.« (Rifkin 2011, 132)

Mit der »dritten industriellen Revolution« beginnt deshalb zugleich das Zeitalter »lateralen Macht«, das »zu einer Umstrukturierung der zwischenmenschlichen Beziehungen von vertikal zu lateral.« (Rifkin 2011, 13) führt.

Aber nicht nur Rifkin versteht die Energiewende als Chance für die Demokratie. So verlangt die Ethikkommission Sichere Energieversorgung (EKSE), die nach dem Reaktorunglück von Fukushima eingesetzt wurde,

um den deutschen Atomausstieg moralisch zu ratifizieren, dass »die Energiepolitik auf das dezentrale Mitmachen und die eigene Entscheidung der Bürger« (EKSE 2011, 18) setzen solle. Auch wenn die scharfe Polemik gegen den Atomstaat hier gerade nicht mehr vorkommt, ist letzterer als Schatten und negative Abgrenzungsfolie doch immer noch präsent: vom Atomstaat zur erneuerbaren Demokratie. Die Energiewende soll Formen der technologischen Staatsbürgerschaft (Barry 2001, 127) Vorschub leisten, in Bürger\_innen als *citoyen* und als *bourgeois* ihren Beitrag leisten können.<sup>175</sup>

Mit Blick auf derartig staatstragende Debattenbeiträge mag die Kritik zentralistischer Großtechnik und zentraler Regierungsgewalt rückblickend als bloßer Katalysator für eine Erneuerung des buchstäblich ausgebrannten Kapitalismus erscheinen. Der Ruf nach Dezentralisierung scheint Machtformen Auftrieb gegeben zu haben, die vielleicht ebenso problematisch sind wie die Zentralmacht. Haben wird nicht gelernt, dass Macht immer schon »lateral« bzw. »kapillar« funktioniert (Foucault 2001, 42)? Ist es bloßer Zufall, dass die Staatsphobie der Alternativbewegungen der 1970er zu demselben Zeitpunkt an Fahrt aufnimmt, als auch der Neoliberalismus vermehrt Formen staatlich-zentralistisch-technokratischen Regierens in Frage stellt? Hat nicht gerade diese Kombination der Kritik zu den dezentralen Machtformen der Gegenwart geführt, die bisweilen noch un(an)greifbarer erscheinen als die entfernten Kraftwerke und Machtzentren?

Anstatt die Atomstaatsthese extern aus der historischen Distanz zu kritisieren, lässt sich die Atomstaatstheorie aber auch mit der praktischen Kritik der Anti-AKW-Bewegung konfrontieren. Während die Proteste der Kernkraftgegner\_innen der 1970er und 1980er Jahren vor allem von Großdemonstrationen, Platzbesetzungen und teils erbitterten Auseinandersetzungen an den Standorten geplanter Kraftwerke und Lagerstätten

---

175 Das angesprochene »Mitmachen« soll nämlich laut der Ethikkommission in mehreren Bezugsregistern entlang der unterschiedlichen Rollen des Bürgers im Energiesystem erfolgen: »Verbraucher haben mehrere Rollen: Sie sind Marktteilnehmer (Nachfrager), »Konsumenten-Bürger« und »Koproduzenten« im Energiesystem. [...] Verbraucher können als Marktteilnehmer zur Energiewende beitragen, indem sie mehr energieeffiziente Produkte und Dienste nachfragen [...]; sie können als »Koproduzenten« dazu beitragen, indem sie ihre Häuser sanieren und selbst dezentral Energie erzeugen und flexibel bereitstellen (smart homes, smart grids, »Zuhausekraftwerke«); und als politische [...] Bürger können sie dazu beitragen, indem sie sich an Beteiligungsverfahren [...] zum Netzausbau beteiligen und versuchen, Zielkonflikte sachgerecht und dem Gemeinwohl verpflichtet zu bearbeiten.« (EKSE 2011, 18)

geprägt waren, kam es in den 1990er Jahren zu einer Neuausrichtung der Aktionsformen. Der Protest gegen die Transporte von Atommüll mobilisierte nun regelmäßig tausende Demonstrant\_innen, die versuchten den Transport auf Schiene und auf der Straße zu blockieren. Auch wenn es bisher nie gelungen ist, den Transport gänzlich zu unterbinden, treiben die Anti-Castor-Proteste doch die Kosten für die Transporte und damit für die Atomkraft in die Höhe. Zudem erzeugt die große Medienaufmerksamkeit für die spektakulären Protestformen regelmäßig ein Forum, in dem die Kritik der Atomkraft, die ungelösten Fragen der Atommüllendlagerung, die Sicherheitsbedenken bezüglich der Transporte etc. öffentlich gemacht werden können. Ironischerweise nutzten die Blockierer\_innen dabei genau die Art von Verwundbarkeiten aus, die dem zentralistischen Atomstaat, den sie so heftig kritisierten, eigen waren. Verwundbarkeiten, auf die Lovins und Lovins in ihrem Bericht für die US-Regierung mehrfach hingewiesen haben: die »long haul distances« (Lovins und Lovins 1982, 32), die aus der Notwendigkeit der Verteilung des Energie von zentralen Standorten an ihre dezentralen Abnehmer\_innen resultieren. Die wenigen zentralen Atomkraftwerke, Wiederaufbereitungsanlagen und Zwischenlager für Atommüll waren nur durch einige wenige Eisenbahnlinien miteinander verbunden. Es waren diese dünnen Linien, die die Anti-AKW-Aktivist\_innen blockierten und damit die Macht des Atomstaats »in ihren äußersten Verästelungen, dort, wo sie haarfein wird [...] in ihren regionalsten und lokalsten Formen« (Foucault 2001, 42) attackierten. Wie bereits die Kohlearbeiter\_innen des frühen 20. Jahrhunderts, die die Transporte der für die gesamte Industrie benötigten Kohle über die Schiene blockierten (Mitchell 2011, 21–27), nutzten die Aktivist\_innen damit die Schwachstellen eines zentralisierten fossil-nuklearen Energieregimes, um ihren politischen Forderungen Nachdruck zu verleihen. Am Ende erwies sich der scheinbar allmächtige Atomstaat als *brittle power*.

Zum Vorschein kommt hier eine grundsätzliche Ambivalenz zentraler (Staats)macht in der Moderne. Um überhaupt von einer zentralen Position aus gleichsam aus der Distanz Macht ausüben zu können (zu den Konzepten des Handelns bzw. Regierens auf Distanz, siehe: Latour 1987, 219–232, Rose und Miller 1992, 173), muss sich diese Macht vernetzen und zerstreuen. »Die Macht [...] [ist] etwas, was zirkuliert und nur als Verkettung funktioniert. [...] Die Macht verteilt sich über Netze« (Foucault 2001, 44). Ein zentrales Machtpotenzial, das nicht ausgeübt werden kann, weil ihm die lokalen Applikationsinstanzen dazu fehlen, ist genauso macht- bzw. nutz-

los wie ein zentrales Energiepotenzial (ein Berg Kohle, ein Atomkraftwerk) ohne Netze, durch die Elektrizität zum Endverbraucher zirkulieren kann. Der Rekurs auf die Infrastruktur der Energie als Infrastruktur der Macht ist gerade im Zusammenhang mit der Frage nach der Macht des Atomstaats nicht nur metaphorisch. Erst die infrastrukturelle oder logistische Form der Machtausübung hat, wie Michael Mann (1984) und Chandra Mukerji (2010) überzeugend argumentiert haben, dafür gesorgt, dass Machtausübung in einem Territorialstaat überhaupt möglich wurde: Straßen, über die das Militär vorrücken kann, Kommunikationsverbindungen, über die Verordnungen zirkulieren können, Dienste öffentlicher Daseinsvorsorge, die den biopolitischen Staat legitimieren etc. Durch diese infrastrukturelle Erschließung des Territoriums haben sich aber auch die Angriffspunkte vergrößert. Eine Macht, die überall ist, kann auch überall angegriffen werden. Gewiss, die Macht des Staates hat sich ebenso wie die Macht großer Energiekonzerne durch die Mobilisierung der Kräfte des Atoms und der fossilen Brennstoffe, durch die Elektrifizierung und massenhafte Motorisierung potenziert. Dennoch sind keine allmächtigen Energieregime entstanden, weil die »networks of power« (Hughes 1993) immer auch zu Netzwerken des Widerstands geworden sind.

### 3.3.3. Vom GAU zum Problem Versorgungssicherheit

Die Reaktorkatastrophe von Fukushima im März 2011 hat die Besorgnis um die Risiken der Atomkraft wieder aufleben lassen. Plötzlich war wieder die Rede von unbeherrschbaren Technologien und Restrisiken – auch in den politischen Lagern, die nur kurz zuvor längere Laufzeiten für Atomkraftwerke beschlossen hatten. In ihrer Regierungserklärung verkündete Angela Merkel nur wenige Tage nach der Katastrophe im deutschen Bundestag:

»Die unfassbaren Ereignisse in Japan lehren uns, dass etwas, was nach allen wissenschaftlichen Maßstäben für unmöglich gehalten wurde, doch möglich werden konnte. [...] Wenn das so ist, wenn also in einem so hoch entwickelten Land wie Japan das scheinbar Unmögliche möglich, das absolut Unwahrscheinliche Realität wurde, dann verändert das die Lage.« (Bundestag 2011b, 10884f.)

Schon in derselben Sitzung des Bundestages wurden eine sogenannte »Anlagenspezifische Sicherheitsüberprüfung (RSK-SÜ) deutscher Kernkraftwerke unter besonderer Berücksichtigung der Ereignisse in Fukushima-I



(Japan)« (siehe: RSK 2011) in Auftrag gegeben und die sieben ältesten Atommeiler für den Überprüfungszeitraum stillgelegt (das Atom-Moratorium). Zudem setzte die Bundesregierung eine Ethikkommission ein, die ein für alle Mal das Schicksal der Atomkraft diskutieren sollte.

Die Ethikkommission, der auch die Soziologen Ulrich Beck und Ortwin Renn angehörten, war sich offenbar einig, dass ein »Atomkonsens« nur durch einen definitiven und beschleunigten Ausstieg aus der Atomkraft erreicht werden könnte. Dabei sind die Argumente für diesen Schritt – der Hinweis auf die Risiken der Atomkraft, die niemals gänzlich auszuschließende Möglichkeit komplexer Störungsfälle und Ereignisverkettungen in hochtechnologischen Anlagen sowie die Schwierigkeiten, eines einmal eingetretenen GAU wieder Herr zu werden (siehe: EKSE 2011, 11f.) – keineswegs neu. Nicht die Argumente sind also das Interessante an der Ethikkommission, sondern dass überhaupt die Form einer Ethikkommission gewählt wurde, um den endgültigen Ausstieg vorzubereiten. Eine Ethikkommission erschien der Bundesregierung in der angespannten Lage nach Fukushima als der geeignetste Weg, einen Atomkonsens zu schmieden und abzusichern. In einer »Lage«, in der es um existenzielle Fragen des Lebens geht, scheint die Ethik,<sup>176</sup> und nicht die offene politische Auseinandersetzung oder das Expert\_innengutachten, das geeignete Terrain zu sein, um Legitimität für politische Entscheidungen zu erlangen. So bemerkt die Ethikkommission selbst, dass es ihr auch darum gehe, »die schädliche Atmosphäre zu beseitigen, in die unsere Gesellschaft durch die Auseinandersetzung über die Atomkraft geraten ist« (EKSE 2011, 9). Auch wenn der Bericht gerade nicht die lauten Töne der Atomstaatskritik anschlägt, so haben die harten Auseinandersetzungen um die Atomkraft seit Ende der 1970er Jahre doch ihren langen Schatten auf die Ausstiegsentscheidung der Bundesregierung und die Einsetzung der Ethikkommission geworfen. Das Ende der technischen Grundlage des Atomstaats sollte offenbar nicht mit den Mitteln des Atomstaats, nicht in Hinterzimmergesprächen zwischen Regierung und Industrie eingeleitet werden. Nicht nur die Technologien sollten sich ändern, die neue Energiepolitik sollte auch aufgeschlossen, partizipativ und reflexiv sein, »Teilhabe« (EKSE 2011, 13) und »Bürgerbeteiligung« (EKSE 2011, 19) ermöglichen. Und was könnte das besser verbürgen als eine Ethikkommission?

---

176 Zur politischen Funktion der Ethik in den Debatten um Biotechnologie siehe unter anderem: Gehring (2006, 110–153), Wehling (2013), Rödel (2014).

Es wäre verkürzt, die Ethikkommission nur als Streitschlichtungsgremium und Konsensmaschine darzustellen. Denn nicht zuletzt verweist sie auch auf neue Problemlagen und Konfliktlinien, die mit dem Atomausstieg einhergehen. Der programmatische Titel der Kommission »Ethik-Kommission Sichere Energieversorgung« bezieht sich nicht nur auf die Sicherheit und den Schutz vor Nuklearreaktorunfällen, sondern ebenso auf eine ganze Reihe anderer Aspekte der Energiesicherheit, die teilweise negativ vom Atomausstieg beeinflusst werden können. Der Atomausstieg erscheint weniger als sicherheitspolitischer Befreiungsschlag denn als Eintritt in eine komplexe Landschaft der Energiesicherheit und unterschiedlicher ökologischer Sicherheitsproblematiken. Zwar wird die Atomenergie und insbesondere die ungelöste Problematik der Endlagerung als ökologisches Risiko wahrgenommen (EKSE 2011, 45). Gleichwohl verursacht die Atomkraft anders als fossile Brennstoffe keine CO<sub>2</sub>-Emissionen, die den Klimawandel beschleunigen.<sup>177</sup> Die Verpflichtung auf den Klimaschutz, die sowohl die Ethikkommission (EKSE 2011, 20f.) als auch die Bundesregierung in ihrem Eckpunktepapier *Der Weg zur Energie der Zukunft – sicher, bezahlbar, umweltfreundlich* (BMW i und BMU 2011) betonen, führt deswegen zur Entscheidung für den Ausbau erneuerbarer Energien im Rahmen einer umfassenden »Energiewende«.

Die Energiewende lässt – neben dem zumindest im Jahr 2011 noch als relativ beherrschbar geltenden Problem der geopolitischen Abhängigkeit von Gaslieferungen (EKSE 2011, 34) aus dem Ausland – das Problemfeld der »Versorgungssicherheit« auf den Plan treten. Bei der Versorgungssicherheit geht es um die Gewährleistung einer ausreichenden, jederzeit verfügbaren, ununterbrochenen Stromversorgung für Bevölkerung und Wirtschaft und damit um eines der Basisgüter gegenwärtiger Gesellschaften. Die Sicherstellung der Strom- und Energieversorgung beinhaltet dabei sowohl die ausreichende Produktion von Strom als auch seine Distribution. Die Erfahrung mit der abrupten Abschaltung von acht Atommeilern während des Moratoriums hat gezeigt, dass die in Deutschland produzierte Strommenge für die Gewährleistung der Stromversorgung auch ohne Atomkraftwerke ausreichend ist (EKSE 2011, 21f.). Allerdings sei, wie

---

<sup>177</sup> Tatsächlich sind seit 2011 die CO<sub>2</sub>-Emissionen gestiegen, nachdem sie zwischen 1990 und 2011 um 27 Prozent gesunken waren. Grund hierfür ist unter anderem der Anstieg der Nutzung von Braunkohle als Folge des Atomausstiegs (zu diesen Zahlen siehe: Minten 2015).

Studien der Bundesnetzagentur betonen, der Koordinierungsaufwand bei der Verteilung des Stroms durch die Übertragungsnetzbetreiber gestiegen.

»Die Analyse der Bundesnetzagentur [...] hat bisher keine Hinweise auf akute Gefährdungen der Systemsicherheit [...] ergeben. Die Übertragungsnetzbetreiber haben jedoch explizit darauf hingewiesen, dass ein deutlich erhöhter Koordinierungsaufwand im operativen Bereich besteht.« (BNetzA 2011b, III)

Unter Bedingungen der Energiewende und eines liberalisierten Strommarkts sind, wie auch die Ethikkommission bemerkt (EKSE 2011, 36ff.), weitreichende Anforderungen an die Energieinfrastruktur und vor allem an das Stromnetz entstanden. Versorgungssicherheit stellt sich hier vor allem als Zirkulations- und Steuerungsproblem und nicht mehr vorrangig als Produktionsproblem – es besteht weniger in der prinzipiellen Knappheit von Energie, sondern in einer gesteigerten Verwundbarkeit des Stromnetzes. Energiesicherheit wird hier zu einem Problem der Sicherung vitaler Systeme.

Um das Themenfeld »Versorgungssicherheit« hat sich eine Reihe von Problematisierungen insbesondere beim BBK (BBK und IM-BaWü 2010, BBK 2014) und bei der Bundesnetzagentur (BNetzA 2006, 2012) gebildet, die reflektieren, wie sich die »Rahmenbedingungen« für die Gewährleistung von Versorgungssicherheit im Zuge der Energiewende, aber auch im Kontext der Liberalisierung und Europäisierung des Strommarktes verändert haben. Durch diese Problematisierungen rücken die Sicherheitsexpert\_innen den sozio-technischen Hintergrund der Stromversorgung in den Vordergrund und machen so komplexe Interaktionen von natürlichen Gegebenheiten und politischen Entscheidungen, von wirtschaftlichem Kalkül und technischer Kontrolle zu einem Gegenstand sichernder Sorge.

Das Stromsystem besteht auf der Angebotsseite aus drei wesentlichen Komponenten: Stromproduktion in unterschiedlichen Kraftwerkstypen, Transmission bzw. Übertragung des Stroms über relativ weite Strecken in Hochspannungsnetzen und lokale Verteilung von Strom in Niederspannungsnetzen (siehe etwa: BBK und IM-BaWü 2010, 5f.). Traditionell waren zumindest Produktion und Transmission in einigen wenigen Großkonzernen gebündelt bzw. vertikal integriert. Diese Konzerne hatten dabei laut dem seit 1938 bestehenden Energiewirtschaftsgesetz (EnWG) Gebietsmonopole inne (siehe: BBK 2014, 38) und waren zugleich im Sinne der Daseinsvorsorge dazu verpflichtet, die sichere und preisgünstige Stromversorgung der Bevölkerung zu gewährleisten. Die Versorgung erfolgte so gewissermaßen aus einem Guss: zentral, hierarchisch und stark reguliert.

Im Zuge der Liberalisierung des Strommarkts im Sinne der EU-Binnenmarktrichtlinie Elektrizität wurde diese Struktur ab Ende der 1990er Jahre aufgelöst (siehe: BBK 2014, 38). Dieses sogenannte *unbundling* (Entflechtung) sorgte für eine Trennung der Bereiche von Produktion, Transmission und Verteilung. Die integrierten Strommonopole wurden in ihre Grundbestandteile zerlegt. Zugleich wurden die Gebietsmonopole abgeschafft und der Strommarkt liberalisiert und europäisiert. In Deutschland entstanden die vier großen Energiekonzerne RWE, EON, Vattenfall und ENBW und die von diesen weitgehend unabhängigen Übertragungsnetzbetreiber (ÜNB) Amprion, Tennet TSO, Transnet BW und 50 Hertz, die allerdings weiterhin als natürliche Monopole die Netze in jeweils klar eingeteilten Gebieten der Bundesrepublik betreiben. Verbraucher\_innen konnten nun mit unterschiedlichen Stromanbietern Verträge abschließen und sich auch von solchen Anbietern versorgen lassen, die über keine Stromproduktionskapazitäten in ihrer Nähe verfügten.

Studien von Sicherheitsexpert\_innen betonen, dass das *unbundling* und die europaweite Marktöffnung zumindest eine gewisse Anspannung erzeugen (siehe etwa: BBK 2014, 99).<sup>178</sup> So führt etwa die europaweite Marktintegration zu einer stärkeren Interdependenz im Stromnetz, die es Störungen ermöglicht, sich weiträumig auszubreiten. Diese Sicherheitsproblematik hat vor allem ein Störfall im Jahr 2006 sichtbar gemacht, als die Trennung einer Hochspannungsleitung über der Ems eine Reihe von Stromausfällen bis in den nordafrikanischen Raum provoziert hat (siehe dazu: BNetzA 2007).

Während die Marktöffnung also größere Netze und verstärkte Interdependenz der Strominfrastruktur erzeugt, führt das *unbundling* vor allem zu neuen Steuerungsproblemen und Intransparenzen im Stromsystem, weil die Koordinierung der Bereiche Verteilung, Produktion und Transmission nicht mehr innerhalb eines Konzerns erfolgt. Es gibt keine einheitliche Organisationsstruktur mehr, die in der Lage ist, das Stromsystem von der Produktion bis zur Verteilung zu steuern und die deshalb auch mit auftretenden Störfällen und Instabilitäten allein umgehen kann. Früher lag die Verantwortung für das Gesamtsystem Strom bei den vertikal integrierten Großkonzernen. Laut Paragraph 13 des Energiewirtschaftsgesetzes tragen

---

178 In den USA ist die Liberalisierung der Stromversorgung und die damit einhergehende Verantwortungslosigkeit der Stromkonzerne immer wieder für den großräumigen *black-out* an der US-amerikanischen Ostküste und in Teilen Kanadas verantwortlich gemacht worden (Luke 2010).

heute nur noch die Übertragungsnetzbetreiber die sogenannte »Systemverantwortung« (EnWG 2005, § 13, § 16) für die Stabilität und Integrität des Netzes. Die Übertragungsnetzbetreiber haben also die Hauptverantwortung für die Sicherheit des vitalen Systems Stromversorgung, ohne zugleich die Verfügungsgewalt und den Überblick über das gesamte System zu haben. Ein Bericht des BBK zu *blackout*-Risiken sieht darin einen Problemhintergrund, der die Verwundbarkeit des Stromsystems erhöht.

»Solche, über die gesamte Wertschöpfungskette vertikal integrierte Unternehmen hatten unter anderem direkten Zugang zu den relevanten Systeminformationen und konnten auf den Betrieb eines Großteils der Erzeugungsanlagen unmittelbar Einfluss nehmen. Vielmehr liegt die Verantwortung für die Stabilität des Versorgungssystems heute bei Unternehmen (den ÜNB), deren unmittelbarer Einflussbereich sich aufgrund der wettbewerbsrechtlichen Entflechtung nur noch auf einen einzelnen Systemteil beschränkt (die Übertragung). Durch die Trennung von Erzeugung und Übertragung steigt also der Kommunikations- und Koordinierungsaufwand der systemverantwortlichen ÜNB, um die Netzstabilität zu gewährleisten.« (BBK 2014, 103)

Mit dem Problem der neuverteilten Systemverantwortung geht zudem das Problem der sogenannten Systemdienstleistungen einher. Diese beinhalten die »Übernahme von stabilisierenden Aufgaben im Netz, wie Frequenzhaltung, Spannungshaltung und Versorgungswiederaufbau« (BBK 2014, 99), Aufgaben und Leistungen, die nicht von den ÜNB, sondern nur von den Stromproduzenten übernommen werden können. Salopp formuliert heißt Systemdienstleistung, dass die richtige Art von Elektrizität im richtigen Frequenzbereich zur richtigen Zeit ins Netz eingespeist wird. Unter den Stromproduzenten im gegenwärtigen Strommarkt finden sich allerdings immer mehr Anbieter, die zwar Strom ins Netz einspeisen, ohne zugleich aber einen Beitrag zu dessen Stabilität zu leisten, also ohne Systemdienstleistungen zu erbringen. Das betrifft insbesondere Stromproduzenten, die Elektrizität aus erneuerbaren Quellen generieren, weshalb auch die Energiewende als Problemhintergrund für die Versorgungssicherheit ausgemacht wird.

»Die wachsende Anzahl der fluktuierend erzeugenden Anlagen der Photovoltaik oder Windkraft können nach dem heutigen Stand der Technik keine oder nur in einem sehr begrenzten Ausmaß und zu unwirtschaftlichen Bedingungen Systemdienstleistungen anbieten. Diese Systemdienstleistungen sind jedoch notwendig, um eine stabile Stromversorgung zu gewährleisten. Auf den Gebieten Frequenzhaltung, der Spannungshaltung, des Versorgungswiederaufbaus und der

Betriebsführung ergeben sich diesbezüglich technische Verwundbarkeitsaspekte.« (BBK 2014, 99)

Aber warum können Wind- und Sonnenenergie keine Systemdienstleistungen übernehmen, warum helfen sie nicht, das vitale System Stromversorgung zu stabilisieren? Der Hauptgrund dafür besteht in der Unstetigkeit dieser Energiequellen, in den »fluktuierend erzeugenden Anlagen« (s.o.). Während konventionelle Kraftwerke (zum Beispiel Atom und Kohle) je nach Bedarf Strom in einem jeweils kalkulierbaren Frequenzbereich zur Verfügung stellen können, liefern Photovoltaik und Windkraft nur genau dann Strom, wenn die Sonne scheint oder der Wind weht. Die Erneuerbaren sind damit so unberechenbar wie das Wetter und deshalb weniger verlässlich als die in Form fossiler Brennstoffe speicherbare Energie, die auf Abruf zur Verfügung stehen.<sup>179</sup> Diese Unbeständigkeit von Wind- und Solarstrom – man spricht auch von Volatilität – ist zunächst einmal deshalb ein Problem, weil sich Strom (noch) nicht in großem Ausmaß speichern lässt. Strom ist nämlich kein Ding, das sich beliebig lagern ließe, sondern ein energetisches Potenzial, das ein hohes Maß an Eigensinn aufweist. So sehr uns Strom im Alltagsgebrauch als gefügige Ressource erscheint, die auf Abruf verfügbar ist und ubiquitär eingesetzt werden kann, so sehr ist er doch aus der Perspektive der Steuerung des Stromsystems eine schwer zu kontrollierende Größe, die sich eben nicht nach Belieben lenken lässt. So ist nicht zuletzt das Wissen über den Eigensinn des Stroms und dessen physikalische Eigenschaften ein Bestandteil der Problematisierungen von Sicherheitsexpert\_innen, wie

---

179 Schon in Martin Heideggers Technikphilosophie findet sich ein interessanter Hinweis, der den ontologischen Unterschied zwischen Photovoltaik und Windkraft einerseits und fossilen Brennstoffen andererseits ins Licht rückt. Letztere können zumindest als Rohstoff für die Stromerzeugung beliebig vorgehalten werden und sind deswegen das, was Heidegger »Bestand« nennt: eine ständig verfügbare Ressource für technologische Operationen. Dagegen etabliert die Windmühle ein anderes ontologische Regime. »Das in der modernen Technik waltende Entbergen ist ein Herausfordern, das an die Natur das Ansinnen stellt, Energie zu liefern, die als solche herausgefördert und gespeichert werden kann. Gilt dies aber nicht auch von der alten Windmühle? Nein. Ihre Flügel drehen sich zwar im Winde, seinem Wehen bleiben sie unmittelbar anheimgegeben. Die Windmühle erschließt aber nicht Energien der Luftströmung, um sie zu speichern.« (Heidegger 2004, 18) Genau dieser ontologische Unterschied zwischen speicherbaren, auf Abruf zur Verfügung stehenden und fluktuierenden Energieträgern bereitet Sicherheitsexpert\_innen heute Kopfzerbrechen. Zu dieser ontologischen Dimension der Sicherheit der Elektrizitätsversorgung siehe: Folkers (2017b).

folgende Passage aus einem Interview mit einer Mitarbeiterin des BBK demonstriert:

»Und der Strom, das ist ja auch so, dass der sich selbst verteilt, der fließt ja dahin, wo gerade der größte Unterschied ist. Also von da weg, wo viel produziert wird, dahin, wo am wenigsten da ist. [...] Das macht der automatisch. Der sucht sich [...] so den Weg. Man kann wohl etwas zuschalten, aber man kann nicht sagen, du gehst jetzt genau diesen Weg und dann biegst du links ab.« (Interview 3)

Steuerung des Stromsystems ist deshalb vor allem Lastmanagement, das heißt die Kontrolle der Strommenge, die im Netz zirkuliert. Die Übertragungsnetzbetreiber können nur in sehr begrenztem Maß die Stromflüsse steuern und müssen sich vornehmlich darauf verlegen, Lastbereiche oder Stromerzeuger temporär vom Netz abzuwerfen. Denn um das Stromsystem auf einer stabilen Netzfrequenz – 50 Hertz im europäischen Verbundsystem (BBK 2014, 100) – zu halten, muss das Stromsystem im Gleichgewicht sein, das heißt es muss in jedem Moment (sic!) genauso viel Strom produziert werden, wie abgenommen wird (siehe: BBK und IM-BaWü 2010, 6). Vor der Liberalisierung des Strommarkts und der Energiewende erfolgte dieses Lastmanagement in den vertikal integrierten Unternehmen, die sowohl die Produktion als auch die Übertragung des Stroms besorgten. Dabei konnten sie von einer Verbrauchskurve ausgehen, die über den Tag verteilt auf relativ berechenbare Weise schwankt. Die Stromkonzerne mussten eine Grundlast (*baseload*), eine Mittel- und eine Spitzenlast (*peakload*) bewältigen. Dabei wurde die Grundlast vor allem von Atomkraftwerken, die ohnehin permanent laufen müssen, sowie von großen Kohlekraftwerken bedient, die Mittellast von kleineren, flexibleren Kohlekraftwerken und die Spitzenlast von Gaskraftwerken oder Wasserkraft, die relativ schnell hochfahren können. Aus der Perspektive von Sicherheitsexpert\_innen stellt sich nun das Problem, dass sich Photovoltaik und Windkraft hier nur schwer einfügen lassen:

»Wind und Sonne sind halt nicht vorhersehbar und können deshalb letztlich keine von diesen drei Stufen wirklich abdecken, weil sie nicht prognostizierbar sind. Also man hat natürlich schon den großen Vorteil, dass zum Beispiel Solarkraft vornehmlich tagsüber da ist und man sie dann auch braucht. Aber es ist halt nicht mehr in diesen klassischen Stufen so abdeckbar.« (Interview 3)

Dennoch speisen Photovoltaik und Windkraft sehr viel Strom ins Netz ein, und zwar nicht nur über den »normalen« Weg ins Hochspannungsnetz zur

Weiterverteilung im Niederspannungsnetz, sondern auch auf umgekehrtem Weg: Denn,

»[d]urch die Förderung der Erneuerbaren Energien treten verstärkt Kleinunternehmen und Privatpersonen als Stromproduzenten auf [...]. Sie speisen auf den unteren Spannungsebenen ein, die vormals nur von den höheren Ebenen mit Strom beliefert worden sind und diesen dort weiterverteilt haben.« (BBK 2014, 41).

Das Auftauchen der hybriden Figur des *prosumers* auf dem Strommarkt – also Haushalte, die über ihre eigenen Photovoltaikanlagen zu bestimmten Zeiten Strom ins Netz einspeisen und zu anderen auf Strom aus dem Netz angewiesen sind – verkompliziert die Steuerung des Stromsystems, indem es die Hierarchieebenen des Stromsystems durcheinander bringt.

Schließlich bereitet auch die geographische Verteilung von Wind- und Solarstromanlagen Probleme. Zwar gibt es tatsächlich dezentrale Anlagen auf Hausdächern, aber im Großen und Ganzen verteilen sich die Anlagen gemäß naturräumlicher Beschaffenheiten und damit nicht unbedingt in der Nähe bevölkerungsreicher Gegenden, in denen besonders viel Strom verbraucht wird. Windanlagen werden vornehmlich in Norddeutschland gebaut, weil dort relativ zuverlässig Wind weht. Der Strom muss deshalb über lange Leitungsnetze transportiert werden, die teilweise noch gar nicht gebaut sind. So entstehen massive räumliche Differenzen im Stromnetz, die nicht mehr von der Spontanität des Stroms selbst ausgeglichen werden können, sondern externe Interventionen der Netzleittechnik benötigen. Wie mir im Interview erläutert wurde:

»Eigentlich schalten die gar nicht bei den Leitstellen, die würden das halt einfach fließen lassen, die würden halt hoch- und runterregeln, und dann würde sich das alles schön verteilen. Aber weil da auf einmal so viel ist und hier so wenig, und der ganze Strom will dahin, dann müssen die sagen – nee Stopp, da darf jetzt aber keiner mehr durch, sonst ist unsere Leitung überlastet.« (Interview 3)

Das Versprechen einer größeren Sicherheit von erneuerbaren Energieträgern als »inherently resilient energy supplies« (Lovins und Lovins 1982, 264) scheint sich zumindest aus Sicht von Institutionen wie dem BBK und der Bundesnetzagentur gegenwärtig noch nicht erfüllt zu haben. Die veränderte Produktionsstruktur, die geographische Verteilung erneuerbarer Energieträger sowie deren Volatilität erzeugt Steuerungsprobleme und Netzinstabilitäten. Gleichzeitig hat sich das Steuerungsumfeld massiv verändert, weil die relevanten Ressourcen, Informationen und Kompetenzen nicht mehr bei den vertikal integrierten Großkonzernen liegen. Freilich



könnten Lovins und Lovins solchen Problematisierungen mit guten Gründen entgegenhalten, dass die Probleme letztlich dadurch entstehen, dass die neuen Energien aktuell in das Korsett eines überkommenen Energiesystems geschnürt werden. Die Energiewende ist mehr als die Ersetzung alter durch neue Energieträger, sondern ein großangelegter Strukturwandel, der sich vollziehen muss, ohne die kontinuierliche Stromversorgung der Wirtschaft und der Bevölkerung zeitweilig zu kompromittieren. Die Problematisierungen der Sicherheitsexpert\_innen betreffen so gesehen weniger die definitive Struktur eines neuen, erneuerbaren Energiesystems, sondern vielmehr die *Energiewende* als infrastrukturelles Interregnum. Noch ist unklar, wie das erneuerte Energiesystem letztlich aussehen wird und was getan werden kann, um mit den erhöhten Steuerungsproblemen fertig zu werden.

An Visionen hierfür mangelt es gleichwohl nicht.<sup>180</sup> Neben den verbesserten Speichertechnologien spielen vor allem neue, »intelligente« Steuerungstechnologien, die das Stromnetz zum *smart grid* machen sollen, eine große Rolle. Der Einsatz von Informationstechnologie – eines »Strom-Internets«, wie Jeremy Rifkin (2011, 66ff.) sich ausdrückt – soll es ermöglichen, das Netz nicht nur über die Angebotsseite, die durch erneuerbare Energien immer unberechenbarer und unkontrollierbar wird, sondern auch über die Nachfrageseite zu regulieren. Intelligente Messinstrumente,<sup>181</sup> sogenannte *smart meter* in Haushalten, die Signale vom Netz erhalten und ans Netz abgeben, sollen dafür sorgen, dass der Strom immer dann verbraucht wird, wenn viel bzw. zu viel davon vorhanden ist. Die Waschmaschine soll also dann laufen, wenn der Wind weht und viel Strom zur Verfügung steht. Das *smart grid* ist aber nicht nur eine technische, sondern vor allem eine marktwirtschaftliche Kontrollvision. Die Bundesnetzagentur argumentiert etwa, dass die Etablierung von *smart grids* mit der Konstruktion von *smart markets* einhergehen solle (BNetzA 2011c). Erst wenn der Strompreis abhängig vom Angebot variiert, besteht schließlich ein Anreiz für Konsument\_innen, Strom dann zu verbrauchen, wenn besonders viel davon verfügbar ist. Die technische Herausforderung, ein Gleichgewicht zwischen Stromproduktion und Verbrauch herzustellen und damit das Stromnetz stabil zu halten, soll durch die regulierenden Kräfte von Märkten angegangen werden, die vermeintlich am besten dazu in der Lage sind,

---

180 Für eine detailliertere Analyse der Integration erneuerbarer Energien in das Stromnetz als Sicherheitsprojekt siehe: Folkers (2017b, 43–51)

181 Zur Technopolitik des *metering* siehe: Marres (2012), Schnitzler (2013).

Angebot und Nachfrage zu equilibrieren. Zentrale Steuerung soll durch dezentrale Marktregulierung ersetzt werden. Die Normalisierung des Frequenzbereichs soll durch die normalisierende Macht von Märkten gewährleistet werden,<sup>182</sup> die durch den Einsatz von Informationstechnologien hervorgebracht werden können.<sup>183</sup>

Allerdings ist die Einführung von *smart grids* unter Sicherheitsgesichtspunkten keineswegs unumstritten. Während die Bundesnetzagentur (BNetzA 2007) vor allem die Chancen des *smart grids* für eine effiziente und sichere Systemsteuerung betont, hebt ein Bericht des BBK die Ambivalenz der forcierten Einführung von Informationstechnologien in das Stromsystem hervor:

»Einerseits wird also die Möglichkeit gesehen, die Verwundbarkeit mit Hilfe eines Smart Grids aufgrund von in Echtzeit abrufbaren Zustandsinformationen oder Steuerungsmöglichkeiten von Anlagen zu beherrschen bzw. zu minimieren. Allerdings steigt mit einer Implementierung solch komplexer Informations- und Kommunikationssysteme gleichzeitig die Verwundbarkeit gegenüber gezielten Angriffen auf diese Infrastruktur« (BBK 2014, 103f.).

Das *smart grid* ist aus dieser Perspektive nicht nur ein Mittel, um größere Sicherheit zu erzeugen, sondern zugleich ein potenzielles Sicherheitsproblem. Schließlich ist die Informationstechnologie als Kritische Infrastruktur ihrerseits ein Gegenstand der Sicherheitsbesorgnis. Wiederum zeigt sich also die Ambivalenz der informatorischen Kontrollrevolution.

### 3.3.4. Der *blackout* als »Verbundkatastrophe«

Auch wenn immer wieder das hohe Niveau der Sicherheit der Stromversorgung in Deutschland betont wird (siehe etwa: TAB 2011, 36, BBK 2014, 21), vermehren sich Befürchtungen, dass auf Grund der veränderten

182 Die Idee, dass Märkte eine normalisierende Funktion übernehmen können, hat eine lange Geschichte (Folkers 2014). Im Zuge der jüngsten Finanzkrise wurde diese Idee jedoch, wie gezeigt (Kapitel 2.4.4. und 2.5.5.), immer wieder kritisiert. Auch in einer jüngeren Untersuchung zum Strommarkt wird argumentiert: »[A]n adaptive power market may cause the opposite effect than intended: power fluctuations are not dampened but amplified instead.« (Krause, Boerries und Bornholdt 2013, 1).

183 Auf die technisch-wissenschaftlichen Voraussetzung für die »Konstruktion« von Märkten hat vor allem Michel Callon (1998c) immer wieder hingewiesen. Dabei hat er jedoch zu wenig betont, dass die Konstruktion von Märkten Teil eines umfassenden gouvernementalen Projekts ist, bei der Steuerungsfunktionen vom Staat auf – gezielt geschaffene – Märkte übertragen wird.

Rahmenbedingungen des Stromsystems »*künftig* die Ausfallwahrscheinlichkeit zunehmen wird« (TAB 2011, 64, Hervorhebung im Original), wie es in einem Bericht des Büros für Technikfolgenabschätzung im Bundestag heißt. Auch die Bundesnetzagentur (BNetzA) argumentiert, dass die verfügbaren Versorgungskapazitäten zwar im Normalfall ausreichen. Die Abnahme von Puffern und Reservekapazitäten durch den Atomausstieg erhöhe aber die Verwundbarkeit des Stromsystems gegenüber komplexen Schadenslagen (BNetzA 2011a, 1). In der Folge einer unglücklichen Verkettung von Umständen könnte es zu einem schwerwiegenden Stromausfall kommen. Vor allem in den Wintermonaten sei die Situation häufig »sehr angespannt« (BNetzA 2012, 10). Ähnlich betont auch das BBK, dass die Energiewende zwar an sich kein Grund für einen Stromausfall sei, aber doch eine Zunahme »neuralgischer Punkte« zu verzeichnen sei, die »ausschlaggebend für die Verwundbarkeit der Stromversorgung« (BBK 2014, 112) sein können. Während vor der Energiewende davon ausgegangen werden konnte, dass der Ausfall einer zentralen Struktur der Versorgung oder Übertragung »nur eine von mehreren Stufen einer ganzen Kaskade von Ereignissen sein« (BBK 2014, 113) könne, müsse man gegenwärtig davon ausgehen, dass »die Kritikalität eines Kraftwerkes oder einer Umspannungslage [...] im Fall einer angespannten Netzsituation sehr viel höher« (BBK 2014, 114) geworden ist. Kurz: Die Energiewende erhöht im Verbund mit der Liberalisierung in den Augen vieler Expert\_innen zumindest temporär die Verwundbarkeit des Stromsystems.

Diese Anspannung des Stromsystems hat die Besorgnis um einen Stromausfall, die spätestens seit einem schwerwiegenden Ausfall im Münsterland im Jahr 2005 auf der Agenda von Sicherheitsexpert\_innen und Bevölkerungsschützer\_innen steht, zusätzlich intensiviert. Eine ganze Reihe von Risikoanalysen und Handlungsanweisungen fokussiert mittlerweile auf das Problem des *blackouts* (ZöS 2008, BBK 2008b, BBK und IM-BaWü 2010, TAB 2011, BBK 2014). Während sporadische Stromausfälle dabei vor allem als Problem der Versorgungsqualität angesehen werden, ist es vor allem das Risiko eines sogenannten »lang anhaltenden und großflächigen Stromausfalls«, das als Katastrophe eingestuft wird und deshalb das Sicherheitsdispositiv der Resilienz aktiviert.<sup>184</sup> Die Definition einer Kata-

---

184 Die Formulierung »großflächig und langanhaltend« taucht in unterschiedlichen Variationen in allen auf Katastrophenschutz bezogenen Berichten zum Stromausfall auf. In einer Studie des BBK wird etwas genauer definiert, was darunter zu verstehen sein könnte bzw. ab wann ein Stromausfall ein Thema für den Bevölkerungsschutz wird: »Die Ver-

strophe über ihre räumliche Ausbreitung und zeitliche Dauer ist wie in Kapitel 2.3.1. bereits skizziert durchaus typisch für die Problemwahrnehmung des Bevölkerungsschutzes, der ja vor allem auf länderübergreifende Schadenslagen ausgerichtet ist. Die gesteigerte Aufmerksamkeit, die ein Stromausfall auf sich zieht, liegt aber nicht nur in seiner geographischen und zeitlichen, sondern vor allem in seiner funktionalen Ausbreitung. Der *blackout* gilt als »Verbundkatastrophe« (TAB 2011, 239), insofern er ein vitales Versorgungssystem betrifft, von dem eine Reihe anderer Kritischer Infrastrukturen in besonders hohem Maße abhängig ist. Er ist, wie BBK-Präsident Christoph Unger sich ausdrückt, ein »Paradebeispiel für kaskadierende Schadenswirkungen« (Unger, zitiert nach: TAB 2011, 35).

Das Ausmaß einer solchen Verbundkatastrophe macht ein Bericht des Büros für Technikfolgenabschätzung im Deutschen Bundestag mit dem Titel *Was bei einem Blackout passiert* deutlich (TAB 2011), der in vielerlei Hinsicht typisch für die Rationalitäten des Sicherheitsdispositivs der Resilienz ist. Der Bericht basiert auf einer »systematischen [...] Folgenanalyse« (TAB 2011, 38), fokussiert also von vornherein nur auf die Effekte und nicht die möglichen Ursachen oder relativen Wahrscheinlichkeiten eines »langdauernden und großräumigen Stromausfalls« (TAB 2011, 30f.). Die systematische Folgenanalyse rückt vor allem die Auswirkungen eines Stromausfalls auf Kritische Infrastruktursysteme in den Mittelpunkt. So wird zugleich ein spezifischer Interventionsrahmen abgesteckt: Die Folgenminderung eines *blackouts* soll durch Maßnahmen zur Verwundbarkeitsreduktion von Kritischen Infrastrukturen erreicht werden.

Der Bericht zeigt sehr anschaulich auf, wie sich ein Stromausfall auf die einzelnen Sektoren Kritischer Infrastrukturen auswirken könnte: Die nahezu ausnahmslos auf elektrischen Strom angewiesenen Informationsinfrastrukturen kollabieren – mit den entsprechenden Folgeschäden für die Bereiche, die ihrerseits auf Informations- und Telekommunikationstechnologien angewiesen sind (TAB 2011, 70–92). Im Straßenverkehr kommt es aufgrund von ausfallenden Ampelanlagen zu Störungen, während der Schienenverkehr ohnehin sofort zum Erliegen käme (TAB 2011, 93–120). Die Wasser- und Abwasserversorgung kann ohne den Einsatz elektrischer Pumpen nicht mehr ordnungsgemäß erfolgen (TAB 2011, 121–140). Die Infrastrukturen der Lebensmittelversorgung bekommen sowohl in der

---

meidung von Stromausfällen ab etwa der doppelten Größenordnung des Münsterland-Ereignisses 2005 (also 500.000 Betroffene) und für eine Dauer von mindestens drei Tagen kann zur Einordnung als Schutzziel formuliert werden.« (BBK 2014, 27)

Produktion als auch in der Distribution – etwa hinsichtlich der Aufrechterhaltung von Kühlketten – schnell große Probleme (TAB 2011, 141–153). Das Gesundheitswesen braucht elektrisch betriebene Medizintechnik, die für viele Patient\_innen unmittelbar überlebensnotwendig ist (TAB 2011, 154–166). Und schließlich ist das Finanzwesen vor allem deshalb betroffen, weil der elektronische Handel und Zahlungsverkehr auf funktionierende ITK angewiesen ist (TAB 2011, 167–186). Kurz:

»Die Folgeanalysen haben gezeigt, dass bereits nach wenigen Tagen im betroffenen Gebiet die flächendeckende und bedarfsgerechte Versorgung der Bevölkerung mit (lebens)notwendigen Gütern und Dienstleistungen nicht mehr sicherzustellen ist.« (TAB 2011, 30f.)

Dabei gilt: Je länger ein Stromausfall dauert, desto gravierender die Folgen. Entsprechend ist die Folgenanalyse entlang von Zeiteinheiten gegliedert – was passiert nach zwei Stunden, vier Stunden, 24 Stunden, nach einer Woche etc. – und macht so die temporale Entwicklung der »Katastrophe« sichtbar. Nicht das katastrophale zukünftige Ereignis, sondern die schrittweise Eskalation zur Katastrophe wird so zur operativen Temporalität der Regierung der Katastrophe. Während der Bericht die Frage der Wahrscheinlichkeit eines zukünftigen Stromausfalls weitgehend ausblendet, erhält der zeitliche Verlauf eines solchen potenziellen Ereignisses besondere Aufmerksamkeit. Das Intervall der Katastrophe und nicht der Horizont möglicher Ereignisse dominieren hier die temporale Dimension der Risikoanalyse (zur Unterscheidung von Horizont und Intervall der Katastrophe siehe: Adey und Anderson 2011). Dabei bildet dieses Intervall zugleich den Interventionsraum, in dem versucht werden kann, die Folgen eines Stromausfalls zu minimieren. Je schneller die Stromversorgung wieder zum Laufen gebracht werden kann und je schneller die Hilfe für unmittelbar bedrohte Teile der Bevölkerung anläuft, desto geringer werden die Schäden eines Ausfalls sein.

Die temporale Struktur der Risikowahrnehmung verweist dabei bereits auf eine spezifische Artikulation des Schutzziels. Dem Schutz der Elektrizitätsinfrastruktur geht es vornehmlich um die permanente Aufrechterhaltung des Stromflusses. Sicherheit heißt also Gewährleistung und Aufrechterhaltung von Zirkulation und *flows* und nicht so sehr schützende Einhegung substanzieller Güter. Diese Ausrichtung verändert auch die Bestimmung von Kritikalität im Stromsystem. So wird in einem Bericht zu Methoden der Risikoanalyse (BBK 2014) vorgeschlagen, Kritikalität mit Hilfe von Methoden aus dem sogenannten *Business Continuity Management*

bzw. der *Business Impact Analyse* zu evaluieren (siehe: BBK 2014, 71). Kritikalität wird damit weniger festen Strukturen, sondern vor allem Prozessen zugeschrieben, die für ein Unternehmen »systemwichtig« sind. Entsprechend soll auch bei der Analyse von Kritikalität im Stromsystem vorgegangen werden: Im Vordergrund stehen die »Prozesse« der Stromversorgung, nicht die fest installierten Elemente des Stromsystems. Das Stromsystem wird als eine Reihe miteinander zusammenhängender Prozesse kartiert.<sup>185</sup> Der Grad der Kritikalität der fokussierten Prozesse bestimmt sich dabei nach der Zeitdauer, die ein Prozess ausfallen kann, bis es zu einem Stromausfall kommt (BBK 2014, 73). Kritikalität kommt den physischen Elementen des Stromsystems nur dann zu, wenn sie für einen Prozess unerlässlich sind und nicht durch andere Elemente ersetzt werden können. Dieses Vorgehen bei der Kritikalitätsbestimmung reflektiert die Eigenschaften der Stromversorgung als Fließsystem. Nicht als Ansammlung von technischen Elementen und noch nicht einmal als angehäuften energetischen Potenzial – als *stock* –, sondern nur als *flow*, als beständiger Stromfluss, kann von einem »Zustand« der Versorgungssicherheit gesprochen werden.

### 3.3.5. Technologie der Resilienz und Resilienz der Technologie

Die Verhinderung der »Verbundkatastrophe« *blackout* ist ein Verbundprojekt einer Vielzahl staatlicher und privater Akteure. Im Stromsystem hängt Infrastruktursicherung zunächst einmal von privatwirtschaftlichen Akteuren ab, die gleichwohl vom Staat reguliert werden und gerade in Notfällen auf staatliche Unterstützung angewiesen sind. Von der linksalternativen Ökobewegung der 1970 und 1980er Jahre wurde dieser enge Zusammenhang von Staat und Stromkonzernen wie dargestellt als gefährliches Konglomerat des Atomstaats kritisiert. Verständlicherweise werden derartige Kooperationen von ihren Akteuren lieber als »Sicherheitspartnerschaften von Staat und Unternehmen« oder »Public Private Partnerships (PPP)« (BBK und IM-BaWü 2010, 11) bezeichnet. Diese »Partnerschaften« haben zum Teil einen losen, informellen Charakter und werden in erster Linie

---

<sup>185</sup> Die Kartierung der Abhängigkeiten erfolgt dabei charakteristischerweise mithilfe von *flow charts* (Flussdiagrammen). Die Kritikalitäts- bzw. Verwundbarkeitskartierung setzt also nicht – wie im anderen Verfahren des *vulnerability mapping* (siehe: Kapitel 2.3.) – auf geographische, sondern auf funktional-temporale Karten, sogenannte »Prozesslandkarten« (BSI 2008, 32). Siehe dazu ausführlich Kapitel 4.2.1.

durch gemeinsame Tagungen, Risikoanalysen oder Übungen kultiviert.<sup>186</sup> Daneben bestehen auch formale Regelungen, die Pflichten, Verantwortlichkeiten und Interventionsbefugnisse von Staat und Unternehmen festlegen. In kritischen Lagen kommt der Bundesnetzagentur (BNetzA) eine wichtige Rolle zu, die das Energiesicherungsgesetz (EnSiG) regelt (BBK 2014, 137).<sup>187</sup>

Zudem würde bei einem gravierenden Stromausfall das Krisenmanagement des Katastrophenschutzes mit seinen unterschiedlichen Trägern aktiviert – und zwar je nach Eskalationsgrad und territorialer Ausbreitung unter Koordinierung von Landes- oder Bundeseite. Staatliche Akteure kommen also operativ nur im Krisenfall zum Einsatz, sind aber regulativ ständig mit der Sicherung der Stromversorgung befasst. Diese verteilte Gouvernamentalität der Stromsicherung in Deutschland reflektiert die Tatsache, dass die Stromversorgung zwar einerseits eine ökonomische Funktion großer Versorgungsunternehmen darstellt, zugleich aber auch ein politischer Anspruch des Gewährleistungsstaates ist.

Freilich ist die Sicherung der Stromversorgung keine ganz neue Entwicklung, die erst im Zuge des Schutzes Kritischen Infrastrukturen etabliert worden wäre.

»Aber als man das Netz [...] aufgebaut hat, hat man ja schon sehr viel Wert auch auf Sicherheit und Stabilität gelegt. [...] Das hieß dann noch nicht Schutz kritischer Infrastrukturen, aber es war natürlich schon klar, wenn man [...] so ein großes Netz haben will, wo alles miteinander verbunden ist, dass man dann [...] gute Sicherheitsvorkehrungen braucht.« (Interview 3)

Dieser Befund wird auch von der Technikforschung zur Geschichte der Elektrifizierung (Hughes 1993) gestützt, die die starke Sicherheitsorientie-

186 Eines dieser Übungsforen ist die Länderübergreifende Krisenmanagement Übung (LÜKEX), bei der Akteure von Hilfsorganisationen, Bund, Ländern und Unternehmen im zweijährigen Rhythmus den Umgang mit jeweils ausgewählten Katastrophenszenarien üben. Gleich die erste dieser Übungen im Jahr 2004 hatte das Thema Stromausfall. Aus dieser Übung ist das Handbuch *Krisenmanagement Stromausfall* hervorgegangen (BBK und IM-BaWü 2010).

187 Das Energiesicherungsgesetz – nicht zu verwechseln mit dem Energiewirtschaftsgesetz (EnWG) –, das 1975 verabschiedet und seitdem mehrfach erweitert wurde, reagierte auf die Ölkrise der 1970er Jahre und ist deutlich von der Rationalität der Daseinsvorsorge getragen. Es sieht eine Reihe rechtlicher Regelungen und staatlicher Eingriffsbefugnisse vor, »[u]m die Deckung des lebenswichtigen Bedarfs an Energie für den Fall zu sichern, daß die Energieversorgung unmittelbar gefährdet oder gestört und die Gefährdung oder Störung der Energieversorgung nicht, nicht rechtzeitig oder nur mit unverhältnismäßigen Mitteln zu beheben ist« (EnSiG 1975, 1).

rung bereits im Kontext des Aufbaus der Stromnetze betont hat. Die großen Verteilerzentralen etwa, die im Zuge der Elektrifizierung seit Beginn des 20. Jahrhunderts entstanden sind, funktionieren als zentrale Überwachungs- und Sicherungseinrichtungen und sind zum Sinnbild eines neuen technischen Kontrollanspruchs geworden. Eine ganze Batterie von Sicherungsvorrichtungen ist so fest in der Technologie des Stromsystems verankert, dass die Unterscheidung zwischen Sicherungstechnik und normalem Betriebsmittel bisweilen nur schwer möglich ist. Gerade für die Stromversorgung trifft die Bemerkung Heideggers (2004, 20) zu, dass »Steuerung und Sicherung [...] die Hauptzüge« der modernen Technik sind. Allerdings ist dieser Zug nicht nur eine notwendige Folge technischer Imperative, sondern stets auch politisch motiviert. Die Sicherung der Technik wird schließlich auch deshalb so wichtig, weil der politische Anspruch auf Versorgungssicherheit stets technisch sichergestellt werden muss. Gerade bei der Stromversorgung wird deutlich, dass die Biopolitik vitaler Systeme als »politische Technologie« (Foucault 2005a) stets auf die Politik von technischen Artefakten (Winner 1980) angewiesen ist.

Dementsprechend müssen Sicherheitstechnologien durch Technologien der elektrischen Sicherung operieren, die ihrerseits stets politisch aufgeladen sind. Dabei lassen sich Techniken zur Verhinderung eines Stromausfalls durch Redundanzen und normalisierende Steuerungsmaßnahmen von Techniken der Resilienz unterscheiden, die nach einem Stromausfall dessen Folgen begrenzen. Schließlich finden sich auf der Ebene des operativen Katastrophenschutzes Maßnahmen des Krisenmanagements als Vorbereitung auf einen katastrophischen Stromausfall, die aber ebenfalls auf technologische Installationen angewiesen sind. Die grundlegendste Ausprägung der Sicherung des Stromsystems vor Ausfällen aller Art besteht in Redundanzen, die ermöglichen sollen, dass der Stromfluss auch dann aufrecht erhalten bleibt, wenn ein Element ausfällt. Es müssen Reservekapazitäten bestehen, die ausreichende Stromproduktion auch in angespannten Lastsituationen ermöglichen. Zudem braucht es Ausweichrouten für den Stromfluss, so dass sich dieser stets ungehindert verteilen kann. Das drückt sich in der sogenannten n-1-Regel aus, die gerade für Netzbetreiber von entscheidender Bedeutung ist. Es muss demnach stets gewährleistet sein, dass auch beim Ausfall eines Betriebsmittels die Stromversorgung weiterhin einwandfrei funktioniert (siehe dazu: BBK und IM-BaWü 2010).

Diese Redundanzen sind die technischen Grundvoraussetzungen für die Steuerungstätigkeit der ÜNB, die diese im Rahmen ihrer »Systemver-



antwortung« ausüben müssen. Die Steuerungstätigkeiten, die das Tagesgeschäft der ÜNB darstellen, lassen sich als Normalisierungsmaßnahmen verstehen. Ihr Ziel ist es, die Netzfrequenz bei den 50 Hertz zu halten, für die das europäische Verbundnetz ausgelegt ist. Sicherheitsprobleme entstehen aus schweren Normabweichungen: in Fällen von Unter- oder Überfrequenz. Bei Unterfrequenz ist die erzeugte Leistung kleiner als die Netzlast, wodurch die Frequenz unter 50 Hertz fällt, bei der Überfrequenz ist es umgekehrt. Bei Überfrequenz werden Kraftwerke vom Netz getrennt, was vor allem ökonomische und rechtliche Probleme erzeugt, weil die Kraftwerke nicht mehr den ÜNB gehören. Großflächige Ausfälle entstehen so jedoch für gewöhnlich nicht, auch wenn durch die erneuerbaren Energien tatsächlich die »Epidemie der Überproduktion« (Marx und Engels 1990, 468) als Steuerungsproblem ins Stromsystem Einzug gehalten hat. Die Unterfrequenz ist wesentlich problematischer. Zur Verhinderung einer Unterfrequenz müssen rechtzeitig Kraftwerke hochgefahren werden, die die Versorgungslücke füllen können. Das funktioniert zwar im Normalfall. Allerdings haben ÜNB und BNetzA schon seit dem Atommoratorium auf die Gefahr komplexer Szenarien hingewiesen, in denen die vorhandenen Versorgungskapazitäten nicht mehr ausreichen könnten (s.o.). In diesem Rahmen sind Forderungen laut geworden, Reservekraftwerke zu betreiben, die im Notfall in Betrieb genommen werden können. So hat die BNetzA schon 2011 gefordert, ein Atomkraftwerk als Reservekraftwerk weiter zu betreiben (BNetzA 2011a), was politisch auf Grund der breiten Ablehnung der Atomkraft freilich nicht unumstritten ist. Ebenso umstritten ist die 2015 tatsächlich erfolgte Vereinbarung zwischen Bundeswirtschaftsministerium und Betreibern von alten Braunkohlekraftwerken. Letztere sollen diese in »Sicherheitsbereitschaft« halten, um »die Versorgungssicherheit in länger andauernden Ausnahmesituationen sicherzustellen« (Bundesregierung 2015, 6).<sup>188</sup>

Sollten die Reserven jedoch nicht ausreichend und zur richtigen Zeit zur Verfügung stehen, bliebe nur noch die Option des »Lastabwurfs«, also der Trennung von Stromverbraucher\_innen vom Netz. Dieser Lastabwurf

---

188 Im Gegenzug erhalten die Braunkohlegesellschaften für diese voraussichtlich nie notwendig werdende Bereitschaft Entschädigungen in Milliardenhöhe. Während die Bundesregierung diesen Schritt als wichtigen Meilenstein im Klimaschutz versteht (Bundesregierung 2015, 2), kritisiert etwa der BUND das »Geschenk an die Kohlekonzerne« (siehe: Kreuzfeldt 2015). Zudem kann an der Leistungsfähigkeit der Sicherheitsbereitschaft gezweifelt werden. Zehn Tage würde ein Kraftwerk benötigen, um betriebsbereit zu sein (Bundesregierung 2015, 6).

erfolgt in fünf Stufen (BBK 2014, 95), die klar durch den sogenannten *Transmission Code* der Übertragungsnetzbetreiber geregelt sind (siehe: VDN 2007). Der Abwurf ist keine aktive Steuerungsleistung der ÜNB, sondern ein in die Netzinfrastruktur eingebauter Sicherheitsmechanismus, der mit der Überstromschutzeinrichtung (»Sicherung«) im Haushalt vergleichbar ist, nur dass die »Sicherung« hier als »Schutzrelais« bezeichnet wird und die Unterbrechung des Stromkreises nicht bei zu viel, sondern bei zu wenig Netzspannung erfolgt (BBK 2014, 95). Die zunehmende Denormalisierung der Netzspannung triggert also einen automatischen Normalisierungsmechanismus, den Lastabwurf. Stufe fünf des Plans sieht dann eine Abtrennung der Kraftwerke vom Netz vor, um Kraftwerksstrukturen wie Turbinen zu schützen, die bei zu starkem Frequenzabfall Schaden nehmen könnten (BBK 2014, 97). Der Stromausfall würde letztlich durch eine technische Sicherheitsvorrichtung ausgelöst. Allerdings wird dieser Vorgang bewusst in Kauf genommen. Denn nur durch eine kontrollierte Abschaltung kann der Betrieb nach einem Ausfall schnell wieder aufgenommen und mithin verhindert werden, dass ein *blackout* lange andauert und zur Katastrophe wird.

Während n-1-Redundanz, Netzsteuerung und Lastmanagement und selbst Reservekraftwerke für Ausnahmefälle noch als Maßnahmen zur Normalisierung des Stromsystems – also zur Frequenzhaltung durch Gleichgewicht von Last und Leistung – angesehen werden können, gehorcht die stufenweise Abschaltung des Stromnetzes dem normativen Regime der Resilienz.<sup>189</sup> Die Schutzrelais gleichen Sollbruchstellen in der Strominfrastruktur, die es dem System ermöglichen sollen, auf eine Weise auszufallen, die eine schnelle Rückkehr in den Normalbetrieb ermöglicht – »falling gracefully« (Lovins und Lovins 1982, 264) ist hier die Devise. Damit das System jedoch nicht nur elegant und kontrolliert fällt, sondern auch schnell und effizient wieder aufstehen kann, also seine »bounciness« (Lovins und Lovins 1982, 181) gewährleistet ist, bedarf es einer weiteren wichtigen Komponente: der sogenannten Schwarzstartfähigkeit.

---

189 Auch in Leitungsredundanzen und Reservekraftwerkskapazitäten können Maßnahmen der Resilienzsteigerung durch Puffer und Systemdesign gesehen werden, insofern sie weniger auf die generelle Verhinderung externer Störungsereignisse (etwa die physische Zerstörung einer Leitung) zielen, sondern auf die Steigerung interner Widerstandskräfte gegenüber diesen Ereignissen. In diesem Zusammenhang macht es aber Sinn, zwischen Maßnahmen zur Verhinderung des Systemereignisses Stromausfall und solchen zur Reaktion auf einen Ausfall zu unterscheiden.

»Schwarzstartfähigkeit [...] stärkt die »Resilienz« des Gesamtsystems. Sie stellt einen Schutzmechanismus dar, der greift, wenn es bereits zum Ausfall einer Struktur bzw. eines Prozesses und in der Folge zu einem Stromausfall gekommen ist. Durch Schwarzstartfähigkeit kann vermieden werden, dass dieser sich zu einem langdauernden Ausfall entwickelt.« (BBK 2014, 94)

Die meisten Kraftwerke brauchen ihrerseits Strom, um Strom produzieren zu können. Ist das *perpetuum mobile* der Elektrizitätsversorgung einmal unterbrochen, ist es also gar nicht so einfach, den Betrieb wieder in Gang zu bringen. Benötigt werden deshalb Kraftwerke, die ohne Strom in Betrieb genommen werden können (»Schwarzstart«), um den übrigen Kraftwerken im Netzbereich Starthilfe geben zu können. Das Problem ist allerdings, dass gar nicht klar ist, welche Kraftwerke im Netz tatsächlich schwarzstartfähig sind, welche Zuständigkeiten herrschen und wie im Fall der Fälle genau vorgegangen werden müsste. Im Bericht des BBK zum Projekt GRASB heißt es ernüchtert, dass es »nicht möglich [war], die tatsächlich vorhandene Schwarzstartfähigkeit und die nach einem großflächigen Stromausfall benötigte Schwarzstartfähigkeit in Erfahrung zu bringen und zu bewerten.« (BBK 2014, 94) Das liegt zum einen daran, dass Stromausfälle, die einen Schwarzstart notwendig machen, so selten vorkommen, dass nur geringe Erfahrungswerte vorliegen. Zum anderen bereitet die mit der Entflechtung einhergehende Ordnung der Verantwortlichkeiten Probleme. So haben die ÜNB als Systemverantwortliche, die das Netz durch Schwarzstarte wieder zum Laufen bringen müssten, keine ausreichende Information über die Kraftwerke, die von wieder anderen Unternehmen betrieben werden. Im Krisenfall müsste es ein zentrales Krisenmanagement geben, was aber aufgrund der entflochtenen Strukturen im Stromsystem nicht mehr ohne weiteres möglich ist. In einem Interview schilderte eine Expertin für die Sicherheit der Stromversorgung beim BBK die Probleme, die in Bezug auf die Schwarzstartfähigkeit entstehen:

»Dann ist die Frage, wer ist denn dafür zuständig, dass es schwarzstartfähige Kraftwerke gibt. Also Wasserkraft ist zum Beispiel schwarzstartfähig. [...] Aber wer ist denn dafür zuständig, dass es das gibt? Das sind die Übertragungsnetzbetreiber, denen die Kraftwerke aber nicht gehören. [...] Aber ob du jetzt in einem kleineren Gebiet [...] ein schwarzstartfähiges Kraftwerk hast, das wissen die Leute selber nicht. Das kann man sie [die Kraftwerksbetreiber] fragen, dann sagen die: Ja, wir schätzen, dass das gehen würde. Ja, wir würden das ausprobieren. Wenn jetzt [...] der Krisenstab mir sagt, versuche dein Kraftwerk hochzufahren, dann würde ich das machen [...] Und dann würde ich später mit dem Übertragungsnetzbetreiber klären, wer das denn jetzt zahlt.« (Interview 3)

Während der schnelle Wiederaufbau der Stromversorgung mit Hilfe schwarzstartfähiger Kraftwerke vor allem die zeitliche Dauer eines Stromausfalls vermindern würde, sind sogenannte Inselösungen eine Vorrichtung zur räumlichen Begrenzung eines Ausfalls. Dabei gibt es unterschiedliche Inselmodelle, die im Prinzip jedoch alle vorsehen, dass Teile des Stromsystems unabhängig weiter operieren, auch wenn große Teile des Systems bereits schwarzgefallen sind. So können einige Großkraftwerke im Inselbetrieb weiterbetrieben werden, ohne Strom ins Netz einzuspeisen, wodurch der Schwarzstart von Kraftwerken überflüssig würde (siehe: BBK 2014, 98). Darüber hinaus können auch größere Netzteile als Inseln weiter funktionieren, wenn es in anderen Bereichen des Netzes bereits zu einem Ausfall gekommen ist, »sodass die Ausbreitung von kaskadenartigen Stromausfällen begrenzt wird« (BBK 2014, 101).

Aus der Sicht des Schutzes Kritischer Infrastrukturen ist das ein attraktives Modell. Ein Ausfall könnte so räumlich begrenzt werden oder es könnten zumindest einzelne Kritische Infrastrukturen – wie zum Beispiel Krankenhäuser – weiter betrieben werden und damit die Notfallmaßnahmen, die bei einem Stromausfall notwendig wären, erleichtern. So schlägt das Büro für Technikfolgenabschätzung des Bundestages Inselösungen für Kritische Infrastrukturen vor, um vitale gesellschaftliche Funktionen zu schützen (TAB 2011, 29f.).

Tatsächlich würde hier die Dezentralisierung der Netze mit einer gesteigerten Resilienz des Stromsystems einhergehen. Gegen den Betrieb von Inselnetzen spricht jedoch die größere Leichtigkeit der zentralen Steuerung von großen Netzen. Im Normalbetrieb fällt die Stabilisierung eines großen Netzes schlicht leichter, weil sich der Strom über eine größere Fläche selbstständig verteilen kann und auf diese Weise dem Entstehen von Ungleichgewichten vorbeugt.

»Und diese Inseln bringen halt verschiedene Probleme mit sich [...]. Deswegen ist das [...] nicht unbedingt von jedem gewollt. Und natürlich ist es insgesamt viel effizienter, wenn ich ein großes Netz habe, in dem sich alles halt verteilen kann, weil ich dann eben nicht für jeden einzelnen Standort regulieren muss, dass das passt, sondern das eben in diesem großen Bereich machen kann.« (Interview 3)

Die »Inselösung« scheint also vor allem deshalb unattraktiv, weil es dem von den ÜNB und der BNetzA favorisiertem Modell möglichst effizienter Netzsteuerung widerspricht. Hier stehen die Sicherheitsansprüche des Katastrophenschutzes, der Maßnahmen gegen sehr seltene Großausfälle der Stromversorgung zu treffen versucht, der Effizienzorientierung der

Netzsteuerung gegenüber. Dahinter verbirgt sich zugleich ein Konflikt zwischen der Normalisierung des Stromnetzes durch alltägliches Lastmanagement und dem Aufbau von Resilienz gegenüber Stromausfällen. Die Schwierigkeit, beide Sicherheitsansprüche gleichermaßen zu befriedigen, liegt nicht zuletzt darin, dass die Technologien der Normalisierung und der Resilienz jeweils an unterschiedliche technische Systemdesigns gekoppelt sind, die tief in der technischen Infrastruktur des Stromnetzes verankert sind bzw. verankert werden müssten.

Der Bevölkerungsschutz stößt an diesem Punkt an seine Grenzen, weil er keine Möglichkeiten hat, auf die technische Ausstattung des Stromsystems substanziell Einfluss zu nehmen. Ihm bleibt zumeist nur, Akteure zu sensibilisieren, sie zu »vernetzen«, Nachfragen zu stellen und Einschätzungen über Gefährdungen und Verwundbarkeiten des Stromsystems abzugeben. Damit kann er allerdings nur dazu beitragen, das Risiko eines langfristigen und großflächigen Stromausfalls überhaupt auf die ohnehin überfrachtete Agenda deutscher Energiepolitik zu setzen. Katastrophenschutz besteht deshalb vor allem in der vorbereitenden Planung für ein effizientes Krisenmanagement nach einem bereits erfolgten Großausfall der Stromversorgung (siehe dazu: BBK 2008b, BBK und IM-BaWü 2010). So stellt das BBK Informationen und Anleitungen zu Möglichkeiten der Notstromversorgung in Behörden und wichtigen Infrastruktureinrichtungen zur Verfügung (BBK 2008b). Dabei können die betreffenden Institutionen zwischen zwei Modellen wählen: der Unterbrechungsfreien Stromversorgung und Notstromaggregaten bzw. Netzersatzanlagen. Erstere können eine schnelle, kurze Überbrückung für temporäre Ausfälle bereitstellen. Sie sind deshalb für den Schutz technischer Systeme geeignet, die unbedingt auf eine kontinuierliche Stromversorgung angewiesen sind. Im Gegensatz dazu benötigen Netzersatzanlagen eine gewisse Zeit, um nach einem Ausfall Strom zu liefern. Dafür sind sie dann länger betriebsfähig (siehe: BBK 2008b, 6). Welche Variante gewählt und in welchem Umfang diese installiert wird, soll in Abhängigkeit von der »Identifikation geschäftskritischer Prozesse« (BBK 2008b, 7) erfolgen.

Allerdings bietet auch eine solche Notstromversorgung nur eine zeitlich begrenzte Lösung, die vor allem von der Verfügbarkeit von ausreichendem Treibstoff abhängt, weil die entsprechenden Generatoren zumeist mit Diesel betrieben werden (zum Anlegen von Kraftstoffreserven siehe: BBK 2008b, 10). Käme es zu einem langfristigen Stromausfall, könnte hier der Bund aushelfen, der über eine strategische Erdöl- und Treibstoffreserve

verfügt, die ursprünglich zur Überbrückung von Rohstoffknappheit in geopolitischen Krisensituationen angelegt wurde. Laut Erdölbevorratungsgesetz muss stets eine für 90 Tage ausgelegte Treibstoffreserve vorgehalten werden. Wenn derartige Lager heute wie ein aus der Zeit gefallenes Relikt des Kalten Krieges wirken, dann liegt das sicher auch daran, dass sich in den letzten Jahrzehnten ein neues Versorgungsregime etabliert hat, das weniger auf der Vorhaltung von festen Beständen basiert, sondern vielmehr auf dem ständigen Fluss von Waren, Gütern, Treibstoffen, Informationen etc. Die alten Lager haben sich in der »flüssigen Moderne« (Bauman 2000) aufgelöst. Sie sind zum *flow*, zum »Strom« geworden. Aber gerade aufgrund dieser »allgemein reduzierte[n] Vorratshaltung sowie einer ausgefeilten Just-in-time-Logistik« (TAB 2011, 221) haben Unterbrechungen im Versorgungsstrom immer gravierendere Folgen. Das zeigt sich im Fall des Stromsystems schon deshalb besonders deutlich, weil hier die Notwendigkeit, den Stromfluss kontinuierlich aufrechtzuerhalten, nicht zuletzt aus der technischen Unmöglichkeit erwächst, Strom zu speichern und als Ressource vorzuhalten. Die sozio-technischen Systeme, von denen das Leben der Bevölkerung abhängt, hängen nicht nur am Draht des Stromnetzes, sie müssen buchstäblich permanent unter Strom stehen, um zu funktionieren. Deshalb ist der Stromausfall ein so gravierendes Sicherheitsproblem gegenwärtiger Gesellschaften. Sicherheit besteht hier nicht nur negativ in der Abwesenheit von Gefahr. »Versorgungssicherheit« ist eine positive Form der Sicherheit, die gerade die beständige *Anwesenheit* von substanziellen Infrastrukturleistungen beinhaltet. Gerade die Abwesenheit von Strom ist mithin die Gefahr, die die Sorge von Sicherheitsexpert\_innen, Netzverantwortlichen und Bevölkerungsschützer\_innen bindet. Nur vor dem Hintergrund dieses Anwesenheitsregimes<sup>190</sup> können alltägliche Wetterphänomene wie Windstille oder ein wolkiger Himmel zu einem Sicherheitsproblem werden.

---

190 Für Martin Heidegger stellt dieses Verständnis des Seins als Anwesenheit das grundlegende Verhängnis moderner Metaphysik dar (siehe bereits: Heidegger 2006). Die moderne Technik ist für Heidegger (2004, 9–40) die Fortsetzung der Metaphysik, indem sie Sein als Bestand und damit wiederum als Anwesenheit, also als permanente Verfügbarkeit energetischer Ressourcen auslegt und diese Seinsauslegung mithilfe der modernen Maschinenteknik praktisch umsetzt. Sicherheit ist in diesem Sinne Bestandssicherung, aber auch Grundsicherung, weil mit der Sicherung des Bestandes zugleich »der Grund« (Heidegger 1957), also das Sein als permanente Anwesenheit, sichergestellt wird. Sicherheitsdispositive haben in diesem Sinne eine geradezu metaphysische Funktion. Siehe dazu ausführlich: Folkers (2017b).

Dass nun genau diese positive Gewährleistung der Versorgungssicherheit Prozesse in Gang setzt (Atomstrom, fossile Brennstoffe), die ihrerseits massive Sicherheitsprobleme für die menschliche Gesundheit und die Umwelt darstellen, macht »Energiesicherheit« zu einem so komplexen Problemfeld. Heute sind die vielfältigen Sicherheitsprobleme, die im Zusammenhang mit der Energieversorgung stehen – Umweltschutz, Versorgungssicherheit, geopolitische Abhängigkeiten, Risiken von Störfällen in Kernkraftwerken etc. – alle gleichermaßen präsent, auch wenn sie gewiss nicht gleichmäßig gewichtet werden. Historisch haben sich diese Problemfelder wie gezeigt aber erst sukzessive herausgebildet. Dabei haben neue Problematisierungen jeweils versucht, die selektiven Rahmungen bisheriger Artikulationen der Energiesicherheit sichtbar zu machen, um so deren Externalitäten als eigenständiges Problemfeld zu konstituieren. So hat Jungk kritisiert, dass die Art und Weise, mit der der Atomstaat auf die Risiken der Kernkraft reagiert, die Freiheit der Bürger\_innen und die Demokratie gefährdet und so die Risiken der Atomkraft durch die des Atomstaats verdoppelt (3.3.1.). Amory und Hunter Lovins haben demgegenüber die blinden Flecken der vorwiegend geostrategisch motivierten Reaktion der US-Regierung auf die Ölkrise in den Blick genommen. Sie haben gezeigt, dass der eingeschlagene harte Weg der Energieversorgung das Problem der Energiesicherheit verschärft, anstatt es zu lösen. Als Alternative dazu haben sie für einen sanftes, dezentrales und dadurch resilientes Energiesystem plädiert, das sowohl Ansprüchen nationaler Sicherheit wie auch denen des Umweltschutzes gerecht werden sollte (3.3.2.). Die deutsche Energiewende ist eine Reaktion auf die Risiken der Kernkraft und soll zugleich im Dienste des Klimaschutzes stehen. Der Umstieg auf erneuerbare Energien hat im Verbund mit der Neuordnung der Verantwortlichkeitsstrukturen des Stromsystems im Zuge der Liberalisierung aber auch neue Sicherheitsprobleme erzeugt. Netzbetreiber und Schützer\_innen Kritischer Infrastrukturen problematisieren die gesteigerten Instabilitäten des Stromnetzes durch den erhöhten Anteil volatiler Energien, die nur unter großem Aufwand reguliert werden können (3.3.3.) und deshalb die Wahrscheinlichkeit von Stromausfällen erhöhen (3.3.4.). Während die ÜNB und die BNetzA auf Lösungen setzen, welche die Effizienz der Steuerung des Stromsystems im Normalbetrieb erhöhen, fordern Katastrophenschützer Maßnahmen, die verhindern sollen, dass ein Stromausfall langanhaltend und großflächig und dadurch zur unbeherrschbaren Katastrophe wird (3.3.5.). Gerade auf Grund dieser Komplexität ist das viel-

schichtige Feld der Energiesicherheit so charakteristisch für die gegenwärtige Biopolitik vitaler Systeme. Sicherheit bewegt sich in einem diffizilen Kraftfeld zwischen Techno- und Ökosphäre, das von staatlichen ebenso wie von privatwirtschaftlichen Akteuren bevölkert ist, die versuchen, mit sichernden Techniken die Sicherheit der Technik zu gewährleisten.

### Exkurs zur Biopolitik: Politik des Lebens jenseits seiner selbst

Von der Daseinsvorsorge zum Schutz Kritischer Infrastrukturen, von der Großen zur Grünen Infrastruktur, vom Atomstaat zur Energiewende: Die Übergänge, die ich in diesem Kapitel skizziert habe, stehen jeweils exemplarisch für eine gleichzeitige Bewegung des Reflexiv-Werdens und der Ausweitung der Biopolitik vitaler Systeme. In dem Maße, in dem Abhängigkeiten und Problemkomplexe bewusst geworden sind, die zuvor von den operativen Sicherheitstechnologien übersehen wurden, wurden diese Probleme zu Gegenstandsbereichen des neuen Sicherheitsdispositivs der Resilienz. Bloß implizite Zusammenhänge wurden expliziert und zu neuen Interventionsoberflächen von Sicherheitstechnologien ausgefaltet: Interdependenzen und endogene Risiken von Infrastruktursystemen, Externalitäten von Energiesystemen, Verwundbarkeiten des Erdsystems. Diese Ausweitungen und Verschiebungen stehen dabei in einem engen Zusammenhang mit dem Aufkommen des ökologischen Denkens in Wissenschaft und Politik. Zum einen hat sich eine bestimmte Art der Umweltforschung überhaupt erst als Folge einer Reihe von Umweltkatastrophen gebildet. Zum anderen hat das ökologische Denken neue Horizonte für Sicherheitstechnologien eröffnet und zugleich deren Stil verschoben: weg von der technokratischen Planung, hin zu flexiblen bzw. resilienten ökologischen Designs.

Ökologische Kritiken der infrastrukturellen Großtechnik haben den biopolitischen Horizont, das Milieu bzw. die »Umwelt« der Biopolitik grundlegend verändert. Ja, sie haben vielleicht sogar das, was wir heute so routiniert als »Umwelt« bezeichnen – eine verwundbare Umwelt, die uns als Lebensgrundlage dient, zugleich von uns bedroht ist und geschützt werden muss – überhaupt erst als Problem der Politik und Zielscheibe der Sicherheitsdispositive erzeugt. Eine Reihe eindrucksvoller Studien hat gezeigt, dass und wie die verletzte und zugleich potenziell verletzende Umwelt



als Problem des Regierens und Gegenstand der Wissenschaft erst seit der zweiten Hälfte des 20. Jahrhunderts durch eine Reihe von industriell-technischen Katastrophen und Krisen zutage getreten ist: die Atombombenabwürfe des US-amerikanischen Militärs und die Forschungen zum »nuklearen Winter« (Masco 2010), die Katastrophen von Bhopal (Fortun 2001) und Tschernobyl (Petryna 2002), die anhaltende Luftverschmutzung in chinesischen Megastädten wie Hong Kong (Choy 2011) und schließlich die Explosion der *deepwater horizon* im Golf von Mexico (Bond 2013). Diese Liste ließe sich noch beträchtlich erweitern. Jede neue Krise hat ein weiteres Stück unserer – materiellen, biologischen, nicht bloß symbolisch-sozialen – Lebenswelt, die bisher als selbstverständlicher Hintergrund betrachtet werden konnte, aus ihrem Schattendasein heraus zum Gegenstand der Sorge, zum *matter of concern* werden lassen:<sup>191</sup> das Ozonloch offenbarte die Abhängigkeit des Lebens von Atmosphären, das Abschmelzen des antarktischen Eises hat auf die Bedeutung der Kryosphäre aufmerksam gemacht, der *BP-oil spill* auf das Ökosystem der Tiefsee etc. Dabei ist »die Umwelt« von vorherein ein hybrides Terrain, das nichts von der Reinheit der »Natur« der Modernen, die nie modern gewesen sind, an sich hat (Latour 2001a, 88). So kann die Umwelt überhaupt nur durch eine Reihe komplexer wissenschaftlicher Apparaturen und Infrastrukturen in Erscheinung treten (siehe dazu u.a.: Edwards 2010). Vor allem aber wird die natürliche Umwelt erst durch ihre technische Beeinträchtigung sichtbar. Hans Jonas (1989, 26f.) bemerkte bereits Ende der 1970er Jahre, dass

»die kritische Verletzlichkeit der Natur [bzw. der Umwelt] durch die technische Intervention des Menschen [hervorgetreten ist] – eine Verletzlichkeit, die nicht vermutet war, bevor sie sich in schon angerichtetem Schaden zu erkennen gab. Diese Entdeckung, deren Schock zu dem Begriff und der beginnenden Wissenschaft der Umweltforschung (Ökologie) führte, verändert die ganze Vorstellung unserer selbst als eines kausalen Faktors im weiteren System der Dinge. Sie bringt durch die Wirkungen an den Tag [...], daß ein Gegenstand von gänzlich neuer

---

191 Tatsächlich legt die ökologische Problematik die Revisionsbedürftigkeit des phänomenologischen Lebenswelt-Konzepts nahe. Die »Kolonisierung der Lebenswelt« (Habermas 1981) besteht nicht nur, wie Habermas meinte, im Vordringen systemischer Integrationsmechanismen in den Bereich symbolisch-kommunikativer Sozialintegration. Vielmehr geht es um die Integrität des vital-materiellen Substrats gesellschaftlicher Vollzüge. Die »Krisis der europäischen Wissenschaften« (Husserl 1982) besteht nicht nur im Vergessen ihrer Grundlage in einer bestimmten kulturellen Lebensform, sondern auch in den Effekten der Technowissenschaft, die sich zerstörerisch auf die materiellen Bedingungen der kulturellen Grundlagen auswirken.

Ordnung, nicht weniger als die gesamte Biosphäre des Planeten, dem hinzugefügt worden ist, wofür wir verantwortlich sein müssen, weil wir Macht darüber haben.«

Allerdings ist diese »Umwelt« im uns mittlerweile vertrauten Sinn als verwundbare und schützenswerte Entität keineswegs die erste und einzige räumlich-ökologische Problematik, die im Rahmen moderner biopolitischer Sicherheitsdispositive aufgetreten ist. Vielmehr modifiziert und ergänzt »die Umwelt« eine Reihe anderer Milieuformationen, die bereits wesentlich früher als Interventionsorte und Problemräume der Sicherheitsdispositive entstanden sind. Fokussiert man auf das Auftreten ökologischer Problematiken innerhalb biopolitischer Sicherheitsdispositive, werden die genealogischen Vorläufer der heutigen Umwelt sichtbar. Es zeigt sich, dass die Umweltpolitiken unserer Tage gegenüber der von Foucault beschriebenen Biopolitik keinen grundlegenden Bruch darstellen. Vielmehr entwickeln sich diese Politiken von vornherein auf biopolitischem Terrain,<sup>192</sup> wobei sie dieses Terrain zugleich erweitern und modifizieren. Während die Biopolitik der Bevölkerung bzw. das Sicherheitsdispositiv der Normalisierung vor allem auf die Regulation eines *historisch-natürlichen Milieus* zielt, liegt der Einsatzpunkt der Biopolitik vitaler Systeme und des Sicherheitsdispositivs der Resilienz dort, wo sich die Aufmerksamkeit verstärkt auf *sozio-technische* und *öko-technische* Milieus richtet.

Foucault hatte gezeigt, wie Ende des 18. und zu Beginn des 19. Jahrhunderts im Zusammenhang mit einer Reihe urbaner Sicherheitsprobleme – »Pauperismus«, Hygieneprobleme, verheerende Stadtbrände, ansteckende Krankheiten – der »Begriff eines historisch-natürlichen Milieus als Zielscheibe einer Machtintervention zutage [getreten ist]« (Foucault 2004, 42). Gerade die Cholera, die Anfang des 19. Jahrhunderts in europäischen Städten wütete, wurde zum paradigmatischen Problem, das zur Herausbildung eines neuen sozial-ökologischen Wissens des Milieus führte (Rabinow

---

192 Die mangelnde historische Einbettung in die Geschichte der Biopolitik ist eine entscheidende Leerstelle in jüngeren Debatten, die mit anspielungsreichen Konzepten wie Kosmopolitik (Stengers 2008, 153–185, Latour 2013) oder Geopolitik (Yusoff 2013, Dalby 2017) versuchen, die Transformation des Politischen im Zuge der Ökologisierung zu theoretisieren. So wird hier diagnostiziert, dass es im Angesicht von Problemen wie dem Klimawandel zu vollkommen neuartigen Vermischung von Natur und Politik gekommen sei, die tatsächlich jedoch schon seit dem »Eintritt des Lebens« (Foucault 1977, 169) in die Politik bestehen. Das heißt nicht, dass mit Foucaults Beschreibung der Biopolitik des 19. Jahrhunderts schon alles gesagt ist. Vielmehr gilt es, seine historischen Diagnosen aufzugreifen und so zu erweitern, dass sie die Verschiebungen der Biopolitik durch ökologische Fragen wie den Klimawandel fassen können.

1995, 30–39).<sup>193</sup> So begann die Medizin in Reaktion auf die Cholera die vielfältigen Beziehungen zwischen Hygiene, sozialen Verhältnissen und natürlichen Faktoren, die zur Ausbreitung der Krankheit führten, zu analysieren. Dieses »historisch-natürliche Milieu« war der Interventionsraum des damals entstehenden Sicherheitsdispositivs und unterschied sich grundlegend vom Raum der Disziplin wie auch vom Territorium der Souveränität (siehe dazu bereits Kapitel 1.3.). »Historisch-natürlich« war dieses Milieu, weil hier historisch gewachsene urbane Strukturen und natürliche Gegebenheiten zusammenkommen und miteinander interagieren. Die Regierung kann diese Wechselwirkungen gerade dann vorteilhaft gestalten, wenn sie die inneren Gesetzmäßigkeiten der natürlichen Phänomene anerkennt und nicht gegen sie, sondern mit ihnen agiert. Das historische-natürliche Milieu ist dadurch zum Interventionsort einer Vielzahl von biopolitischen Regierungsinterventionen geworden. So versuchte etwa eine »Medizin der Dinge« (Foucault 2003, 291) durch verbesserte Hygieneinfrastrukturen die Ausbreitung ansteckender Krankheiten zu verhindern. Eine »soziale Ökonomie« (siehe: Ewald 1993, 115) nahm sich vor, durch Verbesserung der Wohnverhältnisse das soziale Elend der arbeitenden Bevölkerung zu lindern. Ewald (1993, 115) sieht in diesen Problemen des städtischen Milieus die »Geburt einer problematischen Beziehung des Menschen zur Umwelt, zum Raum, einer ökologischen Problematik«. Aber nicht nur die problematische Beziehung des Menschen zum Raum ähnelt der ökologischen Problematik der Gegenwart. Auch die problematische Beziehung zu den eigenen Immunisierungssystemen verbindet die urbane mit der planetarischen Sicherheitsproblematik der Gegenwart. Die Stadt war schließlich immer das, was vor den Zumutungen der unzivilisierten Natur schützen sollte (Jonas 1989, 20f.). Im Zuge des Wachstums der Städte im Rahmen der Industrialisierung wurde plötzlich der städtische Schutzraum selbst zu einem Bedrohungszusammenhang. Die Zusammenballung von Menschenmassen auf engem Raum, industrielle Produktion, Kriminalität, ansteckende Krankheiten etc. machten die Stadt zu einem Gefährdungszusammenhang, den die Gesellschaft nicht mehr fremden, natürlichen Mächten zuschreiben konnte, sondern auf ihre eigenen Strukturen beziehen musste.

Paul Rabinow, der den von Foucault gelegten Faden aufgenommen hat, diagnostiziert eine Zäsur im Milieudenken nach dem Ende des Ersten

---

193 Siehe allgemein zur Geschichte des Milieubegriffs in den Naturwissenschaften des 19. und beginnenden 20. Jahrhunderts: Canguilhem (2008, 98–120).

Weltkriegs und identifiziert die Emergenz eines neuen Problemraums, den er als »socio-technical milieu« (Rabinow 1995, 13) bezeichnet. Dessen Anwendungsbereich war nunmehr die gesamte »Gesellschaft«, die als autonome Instanz aufgerufen wurde und technisch bzw. technokratisch gestaltet werden sollte, ohne von Natur und Geschichte eingeschränkt zu sein.<sup>194</sup> Das technokratisch-kybernetische Ideal dieses Milieus war das »closed system« (Hughes 1987, 53). Insbesondere die beiden Weltkriege und die ständige Besorgnis um ein »Heiß-werden« des Kalten Krieges haben die Abhängigkeit des Lebens der Bevölkerung von sozio-technischen Netzwerken gezeigt, die man nach dem Ende des Zweiten Weltkriegs zunehmend als Infrastrukturen bezeichnet hat.<sup>195</sup> Forsthoffs (1938, 4) »effektiver Lebensraum« ebenso wie die »vitalen Systeme« (Collier und Lakoff 2015) der US-amerikanischen Militärstrategen des Kalten Krieges bilden solche »sozio-technischen Milieus«, die der Bevölkerung die Lebensgrundlage bereitstellen. Die zunehmende Technisierung und Digitalisierung sowie neue Bedrohungen wie der Terrorismus haben diese Sorge in der Gegenwart noch einmal intensiviert. Zugleich hat sich der Ort der Infrastrukturentwicklung immer mehr vom nationalen Territorium auf transnationale »infrastructural zones« (Barry 2006, 239) verschoben. Vor allem ist aber die Ambivalenz der Immunisierungsfunktion sozio-technischer Infrastrukturmilieus immer schärfer zu Bewusstsein gekommen. Infrastrukturleistungen sind lebenswichtig und bilden gerade deshalb immer mehr den »effektiven Lebensraum« der Gesellschaft. Zugleich ist durch diese technische Schutzhülle das menschliche Leben auf eine ganz neue Art von Infrastrukturen abhängig und durch diese verwundbar geworden; eine Verwundbarkeit, die sich durch die Komplexität und Interdependenz der Infrastrukturen noch erhöht hat.

---

194 »[S]ociety became its own referent, to be worked on by means of technical procedures [...]. [N]orms and forms were becoming increasingly autonomous – freed from previous historical and natural constraints, defined by their own operations, and claiming universal status.« (Rabinow 1995, 13)

195 In diese historische Konjunktur fällt auch der Beginn eines »ökologischen Krieg[s]« (Virilio 2011, 72), bei dem nicht mehr unmittelbar der Körper des Feindes, sondern dessen Umwelt angegriffen wurde. Die Umwelt ist hier weniger ein Schutzobjekt, sondern ein Übertragungsmilieu für neue Kampfstoffe wie Giftgas. Sowohl Virilio (2011, 61–83) als auch Sloterdijk (2004, 89–126), die diese Zusammenhänge untersucht haben, argumentieren, dass in diesen Formen der Kriegsführung ein, gewiss perverser, Vorläufer des ökologischen Denkens und Handelns gesehen werden kann.

Eine weitere Sicherheitsambivalenz des technischen Milieus wurde im Zuge der ökologischen Kritik seit den 1970er Jahren immer offensichtlicher. Denn nur scheinbar hat sich die sozio-technische Umwelt zu einem geschlossenen System formieren können, das die Abhängigkeiten von einem unkontrollierbaren Außen beseitigen kann. In Wirklichkeit bleiben – so die ökologischen Kritiker\_innen – die Großtechnik und ihre Gesellschaft nicht nur auf eine natürliche Umwelt angewiesen. Zudem hat die Gesellschaft, und zwar gerade weil sie die Natur nur als zu vernachlässigende Externalität behandelt hat, so massiv in diese eingegriffen, dass bisher selbstverständlich zur Verfügung stehende Ökosystemdienstleistungen prekär geworden sind. Das, was anfangs nur Externalität war und häufig buchstäblich erst durch das Überfließen technischer Rahmungen in Form von Öllecks, CO<sub>2</sub>-Emissionen und radioaktiven Wolken hervorgetreten ist, wurde in jüngerer Zeit als eigenständiger Problembereich eingeraht. Der anthropogene Klimawandel und Umweltkatastrophen, auf ihre Weise Ausdrücke der autoimmunen Effekte des sozio-technischen Sicherheitsmilieus, bilden das paradigmatische Problem, um das herum sich ein neues Denken des Milieus und eine neue Politik des Umweltschutzes formiert haben.

Durch diese Entwicklungen hat sich die Sphäre vitaler Systeme radikal erweitert. Mit der Umwelt – ein Gefüge aus Atmosphäre, Ökosystemen, geologischen und kryologischen Komplexen, das zudem stets mit technischen Faktoren vermischt auftritt – ist ein neuer Problem- und Interventionsraum der Sicherheit entstanden. Die Konzepte von Foucault und Rabinoz fortschreibend lässt sich von einem »öko-technischen Milieu« sprechen,<sup>196</sup> das in der jüngeren Vergangenheit entstanden ist und immer wichtiger für die gegenwärtige Politik des Lebens wird. Ich spreche von »öko-technisch«, weil die Milieus der Gegenwart durch eine intensive Vermischung von technischen und ökologischen Elementen gekennzeichnet und deswegen mehr als nur »natürliche Umwelt« sind. Zugleich erlaubt es ein verallgemeinertes Systemdenken, diese hybriden Gebilde als konsistente Ökologien oder eben Systeme zu beschreiben (Hörl 2011, 23–34) und richtet sie so als Zielscheibe von Kontrolltechniken und Sicherheitsinterventionen auf. Die Problematisierung der »Umwelt« markiert also gerade nicht eine Rückkehr zum historisch-natürlichen Milieu, sondern verweist auf ein komplexes *re-entry* des Natürlichen zu einem Zeitpunkt, an dem die

---

196 Siehe auch das Konzept des »ecotechnological environment« in: Hughes (2004, 153–173).

vollständige Technisierung der Welt, der Triumph von Technokratie und Kybernetik schon entschieden schien und sich die Welt in ein scheinbar geschlossenes System technischer Mechanismen verengt hatte. So muss gegenwärtig auch beim Design technischer Systeme auf deren »Umweltverträglichkeit« geachtet werden. Das wird vor allem am Beispiel des Energiesystems deutlich, das aktuell in einem komplexen Spannungsfeld unterschiedlicher Anforderungen an Sicherheit steht. Die Energiewende versucht deshalb ein »seamless web« (Hughes 1986) zwischen technischen Elementen (Windräder, Sonnenkollektoren) und »natürlichen« Faktoren (Wind, Sonne etc.) zu erstellen, die Natur also zum Teil der Energieinfrastruktur zu machen, anstatt sie als Externalität durch Emissionen zu belasten. Diese Integration der Natur in Form erneuerbarer Energiequellen wie Wind und Sonne erzeugt aber zugleich neue Unverfügbarkeiten und Unberechenbarkeiten im Inneren des Stromsystems, die wiederum nach technischen Innovationen – von Speichertechnologien bis zum *smart grid* – verlangen. Zudem zeichnet sich das »öko-technologische Milieu« dadurch aus, dass hier die Umwelt keine schlichte Gegebenheit mehr ist, sondern selbst zum technischen Projekt geworden ist. Flüsse müssen renaturiert, die fragmentierte Grüne Infrastruktur wieder verbunden werden und das bedrohte Erdsystem soll notfalls durch *geo-engineering*<sup>197</sup> geschützt werden. »Wo »Lebenswelt« war, muß Klimatechnik werden.« (Sloterdijk 2004, 69) Gleichzeitig funktioniert die Umwelt selbst wie technische Systeme, sie operiert wie eine Infrastruktur, Ökosysteme erbringen vitale Dienstleistungen. Die Erde ist nichts anderes als ein gigantisches »life support system« (Young und Steffen 2009). Das öko-technische Milieu unterliegt zwar (natur)wissenschaftlich bestimmbaren Gesetzmäßigkeiten und ist auch technisch gestaltbar. Der Stil der Regierung dieser Systeme ist trotzdem distinkt – er unterscheidet sich sowohl von der auf natürliche Selbstregula-

---

197 Auch prominente Vertreter\_innen der Erdsystemdebatte wie Paul Crutzen (Rasch, Crutzen und Coleman 2008) und James Lovelock (2000, 139–158) befürworten Techniken des *geo-engineering*, bei dem die Folgen des anthropogenen Klimawandels durch gezielte, großflächige Eingriffe in die Atmosphäre vermindert werden sollen. Derartige Techniken basieren häufig auf den gleichen oder ähnlichen Techniken, die bislang als Umweltgefahren eingestuft wurden, wie etwa die Vorgänge, die Crutzen in seinen Arbeiten zum nuklearen Winter beschrieben hatte (siehe dazu: Fleming 2006, Masco 2010). Die autoimmunen Effekte des *geo-engineering* liegen daher auf der Hand (siehe etwa: Cooper 2010, 183ff.). Allerdings lässt sich *geo-engineering* eher als *preemption* denn als Resilienztechnologie verstehen (Anderson 2010, 790) und wird daher hier nicht ausführlicher untersucht.

tion setzenden Regierung des 19. Jahrhunderts wie auch von den kybernetischen Kontrollansprüchen der Systemlenker\_innen des 20. Jahrhunderts. Die natürlichen Gesetzmäßigkeiten, die Normen, Gleichgewichtspunkte und Regulationsmuster der Systeme stehen für diesen Regierungsstil nicht fest, sondern können sich jenseits bestimmter Schwellen grundlegend ändern. Die technische Kontrollierbarkeit der Systeme ist durch solche nicht-linearen Abläufe begrenzt. Nicht mehr Dauersicherheit und reibungslose Kontrolle, sondern nur noch Resilienz kann angestrebt werden. Das unterscheidet auch die Neuauflage der Infrastruktursicherung im 21. von seinen Vorgängern im 20. Jahrhundert. Die vitalen Systeme werden als unübersichtliches, potenziell unbegrenztes, komplex-vernetztes *system of systems* verstanden.

Diese Transformation des Milieus als Interventions- und Problemraum der Sicherheitsdispositive bricht zwar nicht mit der biopolitischen Problematik, die Foucault beschrieben hat, transformiert sie aber tiefgreifend. Wenn die »biologische Modernitätsschwelle« damit überschritten wurde, dass das Leben der Gattung von einer stummen Grundlage der Politik zu einer Zielscheibe politischer Interventionen geworden ist (Foucault 1977, 170), dann haben wir vielleicht eine weitere, neue Schwelle überschritten, seit die Umwelt nicht mehr nur als Grundlage und selbstverständlicher Hintergrund unseres Lebens gilt, sondern selbst zu einem großtechnischen Projekt ungekannten Ausmaßes geworden ist: die ökologische Modernitätsschwelle. Wir haben es folglich nicht mehr nur mit einer Politik des Lebens selbst (Rose 2007) zu tun, in der das Leben auf der mikrologischen Ebene isoliert und manipuliert wird, sondern mit einer *Politik des Lebens jenseits seiner selbst*, die versucht, die Bedingungen des Lebens – von Mensch, Tier und Pflanze – in einem planetarischen Maßstab zu erhalten und dabei mit der irreduziblen Komplexität offener Systeme und hybrider Ökologien zu kämpfen hat. Die Politik des Lebens jenseits seiner selbst operiert nicht als individualisierende Biopolitik, die ein Subjekt an ein biologisches Wahrheitsregime bindet und dadurch sein Verhalten führt. Sie adressiert ökologische Komplexe, die aus organischen und technologischen Gefügen, Atmo- und Kryosphären etc. zusammengesetzt sind. Die Regierung des Lebens kann dann nicht mehr nach dem *conduct of conduct*-Modell gedacht werden. Vielmehr formiert sich eine »Gouvernementalität, die auf die Umgebung Einfluß nehmen und systematisch die Variablen dieser Umgebung verändern wird« (Foucault 2006, 372), eine »environmentality« (Massumi

2009, 155). Darin liegt das Kennzeichen der gegenwärtigen Biopolitik vitaler Systeme als Politik des Lebens jenseits seiner selbst.<sup>198</sup>

Aspekt	Historisch-Natürliches Milieu	Sozio-Technisches Milieu	Öko-Technisches Milieu
Ort, Gegenstand	Stadt, urbaner Raum	Nationales Territorium, transnationale infrastrukturelle Zonen	Planet Erde, <i>gaia</i>
Paradigmatische Probleme	Cholera, Pauperismus	Weltkriege und Kalter Krieg	Klimawandel, Ökologische Katastrophen
Immunisierung	Stadt schützt vor Feinden und unzivilisierter Natur	Daseinsvorsorge für lebenswichtige Infrastrukturen	Schutz der »Dienstleistungen« des Erdsystems
Auto-immunisierung	Urbane Zusammenballungen erzeugen soziale und gesundheitliche Probleme	Abhängigkeit von der Infrastruktur erhöht Verwundbarkeit der Bevölkerung, Interdependenz der Infrastruktur erhöht Potenzial weitreichender Unterbrechungen	Folgen technischer Entwicklung bedrohen die Integrität der natürlichen Umwelt <i>Geo-engineering</i> verstärkt die Effekte, die es bekämpfen soll
Regulation	Natürliche Selbstregulation	Kybernetische Kontrolle	Nicht-lineare Dynamiken, Resilienz
Wissenschaftlich-technisches Modell	Milieutheorien des 19. Jahrhunderts	Geschlossenes System: Kybernetik erster Ordnung	Offene Systeme, Netzwerke, Ökologien: Kybernetik zweiter Ordnung

Tabelle 5: Biopolitische Milieukonstellationen

Gleichwohl gehören die Biopolitik der Bevölkerung und die Biopolitik vitaler Systeme aufs Engste zusammen. Sie haben zwar unterschiedliche Interventionsoberflächen – die Bevölkerung und den Individualkörper auf der einen, Infrastrukturen und vitale Systeme auf der anderen Seite –, verfolgen aber das gleiche Ziel: Schutz und Gewährleistung des Lebens. Zwar unterscheidet sich, was hier jeweils Leben heißt – hier geht es um das Leben selbst (das menschliche Leben auf der Ebene von Molekülen, Organismen und Gattungen), dort geht es um das Leben jenseits seiner selbst

<sup>198</sup> Für eine Variation dieses Themas mit Bezug auf Deleuze und Guattaris Ökologiedenken siehe: Folkers (2017e).



(das anorganische Leben der gesellschaftlichen Systeme und sozio-technischen Zirkulationen ebenso wie das öko-sphärische Leben von Ökosystemen und Atmosphären). Aber letztlich – und das ist die eigentliche Einsicht der ökologischen Wende der Biopolitik – sind beide Arten des Lebens verschränkt und für ihr Leben aufeinander angewiesen. Im Zeitalter des Anthropozän sind der Mensch und seine Artefakte, insofern sie zur geologischen Kraft geworden sind, nicht mehr bloß von einer Umwelt umgeben, sondern selber eine Umwelt für anderes Leben geworden. Deshalb operieren beide Formen der Biopolitik auch nicht auf unterschiedlichen Maßstabsebenen<sup>199</sup> – wie Mikro- und Makro –, sondern sind aufeinander angewiesen.

---

199 Das betont auch Bruno Latour (2013, 71) in Bezug auf seine Konzeption von Gaia: »Scale is what has been generated by the success of living forms. If there is a climate for life, it's not because there exists a *res extensa* inside which all creatures would passively reside. Climate is a historical result of reciprocal, mutually interfering connections among all growing creatures. [...] The Nature of olden days had levels, layers and a well ordered zoom; Gaia subverts levels. [...] If climate and life have evolved together, space is not a frame, nor even a context: space is time's child.«

## 4. Kontinuitätsmanagement: Betriebliche Katastrophenvorsorge

Die Regierung der Katastrophe und der Schutz vitaler Systeme sind schon seit langem keine reine Staatsangelegenheit mehr. Eine Vielzahl halb-öffentlicher Hilfsorganisationen und Freiwilligenorganisationen ist Kernbestandteil des operativen Katastrophenschutzes, und der Schutz Kritischer Infrastrukturen ist unter Bedingungen der Liberalisierung auch zur Aufgabe privatwirtschaftlicher Konzerne geworden. Der Staat bemüht sich zwar weiterhin im Sinne seiner »Gewährleistungsverantwortung« um das reibungslose Funktionieren der voneinander abhängigen Infrastruktursysteme. Er ist aber schon lange nicht mehr der souveräne Steuermann der Vorsorgemaschine. Infrastrukturschutz erfolgt immer häufiger in Kooperationen zwischen Staat und Unternehmen bzw. in »Sicherheitspartnerschaften« und *Public Private Partnerships*. Die Regierung der Katastrophe ist folglich nicht im Staatsapparat konzentriert, sondern verstreut sich über die Netze des Sicherheitsdispositivs der Resilienz. Das Dispositiv versammelt diverse öffentliche und private Akteure und Institutionen und richtet ihre Sicherheitsbemühungen aus, ohne dass es eine zentrale Steuerungs- oder Koordinierungsinstanz gäbe, die vorschreibt, wer was wann zu tun hat. Durch diese dispositivanalytische Perspektive lässt sich der Anspruch der *Governmentality Studies* einlösen, »political power beyond the state« (Rose und Miller 1992) zu analysieren.

Umso verwunderlicher ist es, dass die internationale Debatte zur Regierung der Katastrophe einen so deutlichen Staatsbias aufweist und bisher fast ausschließlich Programmatiken und Initiativen staatlicher Behörden in den Blick genommen hat (Adey und Anderson 2011, Aradau und Munster 2011, Collier und Lakoff 2015). Wenn doch einmal der privatwirtschaftliche Anteil der Regierung der Katastrophe in den Blick gerät, dann zumeist durch Bezugnahme auf die Versicherung bzw. die Finanzialisierung von Sicherheit (Bougen 2003, Ericson und Doyle 2004). Es wird dann gezeigt, wie die private Versicherung gegen Katastrophen als Mittel gegen die Pa-

thologien staatlicher Katastrophenvorsorge aufgerichtet wird (Collier 2014) und wie Katastrophenversicherungen komplexe Finanzprodukte ins Spiel bringen, die das spekulative Moment kommender Katastrophenlagen – etwa durch Katastrophenanleihen – in ein Investitionsobjekt für risikofreudige Anleger verwandeln (Cooper 2010). So wichtig diese Arbeiten sind: Durch die Polarisierung von öffentlich und privat entsteht ein falsches Bild, wonach private Sicherheit vornehmlich durch finanzielle Techniken operiert, während substanzielle Katastrophenvorbereitungsmaßnahmen ausschließlich das Metier des Staates darstellen.

In diesem Kapitel möchte ich deshalb eine symmetrische Perspektive auf öffentliche und private Sicherheit einnehmen, indem ich auf organisatorische Katastrophenvorbereitungsmaßnahmen auf Unternehmensebene eingehe und damit eine wichtige Leerstelle in der Literatur zur Regierung der Katastrophe adressiere. Denn auch im privatwirtschaftlichen Bereich werden mittlerweile verstärkt Maßnahmen getroffen, die durch Kontingenzplanung und den Aufbau von Resilienz das Unternehmen auf unerwartete Großschadensereignisse vorbereiten sollen. Besonders das sogenannte *Business Continuity Management* (BCM) hat in jüngerer Zeit als Krisenmanagement und Katastrophenvorbereitungsprogramm für Betriebe stark an Bedeutung gewonnen, ohne bisher jedoch entsprechende sozialwissenschaftliche Aufmerksamkeit auf sich gezogen zu haben.<sup>200</sup> Ziel des BCM ist es, die Resilienz eines Unternehmens vorbereitend zu erhöhen, um kritische Geschäftsprozesse auch im Krisenfall aufrechterhalten zu können. Damit leistet BCM einen Beitrag zum Schutz Kritischer Infrastrukturen und vitaler Systeme. Im Folgenden steht insbesondere das BCM in Banken im Fokus. Gerade in Banken wurden aufgrund der Erfahrungen mit den Terroranschlägen vom 11. September 2001 in den letzten Jahren verstärkt *Business Continuity Management*-Systeme implementiert. Reizvoll ist der Fokus auf Banken zudem, weil sich so eine technisch-organisationelle Form der Katastrophenvorsorge ausgerechnet im Kernbereich der Finanzialisierung beobachten lässt. BCM in Banken antwortet auf Probleme – wie *operational risk* und *systemic risk* –, die auch mit finanziellen Vorsorgetechniken adressiert werden (siehe dazu bereits Kapitel 2.5.). So kann nicht nur der prinzipielle Unterschied von finanziellen und organisatorischen Sicherheitsstrategien, sondern vor allem auch ihr faktisches Zusammenspiel auf der Ebene des Sicherheitsdispositivs deutlich gemacht werden.

---

200 Einer der wenigen sozialwissenschaftlichen Texte, die *Business Continuity Management* überhaupt erwähnen, stammt von Power (2009).

Viele der zum Einsatz gebrachten Techniken des BCM weisen große Ähnlichkeiten zu bereits besprochenen Sicherheitspraktiken auf: Es wird auch hier erneut versucht, Verwundbarkeiten im Betrieb zu kartieren, Vorbereitungsmaßnahmen für generische Gefährdungen zu treffen und so Resilienz aufzubauen. Allerdings modifizieren die Strategien des BCM die bisher in der Arbeit diskutierten Technologien auf interessante Weise. Die vornehmliche Konzentration auf die *Kontinuität* des Geschäftsprozesses – und nicht etwa auf die Integrität von Infrastrukturnetzen oder den Schutz der Bevölkerung – betont eine vor allem temporal-prozesshafte Artikulation von Sicherheit bzw. Resilienz.

Im Folgenden werde ich zunächst auf die historische Entwicklung der Strategie des Kontinuitätsmanagements eingehen. Im *Continuity of Government Planning* während des Kalten Krieges, das die Fortsetzung der Regierungstätigkeit nach einem Atomangriff sicherstellen sollte, kann ein erster Vorläufer des modernen *Business Continuity Managements* gesehen werden. Das seit der Jahrtausendwende zu beobachtende Wandern der Strategien des Kontinuitätsmanagements aus dem staatlichen in den privaten Bereich hat deren Bedingungen gleichwohl entscheidend verändert (4.1.). Anschließend gehe ich genauer auf die Rationalitäten und Techniken des gegenwärtigen BCM ein. Planungen für ein operatives Krisenmanagement sind ebenso Teil von BCM wie strukturell-technische Vorkehrungen zum Schutz kritischer Geschäftsprozesse (4.2.). Danach beleuchte ich die Besonderheiten des *Business Continuity Managements* in Banken und untersuche, wie sich BCM in die elaborierte Risikokultur im Finanzwesen einschreibt (4.3.). Schließlich gehe ich auf zwei Ereignisse ein, bei denen Techniken des *Business Continuity Managements* in Banken zum Einsatz gebracht wurden: Hurricane Sandy in New York und die sogenannten Blockupy-Demonstrationen in Frankfurt am Main. Dabei interessiert mich vor allem, wie BCM im Zuge dieser beiden Ereignisse zum Gegenstand von Kritik geworden ist (4.4.). Schließlich werde ich versuchen, der Bedeutung von Kontinuität als maßgeblicher Temporalität der Sicherheit auf den Grund zu gehen. Warum ist die Kontinuität ihrer Operationen für die Gegenwartsgesellschaft so wichtig geworden, dass sie Unterbrechungen *per se* als Katastrophen erlebt? Auf welche gesellschaftlichen Bedingungen, auf welche Ontologie der Zeit verweist dieses Beharren aufs »Weitermachen« und welche Momente und Erfahrungen des gesellschaftlichen Lebens werden dadurch verdrängt (Exkurs III)?

#### 4.1. Geschichte und Gegenwart des Kontinuitätsmanagements

Wie es Gesellschaften beständig gelingt, ihre eigenen Operationen fortzusetzen, ist ein Grundthema der Soziologie, das durch die »Temporalisierung des Sozialen« (Nassehi 2009, 234–241) gerade in neueren soziologischen Theorieansätzen an Bedeutung gewonnen hat. Heinz Bude argumentiert sogar, dass die Soziologie überhaupt nur möglich ist, weil sie sich mit dem Phänomen beschäftigt, dass es »immer irgendwie weitergeht« (Bude, zitiert nach: Reemtsma 2010, 90). Folgt man dieser Argumentation, dann würde Soziologie also mit dem Staunen über die Beharrlichkeit des sozialen »Weitermachens« beginnen und folglich untersuchen, welche Mechanismen, welche formellen und informellen Institutionen sich in Bezug auf die sich immer wieder stellenden Fortsetzungsprobleme gebildet haben. Krisensituationen stellen Gesellschaften vor allem insofern auf eine harte Probe, weil Fortsetzung in ihnen aufhört, selbstverständlich zu sein. Krisen erfordern ein von den Fortsetzungsroutinen abweichendes Handeln, das wiederum ermöglichen soll, dass es »trotzdem weitergeht«. Diese Fortsetzungsbemühungen erscheinen mitunter als absurde Geschäftigkeit, die Übersprunghandlungen oder blinden Ritualen mehr ähneln als einer zielgerichteten Praxis zur Überwindung der Krise. Oder sind die Notfallroutinen im Flugverkehr, die dem Fluggast vor Abflug aufgesagt werden – anschnallen, Schwimmweste anziehen, Atemmaske aufsetzen – etwas anderes als Rituale, die im Notfall die Zeit überbrücken sollen, bis das Flugzeug abgestürzt ist? Sich der grotesken Inadäquatheit sozialer Weitermachrituale vollends bewusst zu werden, erfordert einen Blick, der sich vom »immer weiter« der Gesellschaft entfernt. Ein ethnologisch-distanzierter Blick wie auch die Genealogie sind dafür bevorzugte epistemische Werkzeuge. Mit letzterer soll dieses Kapitel beginnen. Es erzählt die Geschichte des *Continuity of Operations Planning* im Kalten Krieg. Das Projekt, die Kontinuität der Regierungsoperationen im Angesicht der Bedrohungen eines thermonuklearen Krieges sicherzustellen, der erstmals die Gesellschaft, ja die gesamte Menschheit, zum Aufhören hätte zwingen können, ist für eine soziologische Beobachtung des Weitermachens besonders aufschlussreich. Fortsetzung der Operationen war hier nämlich nicht mehr nur ein stummer gesellschaftlicher Imperativ, sondern ist zu einem explizit gestellten Problem und politisch-organisatorischen Sicherheitsprojekt geworden.

Ich werde zunächst die historischen Hintergründe (die Bedrohung durch einen Atomkrieg) und die wesentlichen Techniken des Kontinuitätsmanagements (die Etablierung von Ausweichstandorten für die Fortsetzung der Regierungstätigkeit) aufzeigen (4.1.1.). Dann werde ich auf die Problematik der Souveränität eingehen, die im Rahmen des *Continuity of Operations Planning* aufgebrochen ist und als durchaus exemplarisch für die Rolle souveräner Macht im Kontext der *vital systems security* angesehen werden kann (4.1.2.). Schließlich werde ich zeigen, wie das *Continuity of Operations Planning* des Kalten Krieges zum gegenwärtigen *Business Continuity Management* (BCM) mutiert ist (4.1.3.).

#### 4.1.1. Der Aufstieg des Kontinuitätsmanagements im Kalten Krieg

Das heutige Kontinuitätsmanagement entwickelte sich historisch aus dem sogenannten *Continuity of Government Operations Planning*, das im Rahmen der Vorbereitungen auf einen Atomkrieg während des Kalten Krieges in den USA ausgearbeitet wurde. Die Unangemessenheit dieser Vorkehrungen wurde von der Friedensbewegung und kritischen Intellektuellen während des Kalten Krieges immer wieder betont, um zu zeigen, wie absurd und bedrohlich das atomare Wettrüsten war. Gegenüber der Zerstörungskraft der ungeheuren Waffenlager, die sich im Verlauf des Kalten Krieges angesammelt hatten und deren Sprengkraft sich ständig weiter potenzierte, wirkten die Empfehlungen der Sicherheitsexpert\_innen an die Zivilbevölkerung, die zumeist nicht über das berüchtigte »duck and cover« hinausgingen, geradezu zynisch naiv. Im Bild des Atompilzes verdichtete sich für die Kritiker\_innen das Destruktionspotenzial des atomaren Endspiels. Vermittelt durch die Bombe, so argumentierte etwa Günther Anders, habe sich nunmehr die Menschheit, und nicht mehr nur der einzelne Mensch, als endliches (Gattungs-)Wesen konstituiert (Anders 1980, 233ff.). Angesichts dieser radikalen und intensiven Erfahrung der Endlichkeit wirkte jedes Projekt, das sich Gedanken darüber machte, wie es nach dem Ende weitergeht, peinlich unangemessen und »apokalypseblind« (Anders 1980, 276–279).

Auch wenn zunächst alles dafür spricht, dass wir es beim *Continuity of Government Operations Planning* abermals mit dem stummen Zwang des sozialen Weitermachimperativs zu tun haben, hat sich doch etwas Entscheidendes verändert. Denn im *Continuity of Government Operations Planning* wird Kontinuität – in diesem Fall des Regierungshandelns – zum Ziel einer

systematisch ausgearbeiteten, reflektierten Praxis. Das Problem der Kontinuität stellt sich hier zudem in Bezug auf eine noch nicht eingetretene Zukunft und verlagert sich damit gewissermaßen vor. Kontinuität ist damit nicht nur eine Technik, die *ad hoc* in Krisensituationen zum Einsatz kommt, sondern Gegenstand der Antizipation und Planung für eine erst noch kommende Katastrophe.

Mit Vorliebe stellen sich die Kontinuitätsmanager\_innen unserer Tage mit Kriegsherren wie Sun Tzu über Perikles bis Clausewitz in eine Filiationslinie. »Es kommt nicht darauf an, die Zukunft vorauszusehen, sondern auf die Zukunft vorbereitet zu sein«, wird Perikles etwa auf der Internetseite BCM-News zitiert.<sup>201</sup> Daran ist richtig, dass die Kriegslogistik seit eh und je mit Problemen der Kontinuität – des Nachschubs an Truppen, Verpflegung und Munition, von Befehlsketten und natürlich der Kriegs- oder Verteidigungshandlungen – befasst war (DeLanda 1991, 105–115). Zu einer expliziten Ausarbeitung von Kontinuität als organisatorischer Strategie auch für nicht unmittelbar militärische Institutionen, die auch das gegenwärtige betriebliche Kontinuitätsmanagement informiert, kam es aber erst während des Kalten Krieges. *Continuity of Government* bzw. *Continuity of Government Operations* ist eine distinkte Sicherheitstechnik, die im Rahmen der während des Kalten Krieges ausgearbeiteten Sicherung vitaler Systeme verortet werden kann.

In ihren genealogischen Arbeiten zum »Nuclear Preparedness Apparatus« (Collier und Lakoff 2015, 28) der USA haben Collier und Lakoff gezeigt, wie wichtig der Kalte Krieg für die Entwicklung neuer Technologien der Sicherheit war. Im Zentrum steht dabei die Strategie der »distributed preparedness« (Collier und Lakoff 2008). Als Reaktion auf die strategischen Bombardierungen feindlicher Infrastruktur, die vor allem im Zweiten Weltkrieg zum entscheidenden Moment der (Luft-)Kriegsführung geworden war, suchten Militärstrateg\_innen nach Wegen, die Verwundbarkeit ihrer heimischen Infrastruktur gegenüber feindlichen Luftschlägen zu reduzieren. Welche sozio-techno-ökonomischen Systeme müssen unbedingt funktionsfähig bleiben, um das Überleben der Bevölkerung und die Kriegsfähigkeit zu gewährleisten, und wie können diese im Falle eines (Atom)Bombenangriffs sichergestellt werden? Die Dezentralisierung, also die geographische Verstreuung (*dispersal*) der vitalen Infrastrukturen durch die Auflösung hochkonzentrierter industrieller Zentren und Vermeidung

---

201 Siehe: <http://www.bcm-news.de/>.

von verwundbaren infrastrukturellen Knotenpunkten, erwies sich als Mittel der Wahl zur Beantwortung dieser Fragen.<sup>202</sup> *Distributed Preparedness* funktioniert dabei vor allem räumlich, weshalb sie von Collier und Lakoff (2008) auch als »spatial logic of domestic security« beschrieben wird. Der Gefahr aus der Luft – *aerial bombing* – sollte mit einer Verteilung der Zielscheiben am Boden begegnet werden. Das sogenannte »vulnerability mapping« (Collier und Lakoff 2008, 8ff.), bei dem Folien über geographische Landkarten gelegt wurden, die den Zerstörungsradius einer Atombombe und damit die Folgen für die Infrastruktur visualisierten, kam deshalb als zentrale Wissenstechnik ins Spiel. Ein US-Militärberater brachte diese räumliche Orientierung der Dispersionsstrategie mit der Formel: »Space is the one thing that really works« (zitiert nach: Galison 2001, 16) auf den Punkt.

Die Sicherung der Regierung als vitales System konfrontierte Sicherheitsexpert\_innen allerdings mit einer Reihe von Problemen, die Modifikationen dieser Strategie erheischten. *Erstens* galt die Regierung als das »Nervenzentrum« des Sicherheitsnetzes, das gerade in Kriegszeiten bzw. in Situationen des Notstandes funktionstüchtig sein musste, um die Verteidigung gegen, den Schutz vor und gegebenenfalls auch die kriegerische Erwidern auf einen feindlichen Angriff zu koordinieren. Dabei musste davon ausgegangen werden, dass die Befehlsgewalt für diese Verteidigungsmaßnahmen hierarchisch operierte. Das wiederum hieß, dass die Infrastruktur des Regierens – anders als das zur gleichen Zeit mit der *Continuity of Operations*-Planung gebaute *Interstate Highway*-Netz, das die Morphologie eines *distributed networks* hat (Galloway 2004, 35) – nicht auf hierarchische Verknüpfungen verzichten konnte, ohne einen geradezu revolutionären Wandel des Regierungssystems einzuleiten. Daraus ergab

---

202 Im Kern ist dies auch die Strategie, die Lovins und Lovins dem amerikanischen Zivilschutz vorschlugen, um die US-amerikanische Energiesicherheit zu erhöhen (siehe Kapitel 3.3.2.). Strenggenommen lässt sich allerdings zwischen dezentralisierten Netzwerken und *distributed networks* unterscheiden. Folgt man etwa der Unterscheidung von Alex Galloway (2004, 29–38) zwischen »decentralized« und »distributed networks«, dann fallen bei letzteren die »hubs«, also zentrale Verbindungspunkte zwischen Punkten im Netzwerk, weg. »[D]istributed networks have no central hubs and no radial nodes. Instead each entity in the distributed network is an autonomous agent.« (Galloway 2004, 33) Natürlich ist es der US-amerikanischen Landesverteidigung de facto nie gelungen, sämtliche vitale Systeme als *distributed networks* zu gestalten. So konnten Lovins und Lovins Anfang der 1980er Jahre noch die Zentralisierung des Energiesystems kritisieren, also lange nach der Entwicklung der Doktrin der *distributed preparedness* in den 1950er Jahren. Und besonders das Regierungssystem konnte nicht – wie im *Continuity of Government Planning* deutlich wurde – komplett dezentralisiert bzw. verteilt werden.



sich *zweitens* der zeitkritische Charakter des Regierungssystems. Während ein Industriezweig wie die Stahlindustrie durchaus für ein paar Tage zum Erliegen kommen kann, bis die kriegs- und lebenswichtige Produktion wieder anläuft, ist die Regierung auf Dauerbetrieb angewiesen. Schließlich müssen gerade im Fall eines Krieges ebenso wie im Fall einer großflächigen Katastrophe sehr schnell Entscheidungen getroffen, kommuniziert und exekutiert werden. Gerade in solchen Situationen muss der Regierungsapparat reibungslos und mit hohem Tempo operieren können. Es geht also um die Kontinuität von *Operationen*, die ständig aufrechterhalten werden müssen und nicht nur um (Infra-)*Strukturen*, die in ihrer Integrität geschützt werden müssen. *Drittens* macht es die Konzentration der Regierung in einer Hauptstadt schwer, sie räumlich zu zerstreuen, ohne ihre Funktionsfähigkeit übermäßig einzuschränken. Auf alle diese Probleme musste die *Continuity of Operations*-Planung eine Antwort finden. Im Zuge dieser Überlegungen sollte sich eine folgenreiche Erweiterung der Strategien zur Sicherung vitaler Systeme ereignen, die vornehmlich im Medium der Zeit und nur sekundär im Raum operieren. Die Genealogie des *Continuity of Operations Planning* erweitert damit die Genealogie vitaler Systeme von Collier und Lakoff und ihrer Fokussierung auf *distributed preparedness* als *spatial logic of security* um die zeitliche Logik der Sicherheit in Dispositiven der Resilienz: Kontinuität.

Wie der Historiker David F. Krugler (2006) in seiner Studie über die Vorbereitungen auf den Atomkrieg in Washington D.C. zeigt, war noch zu Beginn der 1950er Jahre die *dispersal* die wichtigste Strategie zum Schutz der Regierungsfunktionen vor einem Atomangriff. Regierungsbehörden sollten um Washington herum angesiedelt werden, um nicht sämtlich in dessen Zentrum konzentriert und damit leichte Beute für feindliche Angriffe zu sein. Die Entwicklung der Wasserstoffbombe Anfang der 1950er Jahre setzte der *dispersal*-Strategie ein Ende. »Dispersal was all but dead in 1953.« (Krugler 2006, 100) Der Zerstörungsradius der Bombe wäre einfach zu groß gewesen, um *dispersal* noch als sinnvolle Sicherheitstechnik ernsthaft in Betracht kommen zu lassen. Stattdessen wurde bereits ab 1952 die *Continuity of Government*-Planung ausgebaut (Krugler 2006, 5).

Kernstück dieser Planungen war ein System von Ausweichstandorten, also eine alternative Infrastruktur für Regierungsoperationen und deren personelle wie materielle Grundlagen. Zum größten Teil handelte es sich bei diesen Ausweichstandorten um (Atom-)Schutzbunker. Der Bunker – egal, ob für die Zivilbevölkerung oder für die Regierung – reagiert als Si-

cherheitstechnologie ähnlich wie der Infrastrukturschutz der *distributed preparedness* auf dieselbe Veränderung in der Kriegsführung des 20. Jahrhunderts, nämlich auf das, was Paul Virilio (2011, 72) als »ökologische Kriegsführung« beschrieben hat. Im 20. Jahrhundert zielen Kriegshandlungen immer weniger unmittelbar auf den Körper des Feindes und zunehmend auf dessen Umwelt. Krieg besteht jetzt – wie Peter Sloterdijk (2004, 97) bemerkt – in »Attentate[n] auf die umweltlichen Lebensvoraussetzungen«. Das *strategic bombing* greift durch die Zerstörung lebenswichtiger Infrastruktursysteme den »effektiven Lebensraum« (Forsthoff) der Bevölkerung an, der Gaskrieg erzeugt ein »kriegerische[s] Neoklima« (Virilio 2011, 71) und verschließt damit die atmosphärische Atemumwelt (zum Gaskrieg als »Atmoterror« siehe: Sloterdijk 2004, 89–125) und durch den Einsatz von Atomwaffen entsteht eine tödliche Hitze- und Strahlenumwelt (Sloterdijk 2004, 138–144). Im Verbund entsteht dadurch ein nie zuvor dagewesenes Vernichtungspotenzial des Krieges, eine ökologische Thanatopolitik, die gleichsam den dunklen Schatten der lebensfördernden Biopolitik vitaler Systeme darstellt. In ebendieser Situation kommt der Bunker als eine Sicherungsinfrastruktur auf, die Schutz vor der lebensfeindlich gewordenen Umwelt gewährleisten soll und somit wie eine »Überlebensmaschine« (Virilio 2011, 65) bzw. eine moderne »Arche« (Virilio 2011, 79) funktioniert.

»Ein anderer, ein für den Mensch [...] von Grund auf unbewohnbarer Planet, das ist es, was die moderne Kriegsführung hervorbringt [...]. Das alles ist in der Charakteristik des Betonmassivs [des Bunkers also] präsent, das gebaut wurde, um Geschossen und Bomben, um Giftgasen und Flammenwerfern zu widerstehen. So wie die Bastion des 18. Jahrhunderts die ballistischen Systeme der ersten Artillerie materialisierte, so wird der Bunker unter Berücksichtigung dieses neuen Klimas erbaut [...]: die Panzerung, Stahltüren, Belüftungsfilter – alles das repräsentiert die Gestaltung eines anderen militärischen Raums, einer neuen klimatischen Realität.« (Virilio 2011, 64f.)

Der Bunker muss als Verteidigung gegen die tödliche Umwelt eine neue, künstliche und schützende Umwelt in seinem Inneren aufbauen. Einerseits muss der Bunker so rigide von der Außenwelt abgeschottet werden, dass die Wucht von Bombeneinschlägen, Giftgase, Strahlen etc. nicht in sein Inneres eindringen können. Andererseits muss er vitale Umweltelemente wie Wasser und Luft durch den Einsatz von Speichern und Filtern bereitstellen. Der Bunker verkörpert damit nahezu in Perfektion das infrastrukturelle Ideal der Epoche des Kalten Krieges: das geschlossene System.

Perfekt wird diese Abschließung allerdings nicht durch die Abkapslung von der Außenwelt, sondern vor allem dadurch, dass sie diese Außenwelt gleichsam in sich selbst hinein holt und in sich einschließt. Das galt gerade für die Regierungsbunker – eine kleine Welt, in deren Innerem der Weltkrieg gesteuert werden sollte. Die Abschließung der Regierungs- und Militärbunker von der Außenwelt ging mit dem medialen Einschluss der gesamten Welt als Bild und Datenkörper einher. Die »windowless spaces« (Masco 2009, 13) von Regierung und Militär wurden mit komplexen Informations- und Überwachungssystemen ausgestattet, die es ermöglichen sollten, die gesamte Welt als Punktgraphik ins Innere der abgeschotteten Bunkermonaden zu bringen. Die Bunker von Militär und Regierung sind damit die »most isolated and most connected site[s] in the United States« (Masco 2009, 17) geworden.<sup>203</sup>

Die wohl berühmteste Bunker- und Regierungsausweichanlage ist Mount Weather im US-Bundesstaat Virginia. Ein Großteil der Anlage besteht aus einem gigantischen Atomschutzbunker, einem System von Tunneln, die in einen Berg – eben den Mount Weather – gegraben wurden. Die 1958 fertig gestellte Anlage umfasst neben direkt auf den Kriegsfall zugeschnittenen Informations- und Kontrollsystemen auch Fernseh- und Radiostudios, ein Krankenhaus sowie Arbeits- und Schlafbereiche für die Beschäftigten. Mit autarker Stromversorgung und eingelagerten Lebensmitteln und anderen Versorgungsgütern sollte Mount Weather mehreren hundert Regierungsmitarbeitern 30 Tage Schutz gewähren und die Regierungsoperationen für diesen Zeitraum aufrecht erhalten können – was danach geschehen würde, war nicht Teil der Planung. Neben Mount Weather wurde in den USA noch eine Reihe ähnlicher Einrichtungen etabliert. Auch das »Presidential Retreat« Camp David war in den Kontinuitätsplänen als möglicher Ausweichstandort vorgesehen.

Die Maßnahmen zur Kontinuierung der Regierung in der Bundesrepublik setzten zwar etwas später ein als in den USA, sind aber nicht weniger spektakulär. Kernstück dieser Bemühungen war der »Regierungsbunker« bzw. der »Ausweichsitz für die Verfassungsorgane des Bundes im Krisen- und Verteidigungsfall zur Wahrung von deren Funktionstüchtigkeit«, wie es wenig handlich im Beamtenjargon hieß. Nahe der damaligen Bundeshauptstadt Bonn wurde von 1962 bis 1970 in Ahrweiler eine gigantische Bunkeranlage gebaut, die die Dimensionen einer Kleinstadt hatte.

---

203 Damit sind die Bunker des Kalten Krieges auch Blaupausen für die Lagezentren der Gegenwart (siehe dazu Kapitel 2.2.2.).

Die insgesamt 17,3 Kilometer langen Tunnel waren bereits im Ersten Weltkrieg angelegt worden und sollten zunächst als unterirdisches Bahnsystem die Kriegslogistik des Deutschen Kaiserreichs unterstützen. Während des Zweiten Weltkriegs wurden dann Teile der V2-Rakete von Zwangsarbeiter\_innen in der Tunnelanlage gebaut, um diese »kriegswichtige Produktion« vor den Luftangriffen der Alliierten zu schützen (Klinke 2015, 155f.). Ob durch seine Geschichte oder seine Nähe zum Sitz der Regierung in Bonn – den Expert\_innen bundesrepublikanischer Verteidigung schien der Standort prädestiniert, auch in einem möglichen Dritten Weltkrieg zum Einsatz zu kommen. Auf 83.000 Quadratmetern sollte es für 3000 Regierungsmitarbeiter 30 Tage lang in die Verlängerung zum nuklearen Endspiel gehen. Der Bunker war der Größte Europas und das größte Bauprojekt der Bundesrepublik, verschlang knapp fünf Milliarden D-Mark und wurde von 200 Mitarbeiter\_innen über Jahre ständig einsatzbereit gehalten. Es gab Sitzungssäle für die Kriegsplanung, Kontrollräume, Büros, Gemeinschaftsschlafräume, aber auch eine Kirche, ein Fernsehstudio und einen Friseursalon – alle Räume ausgestaltet im Charme der Bundesrepublik der frühen 1960er Jahre. Alle zwei Jahre wurde im Rahmen der NATO Wintex-Übungen hier der Ernstfall trainiert, wofür ein eigener Bundeskanzler-Darsteller (bis dahin bekanntlich ausschließlich Männer) angeheuert wurde (zu diesen Angaben siehe: Peter 2008). Ähnlich wie das US-amerikanische Mount Weather konnte auch der Regierungsbunker nicht lange effektiv geheim gehalten werden. Zeitungen berichteten zur Empörung der Obrigkeit über die Anlage und die DDR wusste dank Spionage ohnehin Bescheid. Der eigentliche Haken des Ausweichsitzes aber war seine mangelnde Schutzfunktion. Ausgelegt war der Bunker ursprünglich nur für die Sprengkraft einer Hiroshima-Bombe. Wasserstoffbomben hatten aber bereits Anfang der 1960er Jahre die 250-fache Sprengkraft der Hiroshima-Bombe erreicht. Obwohl das durchaus bekannt war, wurde der Bunkerbau unbeirrt fortgesetzt. Abermals erscheinen Sicherheitstechniken als leeres Weitermachritual. Die Bunkertechnologie scheint jedenfalls erfolgreicher in der Regulation affektiver Atmosphären im Angesicht eines möglichen Atomkriegs gewesen zu sein, als sie im Schutz gegen das lebensfeindliche Klima gewesen wäre, das ein tatsächlicher Atomkrieg mit sich gebracht hätte.

#### 4.1.2. Protokollarische Souveränität

Neben den physischen Infrastrukturen der Regierungskontinuierung, den Bunkern, *relocation sites* bzw. *emergency standby facilities*, sind es aber vor allem eine ganze Reihe genuin organisatorischer und politisch-juridischer Maßnahmen, die das *Continuity of Government Planning* ausmachen. Während der Bunker immer noch eine vor allem räumliche Sicherheitsstrategie darstellt, geht es in den organisatorischen Überlegungen zentral um die zeitliche Dimension der *vital systems security*. Zentral sind hier vor allem Notfallpläne in Form von Entscheidungsalgorithmen und Kommandoprotokollen. Detaillierte Pläne sollten im Voraus genau festlegen, wer wann was und wo zu tun und zu entscheiden hat, wer welche Rolle im Notfall zu übernehmen hat und wer wen ersetzen kann, falls wichtige Entscheidungsträger\_innen bei feindlichen Angriffen ums Leben gekommen sein sollten. Übungen des Atomkriegs in den USA, die sogenannten *operations alert*-Übungen, hatten nämlich Schwachstellen aufgezeigt: » [A] nuclear attack would cause a nearly total breakdown in the command and control structure of the federal government, and that most government agencies were unable to identify priority emergency actions.« (Collier und Lakoff 2015, 32)

Nicht nur die materiellen Versorgungsketten waren also durch einen Atomangriff bedroht, sondern auch die Befehls-, Entscheidungs- und Hierarchieketten, nicht nur die *supply chains*, sondern auch die *chain of command*. Gefährdet war also das, was aus Sicht der Organisationstheorie Luhmanns (2000) ohnehin die vitalen Operationen einer Regierung bzw. einer Organisation sind, nämlich Kommunikationen von Entscheidungen, also *commands*. Und auch für die Systemdenker\_innen der *vital systems security* war die Fortsetzung der Entscheidungs- und Kommandostruktur ein zentrales, wenn nicht sogar das vorrangige Ziel des *Continuity of Government Operations Planning*. Schließlich sollte es in erster Linie nicht darum gehen, einen Rückzugsort für die Elite zu schaffen, sondern um die Aufrechterhaltung der Regierung als *Nervensystem* des Netzes vitaler Systeme. Das setzte aber auch einen ungewohnten Blick auf die eigene Organisation voraus. Die Regierung musste sich selbst als Organisation, die »operativ aus (der Kommunikation von) Entscheidungen besteht« (Luhmann 2000, 123), beobachten und ihr kontinuierliches Operieren zu einem expliziten Problem und organisatorischen Projekt machen.

Aufs Dramatische zugespitzt wurde diese Entscheidungsproblematik noch dadurch, dass im Notfall normale Entscheidungsprozesse und Kanä-

le wahrscheinlich nicht die benötigte Funktionsfähigkeit aufgewiesen hätten. Der gewohnte Dienstweg war zu verzweigt und schwerfällig, als dass er ein im Notfall erforderliches, vor allem schnelles und effizientes Agieren und Reagieren ermöglicht hätte. Diese Blockierung des gewohnten Geschäftsweges brachte gerade das in Bedrängnis, was für Luhmann der wesentliche Vorzug von Organisationen in Risikolagen ist: ihre Fähigkeit zur »Unsicherheitsabsorption« (Luhmann 2000, 184). Unsicherheitsabsorption in Organisationen wird möglich, indem Entscheidungsprozesse auf geregelte Bahnen gesetzt werden, damit diese sich dann quasi automatisch fortsetzen. Die Verantwortung Einzelner, und damit das Risiko der Entscheidung, wird so zergliedert, dass die Entscheidungsfreudigkeit gesteigert wird. Gemäß der Logik der *vital systems security* lässt sich darin ein *temporally distributed decision making* sehen. Sicherheit wird durch die Zerstreung zentraler Entscheidungsknoten erreicht. Das Problem ist allerdings, dass in einer Notfallsituation der zeitliche Horizont, über den diese Entscheidungen verteilt werden könnten, derart kontrahiert ist, dass die gewohnte Unsicherheitsabsorptionsfunktion praktisch unbrauchbar wird.

Klassischerweise gelten durchgreifende Entscheidungen von der Spitze der Hierarchie, die sich damit zum Souverän des Ausnahmezustandes macht, als Möglichkeit, mit den Tempoanforderungen von Krisensituationen umzugehen. Der prominenteste Befürworter dieser Option ist sicherlich Carl Schmitt, der die liberal-demokratische Entscheidungspraxis für zu schwerfällig hielt, um angemessen mit den Krisensituationen der modernen Gesellschaft umzugehen (Scheuerman 1999). Die im Rahmen der *vital systems security* ausgearbeitete Kontinuitätsplanung stellt demgegenüber eine Alternative dar. Geregelte Verfahren sollen hier auch unter erhöhten Tempoanforderungen erhalten bleiben, indem eine Priorisierung von Maßnahmen und die geeigneten Entscheidungsinstanzen im Voraus festgelegt werden. Für den Notfall erstellte *command and control protocols* sollten das gewährleisten.<sup>204</sup> Im Idealfall erfüllen diese Protokolle unter Bedingungen komprimierter Zeitressourcen die gleiche Funktion wie gewöhnliche organisiert-zergliederte Entscheidungsverfahren.<sup>205</sup>

---

204 Diese Entscheidungsprotokolle lassen sich mit Luhmann (2000, 263–265) als Konditionalprogramme verstehen, in denen jeweils abhängig von zuvor eingetretenen Situationen neu entschieden wird, anstatt – wie in Zweckprogrammen – stets nach gegebenen Richtwerten zu entscheiden.

205 Die *continuity*-Pläne in den USA sahen vor, die Regierungstätigkeit auf zentrale Bereiche wie *manpower, production, energy, food, fuel, transportation, telecommunication* etc. aufzuteilen und neu zusammenzusetzen (Conaty 2010, 634); und zwar auf eine Weise, die nur noch ent-

Gleichwohl verändern die alternativen Handlungsprotokolle die Tätigkeit der Regierung tiefgreifend. Insbesondere der US-amerikanische Präsident Dwight D. Eisenhower, der vor seiner Präsidentschaft Oberbefehlshaber der alliierten Streitkräfte in Europa gewesen war, war sich offenbar über die umwälzenden Veränderungen der immer wieder geübten Notsituationen im Klaren. Bei der Evaluation einer *operation alert*-Übung im Jahr 1955 kam er zu dem Schluss: »[U]nder the circumstances of chaos assumed in Operation Alert, we would have to run this country as one big camp – severely regimented.« (zitiert nach: Conaty 2010, 643) Die Drastik solcher Stellungnahmen macht deutlich, wie eng sich in der Sicherheitstechnik des *Continuity of Government Planning* souveräne und biopolitische Taktiken und Zielsetzungen vermischen. Denn tatsächlich wäre die Regierung des »nuclear state of emergency« (Bussolini 2014) ohne den Einsatz von juristischen Ausnahmerechtstechniken, die zum Ziel haben, die Souveränität zu sichern und die Integrität des nationalen Territoriums zu schützen, nicht möglich gewesen. Entsprechend haben die Kontinuitätsplanungen auch juristische Überlegungen darüber angeregt, welche rechtlichen Vehikel – etwa Kriegsrecht oder Notstandsrecht – besonders geeignet sind, um der Ausnahmesituation angemessen zu begegnen (zu diesen rechtlichen Fragen ausführlich: Conaty 2010). Jenseits der souveränen Sicherheitsproblematik ging es aber auch um das biopolitische Problem, das nackte Überleben der Bevölkerung zu ermöglichen. Die Voraussetzung für beide Zielvorstellungen wurde allerdings in der Funktionsfähigkeit von Systemen gesehen, die weder als juristisch souveräne Körperschaften noch als lebendige Bevölkerung verstanden werden können, sondern als Serie von Operationen: die Flüsse von Energie, Wasser, Strom, Verkehr, Kommunikation und eben auch von Entscheidungen und Befehlen. Die Regierung ist dabei nur ein – wenn auch zentrales – System unter anderen. Diese Verflechtung von souveräner Sicherheit, klassischer biopolitischer Sicherheit und *vital systems security* führte zu einer tiefgreifenden Modifikation sowohl der Stellung und Zielsetzung des Ausnahmezustands als Technik des Regierens als auch des souveränen Deziisionismus.

---

fernt an den Zuschnitt klassischer Zuständigkeiten und Ressorts erinnert. Zudem sollte das Office of Defense Mobilization (ODM) eine entscheidende Rolle spielen, indem es Zuständige aus den Bundesministerien, die möglicherweise zu sehr in ihren Routinen gefangen bzw. nicht auf die neue Situation der Landesverteidigung vorbereitet waren, einsetzen sollte (zur zentralen Rolle von ODM siehe: Collier und Lakoff 2015, 29, Conaty 2010, 634).

Giorgio Agambens (2004, 7) einflussreiche Arbeit zum »Ausnahmezustand als Paradigma des Regierens« sieht im römischen Recht die Matrix des modernen Ausnahmerechts. Für Agamben sind also bereits in der römischen Antike die Grundlagen und Aporien der souveränen Ausnahme angelegt, mit denen wir heute noch konfrontiert sind. Agambens genealogische Strategie neigt allerdings dazu, eine Reihe von signifikanten historischen Differenzen zwischen Antike und Moderne, insbesondere zwischen römischem Recht und dem Ausnahmeregieren des Kalten Krieges, zu verwischen. Die Zielsetzung des römischen *Justitiums* unterscheidet sich grundlegend vom modernen und gegenwärtigen Ausnahmemangement der Kontinuität. Das *Justitium* sah im Falle des Notstandes – eines sogenannten *tumultus*, also zum Beispiel: Krieg, Aufstand oder Bürgerkrieg – eine Suspendierung des gewöhnlichen Rechts und damit eine Machterweiterung des Souveräns vor, eine befristete Quasi-Diktatur (Agamben 2004, 52–63). *Justitium* heißt eng übersetzt so viel wie Stillstand des Rechts und wurde bisweilen auch als »Rechtsferien« bezeichnet (Agamben 2004, 56). Aber nicht nur das Recht sollte während der Zeit der Gültigkeit des *Justitiums* aussetzen. Auch alle Geschäfte, aller Handel, das, was wir heute als das ökonomische Leben bezeichnen, sollte stillstehen, aussetzen, pausieren. » [T]he *iusitium* also involved a closing of shops and a general suspension of public business« (Bussolini 2014, 7). Der Kontrast zum Ausnahmezustand unter Bedingungen der *vital systems security* könnte schärfer nicht sein. Denn hier werden außergewöhnliche Maßnahmen gerade zur Fortsetzung des Geschäfts, des Betriebs oder der Regierungsoperationen getroffen. Das Ziel besteht in der Kontinuierung und gerade nicht in der Stillstellung des ökonomischen Lebens.

Auch die Theorie des souveränen Dezisionismus von Carl Schmitt findet sich unter Bedingungen der *vital systems security* vollkommen transformiert. Der Kalte Krieg ist keine Welt, in der – im Sinne Carl Schmitts (2004, 13) – souverän ist, wer über den Ausnahmezustand entscheidet. Und das liegt vor allem an einer grundlegenden Rekonzeptualisierung und -positionierung der Entscheidung unter den Bedingungen eines möglichen Atomkrieges. Die Entscheidung wird nicht mehr der Willkür eines Souveräns überlassen, sondern zum Gegenstand der Reflexion der Wissenschaft und der Formalisierung von rationalen Entscheidungstheorien (*game theory*, *decision theory*, *operations research*). Nun geht es um die Frage, wie im Ausnahmezustand eines Atomkrieges – der, wenn man der Spieltheorie glaubt, niemals rational hätte entschieden werden können, weil es sicher die letzte



zu treffende Entscheidung gewesen wäre (Ghamari-Tabrizi 2005, Pias 2009) – die Entscheidungsfähigkeit der Regierung, verstanden als Operationen eines vitalen Systems, aufrecht erhalten werden kann. Mit Souveränität geht klassischerweise die Erhabenheit über und ein externes Verhältnis zu den regierten Materien einher. Im *Continuity of Government Planning* findet sich die Regierung jedoch impliziert bzw. »eingefaltet« in das Prozessgeschehen, das zu sichern sie sich anschickt. Im Falle des Falles wäre sie genauso von den Auswirkungen eines Atomkrieges betroffen wie alle übrigen Systeme in ihrem Einflussbereich. Mit einer Strategie vorbereiteter Entscheidungsalgorithmen sollte diese missliche Lage bearbeitet werden. Die Regierung kann in der Gegenwart Entscheidungen darüber treffen, wie sie in Zukunft entscheiden wird. Durch diese Festlegung auf bestimmte Entscheidungen in der gegenwärtigen Zukunft ist die Regierung in der zukünftigen Gegenwart ihren vergangenen Entscheidungen unterworfen und damit gerade nicht mehr souverän.<sup>206</sup> Die Vorbereitung durch *command and control*-Protokolle erzeugt eine Zeitbindung (zum Konzept der Zeitbindung siehe: Luhmann 2003, 59ff.) und somit eben Kontinuität. Sie erzeugt dadurch aber auch eine Selbstbindung oder Selbstunterwerfung der souveränen Macht. Die entscheidende Macht, die Macht der und zur Entscheidung, ist nun weniger souverän als protokollarisch: es handelt sich um eine *protokollarische Souveränität*. Souverän ist, wer über das Notfallprotokoll entscheidet. Die atomare Tragödie und damit auch das souveräne Trauerspiel sind bislang ausgeblieben und damit auch der Härtestest der Funktionsfähigkeit der *continuity*-Pläne. Es steht jedoch zu befürchten, dass es im Ernstfall ähnlich – wenn auch weit weniger unterhaltsam – zugegangen wäre wie in Stanley Kubricks Film *Dr. Strangelove*, in dem der Souverän, der US-Präsident, den menscheitsvernichtenden Atomkrieg nicht stoppen kann, weil die Technokraten der Apokalypse, verkörpert durch Dr. Strangelove (eine Parodie auf Hermann Kahn), bereits alle Entscheidungen so fest vorprogrammiert haben, dass es nichts mehr zu entscheiden gibt und die Katastrophe genau deshalb nicht mehr abzuwenden ist.

---

206 In der Systemtheorie wird zwischen gegenwärtiger Zukunft und zukünftiger Gegenwart unterschieden, um die Differenz von Erwartungen über die Zukunft und tatsächlich eingetretener Zukunft zu markieren (siehe etwa: Luhmann 1992a, Esposito 2007, 50–67).

#### 4.1.3. Vom IT disaster recovery zum Business Continuity Management

Nach dem Ende des Kalten Krieges wurde in der BRD damit begonnen, die zahlreichen Regierungsbunker von Bund und Ländern zurückzubauen. Vom Regierungsbunker bei Bonn ist inzwischen nur noch ein Bruchteil erhalten, der seit 2008 als Museum dient. Ähnlich erging es den meisten Bunkeranlagen der Länder und Städte. Trotz des beschränkten Nutzens des Bunkerarchipels, das uns heute über seine musealisierten Überreste als längst erloschene Geschichte entgegentritt, sollte man in den geplanten, geübten und gebauten Kontinuitätsprojekten der Vergangenheit mehr sehen als Kalten Kriegs-Kitsch. Denn das organisatorische Wissen und die technischen und architektonischen Blaupausen des *Continuity of Government* sind in Gestalt des sogenannten *Business Continuity Management* (BCM) weiterhin wirksam, wenn auch auf einem ganz anderen Schauplatz – die Bunker des Kalten Kriegs mögen stillgelegt sein, die sogenannten *hot sites* der Banken, in denen zu jeder Zeit der Geschäftsbetrieb bruchlos fortgesetzt werden kann, sind es nicht. Die Materialbevorratung mit Kriegsrohstoffen mag reduziert worden sein, doch die kritischen Materien der Informationsgesellschaft – Daten und Informationen – werden in riesigen Serverräumen gespeichert, um im Notfall auf Abruf verfügbar zu sein. Und auch das Wissen um die Notwendigkeit von Planungen und Entscheidungsalgorithmen für den Notfall, die Priorisierung von Aufgaben im Krisenmanagement und die Sensibilität für zeitkritische und vitale Operationen wurden in den vergangenen Jahren weiter ausgearbeitet. Die *Continuity of Government*-Planung im Kalten Krieg ist nicht deshalb eine Geschichte der Gegenwart, weil sie aufgrund ihres Erfolges bis heute ungebrochen fortbesteht, sondern weil sie erstmals Probleme aufgeworfen hat, die noch heute Bestand haben – darin besteht ihre historische Kontinuität.<sup>207</sup>

Tatsächlich fließt das militärische Wissen des Krisenmanagements in das gegenwärtige BCM ein. Der genealogische Einfluss ist dabei jedoch eher indirekt, weil eine entscheidende Episode zwischen *Continuity of Government Planning* und gegenwärtigem *Business Continuity Management* liegt: der Aufstieg der IT-Sicherheit als zentraler Brennpunkt der Ausarbeitung betrieblicher Sicherheitsstrategien. Ähnlich wie im Fall des Schutzes Kriti-

---

207 Entsprechend verwundert es nicht, dass die militärische Herkunft des *Continuity Management* heute noch zu spüren ist. So betonte ein Unternehmensberater, der sich auf BCM-Beratung spezialisiert hat, im Interview mit mir mehrfach die Vertrautheit des Militärs mit Krisensituationen: »Im Militärischen kennen wir das, dass dort auch tatsächlich ausgebildet wird, wie in einer Krise im Prinzip gehandelt wird.« (Interview 6)

scher Infrastrukturen (Dunn Caverty 2008) ist mit der wachsenden Bedeutung von Informations- und Telekommunikationstechnologien in den 1980er Jahren auch die Besorgnis um Störungen der digitalen Infrastruktur gewachsen. Im Feld des *IT disaster recovery* wurde an Konzepten und technischen Lösungen gearbeitet, die sicherstellen sollten, dass Unterbrechungen im digitalen Informationsfluss und Schädigungen der digitalen Infrastruktur möglichst wenige Folgeschäden für Unternehmen verursachen. Im Fokus stand dabei die Gefahr des Datenverlustes. Es ging also vor allem um die Sicherung informatorischer *assets* – um die Sicherung von Daten über unterschiedliche *backup*-Systeme.

Diese Fokussierung auf die technischen Aspekte betrieblicher Sicherheit und damit auf die *assets* der digitalen Welt wurde jedoch seit den späten 1990er Jahren vermehrt infrage gestellt. Ein BCM-Experte, der das BCM einer großen deutschen Bank koordiniert, identifizierte im Interview zwei »Wendepunkte« (Interview 4), die zu einer Erweiterung betrieblicher Sicherheitsstrategien hin zum Kontinuitätsmanagement beigetragen haben. Der erste »Wendepunkt«, der von Expert\_innen betrieblicher Sicherheit immer wieder erwähnt wird, ergab sich dabei noch aus der Logik der IT-Sicherheit: das »Jahr 2000-Problem«. Zwar stellte sich das Problem selbst noch vor dem Hintergrund interner Schwierigkeiten von Informationssystemen. Computerprogramme, die nur auf zweistellige Jahresnummerierungen (zum Beispiel 99) programmiert waren, hätten Probleme bereiten können, weil sie nach 99 nicht einfach weiter bis 100 hätten zählen können, sondern stattdessen auf 00 gesprungen wären. Falsche Datenanzeigen hätten zu massiven Terminproblemen führen können, die gerade bei terminsensiblen Geschäftsmodellen (insbesondere in der Finanzbranche) zu sehr empfindlichen Störungen geführt hätten. So hat das »Jahr 2000-Problem« Kontinuitätsschwierigkeiten auf der organisatorischen, vor allem aber zeitlichen Ebene von Geschäftsprozessen sichtbar gemacht. Die potenzielle Störung der digitalen Infrastruktur der Zeitmessung ließ den kritischen Faktor Zeit bewusst werden. Neben *assets*, so zeigte sich, mussten zeitlich und terminlich eng getaktete *Prozesse* geschützt werden.

Drastisch verschärft wurden diese Sorgen (gerade im Bankensektor) durch die Terroranschläge vom 11. September 2001, die eine schwerwiegende Unterbrechung von Geschäftsprozessen mitten im Herzen des globalen Finanzkapitalismus bewirkt hatten. Zwar gab es zum Zeitpunkt des 11. September bei Banken in New York bereits rudimentäre Ansätze im *Contingency Planning*, die durch das »Jahr 2000-Problem« sowie die Terroran-

schläge auf das World Trade Center im Jahr 1993 angeregt worden waren (siehe dazu: Beunza und Stark 2003). Aber erst nach dem 11. September ist es zur Neuorientierung und Etablierung des BCM in seiner gegenwärtigen Form gekommen. Denn der 11. September gilt in der Branche als der erste große genuine *business incident*, der die Mängel einer rein IT-basierten Sicherheitsstrategie aufgezeigt hat.

»Der zweite Wendepunkt war 9/11 in den USA, als – heute würde man sagen – schwarze Schwäne eingetreten sind, als nämlich Szenarien eingetreten sind, die vorher unvorstellbar waren. Nämlich, dass zwei große Bürogebäude mitten in New York zerstört werden, und Unternehmen dann also viele Mitarbeiter verlieren und nicht mehr arbeitsfähig sind. Auch das eine Business-Seite, das war kein IT-Incident, sondern das war ein richtiger Business-Incident durch Terrorismus. Das hat den Schwenk geführt zum Business Continuity Management.« (Interview 4)

Dass es sich beim BCM noch um eine sehr junge Disziplin handelt, zeigt sich auch daran, dass die Bedeutung und die Spezifität des BCM von Expert\_innen und Regulator\_innen immer noch gegen das ältere, IT-basierte *disaster recovery* stabilisiert werden muss. BCM ist »mehr als IT-Notfallmanagement« (BSI 2008, 4), »mehr als Back-up« (Interview 5) und erfordert deshalb eine »ganzheitliche Betrachtung«, die nicht nur die »Resource Informationstechnik« (BSI 2008, 1) im Blick hat. Ein zeitgemäßes »Sicherheitsmanagement muss ganzheitlich und prozessorientiert sein und nicht auf IT fokussiert« (BSI 2008, 23), denn »Technologien alleine lösen keine Probleme« (BSI 2008, 26).

Durch die Wende zum gegenwärtigen *Continuity Management* hat sich auch die Rationalität der Sicherheit sowohl im Hinblick auf ihr Leitbild als auch auf ihre grundlegende Zielvorstellung geändert. Ging es in der klassischen IT-Sicherheit noch um den *Schutz von assets*, also Gütern, geht es im *Business Continuity Management* nun um das *Aufrechterhalten von Prozessen*. Damit kommt es zu einer dreifachen Verschiebung. Nicht mehr Integrität, sondern Kontinuität ist das Ziel der Sicherheit. Nicht mehr Schutz, sondern Gewährleistung und Ermöglichung ist ihre praktische Maxime. Und weniger Güter und Produkte (ob materielle oder immaterielle, Daten, Geld, oder Industrieprodukte), sondern Prozesse und Zirkulationen bilden den »Gegenstand« der Sicherheit. Damit schließt das gegenwärtige *Business Continuity Management* an das *Continuity of Government Planning* des Kalten Krieges an. Schon damals wurde den staatlichen Sicherheitsexpert\_innen klar, dass nur durch fortgesetzte Operationsfähigkeit der Regierung und der vitalen Systeme die wesentlichen *assets* des Landes – die Bevölkerung

und der Wohlstand der Gesellschaft, die Integrität von Souveränität und Territorialität – geschützt werden können. So ist es auch beim BCM: Nur, wenn das Unternehmen operationsfähig bleibt, kann es seine *assets* (ob dies nun Daten, Geld oder materielle Güter sind) effektiv schützen und bewahren.

#### 4.2. Krisenroutine. Die Organisation des Notfalls im BCM

Kontinuität ist das Leitbild der Sicherheit im *Business Continuity Management*. Die Konzeption von Sicherheit als möglichst ununterbrochene Fortsetzung von Prozessen entspricht dem normativen Leitbild des Sicherheitsdispositivs der Resilienz. Schließlich geht es bei Resilienz nicht um fixe Stabilitätswerte, sondern vielmehr darum, überhaupt »im Spiel« zu bleiben. Ziel ist es, wie Crawford Holling bereits in den 1970er Jahren in Bezug auf Ökosysteme formuliert hatte: »to stay in the game [...] by maintaining flexibility« (Holling 1973). Insofern verbindet Resilienz »learning with continuity« (Holling 2001, 390) und darf nicht statisch von festen Normwerten her verstanden werden.

Aber wie lässt sich Kontinuität konkret organisieren? Wie gelingt der Transfer des Resilienzkonzepts von ökologischen auf organisatorische Prozesse?<sup>208</sup> Zur Beantwortung dieser Fragen möchte ich im Folgenden näher auf die organisatorische Logik des *Business Continuity Management* eingehen. Dabei widme ich mich zunächst der Rolle von Gesetzen und Standards für die Ausbreitung der generischen Praxisform des Kontinuitätsmanagements (4.2.1). Sodann werde ich die zeitliche Logik des BCM

---

208 Fragen nach der Resilienz von Organisationen in Anbetracht von potenziellen Störungen und Katastrophen sind Gegenstand einer breiten Debatte zu sogenannten *High Reliability Organizations* (HRO) (siehe etwa: Weick und Sutcliffe 2011). Die HRO-Forschung argumentiert im Gegensatz zur *Normal Accident Theory* von Charles Perrow (1987), dass auch in komplexen und risikobehafteten Organisationen, etwa auf Flugzeugträgern (Rochlin, La Porte und Roberts 1998), Katastrophen ausgeschlossen werden können, wenn geeignete Organisationsstrukturen und »collective mindfulness« (Weick, Sutcliffe und Obstfeld 2008) eine besonders große Störungsresistenz erzeugt. Letztlich geht es in der HRO-Debatte zumeist darum, in normativer Absicht Beiträge zur Erhöhung betrieblicher Verlässlichkeit zu leisten. Insofern ist diese Debatte für meine Forschungsanliegen nur von begrenztem Nutzen. Allerdings darf nicht übersehen werden, dass diese auch in der soziologischen Organisationsforschung geführten Debatten Konzepte des Kontinuitätsmanagements beeinflussen.

beleuchten, die sich vor allem in der veränderten Wahrnehmung eines Betriebs als Prozess und in der Bestimmung von Kritikalität als zeitkritisch zeigt (4.2.2.). Das Problem, wie im Notfall schnelle und richtige Entscheidungen getroffen werden können, das schon in der Geschichte des *Continuity of Government Planning* eine große Rolle gespielt hat, führt dazu, dass Kontinuitätsmanager\_innen die Rolle von Entscheidungsstrukturen in ihren Organisationen reflektieren müssen (4.2.3.). Die betriebswirtschaftliche Logik des BCM zeigt sich vor allem in der Anforderung an Kostenbegrenzung von Kontinuitätsmaßnahmen einerseits und andererseits in Überlegungen, wie Krisen für den Betrieb als »Chance« genutzt werden können (4.2.4.). Schließlich werde ich auf die generischen Maßnahmen des Kontinuitätsmanagements eingehen. Obwohl es um die Aufrechterhaltung des abstrakt-zeitlichen Gutes »Prozess« geht, ist es nur über konkrete, materielle, räumliche Installationen und Techniken möglich, diesen Prozess zu erhalten (4.2.5.).

#### 4.2.1. Standardisierung und Globalisierung des BCM

In der jüngeren Geschichte konnte sich BCM als eigenständige Sicherheitstechnologie etablieren. Eine Reihe gesetzlicher und regulatorischer Initiativen auf nationaler und internationaler Ebene hat das Management von Kontinuität zu einer wesentlichen Praxisform der Sicherheit insbesondere in der Privatwirtschaft werden lassen. In Deutschland sind gerade für Betreiber Kritischer Infrastrukturen Katastrophenvorsorgemaßnahmen obligatorisch (siehe Kapitel 3.1.3.). Schließlich sind Infrastrukturbetreiber und Unternehmen so miteinander vernetzt und aufeinander angewiesen, dass schlechte Katastrophenvorsorge in einem Unternehmen schnell gravierende Auswirkungen auf ganze Branchen bzw. ganze Infrastrukturnetze haben kann. Der einzelne Betrieb erscheint aus der Regulationsperspektive also vor allem als Knotenpunkt in einem Netzwerk vitaler Systeme. BCM hat dabei den größten Bekanntheitsgrad bei Unternehmen und ist deshalb für viele das Katastrophenvorsorgeprogramm der Wahl. Das hat auch eine Mitarbeiterin im BBK mit Zuständigkeiten im Bereich Schutz Kritischer Infrastrukturen so bestätigt:

»Mit dem Begriff Risiko- und Krisenmanagement kommt man in Unternehmen häufig nicht viel weiter. Sobald eben das Thema BCM aufscheint, dann wissen die etwas damit anzufangen und können es auch nach oben, gegenüber ihrem Vorstand besser verkaufen.« (Interview 1)

Jenseits von gesetzlichen Vorschriften zur betrieblichen Katastrophenvorsorge in einzelnen Ländern und Branchen sind auf internationaler Ebene vor allem Standards wichtig zur Etablierung und Ausbreitung von BCM. Fraglos am wichtigsten ist hier der ISO-Standard 22301 für BCM, der zunächst im Jahr 2012 aufgesetzt wurde (ISO 2012b). Der Standard fasst eine Reihe von mittlerweile als *best practice* angesehenen Verfahren des Kontinuitätsmanagements zusammen und repräsentiert gegenwärtig den Goldstandard des BCM. Als Produkt der International Organization for Standardization (ISO) hat der Standard einen globalen und universellen Geltungsanspruch. Er soll auf alle möglichen Arten von Unternehmen anwendbar sein. Programmatisch heißt es: »The requirements specified in this International Standard are generic and intended to be applicable to all organizations, or parts thereof, regardless of type, size and nature of the organization.« (ISO 2012b, 1) Diese »generische« Ausrichtung macht den Standard zunächst wenig aussagekräftig. Sowohl die 24 Seiten langen *requirements* (Anforderungen) als auch die etwa doppelt so lange *guidance* (ISO 2012a) bieten nur wenig Aufschluss darüber, was BCM ist. Gehaltvolle Ausführungen dazu, was konkret unternommen werden kann, um ein Unternehmen sicherer zu machen, finden sich kaum. Stattdessen wird sehr ausführlich geschildert, was gemacht werden muss, um sicher zu gehen, dass man den Standard erfüllt hat. Vor allem eine ausführliche Dokumentation (ISO 2012, 14) aller vorgenommenen Schritte und die regelmäßige und vielfältige Evaluation der Maßnahmen (gefordert wird: »monitoring, measurement, analysis and evaluation, internal audit, management review« (ISO 2012b, iii)) soll diese Sicherheit schaffen – es gilt zu dokumentieren und zu beweisen, dass man etwas für die Sicherheit getan hat. Hier zeigt sich bereits ein erstes Charakteristikum von Kontinuitätsmaßnahmen im Rahmen betrieblicher Sicherheit. Vor allem Michael Power (2007) hat mehrfach herausgearbeitet, dass betriebliche Sicherheit mindestens ebenso sehr eine Anforderung interner Kontrollprozeduren – *internal audit* – wie externer Bedrohungen ist. Die »Risikogesellschaft« ist hier gewissermaßen ein Produkt der »audit society« (Power 1999), Reflexivität wird durch die ständige Beobachtung durch ein Heer von Wirtschaftsprüfer\_innen erzeugt. Dabei ist die Standardisierung des Risikomanagements in Betrieben wiederum die Voraussetzung für deren Überprüfung im *audit* (siehe: Power 2007, 66–102 sowie 152–182). Denn erst die Standards erzeugen einheitliche Referenzpunkte für Prüfer\_innen und Überprüfte und erzeugen so die für die Evaluation notwendige Einheitlichkeit.

Dieser Zusammenhang zeigt sich auch im BCM sehr deutlich. Indem sie auf die Einhaltung von *benchmarks* im Kontinuitätsmanagement verweisen können, sind die Unternehmen zwar nicht unbedingt gegenüber allen Gefahren, aber zumindest gegenüber kritischen Nachfragen, den vielfältigen internen und externen *audits* und *evaluations* abgesichert. Selbst wenn sich einzelne Maßnahmen rückblickend als falsch herausstellen sollten, verbürgt die Orientierung am Standard ein verantwortliches und risikosensibles Verhalten. Umgekehrt nutzen auch die internen und externen Beobachter\_innen, Wirtschaftsprüfer\_innen und Beratungsunternehmen die Standards, um zu ermitteln, ob ein Unternehmen ein gutes Kontinuitätsmanagement hat. Das wird vom ISO-22301 sogar als einer seiner zentralen Gebrauchswerte angepriesen:

»The International Standard is applicable to all types and sizes of organizations that wish to [...] seek certification of its BCMS by an accredited third party certification body [...] [and/or] make a [...] self-declaration of conformity with this International Standard.« (ISO 2012b, 1)

Der Standard wird also angewendet, um den Anforderungen an die Standardisierung zu genügen. So selbstbezüglich und absurd diese Logik erscheinen mag, sie bleibt nicht folgenlos. Denn das Spiel von interner Risikokontrolle von Unternehmen und externer Kontrolle durch *auditors*, die sich alle auf dieselben Standards beziehen, trägt zur weltweiten Ausbreitung einer bestimmten Version von BCM ebenso wie zur Proliferation eines weitläufigen Praxis- und Professionsfeldes betrieblicher Sicherheit bei.

Letztlich ist ISO-22301 also eine Art Meta-Standard, der andere Standards und Regelwerke aufgreift und zusammenfasst. Er bezieht sich auf bereits bestehende nationale Regulierungen und Standardisierungsbemühungen zur betrieblichen Sicherheit und zum *Business Continuity Management*. Auch der Standard für 100-4 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zum Notfallmanagement bzw. *Business Continuity Management* ist bereits 2008, also vier Jahre vor dem ISO-Standard, erschienen und im Vergleich mit diesem wesentlich gehaltvoller. Vor allem die angelsächsischen<sup>209</sup> und asiatischen Länder waren aber Vorreiter im BCM.

---

209 Einer der ersten Standards für *Business Continuity Management* ist der britische Standard BS-25999-1:2006 (BS 2006), der bereits wesentliche Aspekte des ISO-Standards vorweggenommen und entsprechend bedeutsam für dessen Entwicklung war.



Für die Verbreitung des BCM in der Privatwirtschaft sind Standards wichtiger als Gesetze. Denn selten wird in Gesetzen spezifiziert, was die einzelnen Katastrophenvorsorgemaßnahmen beinhalten müssen. Diese Lücke füllen die Standards – und zwar selbst noch die sehr abstrakten und generischen. Sie fungieren gleichsam als globale Protokolle für die Erstellung jeweils firmenspezifischer Notfallprotokolle und versammeln so die verstreuten Netze des globalen Sicherheitsgefüges des Kontinuitätsmanagements. »Also dass etwas gemacht wird, kommt aus der Regulierung heraus. Die Regulierung sagt nicht, wie es gemacht werden muss. [...] Wie ich etwas tue, das kommt aus den Standards heraus« (Interview 4). Die Orientierung an Standards sorgt also für eine Globalisierung der immer gleichen *Business Continuity*-Maßnahmen, obwohl diese von ganz unterschiedlichen nationalen Regularien und Körperschaften eingefordert werden. Standardisierungen führen dazu, dass sich BCM als abstrakte Sicherheitstechnologie globalisieren kann. BCM bildet ein globales Sicherheitsgefüge, obwohl es von keiner Weltregierung implementiert wurde und von nationalen Regulationen häufig nur angeregt, aber nicht vorgeschrieben wird.

Gerade die Abstraktheit von internationalen Standards ist dazu geeignet, unterschiedliche »communities of practice« (Lampland und Star 2009, 7) zu koordinieren bzw. überhaupt erst entstehen zu lassen. Denn das Generische der Standards lässt seinerseits eine Lücke, die dann wiederum von neu entstandenen Sicherheits- bzw. BCM-Expert\_innen gefüllt werden kann. Denn wie genau die generischen Vorgaben in konkreten Unternehmen umgesetzt werden können, ergibt sich aus den Standards nicht. Wenn die Gesetze sagen, *dass* etwas getan werden muss, und die Standards sagen, *was* getan werden muss, dann braucht es zusätzliche Berater\_innen, die sagen, *wie* etwas umgesetzt werden kann. Unternehmen können dann entweder spezielle Fachkräfte als *Business Continuity Manager* einstellen oder Unternehmensberater\_innen beauftragen. Ein Unternehmensberater, mit dem ich ein Interview geführt habe, hat seine Aufgabe so definiert:

»Ok, in den Standards, da steht drin: mach einen Krisenstab, mach Übung usw. Aber: wie besetze ich denn eigentlich ein Krisenteam? Welches sind die Keyplayer in so einem Krisenteam, Krisenstab? Gibt es dafür Unterschiede? Und wie soll ich das aufbauen, wie häufig sollte ich üben? Was soll ich eigentlich üben? Also die Sachen kommen in dem Umfeld eigentlich relativ kurz und da setze ich halt mit meiner Beratung an.« (Interview 6)

Mittlerweile hat sich eine ganze Szene bzw. *community of practice* für BCM entwickelt. Es gibt Konferenzen und Fachtagungen, Fortbildungen und Workshops, Online-Foren, Internetseiten und Blogs für BCM.

#### 4.2.2. Die Vordringlichkeit des Zeitkritischen

Das Sicherheitsleitbild der Kontinuität im BCM geht mit einer Konzeptualisierung des Betriebs als Prozess bzw. als Reihe miteinander verzahnter Wertschöpfungsketten einher. Das wird vor allem im Rahmen der Verwundbarkeitsanalyse im BCM sichtbar: der sogenannten *Business Impact Analyse* (BIA). Die BIA entwirft eine Morphologie des vitalen Systems »Betrieb« als Kette von Verkettungen, als Prozess von miteinander verzahnten Prozessen.<sup>210</sup> Jeder Prozess ist dabei auf *inputs* angewiesen und produziert *outputs* für wieder andere Prozesse. Im 2015 veröffentlichten ISO-Standard 22317 zur BIA heißt es etwa: »A process is a set of interrelated or interacting activities which transform inputs into outputs.« (ISO 2015, 9)<sup>211</sup>

Dieses Verständnis des Geschäfts als System interdependenter Prozesse führt zu einem charakteristischen Verständnis von Kritikalität. »Kritisch im Sinne des Notfallmanagements bedeutet »zeitkritisch«, also dass dieser Prozess eine schnelle Wiederaufnahme der Tätigkeit erfordert, da sonst ein hoher Schaden für die Institution zu erwarten ist.« (BSI 2008, 28) Zur Identifizierung zeitkritischer Prozesse ist ein durchaus ungewohnter Blick auf das eigene Unternehmen erforderlich. Zeitkritische Prozesse können unter Umständen nebensächlich erscheinen, etwa wenn es sich um basale Infrastrukturleistungen handelt, die überhaupt nur dann auffallen, wenn sie ausfallen. Der Betrieb muss daher nicht nur von seinem Kern – den für

---

210 Aus der Sicht der wissenschaftlichen Organisationsforschung ist das freilich keine ungewöhnliche Beschreibung eines Betriebs. So beschreiben auch die organisationssoziologischen Ansätze etwa von Latour (2014, 517–557) und Luhmann (2000) die Organisation als Prozess bzw. versuchen, die Organisation vom Prozess des Organisierens her zu verstehen. Die Arbeiten von Karl Weick (1985), der diese Position schon lange vertritt, werden auch in den Zirkeln des *Business Continuity Management* rezipiert.

211 Ähnliche Formulierungen finden sich auch im Standard für Notfall- und *Business Continuity Management* vom Bundesamt für Sicherheit in der Informationstechnik (siehe etwa: BSI 2008, 31). Die Tatsache, dass das Bundesamt für Sicherheit in der Informationstechnik – und nicht das Bundesamt für Bevölkerungsschutz – den Standard zum *Business Continuity Management* erstellt hat, zeugt von der starken Verwurzelung von BCM in der IT-Sicherheitslandschaft.

das Unternehmen prestige- oder gewinnträchtigsten Geschäften –, sondern ebenso von seinen infrastrukturellen Rändern her betrachtet werden.

Gerade wegen dieser häufig versteckten Kritikalität wird eine angemessene Kartierung der Abhängigkeiten zwischen unterschiedlichen Prozessen und ihrer spezifischen Verwundbarkeit als Voraussetzung für ein gelungenes Kontinuitätsmanagement betrachtet. Die Kartierung von Verwundbarkeiten als Mittel der Risikoanalyse ist, wie gezeigt, ein Standardverfahren der Katastrophenvorsorge (siehe Kapitel 2.3.3.). Das Besondere der *Business Impact*-Analyse im BCM ist aber ihre zeitliche – und gerade nicht primär räumliche – Logik der Kartierung. So soll eine »Prozesslandkarte [...], die die Prozesse listet und die verschiedenen Abhängigkeiten zwischen den einzelnen Geschäftsprozessen aufzeigt« (BSI 2008, 32), erstellt werden. Abhängigkeiten konstituieren sich dabei nicht durch räumliche Nähe oder topologische Nachbarschaft, sondern durch ihre zeitliche Stellung im Vorher und Nachher des umfassenden Geschäftsprozesses. Der »Abhängigkeitsgrad ist für beide Richtungen zu ermitteln, also in Richtung Vorgänger und in Richtung Nachfolger.« (BSI 2008, 43) In einer geradezu evolutionären Sprache wird daher auch von der »Vererbung« (BSI 2008, 42) von Störungen eines Prozesses auf einen anderen gesprochen. Verwundbarkeit erwächst hier nicht nur aus der Vernetzung von physischen Strukturen oder interdependenten Akteuren – schließlich geht es beim *Business Continuity Management* zunächst einmal immer nur um ein einzelnes Unternehmen. Sie ergibt sich vielmehr auch aus dem spezifischen Rhythmus des Geschäfts, aus dem »Eingetaktet-Sein« in Abläufe und Anforderungen, die *just-in-time* erfüllt sein müssen und nicht aufgeschoben werden dürfen. Denn neben zeitkritischen Prozessen, die nicht lange zum Erliegen kommen dürfen, gibt es auch kritische Zeiten. Dazu gehören zeitkritische Perioden im Geschäftsprozess, die durch – teilweise vorhersehbare – »fluctuations in demand or peak operating periods« (ISO 2015, 11) entstehen.<sup>212</sup> Zudem können wichtige Termine und Fälligkeiten, wie die »tägliche Cut-Off Time [...] in Banken, Redaktionsschluss für Anzeigen einer Wochenzeitung, das Jahresende für einen Jahresabschluss« (BSI 2008, 37), kritische Punkte im Geschäftsprozess erzeugen. Hier ist es nicht die Ausfallzeit, die Kritikalität erzeugt, sondern der Termindruck, der teils extreme Verwundbarkeiten

---

212 Solche »Fluktuationen« von Angebot und Nachfrage treten, wie gesehen, auch im Stromsystem auf. Deshalb verwundert es nicht, dass auch hier die BIA zum Einsatz kommt (siehe Kapitel 3.3.4.).

gegenüber Geschäftsunterbrechungen zu bestimmten Zeiten bewirkt. Werden Termine nicht eingehalten, drohen Verluste, Imageschäden und vor allem auch Vertragsstrafen für die betroffenen Unternehmen.

Die zeitliche Logik der Kritikalitätsbestimmung hat vor allem einen praktischen Sinn. Die vorsorgliche Identifizierung zeitkritischer Prozesse soll im Ereignisfall eine angemessene Notfallreaktion anleiten. »Ein bei der BIA als »unkritisch« eingestufter Geschäftsprozess bedeutet nicht, dass dieser für die Institution unwichtig ist, sondern lediglich, dass er eine geringere Priorität für die Wiederherstellung hat.« (BSI 2008, 28) Im Falle einer Unterbrechung kommt es darauf an, nicht nur schnell, sondern auch in der richtigen Reihenfolge zu reagieren. Dabei hängt die »Umsetzungsreihenfolge« (BSI 2008, 62) für Notfallmaßnahmen entscheidend von der Vorhergehenden »process prioritization« (ISO 2015, 9f.), also der Bestimmung zeitkritischer Geschäftsprozesse ab. Im Angesicht knapper zeitlicher Ressourcen und eines sich schnell eskalierenden Krisengeschehens muss gewissermaßen die Vordringlichkeit des Zeitkritischen beachtet werden.<sup>213</sup>

Hierin liegt eine nicht zu unterschätzende Schwierigkeit jeder Art des Notfallmanagements in Organisationen. Wenn etwas schiefgeht, dann nämlich nicht entlang der gewohnten Geschäftsgänge eines Betriebes. Die Unterbrechung kann nicht wie andere Aufgaben abgearbeitet oder im Zweifel vertagt werden. Chaotisch ist ein katastrophischer Vorfall in zeitlicher Hinsicht schließlich darin, dass er die temporale Komplexitätsreduktion einer geordneten Sukzession von Ereignissen (siehe dazu: Luhmann 1980), die gerade auch für Organisationen so wichtig ist, über den Haufen wirft. Bei einer Katastrophe geht nicht nur alles schief, was schiefgehen kann – wie das in Katastrophenzusammenhängen immer wieder gerne zitierte Gesetz Murphys besagt (siehe etwa: BSI 2008, 38) –, sondern es geht schlimmstenfalls auch alles zur gleichen Zeit schief, oder zumindest viel zu schnell und in ungeahnter Reihenfolge. Erfahrungen mit Übungen und tatsächlichen Katastrophen haben immer wieder gezeigt, dass es Verantwortlichen und Betroffenen gerade in diesen chaotischen Situationen schwer fällt, Wichtiges von Unwichtigem zu unterscheiden. In der Katastrophenmedizin wird diesem Problem mit der Technik der Triage begegnet (siehe dazu: Redfield 2008, Ellebrecht 2009). Bei der Triage geht es

---

213 Damit spiele ich auf Luhmanns (1971a) Aufsatz *Die Knappheit der Zeit und die Vordringlichkeit des Befristeten* an, in dem er gezeigt hat, dass Termine und Befristungen in Organisationen wie mehr oder weniger stumme Imperative funktionieren, die festlegen, welche Tätigkeiten vorrangig ausgeübt werden.

darum, diejenigen Personen zuerst zu behandeln, bei denen Hilfe am dringlichsten geboten ist. Hier ist die Frage der Zeit und des Tempos der Hilfe im Wortsinne vital. Eine ähnliche Selektion muss auch beim betrieblichen Kontinuitätsmanagement vorgenommen werden. Es bedarf gleichsam einer Prozesstriage, die Vordringliches von Nachrangigem und vitale von weniger »überlebenswichtigen« Prozessen unterscheiden kann. Im Idealfall wird ein entsprechendes Aufgabenprotokoll bzw. ein Reaktionsalgorithmus im Vorhinein durch einen Notfallplan festgelegt. Der Imperativ schnellen Reagierens macht den Notfallplan, meist in Form eines »Notfallhandbuchs« (BSI 2008, 79), zu einem obligatorischen Bestandteil des Kontinuitätsmanagements. Aus diesen Protokollen soll möglichst klar und für alle beteiligten Akteure verbindlich hervorgehen, wer wann was zu tun hat und welche Prozesse zuerst beachtet werden müssen.

Die Bindung an ein Notfallprotokoll stiftet Orientierung in einer Situation, in der gewohnte Handlungsmuster durchbrochen sind. Allerdings geht mit dieser »Sicherheit« ihrerseits ein Risiko einher, weil die Verpflichtung auf einen vorgefertigten Plan die Flexibilität reduziert, angemessen auf anfallende Situation reagieren zu können. Wie Klaus Japp (1990, 34) einmal formuliert hat, bedarf es im Notfall zuweilen der »Rationalität« impressionistisch geführter Entscheidungen«, die sich gerade nicht an den Entscheidungsalgorithmen des Notfallplans orientieren. Die Standards zum betrieblichen Kontinuitäts- und Notfallmanagement adressieren diese Problematik mit Hilfe einer Unterscheidung zwischen »Notfall« und »Krise«, die jeweils unterschiedliche Reaktionsformen erforderlich machen.

»Der wesentliche Unterschied zwischen einem Notfall und einer Krise besteht darin, dass ein Notfall im Wesentlichen mit Hilfe von Notfallplänen gemeistert werden kann. Eine Krise erfordert weitergehende Kompetenzen. Sie ist einzigartig, kann auf kein vorgedachtes Muster aufsetzen und erfordert schnelle und kompetente Entscheidungen.« (BSI 2008, 70)

Was hier auffällt, ist der selbstbezügliche Charakter der Definitionen von Krise und Notfall. Denn die unterschiedlichen Fälle werden nicht gemäß eines objektiven oder den Ereignissen intrinsischen Charakteristikums voneinander abgegrenzt, sondern nach der internen Bearbeitungslogik, der Reaktion auf die Unterbrechungsereignisse.<sup>214</sup> Wir haben es gleichsam mit

---

<sup>214</sup> Das gilt genauso für die Klassifikation der Störung. Eine Störung zeichnet sich dadurch aus, dass sie auch ohne Notfallplan und nur mit den einer Organisation ohnehin zur Verfügung stehenden Mitteln behoben werden kann. Die Katastrophe steht am äußersten Ende der Eskalationsskala. Die Katastrophe ist ein Ereignis, das das Ausmaß der

konstruktivistischen Konzepten von Störung, Notfall, Krise und Katastrophe zu tun, insofern diese durch eine organisationsinterne Interpretationsarbeit und Reaktionsform erst »produziert« und als distinkte Fälle institutionell in Kraft gesetzt werden. Krisen sind also keine hereinbrechenden Ereignisse aus der Umwelt, sondern stellen Impulse dar, die immer erst system- bzw. organisationsintern verarbeitet werden müssen und aufgrund systeminterner Unterscheidungen als spezifischer Fall etabliert werden. Damit stellt sich aber organisationsintern die schwierige Frage der Gestaltung dieser Definitionsarbeit. »Das größere Dilemma ist, wann rufe ich eine Krise aus. [...] Erst mal intern. Intern muss ja erst mal jemand hingehen und sagen, ich habe eine Krise.« (Interview 6) Aber wer soll dieser Jemand sein? Und wie und von wem wird eine Krise gemanagt, die »schnelle und kompetente Entscheidungen« erfordert?

#### 4.2.3. Krise der Entscheidung, Krise der Hierarchie

Die »Paradoxie des Entscheidens« (Luhmann 2000, 123–151), manchmal auch als Aporie der »Unentscheidbarkeit« (Derrida 1998, 49–53) adressiert, besteht darin, dass eine Entscheidung im emphatischen Sinne nur dann getroffen werden kann, wenn es keine sichere Grundlage für diese Entscheidung gibt. »Only those questions that are in principle undecidable, we can decide« (von Foerster, zitiert nach: Stäheli 2000, 253) Erst durch den Akt der Entscheidung wird performativ die Situation hergestellt, die rückwirkend als »Grundlage« der Entscheidung angesehen werden kann. Im BCM findet sich eine solche Entscheidungsparadoxie. So soll die betriebliche Bearbeitung des Notfalls gleichsam dem Ereignis folgen, das heißt es soll eine vom Normalfall abweichende Krisenroutine greifen, die auch alternative Entscheidungsstrukturen für die Zeit des Notfalls vorsehen kann. Zugleich muss das Notfallereignis, dem der Notfall- bzw. Kontinuitätsplan folgt, organisationsintern zuallererst konstruiert werden. Schließlich kann man sich nicht darauf verlassen, dass die Krise »von außen« als Krise definiert wird und damit auch intern als solche behandelt werden muss. »Es wird dann leicht, wenn die Medien es ausrufen würden.

---

Krise übersteigt. Es ist also »zeitlich und örtlich kaum begrenzbar« (BSI 2008, 5), weil hier über die Organisation hinausgehende, im Fall der »bundesrelevanten Katastrophe« (siehe dazu Kapitel 2.3.1.) sogar bundesweite Hilfeleistungen in Anspruch genommen werden müssen. Zur Definition der Begriffe Störung, Notfall, Krise und Katastrophe im BCM siehe: BSI (2008, 5).

So lange es aber nicht wirklich von außen herangetragen wird, ist die Gefahr, dass es einfach verschleppt wird« (Interview 6).

Eine erste konkrete Schwierigkeit entsteht für die Kontinuitätsmanager durch die Frage nach dem Verfahren zur Entscheidung über die Krise.

»Also in meinem Beratungsansatz sage ich: Es gibt bestimmte Leute, die dürfen einen Krisenstab einberufen. Das müssen mehrere Leute dürfen. Und zwar ohne Rang, sondern aufgrund ihrer Rolle. Der Krisenstab entscheidet dann, weil jetzt haben wir ein Gremium.« (Interview 6)

Hier wird also vorgeschlagen die organisationsinterne Konstruktions- bzw. Interpretationsarbeit der Krise aufzuteilen. Es soll eine Detektionsinstanz, unabhängig von einer Entscheidungsinstanz geschaffen werden, der es zukommt den Prozess, der schließlich zur Entscheidung über die Krise führt, zu initiieren. Dabei soll diese Initiationskompetenz nicht an der Spitze der Hierarchie konzentriert sein, sondern Personen gemäß ihrer »Rolle« zukommen, die möglichst sensibel für Störungen in der Organisation ist. »Könnte bei Personal sein, nach dem Motto: Und wenn ich die dreißigste Krankmeldung aus irgendeinem Bereich habe, dann sehe ich hier eine Krise.« (Interview 6) Das gewählte Beispiel zeigt, warum die Initiierung eines Krisenprozesses ein so schwieriges Problem sein kann. Denn nicht selten ist eine Krise eine schleichende Entwicklung, die erst in einer bestimmten Intensität »kritisch« wird. Es wird daher auch empfohlen, im Vorhinein »Kriterien und Schwellenwerte festzulegen« (BSI 2008, 66), die klären sollen, ab wann kumulierende Störungen sich zu einer Krise ausgewachsen haben. Schließlich müssen die Initiator\_innen einer Krise damit rechnen, zur Rechenschaft gezogen zu werden, wenn sie unbegründet Alarm schlagen, denn ein verfrühter Alarm stellt selbst den Tatbestand einer Geschäftsunterbrechung dar. Zu große Zurückhaltung beim Alarm schlagen ist aber ebenfalls ein Problem. »Auch niedrige Rollen, die merken, dass etwas eng wäre, die müssen im Prinzip den Krisenstab einberufen dürfen, und zwar ohne – sage ich mal – Konsequenz, wenn sie das mal zu häufig tun.« (Interview 6)

Ein weiteres Problem besteht in der Zusammensetzung des Krisenstabes. Wie bei der Frage der Initiierung wird auch hier immer wieder betont, dass der Krisenstab nicht zwangsläufig aus Führungskräften des Unternehmens bestehen muss. Ein geeigneter Vertreter des Krisenstabes muss nämlich bestimmte habituelle Voraussetzungen mitbringen, die unter Umständen gerade im Vorstand gering ausgeprägt sind.

»Nicht alle Funktionsträger sind unter hoher Belastung automatisch auch gute Strategen und können im Extremfall die Arbeit eines Krisenstabes eher behindern als fördern. Mitglieder der Leitungsebene sind es gewohnt, die vollständige Kontrolle über die Situation zu haben, Entscheidungen vollständig durchzudenken und die Folgen abwägen zu können. Die Grenzerfahrung des »Kontrollverlustes« in einer Krisensituation [...] kann daher zu einem Gefühl der persönliche[n] Bedrohung bis hin zur völligen Handlungsunfähigkeit führen.« (BSI 2008, 19)

In der Krise schlägt die Stunde impulsiven Handelns unter Bedingungen von Stress; eher körperlich-affektive Reaktionsbildungen als rationales Kalkül bestimmen die Handlung:

»Die Stressursachen in einer Krise [...] reichen vom Schock über die Ereignisse, über Angst vor dem eigenen Versagen, Angst um Angehörige, emotionale Belastung, Angst vor dem Unbekannten, Reizüberflutung durch zu viel Information, widersprüchliche Informationen, unzureichende Informationen, Zeitdruck. [...] Aggressivität bis hin zu völligem Kontrollverlust kann Folge von Stress sein. Doch hat Stress nicht nur negative Seiten, sondern auch positive. Stress kann Antriebsfeder sein und Menschen zu Höchstleistungen motivieren. [...] Krisenstabsmitglieder sollten daher von Grund auf eine gewisse Stressresistenz und Selbstvertrauen mitbringen.« (BSI 2008, 75)

Die Resilienz der Organisation, so scheint es hier, ist also wesentlich auch auf die Stressresilienz, die psychische Krisenfestigkeit der Entscheidungsträger\_innen angewiesen.

Eine Möglichkeit, mit diesem Problem umzugehen, besteht darin, »Notfallbeauftragte« (BSI 2008, 75) oder gar ständige Krisenmanager\_innen zu designieren, der/die häufig auch der Business Continuity Manager ist. »Für den Krisenstabsleiter spricht, dass eine weitere Eskalationsstufe entfällt und [...] die Kompetenz zur Einschätzung von Situationen vorhanden ist. Bedenken [...] bestehen darin, dass [die] Krisenstabsleitung [...] die »Macht« in der Institution übernehmen könnte.« (BSI 2008, 67) Interessanterweise wiederholen sich hier die Probleme, die auch Verfassungen mit Ausnahmeständen haben. Wie ist es möglich, einerseits in Ausnahmesituationen bestimmten Personen einen erweiterten Handlungsspielraum zuzugestehen, damit sie schnell und effektiv auf eine kritische Situation reagieren können, und zugleich die Dauer der Ausnahmebefugnisse zu begrenzen und deren Missbrauch zu verhindern? Die Antwort soll auch im Kontinuitätsmanagement in einem System von *checks* und *balances* bestehen. »Dieser hypothetischen Problematik kann dadurch entgegen gewirkt werden, dass als Sicherungsmaßnahme eine oder mehrere Kontrollinstanzen eingeführt werden, die die Feststellung der Krise überprüfen



und widerrufen können.« (BSI 2008, 67) Dass diese Kontrollvorkehrungen ausgerechnet als »Sicherungsmaßnahmen« bezeichnet werden, zeigt, dass sich die Notfallexpert\_innen durchaus darüber im Klaren sind, dass die von ihnen empfohlenen Sicherheitsmaßnahmen selbst riskant sind. Sie sind riskant, weil sie organisatorische Entscheidungsbefugnisse neu verteilen und damit neue Unberechenbarkeiten erzeugen.

#### 4.2.4. Betriebswirtschaftliche Kalküle im Kontinuitätsmanagement

Seinem generischen Anspruch entsprechend soll das BCM auf alle Arten von Organisationen anwendbar sein – sowohl auf staatliche Bürokratien als auch auf kapitalistische Betriebe. Gleichwohl deutet schon die Betonung des »Business« im Titel der Sicherheitstechnik an, dass BCM vor allem für kapitalistische Betriebe gedacht ist. Entsprechend stellen betriebswirtschaftliche Kalküle einen zentralen Baustein im Rationalitätsgefüge des BCM dar. So erheischt die *Business Impact*-Analyse ein betriebswirtschaftliches Wissen über Prozesse und Probleme von Unternehmen und eben nicht nur technische Expertise über deren technische Abläufe und Installationen. Einem meiner Interviewpartner war es sehr wichtig, die Überlegenheit seiner betriebswirtschaftlichen Expertise gegenüber einem rein technischen *know-how* darzulegen.

»Ich selber bin Wirtschaftswissenschaftler, auch mit Finanzdienstleistungshintergrund, was wichtig ist, dergestalt, so ein betriebswirtschaftliches Know-how zu haben, weil die Business Impact Analyse eines der Kernelemente des BCM ist. [...] Das [...] reine [...] IT-Know-how, das greift da an der Stelle zu kurz, weil man Auswirkungen auf Bilanz [...] ermesen können muss.« (Interview 4)

Neben der zeitlichen Logik hat die BIA eine eminent finanzielle Schlagseite, denn Zeit ist Geld. »Bei einer BIA wird im Gegensatz zu einer Schutzbedarfsfeststellung nicht nur bewertet, welche Auswirkungen ein Ausfall eines Prozesses für die Institution hat, sondern auch, wie sich der Schaden zeitlich entwickelt.« (BSI 2008, 36). Zwar soll vermieden werden, ausschließlich finanzielle Schäden bei der Schadensbemessung in Betracht zu ziehen (BSI 2008, 34). Der ISO-Standard zur BIA unterscheidet gar zwischen insgesamt fünf unterschiedlichen Schadensgruppen bzw. »impact

categories: financial, reputational,<sup>215</sup> legal and regulatory, contractual, business objectives« (ISO 2015, 7). Klar ist aber auch, dass jede »Prozesskette« (BSI 2008, 31) immer zugleich eine »Wertkette« (BSI 2008, 32) ist, so dass beständig zeitliche und monetäre Größen ineinander übersetzt werden müssen, um den »impact« einer Geschäftsunterbrechung ermitteln zu können.

Geschäftsunterbrechungen sind kostspielig. Kostspielig – und das ist die andere Seite der Medaille – sind aber auch Sicherheits- bzw. Kontinuitätsmaßnahmen. Sicherheitsmaßnahmen binden Personen und Ressourcen, die nicht produktiv eingesetzt werden können. Die umfassenden Kontinuitätsmaßnahmen für die fortgesetzte »Funktionstüchtigkeit« von Regierungen während des Kalten Krieges waren unter anderem nur deshalb möglich, weil sie aufgrund ihrer Geheimhaltung nie einen Haushaltsausschuss oder auch nur irgendeine ernsthafte Budgetüberprüfung passieren mussten. Ein solch verschwenderischer Umgang mit Ressourcen – der dysfunktionale und nie genutzte bundesrepublikanische Regierungsbunker verschlang über drei Milliarden D-Mark – wäre für ein privatwirtschaftliches Unternehmen wie auch für einen fiskalisch begrenzt handelnden, »schlanken« Staat wohl undenkbar.

Zur Begrenzung der Kosten für BCM wird in Standards und von Akteuren des Kontinuitätsmanagements stets die Notwendigkeit von Kosten-Nutzen-Kalkulationen betont (siehe etwa: BSI 2008, 54). Hohe Kosten für Kontinuitätsmaßnahmen entstehen vor allem durch Vorhaltung kompletter redundanter Infrastrukturen, die sofort in Betrieb genommen werden können – man spricht von sogenannten »hot-Lösungen« (BSI 2008, 55). »Cold-Lösungen« (BSI 2008, 55) kosten weniger, haben aber auch einen geringen Nutzen und lassen eine längere Wiederanlaufzeit der Geschäftsprozesse erwarten. Der Nutzen der unterschiedlichen Lösungen verringert sich also – so wird kalkuliert – mit sinkenden Kosten für die Sicherheitsmaßnahmen. Deshalb soll der »sweet spot« (Interview 5) getroffen werden, an dem Kosten (für Wiederanlaufmaßnahmen) und Nutzen (die Geschwindigkeit des Wiederanlaufs) in einem idealen Verhältnis miteinander stehen (BSI 2008, 55).

Diese Kalküle wirken auf den ersten Blick überzeugend. *Continuity Manager* stehen unter dem ständigen Zwang, nicht nur die Notwendigkeit,

---

215 Zum Aufstieg des *Reputational Risk Management*, also den gezielten Versuchen, die öffentliche Meinung von Unternehmen nicht zu gefährden, siehe: Power (2007, 152–182).

sondern auch die ökonomischen Rationalität von Kontinuitätsmaßnahmen deutlich zu machen. Insofern ist die Kosten-Nutzen-Rechnung keineswegs wirkungslos: sie leitet organisationsinterne Entscheidungen an und schlägt innerhalb der Bilanzierungen zu Buche. Die Frage ist allerdings, wie effektiv sie in der Lage ist, den tatsächlichen Nutzen faktisch eingetretener Schadenslagen zu kalkulieren. Schließlich ist das BCM einer generischen Logik verpflichtet, die eben nicht mit konkreten Szenarien hantiert, sondern für beliebige Geschäftsunterbrechungen Vorsorge treffen können soll. Aber unterscheiden sich die möglichen Fälle – Pandemie und Stromausfall, Terroranschlag und Computervirus etc. – nicht so massiv voneinander, dass es unmöglich ist, Schadenshöhen im Vorhinein angemessen zu berechnen? Und wie hilfreich sind Maßnahmen zur Etablierung redundanter Infrastrukturen, wenn es nicht die Infrastrukturen sind, die ausfallen, sondern die Belegschaft? Anders formuliert: Was bringt ein redundantes »hot environment« (Interview 5), wenn alle Mitarbeiter aufgrund einer Grippe-Pandemie mit Fieber im Bett liegen? Wie lassen sich Wiederanlaufzeiten berechnen, wenn doch mit komplexen Schadensverläufen gerechnet werden muss, bei dem sich unterschiedliche Ereignisse verketteten und kaskadenartig fortsetzen? Und: sprengt nicht die Tatsache, dass jede Organisation durch *outsourcing* und Zulieferbetriebe in ein komplexes Netz mit anderen Organisationen eingewoben ist, jedes *framing*, das für eine Kosten-Nutzen-Kalkulation unerlässlich ist? In den gängigen Standards zum BCM finden sich nur zwischen den Zeilen Reaktionen auf diese Fragen. Die Rede ist dann von »äußeren Faktoren und innerbetrieblichen Abhängigkeiten« (BSI 2008, 57), auf die zu achten sei. Es wird empfohlen, »pragmatische Ansätze« (BSI 2008, 54) bei der Kosten-Nutzen-Analyse zu verfolgen – eine verklausulierte Formulierung dafür, nicht zu viele Komplexitäten ins Kalkül einzubeziehen. Wenn man Akteure des BCM danach fragt, wie das »Udenkbare« nicht nur gedacht, sondern auch noch berechnet werden könne, wird in den Antworten das Register gewechselt und die streng ökonomische Rationalität der Kostenkontrolle aufgegeben.

»Ja, ich mache die Analogie immer gerne vom BCM zu einer Versicherung. [...] Also niemand, der jetzt sein Auto versichert, macht ja eine Kosten-Nutzen-Analyse. [...] Er macht eine Haftpflichtversicherung, weil er es machen muss. Wir machen in den Kritischen Infrastrukturen BCM, weil wir es tun müssen [...] Und dann gibt es Kollegen, die machen eine Vollkaskoversicherung, [...] weil sie sagen, wenn ich denn einen Schaden erleide, dann kann ich mir kein neues Auto leisten. [...] Genau das gleiche ist auch im BCM. Also den Return on Invest fürs BCM zu erstellen, ist schier gar unmöglich, weil ich ja nicht sagen kann, alle fünf Jahre habe

ich einen BCM-Fall oder alle zehn Jahre, und dann kann ich so viel investieren.« (Interview 4)

In diesem Zitat lassen sich zwei unterschiedliche Rationalitäten finden, die es erlauben, die strenge Beachtung von Kosten-Nutzen-Kalkülen zu umgehen. Zunächst wird eine juristische Rationalität aufgerufen, die rechtliche Regelungen in den Vordergrund stellt, die insbesondere Betreiber Kritischer Infrastrukturen zu BCM-Maßnahmen verpflichtet. BCM wäre dann weniger eine Frage ökonomisch-rationalen Handelns, sondern eine Frage betrieblicher *compliance*. BCM sichert gegen die »legal and regulatory impacts« (ISO 2015, 7) einer Geschäftsunterbrechung ab. Daneben wird eine genuine Risikorationalität stark gemacht, die sich nicht vollständig in eine ökonomische Rationalität übersetzen lässt. Sicherheit ist ein Gut, für das zwar Geld ausgegeben werden muss – »Sicherheit kostet« (Interview 5) –, das aber nicht in gleicher Münze zurückgezahlt werden kann. Wie eine Versicherung versprechen auch *Business Continuity*-Maßnahmen Sicherheit im Ernstfall, ohne dass sich eine entsprechende Investition zwangsläufig rechnen muss. Man verhält sich dann risikorational, wenn man sich gegen schwerwiegende und intolerable Schäden absichert, und zwar insbesondere Schäden jenseits der »Katastrophenschwelle« (Luhmann 2003, 11). Im *Business Continuity Management* ist die Katastrophenschwelle der Punkt, an dem das Unternehmen dauerhaft nicht mehr operationsfähig ist: die »Bestandsgefährdungslinie« (BSI 2008, 55). Die Überschreitung der Katastrophenschwelle muss also »um jeden Preis« vermieden werden.

»[E]s gibt ja auch viele Studien, die belegen, wer gar kein BCM hat und nicht innerhalb von einer Woche in der Lage ist, sein Business wieder aufzunehmen, die Firma ist nach anderthalb Wochen tot. Dann brauchen wir nicht mehr über Geld reden.« (Interview 6)

Dieses Changieren zwischen drei unterschiedlichen Rationalitäten – ökonomisches Kalkül (Kosten-Nutzen-Rechnung bzw. *return on invest*), juristische Rationalität (*compliance*) und Risikorationalität (Absicherung gegen intolerable Schäden) – ist mehr als eine bloße Inkonsistenz oder Widersprüchlichkeit. Es zeigt sich nämlich, dass dem Problem der Ungewissheit durch unbestimmte Gefährdungen nur durch ein ständiges Verschieben der Problemsubstanz durch unterschiedliche Modi der Problematisierung begegnet werden kann.

Mögliche und tatsächlich eingetretene Krisen sind aber nicht nur Kostenfaktoren, sondern im Grenzfall auch Profitmöglichkeiten, die es zu

erkennen und zu ergreifen gilt. Aus der Sicht des Unternehmensberaters muss man auch die »Chancen« von Krisen- und Notfallsituationen sehen.

»Man müsste mehr Bewusstsein schaffen, was eine Krise tatsächlich heißt. Und welche Chancen die auch birgt. Weil, so hart es nun mal ist, jede Krise hat eine Chance. Ich nenne mal Versicherung. [...] [W]enn die Krise ist – wie wird denn die Bevölkerung reagieren? [...] [D]ie meisten – gerade bei einer Pandemie – werden wahrscheinlich jetzt gerne eine Versicherung haben wollen für Zusatzkrankenversicherung oder sonstiges. Dann muss ich klären: will ich das anbieten? [...] Aber man müsste sich das *heute* überlegen, denn es könnte ja sein, da werden jetzt [...] 100.000 die Versicherung abschließen, und nur 1.000 wollen von mir Geld. Und wenn ich das mal hochrechne, das ist ein Geschäftsmodell, da mache ich sogar noch Gewinn [...] Dann muss ich darauf vorbereitet sein [...] Ich muss ein Modell haben, das im Prinzip per Knopfdruck geht [...]. Also das sind so Dinge, [...] die werden noch nicht überall [...] ganzheitlich betrachtet.« (Interview 4)

Die »ganzheitliche« Betrachtung überschreitet hier das Defizitmodell der Krise in Richtung einer positiven Konzeption der Krise – ein durchaus charakteristischer Vorgang in der aktuellen Geschäftswelt. Schon in den 1990er Jahren hatte Beck dazu bemerkt: »[R]isks are no longer the dark site of opportunities, they are also market opportunities« (Ulrich Beck, zitiert nach: Power 2009, 850). Diese Umwertung der Krise von einem Schadensfall zu einer Gelegenheit ist der Punkt der Sicherheitskultur des BCM, an dem sich vorbereitende Planung mit einem Ethos des »embracing risk« (Baker und Simon 2002) trifft, bei dem Risiken nicht *per se* abgewehrt werden, sondern immer auch als Chance begriffen werden sollen. Eine Chance liegt allerdings nicht nur darin, dass Krisen neue Geschäftsmöglichkeiten kreieren. Schon der analytische Blick auf das Unternehmen aus der Perspektive der BIA soll Hinweise geben, wie die »efficiency of the organization« (ISO 2015, 24) erhöht werden kann. Die BIA blickt schließlich gleichsam vom Standpunkt der Unterbrechung aus auf das Unternehmen und ermöglicht so ein aufschlussreiches Verständnis organisationaler Abläufe, das es insbesondere erlauben soll, Interdependenzen und Zeitimperative stärker zu gewichten.

»The overview of the operation of an organization that emerges from the BIA process may enable participants in the process to identify changes that can improve its efficiency. These changes may not have been apparent until the organization explores its web of interdependencies. A better understanding of the time imperatives of product and service delivery could improve scheduling and prioritization when resources are temporarily limited. Knowing the time imperatives of

various parts of a manufacturing process could improve the optimization of stocks of raw materials or spare parts.« (ISO 2015, 24f.)

Schon die Antizipation der Krise soll also Lerneffekte ermöglichen und eine günstige »evolutionäre« Fortentwicklung des Unternehmens anregen, die im besten Fall sowohl dessen Resilienz als auch deren Effizienz steigert. Während also auf dem Finanzmarkt das Denken der Resilienz in einen Gegensatz zur Effizienzorientierung ökonomischer Theorien gebracht wird, finden sich im BCM zumindest Bemühungen um eine Versöhnung beider Perspektiven.

#### 4.2.5. Autopoiesis jenseits gewohnter (Infra)Strukturen

Beobachtet man das Krisenmanagement mithilfe von Niklas Luhmanns Unterscheidung von Struktur und Autopoiesis, wird sichtbar, wie sich in Krisenlagen eine Autopoiesis jenseits gewohnter Strukturen entfaltet. Autopoiesis ist für Luhmann (1998a, 65ff.) das fortlaufende Aneinander-Anschließen zeitlicher Systemelemente (für soziale Systeme Kommunikationen). Strukturen sind ebenso verzeitlicht, insofern sie als Erwartungsstrukturen verstanden werden (Luhmann 1991b, 377ff.). Strukturen beziehen sich auf eine zukünftige Entwicklung, bilden sich zumeist durch vergangene Erfahrung und sind zugleich in der Gegenwart präsent, weil sie hier erwartet und kommuniziert werden müssen. Die Aufgabe von Strukturen ist es, über feste Erwartungsstrukturen das sinnhaft-kommunikative Anschlussgeschehen der Gesellschaft zu erleichtern. Sie fungieren gleichsam als Schmiermittel für soziale Operationen. Zugleich wird dadurch das System geschützt. Schließlich würde es »aufhören [...] zu existieren, wenn es die momenthaften Elemente, aus denen es besteht, nicht mit Anschlussfähigkeit, also mit Sinn, ausstatten und so reproduzieren würde.« (Luhmann 1991b, 28f.)

Im Katastrophenfall brechen die gewöhnlichen Erwartungsstrukturen zusammen. Routinen werden unterbrochen und führen zur Orientierungslosigkeit. Im Angesicht der Durchbrechung des Erwarteten müssen Organisationen Formen finden, wie sie sich mit dem Unerwarteten so arrangieren können, dass sie ihre fundamentalen Operationen, ihre Autopoiesis also, fortsetzen können. Denn glaubt man den Beschwörungen des BCM, würden auch die vitalen Systeme aufhören zu existieren, wenn ihre *downtime* zu lange dauert. Auch hier findet sich ein radikal verzeitlichtes Verständnis der Autopoiesis als kontinuierlicher Geschäftsbetrieb. Und wir haben be-

reits gesehen, wie Organisationen durch BCM tatsächlich alternative Strukturen etablieren, die ihnen die Erwartung des Unerwarteten und somit eine Krisenroutine ermöglichen sollen: Szenarien, Übungen und Notfallpläne etablieren vorwegnehmend alternative Erwartungswerte, also Strukturen, auf die im Notfall zurückgegriffen werden kann.

Solche Strukturen, die eine »sekundäre Normalität« in Reaktion auf die Unterbrechung der »Normalform« (Luhmann 2003, 1) etablieren, hat Luhmann mit seiner Theorie der sozialen Immunisierung theoretisiert.<sup>216</sup> Auf temporär auftretende Störungen oder Unterbrechungen des Systems reagiert ein Immunsystem, das ein Weiteroperieren trotz Störungen und Erwartungsirritationen ermöglicht. »Das Immunsystem schützt nicht die Struktur, es schützt die Autopoiesis, die geschlossene Selbstreproduktion des Systems.« (Luhmann 1991b, 507) Dies kann das Immunsystem leisten, weil es alternative semantische Ressourcen mobilisiert, die das System weiter mit Sinn ausstatten und einen vollständigen »Sinnzusammenbruch« (Stäheli 2000), der zugleich einem Systemzusammenbruch gleichkäme, verhindern. Wie im generischen BCM, bei dem Vorbereitung nicht für ganz bestimmte, sondern beliebige Unterbrechungsereignisse getroffen werden soll, gilt dabei: »Das erfordert hohe Mobilität, ständige Einsatzbereitschaft, okkasionelle Aktivierbarkeit, universelle Verwendbarkeit« (Luhmann 1991b, 506).

Was Luhmann allerdings nicht in Betracht zieht, sind die materiellen Installationen, die Voraussetzung, Träger und Operatoren der Immunisierung sind, die das Weitermachen ermöglichen. Nicht nur Erwartungen brechen durch Notfallereignisse zusammen, sondern auch Gebäude, Datenverbindungen, die Stromversorgung etc. Nicht nur die Strukturen (Erwartungen für kommunikative Operationen), sondern auch die Infrastrukturen (sozio-technische Netzwerke für materielle Operationen) werden durch das Ereignis beschädigt. Alternative Strukturen müssen daher mehr sein als semantische Ressourcen, die Orientierung in einer plötzlichen, unerwarteten Situation geben. Es muss auch alternative, redundante *Infrastrukturen* geben, die das materielle und sozio-technische Weiteroperieren gewährleisten und so die Resilienz der Organisation erhöhen. Materialität spielt aber nicht nur eine entscheidende Rolle, wenn es um Ausweichstandorte, Datencenter, Notstromaggregate etc. geht, also um alternative Infrastrukturen im engeren Sinne. Auch bei der Batterie an Vorsorgemaßnah-

---

216 Für einen Versuch, Luhmanns Theorie des Risikos und seine Theorie der Immunisierung mit Foucaults Normalisierungsanalytik zusammenzubringen, siehe: Folkers (2013a).

men, die genau darauf zielen, alternative Erwartungsstrukturen für den Ereignisfall verfügbar zu halten, gilt: *materiality matters*. Alternative Erwartungsstrukturen werden im BCM durch eine Reihe von Medien erzeugt und vorgehalten: Notfallpläne und Handbücher (BSI 2008, 14), Evakuierungs- und Fluchtpläne, »Checklisten« (BSI 2008, 12), *flow-charts* (siehe: BSI 2008, 65), »Datenflussdiagramm[e]« (BSI 2008, 67), »standardisierte [...] Ereignistagebücher oder Meldeprotokolle« (BSI 2008, 79f.) und »Software-Tools« (BSI 2008, 98). All diese Medien fungieren im Krisenfall als Entscheidungsalgorithmen, die eine abseits der Routine liegende Erwartung strukturieren sollen. Dabei müssen diese Protokolle vor allem dem Zeitdruck einer Notfallsituation standhalten, in der »schnelle Entscheidungshandlungen erforderlich sind« (Interview 6). Sie müssen daher übersichtlich, klar strukturiert und eindeutig sein. *Flow-charts* und Entscheidungsbaumdiagramme sind eine immer wieder eingesetzte Medialisierungsform für Notfallprotokolle. Sie verschalten alternative Szenarien und Entscheidungsoptionen miteinander und sollen es so ermöglichen, klare und der Situation angepasste Handlungsoptionen aufzuzeigen. Hier bestehen Ähnlichkeiten zur Beschilderung für Fluchtwege und Notausgänge, die ebenfalls »Sinn« in einer Notsituation ermöglichen sollen, indem sie klare Richtungen aufzeigen. Die Materialität dieser Medien ist entscheidend. Sie müssen nicht nur eine materielle Grundlage haben, um kommunizierbar zu sein (verschriftlicht, graphisch dargestellt und »zu Papier gebracht«), auch die Art ihrer Materialität und Medialität ist für ihre Handhabbarkeit und Funktionsfähigkeit im Ereignisfall entscheidend. Sie müssen nicht nur dem Zeitdruck des Notfalls standhalten können, sondern auch den adversen physischen Bedingungen der Krisensituation.

»Für das Notfallhandbuch und alle weiteren für die Notfallbewältigung benötigten Unterlagen empfiehlt es sich, diese als Dokumente in Papierform oder/und elektronisch in einem einfachen und gängigen Format [...] schnell griffbereit zu halten. Die Lösung muss die Verfügbarkeit im Notfall garantieren, sowohl bei Stromausfall wie auch bei Brandschäden und sonstigen Risiken, die die Dokumente unbrauchbar machen, Daten zerstören oder den Zugriff darauf verhindern können. Daher empfiehlt es sich, Kopien an einem Ausweichort aufzubewahren. [...] Es gilt, in Stresssituationen dem Nutzer zusätzliche Sicherheit zu geben.« (BSI 2008, 13)

Die adäquate Materialität und Darstellungsform der Notfalldokumente verspricht einen Mehrwert, der über den semantischen Inhalt hinausgeht: »zusätzliche Sicherheit«. Die Materialität hat zwar keine unmittelbare Aus-



wirkung auf die Semantik der Dokumente, wohl aber auf ihren praktischen Nutzen. Erst die Kombination von kommuniziertem Sinn, praktischer Handhabbarkeit und materieller Widerstandsfähigkeit der Medien des Notfalls verbürgt deren »sichernde« Funktion.

Wenn schon bei der Kommunikation alternativer Erwartungsstrukturen Materialität und Lokalität entscheidend sind, dann gilt dies umso mehr für alternative Infrastrukturen. Über die Notwendigkeit zur Schaffung redundanter Infrastrukturen herrscht im Allgemeinen große Einigkeit im BCM, auch wenn sich die Art der Lösungen durchaus unterscheidet. So gibt es Versuche, Redundanzen schon an den normalen Geschäftsorten zu implementieren. Dazu gehören etwa Notstromaggregate oder die Lagerung von bestimmten, für den Geschäftsprozess entscheidenden technischen Komponenten (siehe: BSI 2008, 106). Datenbackup ist ebenso ein Standardverfahren, das zumeist über externe Server (*clouds*) gewährleistet wird. *Cloud*-Lösungen unterstützen auch die Implementierung einer »verteilte[n] Geschäftstätigkeit« (BSI 2008, 102). Dadurch soll es idealerweise möglich sein, den Ausfall bestimmter Standorte oder einzelner Elemente an diesen Standorten kompensieren zu können. Auch Kontinuitätsmanagement beinhaltet also Techniken aus dem Repertoire der *distributed preparedness*.

Vorsorge muss aber auch für Fälle getroffen werden, die einen Standort unbrauchbar machen. Dann schlägt die Stunde der Ausweichstandorte. Hier kann auf drei unterschiedliche Modelle zurückgegriffen werden. Möglich ist eine sogenannte »remote-Lösung« (BSI 2008, 103), bei der die Mitarbeiter\_innen ihre Arbeitstätigkeiten von zu Hause aus erledigen. Dieser Lösung sind Grenzen gesetzt, da der Geschäftsbetrieb vieler Unternehmen nur weiterlaufen kann, wenn ihre Mitarbeiter\_innen kooperieren können. Räumliche Nähe und eine bestimmte Raumaufteilung ist dafür häufig eine notwendige Voraussetzung. Untersuchungen zur Arbeitsorganisation in modernen Unternehmen wie der Finanzbranche unterstreichen die Bedeutung dieser räumlichen Nähe von Mitarbeiter\_innen (Beunza und Stark 2003). Flurgespräche, gemeinsame Essen, das Mithören von Gesprächen am Nachbararbeitsplatz, ganz zu schweigen von gezielter Koordination und Kooperation in Form von Besprechungen sind wesentliche Voraussetzungen einer erfolgreichen Arbeitsorganisation. Die sozial-räumliche Dimension »sozialer Netzwerke« kann nur schwerlich und gewiss nicht ohne Reibungsverluste durch digital vernetzte Arbeitsplätze ersetzt werden. Hier liegt – wie noch deutlicher zu zeigen sein wird – eine Grenze der vermeintlichen Ortslosigkeit des gegenwärtigen Kapitalismus. Da es also

nicht vollkommen egal ist, wie und wo die individuelle Arbeit geleistet wird, empfiehlt sich die Einrichtung von »relocation-sites« beziehungsweise »Ausweich-Lokationen« (BSI 2008, 81, 102). Dabei wird – wie bereits erwähnt – zwischen sogenannten *hot*, *cold* und *warm sites* unterschieden. Die »Temperatur« eines Ausweichstandorts gibt an, wie komplett der Ausweichsitz mit IT-Infrastruktur ausgestattet ist und wie schnell der Geschäftsbetrieb hier aufgenommen werden kann. Die Ausweicarbeitsplätze können entweder vom Unternehmen selbst betrieben oder durch externe Dienstleister bereitgestellt werden. Dabei ist der Rückgriff auf externe Dienstleister meist günstiger. Die auf IT-Dienstleistungen spezialisierte Firma Sungard etwa betreibt unzählige Ausweichstandorte in den USA, die sie von ihrem Kontrollzentrum in Colorado aus »fernsteuern« kann. Diese Ausweichsitze können von unterschiedlichen Firmen genutzt werden. Im Bedarfsfall bespielt dann Sungard die Computer ihrer generischen Büroräume mit den Daten der entsprechenden Firma. Der Nachteil dieser Lösung besteht allerdings darin, dass die Ausweichstandorte bei gesteigertem Bedarf – etwa durch ein großflächiges Katastrophenereignis – von zu vielen Unternehmen gleichzeitig nachgefragt werden könnten (siehe dazu 4.4.2). In diesem Fall können nur die Unternehmen, die besonders hohe Prämien an den externen Dienstleister gezahlt haben, mit einem Ausweichsitz in ihrer Nähe ausgestattet werden, während alle andere Unternehmen unter Umständen auf sehr weit entfernte Standorte verwiesen werden.

Die Krux der richtigen Dislozierung der Ausweichstandorte liegt darin, dass diese so weit vom eigentlichen Geschäftsstandort entfernt sein müssen, dass das Schadensereignis sie nicht erreicht. In Empfehlungen der Europäischen Zentralbank für gutes BCM von Banken heißt es entsprechend:

»The traditional approach tends to limit geographic separation to reduce the relocation time of key staff to the secondary site. However, when both primary and secondary sites depend on the same labour pool or infrastructure components [...], major events could render both sites inaccessible or inoperable.« (ECB 2006, 6)

Räumliche Erwägungen spielen damit aus zweierlei Gründen eine entscheidende Rolle: zum einen sollte das räumliche Arrangement des Ausweichstandorts die Art von Interaktion ermöglichen, die auch im normalen Firmensitz eine produktive Arbeitsorganisation ermöglicht. Zum anderen ist die Lage des Ausweichsitzes ein entscheidender Faktor, der die Wiederanlaufzeit des Geschäftsprozesses nach einer Unterbrechung bestimmt.

Spätestens hier zeigt sich, inwiefern der Raum für die temporalisierte Kontinuitätslogik von Bedeutung ist. Distanz übersetzt sich in die Zeit des Wiederanlaufs.

Zusammen sollen die alternativen Strukturen die Resilienz der Organisation erhöhen: die alternativen Erwartungsstrukturen von Notfallprotokollen und Entscheidungsalgorithmen stärken die operative Resilienz, indem sie eine schnelle Reaktion des Krisenmanagements erlauben, die Redundanzen und Systemdesigns alternativer Infrastrukturen hindern eine Unterbrechung an ihrer schnellen Ausbreitung bzw. federn deren Folgen durch vorhandene Puffer ab. Selbst die besten Alternativstrukturen nutzen jedoch nichts, wenn es keine Mitarbeiter\_innen gibt, die gemeinsam mit diesen materiellen und medialen Vorrichtungen den Geschäftsprozess fortsetzen können. Darauf soll die *Übung* antworten, die beide Strukturelemente mit Personal, Technik und *know-how* zusammenbringen soll. Die Übung dient einerseits zur Überprüfung der technischen Komponenten und der Angemessenheit der Notfallpläne. Andererseits soll sie aber auch die notwendigen Handlungsabläufe im Notfall und an den Ausweichstandorten trainieren. »Also Übungen sind zentral, weil Übungen einmal der Überprüfung der Funktionsfähigkeit der Pläne dienen und weil sie zum Training dienen. [...] Deswegen sind Übungen zentral, ist Key.« (Interview 4) Es geht nicht nur um die Etablierung alternativer semantischer Erwartungsstrukturen und sozio-technischer Infrastrukturen, sondern zudem auch um habituelle Verhaltensstrukturen. Idealerweise können Notfallroutinen in Übungen erlernt und verkörpert werden, um dann im Notfall abrufbereit zu sein.

Dieser Idealfall sollte allerdings ebenso wenig wie ein reibungsloses Funktionieren der alternativen Infrastrukturen und der Notfallpläne erwartet werden. Vielmehr kommt es im Notfall nicht nur zur Abweichung von der Normalform, sondern auch noch zur Abweichung von der »sekundären Normalität«, die durch redundante Infrastrukturen, Handlungsprotokolle und Notfallroutinen etabliert wurde. Nur im absoluten Ausnahmefall verläuft eine Krise wie im Drehbuch einer Notfallübung und nur selten wird im Krisenfall dem Skript eines Notfallplans gefolgt. Ebenso häufig versagen die »Inskriptionen« (Akrich 2006, 411)<sup>217</sup> der Notfallartefakte und

---

217 Akrich (2006, 411) versteht Inskriptionen als die Operation durch die eine bestimmte »Vision der Welt (oder der Vorhersage darüber)« in den »technischen Inhalt eines Objekts« eingebracht wird. Klarerweise gehen auch in die redundanten Infrastrukturen und

der redundanten Infrastrukturen, wenn sie nicht sogar von vornherein missachtet werden. Die Erwartung des Unerwarteten ist und bleibt ein paradoxes Unterfangen und kann deshalb nicht ohne Friktionen bewältigt werden. Es wäre allerdings billig, den Kontinuitätsmanager\_innen diese Paradoxie nachzuweisen, ohne anzuerkennen, dass die Grenzen der Planbarkeit des Ungeplanten durchaus reflektiert und problematisiert werden. »[M]an kann einen Teil beplanen. Und dazu gibt es dann ja noch ergänzend das Krisenmanagement, das das abfedert, was nicht konkret beplant ist.« (Interview 4) Die Möglichkeit zum Ausrufen einer Krise, bei der ein Krisenmanagement aktiv wird, das flexibel auf die sich entwickelnde Notfallsituation reagieren soll, ist gleichsam auch ein Immunmechanismus gegen die autoimmunen Effekte des Notfallplans und vorgegebener Entscheidungsalgorithmen.

### 4.3. Kontinuitätsmanagement im Finanzsektor

Banken handeln mit Risiken (Baecker 1991). Diese – in den 1990er Jahren noch provokative – These, wonach Risiko das Kerngeschäft von Banken darstellt, ist mittlerweile nahezu ein Gemeinplatz geworden. Denn spätestens seit Beginn der jüngsten Finanzkrise hat das Risikomanagement in Finanzinstitutionen (Banken, Hedgefonds, Versicherungen) große akademische und öffentliche Aufmerksamkeit und die Diagnose über den Zusammenhang von Risiko und Bankhandeln eine weitere Zuspitzung erfahren. Nicht enden wollende Krisen, Markteinbrüche und sonstige finanzpolitische Notstände verfestigen den Eindruck, dass Bankenmanagement nicht nur den Umgang mit Risiken einschließt, sondern geradezu zum Notfall-, Krisen- oder gar Katastrophenmanagement geworden ist. Mit der Finanzkrise sind Konzepte des Katastrophenschutzes in die Finanzwelt eingedrungen. So versucht man den »financial meltdown« mit Charles Perrows *Normal Accident Theory* zu erklären (Palmer und Maher 2010) und das Konzept der Resilienz ist aus den Sicherheitstechnologien im Finanzwesen gar nicht mehr wegzudenken (Cooper und Walker 2011, siehe auch Kapitel 2.5.)

---

Notfallartefakte bestimmte Szenarien über ihre mögliche Funktion in einer Katastrophensituation ein.

In diesem Kapitel werde ich die Debatte um Notfallmanagement im Finanzsektor vertiefen, indem ich die Voraussetzungen und Einsatzpunkte des *Business Continuity Management* bei Banken beleuchte. Besonders interessant ist BCM in diesem Zusammenhang, weil es hier um etwas anderes als beim finanziellen Risikohandeln geht. Es geht beim BCM nämlich nicht unmittelbar um Marktrisiken, Kreditrisiken oder systemische Finanzrisiken. Vielmehr geht es um sogenannte operationelle Risiken – Risiken also, mit denen gerade nicht »gehandelt« werden kann, mit denen aber dennoch gerechnet werden muss. Es handelt sich um Risiken, die die Organisation und den Geschäftsbetrieb der Banken selbst betreffen, ihre alltäglichen Arbeitsvorgänge, ihre sozio-technischen Prozesse und ihre materiellen wie auch räumlichen Vollzüge, die durch Notfälle aller Art unterbrochen werden können. Innerhalb der mittlerweile überbordenden sozialwissenschaftlichen Literatur zum Umgang mit Risiken während und seit der Finanzkrise ist der Umgang von Banken mit operativen Risiken erstaunlicherweise bisher kaum (Beunza und Stark 2003, Power 2005, Pelzer 2007, Brückner und Wolf 2014) und das BCM so gut wie gar nicht behandelt worden (Folkers 2017a). Den Vorbereitungen von Banken auf nicht unmittelbar marktbezogene Katastrophen wie Stromausfälle, Terroranschläge, Pandemien und Naturkatastrophen wurde bisher kaum sozialwissenschaftliche Aufmerksamkeit zuteil. Das ist umso bedauerlicher, wenn man sich die wachsende Bedeutung des BCM bei Banken vor Augen führt. Schließlich ist BCM, das vor operationellen Risiken schützen soll, mittlerweile zum entscheidenden Teil des Risikomanagements von Banken geworden. Zudem betonen Finanzregulator\_innen immer wieder die Schnittfelder von systemischen Marktrisiken und Finanzkrisen einerseits und operationellen Unterbrechungen andererseits (BIS und IOSCO 2012, 18).

Die folgenden Ausführungen adressieren dieses Forschungsdesiderat. Zunächst werde ich kurz die Unterschiede und Schnittflächen zwischen operationellem Risikomanagement und *Business Continuity Management* bei Banken beleuchten (4.3.1.). Sodann werde ich auf die besonderen Herausforderungen des BCM in einem so hoch vernetzten und globalen Feld wie dem Finanzsektor eingehen (4.3.2.). Schließlich diskutiere ich die besondere Problematik der Zahlungssysteme bzw. der Zahlungsinfrastruktur des Finanzwesens (4.3.3.).

#### 4.3.1. Operationelles Risiko als Grenzobjekt

Gerade für die Entwicklung des BCM bei Banken war der 11. September das Initialereignis. Schließlich ereigneten sich die Terroranschläge im Herzen des globalen Finanzkapitalismus: im *financial district* von Manhattan. Allerdings waren die Banken schon damals nicht vollkommen unvorbereitet. Daniel Buenza und David Stark (2003) haben die *recovery*-Maßnahmen einer internationalen Investmentbank beschrieben, die wochenlang nicht an ihren Hauptarbeitssitz unmittelbar neben dem WTC zurückkehren konnte und deshalb in einen improvisierten Ausweichfirmensitz in New Jersey umziehen musste. Jeffrey Bussolini (2014, 16ff.) berichtet über die Erfahrung eines IT-Spezialisten von Morgan Stanley, der, einen Tag nachdem er sich gerade noch aus dem vom Einsturz bedrohten WTC retten konnte, ebenfalls in New Jersey an der Wiederherstellung kritischer Daten arbeiten sollte. Diese Berichte vermitteln einen Eindruck davon, wie tiefgreifend die Finanzwelt vom 11. September betroffen war. Beschäftigte hatten Kolleg\_innen, Freund\_innen und Bekannte verloren und mussten ohne Zeit zu trauern an der Wiederherstellung des Bankbetriebs arbeiten. Banken war ihre Verwundbarkeit gegenüber katastrophischen Ereignissen bewusst geworden, aber auch ihre Abhängigkeit von einzelnen Beschäftigten, ohne die auch die besten Datensicherungssysteme nichts helfen. Der 11. September wurde dementsprechend als genuiner »Business Incident« (Interview 4) wahrgenommen, der ein viel umfassenderes *Continuity Management* notwendig macht als die Bereitstellung redundanter IT-Infrastruktur. Der 11. September war aber längst nicht der einzige Faktor, der das BCM bei Banken so forciert hat, dass man heute durchaus von einer Vorreiterrolle von Banken bei betrieblichen Sicherheitsmaßnahmen sprechen kann.

Ein wesentlicher Hintergrund für die Ausbreitung des Kontinuitätsmanagements bei Banken ist sicherlich der Aufstieg der Kategorie des operationellen Risikos (siehe dazu: Power 2005). »Operational Risk Management, das hat ja eine nahe Verwandtschaft. Da geht es ja auch um die Unterbrechung von Geschäftsprozessen.« (Interview 4) Das *operational risk management* verdankt seinen Aufstieg allerdings einer anderen Problemkonstellation als das BCM. Eine Reihe von Bankskandalen Mitte der 1990er Jahre, die allesamt auf das Fehlverhalten einzelner Mitarbeiter\_innen zurückzuführen waren, hatte das operationelle Risiko zu einem Problem der Finanzwelt gemacht (Brückner und Wolf 2014, 142). Regulierungsbehörden, allen voran die Bank for International Settlements in Basel, haben in

der Folge begonnen, diese Problematik zu adressieren. Bereits in der Eigenkapitalverordnung Basel II von 2004 wurde operationelles Risiko neben Kreditrisiken und Marktrisiken als eigenständige Risikokategorie aufgeführt, für die Zurückstellungen von Eigenkapital notwendig sind. Operationelles Risiko wird hier definiert als »the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events« (BIS 2004, 149). Dadurch wurde operationelles Risiko von einer Residualkategorie des Risikomanagements zu einem zwar immer noch sehr weiten, aber doch klarer definierten Gegenstand und »boundary object« (Power 2005, 584) des Risikomanagements.

Geschäftsunterbrechungen, die im Fokus des betrieblichen Kontinuitätsmanagements stehen, sind ein Teilbereich des operationellen Risikos. Beim BCM wie auch beim Management operationeller Risiken geht es um mögliche Ereignisse, die nicht unmittelbar Marktvorgänge betreffen (Kreditrisiken, Marktrisiken). Sowohl operationelles Risiko als auch BCM sind reflexive Risikomanagement-Konzepte, die die eigenen internen Prozesse beobachten und nicht nur externe Faktoren wie Marktentwicklungen. »Das Risikomanagement nimmt gleichsam eine reflexive Wendung und erlebt fortan auch die eigenen Strukturen als riskant.« (Brückner und Wolf 2014, 142) Diese Verwandtschaft zwischen operationellem Risikomanagement und BCM ermöglicht die gängige Praxis, dass *Business Continuity Management* und *Operational Risk Management* in einigen Finanzinstitutionen von ein und derselben Person ausgeführt werden. Das heißt aber auch, dass diese Person die Unterschiede und Widersprüche beider Sicherheitsrationalitäten in sich austragen muss. Während BCM einen »generischen« Ansatz verfolgt, also nur die Auswirkungen von Geschäftsunterbrechungen durch beliebige Ursachen im Blick hat, arbeitet das *Operational Risk Management* mit Szenarien. In einem Interview mit einer Risikomanagerin, die sowohl für *Operational Risk Management* als auch für BCM einer großen deutschen Bank in deren New Yorker Dependence zuständig ist, zeigten sich die widersprüchlichen Konsequenzen der Verkörperung dieser zwei unterschiedlichen Logiken im Aufgabengebiet einer Person. Fragte ich die Kontinuitätsmanagerin nach dem Stellenwert von Szenarien für ihre Arbeit, erhielt ich Antworten wie: »Das ist mir wurscht, was da passiert. Wichtig ist nur, gibt es eine Unterbrechung, wie schwer ist die und wie lange dauert sie.« (Interview 5) In ihrer Funktion als *Operational Risk Manager* muss sie gleichwohl mit Szenarien arbeiten, weil hier Eintrittswahrscheinlichkeiten und Schadensausmaße, also quantitative Kalküle, wichtig sind. »Da geht es um

Schadenshöhe, für die man vorsorgen muss für bestimmte Szenarien.« (Interview 5) Schließlich ist das *operational risk* eine Kategorie der Baseler Eigenkapitalanforderungen. Entsprechend müssen Banken ihre Ausgesetztheit gegenüber bestimmten operationellen Risiken mit quantifizierenden Kalkülen ausweisen und ihren Eigenkapitalbedarf entsprechend anpassen. Es geht beim *Operational Risk Management* zwar um nahezu die gleiche Art von Risiken, aber dennoch um eine andere Logik der Absicherung gegen diese Risiken, die wiederum eine andere Risikoanalytik notwendig macht. Im operationellen Risikomanagement geht es nur um eine Absicherung gegen finanzielle Schäden, die aus Geschäftsunterbrechungen entstehen können – und nicht darum, diese Schäden gering zu halten oder sich gänzlich gegen sie zu schützen.

Mit operationellem Risikomanagement und BCM haben sich im Finanzsektor zwei unterschiedliche Sicherheitsstrategien etabliert, die auf die gleiche Art von Gefährdungen antworten. Operationelles Risiko ist dadurch zu einem »boundary object« geworden: ganz unterschiedliche Akteure und Sicherheitsmaßnahmen können sich ihm widmen, ohne sich dabei in die Quere zu kommen oder notwendigerweise ihre Maßnahmen koordinieren zu müssen. Dass operationelles Risikomanagement größere Bekanntheit in der Finanzwelt und größere Prominenz in den relevanten Regulierungsvorgaben (Basel II) erlangen konnte, liegt wohl an der höheren Anschlussfähigkeit quantifizierender Logiken, die operationelles Risikomanagement kennzeichnet. Durch ihre Übersetzung in konkrete Schadenswerte werden operationelle Risiken wieder in die Sprache des Finanzwesens integriert – so absurd die Quantifizierung solcher Schäden bisweilen auch anmutet.<sup>218</sup> Interessant am BCM ist demgegenüber, dass es mit dieser Quantifizierungslogik bricht und sich nicht mehr mit der von kalkulativen Verfahren suggerierten Pseudogewissheit zufrieden gibt. Das BCM zieht die Konsequenzen aus den Grenzen der Berechenbarkeit, indem es nicht mehr primär auf die Höhe entstandener Schäden achtet, sondern auf zeitkritische Geschäftsprozesse und Strategien ihrer Fortsetzung. Die qualitative und systemische Logik des BCM – aus welchen Prozessen setzt sich das Bankgeschäft zusammen, welche Verbindungen und Abhängigkeiten bestehen im System, wie lassen sich gefährliche Abhängigkeiten und verwundbare Knotenpunkte auflösen etc.? – können vielleicht sogar

---

218 Die Grenzen der Quantifizierung werden ausführlich in der sozialwissenschaftlichen Literatur zum *operational risk* diskutiert. Siehe: Power (2005), Pelzer (2007), Brückner und Wolf (2014).



als richtungweisend für eine alternative Risikoregulation auf dem Finanzmarkt angesehen werden (Power 2009).

Freilich sind quantitative Erwägungen für das BCM keineswegs unwichtig. Hier geht es aber weniger um die Rationalität der Sicherheit selbst, sondern um das Kalkül, das für oder gegen ihre Implementierung spricht. BCM-Maßnahmen wirken sich nämlich positiv auf die Eigenkapitalanforderungen der Banken aus (Power 2005, 587). Die Notwendigkeit operationellen Risikomanagements liefert genuine Anreize für die Implementierung von Kontinuitätsmaßnahmen.

»Ein [...] Beispiel wäre, dass der Kostenaufwand für ein zweites (oder drittes) Rechenzentrum der Ausfallwahrscheinlichkeit und den bei einem Ausfall entstehenden Kosten gegenüber gestellt wird: rentiert sich der Betrieb eines weiteren Rechenzentrums, gemessen an den daraufhin geringeren bereit zu haltenden Eigenmitteln, wird diese Investition vorgenommen.« (Brückner und Wolf 2014, 143)

Ein ähnlich gelagerter Anreiz zum *Business Continuity Management* entsteht durch die Aufmerksamkeit für das Thema bei Wirtschaftsprüfungsunternehmen. »[D]adurch dass die Regulierung [...] zunimmt und die Schadensfälle auch da sind, sind auch die Wirtschaftsprüfer entsprechend stark eingestiegen. Also der Druck kommt auch ganz massiv von der Prüfer-Seite.« (Interview 4)

Neben *audits* sind es vor allem regulatorische Vorgaben und damit Fragen der *compliance*, die das BCM bei Banken vorantreiben. Regulierungsbehörden haben nämlich die Befürchtung, dass allein intrinsische Anreize nicht ausreichen, damit Banken ein umfassendes Kontinuitätsmanagement implementieren, das nicht nur sie selbst, sondern mittelbar auch die von ihnen abhängigen Finanzinstitutionen vor Geschäftsunterbrechungen schützt.

»Because financial industry participants typically consider only their direct benefits and costs whereas financial authorities are expected to consider the broader public dimension, a natural tension exists between the level of resilience that financial industry participants might consider reasonable for their own business purpose and the objectives of financial authorities for the resilience of the financial system as a whole.« (Joint-Forum 2006, 8)

Aus der makroprudenziellen Perspektive auf das »financial system as a whole« lässt sich der Wert von BCM-Maßnahmen einzelner Banken nicht mehr durch Kosten-Nutzen Rechnungen überprüfen. Spätestens an diesem Punkt zeigt sich BCM als Sicherheitstechnologie, der es um die qualitative Analyse von Interdependenzen und um die Steigerung der Resilienz

systemwichtiger Operationen und nicht bloß um die Vermeidung quantifizierbarer Schäden geht.

#### 4.3.2. BCM als globales Sicherheitsgefüge

Eine Vielzahl sozialwissenschaftlicher Diagnosen des gegenwärtigen Kapitalismus betont, dass dieser einerseits aufgrund der Globalisierung komplexer – und das heißt vor allem vernetzter – geworden ist (Hardt und Negri 2002, Castells 2010) und sich zudem durch technologische Innovationen und neue Produktionsformen beschleunigt hat (Rosa 2003). Diese Globalisierung und Beschleunigung des Kapitalismus gehe, so wird immer wieder argumentiert, mit Ortslosigkeit (Rosa 2003, 6) und Dematerialisierung (Hardt und Negri 2002) einher. Der Finanzkapitalismus gilt dabei nicht nur als Kapitalismus in Reinform, der alle räumlichen und zeitlichen Grenzen überschreitet, sondern auch als hypertechnologisierte Sozialitätsform, wo Algorithmen Geld über ultraschnelle Informationsleitungen über die ganze Welt verschieben, ohne dass diese Transaktionen noch etwas mit der materiellen Produktion der »Realökonomie« zu tun haben.

Diese »globalen« Theorien der Globalisierung sind in jüngerer Zeit von *global assemblage*-Ansätzen (Ong und Collier 2005a, Sassen 2008) ebenso kritisiert worden wie von der Akteur-Netzwerk-Theorie, die fordert, das »Globale zu lokalisieren« (Latour 2007, 299ff.). Zwar operieren Banken und damit der Finanzkapitalismus global, aber sie können dies nur, weil sie von konkreten Orten aus ihre globalen Operationen organisieren und weltumspannende Netze weben. Insbesondere die *Social Studies of Finance* haben den gesellschaftstheoretischen Großdiagnosen einer »flachen« (Friedman 2006), ortlosen Finanzwelt eine Absage erteilt. »In the apparently »flat«, geography-less world of financial globalization and automated trading, particular places still matter.« (MacKenzie 2013, 1) Die globalisierte Finanzwelt operiert über konkrete Orte und ist daher in Form von »global microstructures« (Knorr-Cetina und Bruegger 2002) organisiert. Die deterritorialisierende Dynamik des Finanzkapitalismus geht mit bestimmten Formen der Reterritorialisierung – in *global cities* (Sassen 1996) wie auch *offshore* (Opitz und Tellmann 2012), an Handelsplätzen und in Bankgebäuden – einher bzw. wird von diesen ermöglicht. Seine »immateriellen« Transaktionen werden von materiellen Techniken – Informationstechnologien, digitale Infrastrukturen, Datenzentren, Computerbildschirmen – erzeugt. Die Analyse des BCM bei Banken kann zu diesen Debatten

einen wichtigen Beitrag leisten. Die Aufmerksamkeit für die operationellen Störungen der Finanzwelt bei den Kontinuitätsmanager\_innen macht nämlich zugleich die materiellen und soziotechnischen Grundlagen der »global operations« (Tellmann, Opitz und Staeheli 2012) des Finanzkapitalismus sichtbar. Beobachtet man, wie im Kontinuitätsmanagement die Herausforderungen eines beschleunigten und globalisierten Kapitalismus thematisiert und adressiert werden, dann wird die Bedeutung von Raum und Materialität überdeutlich. Wie Marx einst den Abstieg in die Welt der Produktion empfahl, um die ideologischen Gespenster der Marktsphäre zu vertreiben, so soll auch hier der Abstieg in die Untiefen des BCM bei Banken gewagt werden, um die luftigen Theorien des globalen Kapitalismus zu erden. Zudem erlaubt diese Perspektive eine Thematisierung globaler Gefährdungslagen jenseits von Becks Weltrisikogesellschafts-Ansatz. Auch Beck (2008) verfolgt eine »globale« und nicht mundane Analyse der Globalisierung, indem er das Bestehen der Globalität immer schon voraussetzt, anstatt zu zeigen, wie das Globale versammelt wird. Risiken ereignen sich dann im gegebenen Raum der Weltgesellschaft, der nur noch ihre kosmopolitischen Institutionen fehlen. Die Analyse globaler Gefüge der Sicherheit, wie sie auch durch BCM gestiftet werden, kann demgegenüber die Globalisierung von Sicherheitstechnologien zeigen, die nicht einfach »in« der Weltrisikogesellschaft verortet sind, sondern vielmehr selbst die Orte erzeugen, die so etwas wie einen weltweiten Risikozusammenhang überhaupt erst möglich machen.

BCM ist durch seine vielfachen Standardisierungsbemühungen und seinen generischen Ansatz zu einer »globalen Form« geworden »that can be decontextualized and recontextualized, abstracted, transported, and reterritorialized, and is designed to produce functionally comparable results in disparate domains« (Ong und Collier 2005a, 11). Auch im Banksektor haben die Regulationsvorschriften zu BCM eine globale Reichweite. Zwar stammen die konkreten Auflagen meist von nationalen Körperschaften (in Deutschland von der Bundesanstalt für Finanzdienstleistungsaufsicht, BaFin), werden aber international koordiniert. Hier spielt die Bank for International Settlements (BIS) mit Sitz in Basel (Schweiz) eine entscheidende Rolle. Die BIS ist ein Zusammenschluss der wichtigsten Zentralbanken und versucht, globale Standards bzw. Prinzipien für die nationale und transnationale Regulierung von Banken vorzugeben. Damit ist die BIS keine »kosmopolitische Institution« einer Weltregierung, sondern versucht vielmehr, ein komplexes Gefüge nationaler, regionaler und transnationaler

Regulierungsinstitutionen zu koordinieren. Ein solcher Koordinierungsversuch für das BCM hat die BIS durch das bereits zitierte Papier *High-Level Principles for Business Continuity* aus dem Jahr 2006 vorgelegt. Das Papier wendet sich gar nicht direkt an Banken, sondern insbesondere an die Regulierungsinstitutionen (Zentralbanken und Finanzaufsichtsbehörden, etwa die BaFin in Deutschland). Entsprechend wird immer wieder die Notwendigkeit von »cross border communications« (Joint-Forum 2006, 16) zwischen den »financial authorities« betont. Die Notwendigkeit für die globale Koordination wird vor allem in den vertieften, weltweiten Interdependenzen des Finanzwesens gesehen. »Because of the deepening interdependencies among financial industry participants across jurisdictions, it is increasingly likely that the impact of a major operational disruption will extend across national borders.« (Joint-Forum 2006, 16) Wiederum wird die grenzüberschreitende Reichweite von Risiken mobilisiert, um die Ausweitung der Netze der Sicherheit zu begründen. Das heißt aber auch, dass die globalisierte Gefährdung den globalen Gefügen der Sicherheit nicht einfach vorgängig oder äußerlich ist. Vielmehr entsteht das spezifische Problem von »major operational disruptions« als Zielscheibe einer bestimmten Sicherheitstechnologie im Innern der Regierungsapparate, die sich auf dieses Problem richten und deshalb die gleiche Reichweite anstreben wie die von ihnen wahrgenommenen Risiken.

Das »Weltrisiko« grenzüberschreitender Operationsstörungen ist aber nicht nur das Korrelat von globalen Regulationskörperschaften, sondern bestimmt auch die Alltagspraxis von *Continuity-Manager\_innen* in einzelnen Banken. Auch ihre Perspektive auf »Geschäftsunterbrechungen« muss globale Abhängigkeiten in Rechnung stellen. Schließlich operieren die meisten Finanzinstitutionen an mehreren über die Welt verteilten Standorten und sind zudem an ein globales Finanzgeschehen angeschlossen. Das wurde insbesondere in meinen Interviews mit den zuständigen *Business Continuity-Manager\_innen* einer international operierenden deutschen Bank in Frankfurt und New York deutlich. Durch ihre unterschiedlichen Standorte unterliegt die Bank unterschiedlichen regulatorischen Auflagen für ihre betrieblichen Sicherheitsmaßnahmen. Das Kontinuitätsmanagement wird gleichwohl in Frankfurt zentral koordiniert und lokal von den entsprechenden Verantwortlichen umgesetzt und überwacht. Für den Frankfurter Leiter des örtlichen *und* globalen *Business Continuity Managements* der Bank ist die »Weltrisikogesellschaft« Alltag: »Ganz akutes Beispiel Hurricane Sandy. Da müssen wir schauen, dass die Niederlassung in New York

weiter funktionsfähig ist. Insofern spielt die Vernetzung international, also die geographische Ausbreitung, eine Rolle.« (Interview 4) Die »geographische Ausbreitung« der Finanzbranche ist aber nicht nur ein Problem, sondern auch ein Vorteil für das BCM. Schließlich besteht in Streuung bereits eine erste Sicherheitsstrategie. Jeder Firmensitz der Bank in den unterschiedlichen Finanzmetropolen bzw. *global cities* ist dann so etwas wie eine *backup-site* für alle anderen Standorte. So erläuterte die Zuständige für BCM in der New Yorker Niederlassung derselben Bank: »Wenn zum Beispiel mein Zahlungsverkehr essen geht und da geht ne Bombe hoch, dann werden diese Prozesse nach Frankfurt oder London verlagert.« (Interview 5) Kontinuität kann nur dann gewährleistet werden, wenn die Operationen an unterschiedlichen Orten miteinander koordiniert und synchronisiert werden. Der Raum bzw. die »geographische Ausbreitung« der Geschäfte des globalen Finanzwesens sind für das BCM sowohl Herausforderung als auch Mittel zur Herstellung der Kontinuität. Herausforderung, weil Unterbrechungen an anderen Orten der Welt sich schockwellenartig auf andere Standorte übertragen können. Mittel, weil sich die Operationen auf andere Standorte verlagern lassen und so bereits die prinzipielle Organisationsform der »global microstructures« als »distributed preparedness«-Technik (Collier und Lakoff 2008) wirkt.

Aber was ermöglicht überhaupt das globale Operieren? Welche materiellen Arrangements und infrastrukturellen Voraussetzungen erlauben die weltweite Reichweite von Finanzmarkttransaktionen? In jüngerer Zeit hat sich auch in den *Social Studies of Finance* ein »material turn« vollzogen (Pinch und Swedberg 2008). Es wird nun nicht mehr nur die Performativität von ökonomischen Theorien und kalkulativen Techniken bei der Konstruktion von Märkten in den Blick genommen, wie im von Michel Callon entwickelten »performing markets«-Ansatz (Callon 1998c). Vielmehr wird die Frage nach den »engines« (MacKenzie 2006) der Ökonomie wörtlich genommen und gefragt, welche Technologien und Infrastrukturen die Operationen des Finanzmarktes ermöglichen. Thematisiert werden die »pipes« (Knorr-Cetina 2003) und das »plumbing« (Toscano 2013) des Finanzkapitalismus und damit die materielle Produktion der Virtualität des Finanzwesens (MacKenzie 2007).

Tatsächlich hat die Herausbildung neuer elektronischer und automatischer Handelsformen den Finanzkapitalismus in den letzten zwanzig Jah-

ren zu einem infrastrukturellen Großprojekt gemacht.<sup>219</sup> Es kann daher nicht verwundern, dass die »physical infrastructure« einen wesentlichen Brennpunkt der Sorge des BCM bei Banken ausmacht. »[T]he financial system is keenly dependent on automation, and in turn on those elements of the physical infrastructure that support automation, such as telecommunications and power.« (Joint-Forum 2006, 5) Die Automation der Finanzindustrie stellt hohe Anforderungen an die Verlässlichkeit und die Sicherung der Infrastrukturen des Finanzwesens. Das zeigt sich besonders deutlich am Beispiel des *High Frequency Tradings*, das gerade nicht zu einem Bedeutungsverlust von Raum und Materialität beigetragen hat. Vielmehr wurde die räumliche und sozio-technische Dimension elektronischer Finanztransaktionen zu einem entscheidenden Thema der Finanzindustrie – und zwar sowohl unter Markt- als auch unter Sicherheitsgesichtspunkten.

Die Geschwindigkeitsanforderungen des Hochfrequenzhandels,<sup>220</sup> bei dem nur mithalten kann, wer mindestens so schnelle Verbindungen und Rechner hat wie die Konkurrenz, haben zu einem technischen Wetttrüben geführt. Die Signalübertragungen der Kauf- und Verkaufsbefehle der Handelsmaschinen haben ihre Geschwindigkeitsgrenze in den von Einstein formulierten Naturgesetzen (nichts kann sich schneller übertragen als das Licht, aber auch das Licht braucht immer noch Zeit, um räumlich übertragen zu werden). Nachdem die technischen Möglichkeiten zur Erhöhung der Übertragungsgeschwindigkeit von Signalen nunmehr weitestgehend ausgeschöpft sind, verbleibt nur noch eine Möglichkeit, weitere Geschwindigkeitsgewinne zu realisieren. Die Entfernungen, die die Signale zurückzulegen haben, müssen reduziert werden. Entsprechend wird versucht, Räumlichkeiten in möglichst großer Nähe zu den Handelsplätzen in New York, London oder Chicago zu mieten. In den letzten Jahren haben sich Datenzentren erstaunlichen Ausmaßes in den Außenbezirken dieser Handelsplätze etabliert, etwa in Aurora in der Nähe der Merc (Mercantile Exchange) in Chicago oder in Mahwah in Nord New Jersey für die New York Stock Exchange (NYSE) (siehe: MacKenzie et al. 2012). Der große Kühlungsbedarf für die Hochleistungsrechner macht das Rechenzentrum in Mahwah zum größten Stromkonsumenten in New Jersey, der mit aufwändigen Sicherungsvorkehrungen gegen Stromausfälle abgesichert ist (Glanz 2012). Zudem ist das Rechenzentrum von Mahwah von der US-

---

219 Zur Geschichte und den sozialen Voraussetzungen der Automation siehe: Pardo-Guerra (2010), MacKenzie (2013).

220 Für einen Einstieg in die Thematik des Hochfrequenzhandels siehe: MacKenzie (2011).

Regierung als Kritische Infrastruktur klassifiziert worden (MacKenzie 2011, 16). Durch die Indienstnahme der Hochtechnologie wurde auch die operative Grundlage des Finanzwesens zu einem Hochsicherheitsprojekt. Jedenfalls sorgen die Sicherheitsvorkehrungen in den Rechenzentren für Begeisterung in der *IT-security-community*. »All of the power and mechanical systems in Mahwah are engineered to at least 2N reliability, with backup equipment available for each piece of critical infrastructure.« (Miller 2011)<sup>221</sup>

Allerdings geht mit der Automatisierung des Handels kein »Verschwinden des Menschen« aus der Finanzindustrie einher. »Comprehensive business continuity management addresses not only technical considerations, but also the human dimension.« (Joint-Forum 2006, 12) Es gibt, wie es in Empfehlungen der Europäischen Zentralbank zu BCM heißt, nicht nur Kritische Infrastrukturen, sondern auch »critical staff« (ECB 2006, 5), und das betrifft »computer operators as well as system control staff and management« (ECB 2006, 6). Schließlich ist auch die elaborierteste Infrastruktur auf menschliches Bedienungspersonal angewiesen. Die Kritischen Infrastrukturen des Finanzsystems setzen sich also aus menschlichen und nicht-menschlichen Elementen zusammen und können nur gemeinsam die »critical functions« (ECB 2006, 5, Joint-Forum 2006, 14) des Finanzsystems aufrecht erhalten.

Neben der Kritikalität von Personen und Infrastrukturen ist es aber vor allem der Faktor Zeit, der die Kritikalität des Finanzsektors ausmacht. Banken – so wird immer wieder betont – haben ein sehr »zeitkritisches Geschäftsmodell« (BSI 2008, 36). Das liegt zunächst einmal daran, dass schon in sehr kurzer Zeit sehr hohe Verluste entstehen können. Das Risiko hoher Verluste betrifft aber letztlich nur eine einzelne Bank und ist daher für Regulatoren wie die EZB und die Bank for International Settlements nicht von vordringlicher Bedeutung. Verluste durch Geschäftsunterbrechungen einzelner Banken sollen schließlich durch operationelles Risikomanagement abgesichert werden. Systemisch relevant wird die Zeitkritikalität aber dadurch, dass das Finanzsystem so eng getaktet ist, dass sich

---

221 Das wohl ambitionierteste Infrastrukturprojekt des Finanzmarkts in jüngerer Zeit ist die Verlegung eines Glasfaserkabels für den Hochfrequenzhandel von Chicago nach New York. Um etwa 1,3 Millisekunden Übertragungszeit einzusparen, wurde in einem 300 Millionen Dollar-Projekt unter anderem ein Tunnel in das Gestein der Allegheny Mountains gebohrt (MacKenzie et al. 2012).

Unterbrechungen an einzelnen Punkten des Finanznetzwerks sehr schnell fortsetzen können.

»The velocity with which money and securities turn over on a daily basis underpins the considerable interdependencies – in the form of settlement risk and, ultimately, credit and liquidity risks – among financial industry participants and investors. The result is that operational disruption at one financial industry participant can cause difficulties at others.« (Joint-Forum 2006, 5)

Interdependenz bekommt hier eine zusätzliche zeitliche Dimension. Die »excessive interconnectedness« (BIS 2010, 7) des Finanzsystems ist nicht nur räumlich oder strukturell, sondern auch zeitlich bedingt. Störungen im kontinuierlichen Fließen des Finanzsystems können auch durch zeitliche Verzögerungen und Probleme bei der temporalen Synchronisierung zwischen unterschiedlichen Finanzinstitutionen hervorgerufen werden. Das heißt auch, dass die Sicherung der Finanzinfrastruktur durch BCM und die Sicherung des Finanzmarkts gegen das Auftreten systemischer Risiken zusammenhängen. So betont die EZB in ihren Empfehlungen zum BCM von kritischen Zahlungssystemen die Problematik systemischer Risiken: »the inability of one participant to meet its obligation in a system or to perform its functions when due will cause other participants to be unable to meet their obligations when due. [...] The inability can be caused by operational or financial problems.« (ECB 2006, 13) Hier wird deutlich, dass sich die Regulierung von systemischen Risiken auf dem Finanzmarkt und der Schutz Kritischer Infrastrukturen nicht nur auf der Ebene von analogen Sicherheitstechnologien, sondern auch faktisch überschneiden, insofern das Finanzsystem auf das Funktionieren eines komplexen sozio-technischen Infrastruktursystems angewiesen ist.

»Conceptually, business continuity management is distinct from financial crisis management in that a financial crisis does not typically entail business continuity concerns. An event that gives rise to business continuity concerns, however, could develop into a financial crisis.« (Joint-Forum 2006, 6)

Die operative Architektur der Finanzindustrie ruft also Sicherheitsprobleme hervor, die seit der jüngsten Finanzkrise im Zentrum öffentlicher Aufmerksamkeit stehen. Die materiellen Infrastrukturen des Finanzsystems sind mehr als ein unwichtiger Nebenschauplatz oder nur die technische Bedingung der Möglichkeit der virtuellen Finanzoperationen. Vielmehr ragen sie in die Geschäfte der Finanzindustrie hinein, wenn sie genutzt



werden, um sich Wettbewerbsvorteile gegenüber Konkurrenten zu verschaffen oder wenn ihr Ausfall zu Krisen auf dem Markt führt.

#### 4.3.3. Sicherung der Finanzinfrastrukturen

Aber was genau macht Banken aus Sicht des BCM und des Infrastrukturschutzes so kritisch und vor allem zeitkritisch? Wodurch entstehen die operationellen Interdependenzen zwischen Banken, so dass Unterbrechungen an einer Stelle des Finanzsystems zu Problemen an anderen Stellen werden? Die einhellige Antwort auf diese Frage ist: der Zahlungsverkehr. »Die zentrale Funktion ist der Zahlungsverkehr. Das ist auch der Grund, warum Banken zu den Kritischen Infrastrukturen zählen.« (Interview 4)

Aber was ist dieser Zahlungsverkehr? Die Frage der Zahlungsinfrastrukturen bzw. Zahlungssysteme bildet eine – im Wortsinn – Leerstelle in der sozialwissenschaftlichen Forschung. Der Ort des Zahlungsverkehrs ist, wie Bill Maurer (2012, 23) bemerkt, der Strich in Marx' klassischer Formel: G-W-G. Aber auch die aktuelle Forschung zu den Spektakeln des Finanzsystems »neglects the infrastructures of payment that make finance possible« (Maurer 2012, 15). Statt der Illusion des einfachen durch Geld vermittelten Austausches zu erliegen, so als wäre die Ökonomie nichts anderes als ein riesiger Tante Emma Laden, wo man mit ein paar Groschen eine klar bepreiste Ware einkauft, muss der Bezug auf »Infrastruktur« in der Rede vom Zahlungsverkehr ernst genommen werden. Bereits alltägliche Zahlungen mit der Kreditkarte nehmen einen weiten Weg durch eine verzweigte Zahlungsinfrastruktur – und das gilt für die Transaktionen im Finanzsystem umso mehr. Auf diesem Weg, den eine Zahlung zurücklegt, bzw. in der Zeit, in der sie sozio-technisch abgewickelt wird, kann einiges schief gehen. Insofern bildet das Problem der Zahlungssysteme einen weiteren Hintergrund für die wachsende Bedeutung von BCM im Finanzsektor. So betont die BIS in ihren *High-Level Principles* die »pivotal role that financial intermediation plays in facilitating and promoting national and global economic activity by providing the means for making and receiving payments, for borrowing and lending, for effecting transactions« (Joint-Forum 2006, 5). Als »intermediäre« Infrastruktur des Finanzsystems sind Zahlungssysteme nämlich nicht nur neutrale Kanäle für Finanztransaktionen, die als Nebenschauplätze bzw. *para-sites* des Finanzkapitalismus abgetan werden könnten. Die Intermediarität macht die Zahlungssysteme vielmehr zu einem Parasiten im Sinne von Michel Serres (1981): Einerseits stellen sie

Verbindungen zwischen den Finanzakteuren überhaupt erst her, andererseits sind sie dadurch auch eine potenzielle Störquelle.

Die geheimnisvolle Welt des Zahlungsverkehrs begegnet uns im Alltag, wenn wir Geld vom Automaten abheben, eine Überweisung tätigen oder etwas mit Kredit- bzw. Geldkarte bezahlen. Zwar bleibt das Infrastrukturnetz, das diese Alltagsgeschäfte ermöglicht, genauso verborgen wie die Kanalisation, wenn wir die Toilettenspülung betätigten, nichtsdestotrotz hat diese Zahlungsinfrastruktur eine »vitale« Bedeutung für das Funktionieren von Gesellschaft, Ökonomie und Staat. Tatsächlich ist Geld in kapitalistischen Gesellschaften ein ähnlich lebenswichtiges Gut wie Wasser und deshalb liegt es nahe, dass der Zahlungsverkehr als Kritische Infrastruktur eingestuft wird. Die »liquid modernity« – vermeintlich ebenfalls »no longer bound, not even slowed down by the resistance of space« (Bauman 2000, 11) – würde austrocknen, wenn man ihr den Geldhahn zudrehen würde, und deshalb ist sie auf den intermediären Raum der Zahlungsinfrastruktur angewiesen. Auch wenn man Geld bekanntlich nicht essen kann, kann man ohne Geld gegenwärtig eben auch nichts essen. Gerade mit Verweis auf die Zahlungsinfrastruktur wird immer wieder die lebenswichtige, biopolitische Bedeutung des Finanzwesens hervorgehoben:

»Die Unternehmen wollen ja auch im Notfall ihren Mitarbeitern Gehälter zahlen können, die die dann am Geldautomaten abheben. Also dazu muss das Gehalt auf dem Konto sein, damit der Bürger das am Geldautomaten wieder abheben kann und Bargeld hat und damit Lebensmittel kaufen kann. Dieser Zyklus, der muss laufen. Und der macht Banken kritisch.« (Interview 4)

Aber dieser »Zyklus«, in dem Unternehmen ihren Mitarbeiter\_innen Geld überweisen, damit diese sich Lebensmittel kaufen können, ist nur die eine, dem Alltag zugewandte Seite der Zahlungssysteme. Neben diesen *Retail Payment Systems* gibt es die *Large Value Payment Systems*, über die vornehmlich Geschäfte zwischen Banken und anderen Akteuren des Finanzmarkts abgewickelt werden. Hier geht es weniger um die finanzielle Flüssigkeit von Bankkund\_innen, sondern um die Liquidität des Finanzsystems, die seit der Finanzkrise zum entscheidenden Problem finanzieller Stabilität geworden ist (Langley 2014, siehe auch Kapitel 2.5.2.). Analyse Riles (2011, 131) beschreibt *Large Value Payment Systems* als die »all-important technology by which funds move from one party to another.« Hinter dieser einfachen Funktion der Zahlungssysteme (die Bewegung und Übertragung von »funds«, also letztlich Geld in der einen oder anderen Form, von einem Finanzakteur zum anderen) verbirgt sich ein komplexes soziotechnisches

Arrangement. Im Normalfall wickeln Banken Geschäfte nicht direkt mit anderen Banken ab, sondern vermittelt über eine sogenannte clearing-Stelle bzw. ein Zahlungssystem. Diese werden dann als Intermediäre zwischen die Parteien geschaltet, so dass jede Zahlung einen obligatorischen Passagepunkt durchqueren muss, bevor sie ihren Empfänger erreicht. Schier unglaublich große Summen werden über diese Systeme täglich prozessiert. Riles (2011, 131) berichtet, dass durch das Zahlungssystem der Bank of Japan jeden Tag 30.000 Transaktionen mit einem Wert von 120 Billionen Yen (etwa 1.26 Billionen US-Dollar) prozessiert werden. Das wichtigste Zahlungssystem der EU, TARGET2, verarbeitet täglich durchschnittlich 360.000 Transaktionen mit einem Wert von 2 Billionen Euro (siehe: EZB 2013, 2), ein Drittel davon wird von der Bundesbank prozessiert.

Als Infrastrukturen des Finanzmarkts sind die Zahlungssysteme aber nicht bloß technische oder physische Kanäle, sondern ebenso ein Set von Regeln und Standards. Finanzinfrastrukturen werden von der BIS definiert

»as a multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling or recording payments, securities, derivatives, or other financial transactions. FMIs [Financial Market Infrastructures] typically establish a set of common rules and procedures for all participants, a technical infrastructure, and a specialised risk-management framework appropriate to the risks they incur.« (BIS und IOSCO 2012, 7)

Entsprechend gibt es ganz unterschiedliche Systemdesigns, die bestimmte Regeln und technische Arrangements verkörpern, die ihrerseits von bestimmten politischen und ökonomischen Überzeugungen beeinflusst sind (Riles 2011, 132). So unterscheiden sich Zahlungssysteme etwa dadurch voneinander, in welcher zeitlichen Taktung und zu welchen Terminen die Zahlungen vollzogen werden. In einigen Zahlungssystemen werden alle Zahlungen am Ende des Handelstages abgewickelt, in anderen mit größerer Zeitverzögerung und in sogenannten *Real Time Gross Settlement Systems* (RTGS) unmittelbar. Schließlich gibt es sogenannte *netting*-Systeme, die durch bestimmte Verrechnungsalgorithmen sicherstellen sollen, dass alle Obligationen und offenen Positionen innerhalb des Systems beglichen werden können. Strenggenommen werden die *funds* dann nicht mehr von einer zur anderen Partei übertragen, sondern auf die beteiligten Parteien ihren Ansprüchen entsprechend aufgeteilt. All diese Systeme sollen – und

das ist der letzte Teil der oben zitierten Definition – eine bestimmte Rolle beim Risikomanagement spielen.<sup>222</sup>

Damit ist das Design der Finanzinfrastruktur und der Zahlungssysteme, die häufig von Zentralbanken (zum Beispiel FEDWIRE von der US-amerikanischen *Federal Reserve*, BOJ von der *Bank of Japan*, TARGET2 von den Zentralbanken der Eurozone) betrieben werden, zu einem Regulierungsinstrument geworden. So wurde, wie in Kapitel 2.5.3. bereits erwähnt, durch die *European Market Infrastructure Regulation* (EMIR) der Handel mit OTC-Derivaten reguliert. Fortan sollen diese Geschäfte nicht mehr direkt zwischen den Finanzakteuren (*over the counter* für OTC) stattfinden, sondern über eine *central counterparty* bzw. ein *clearing house* abgewickelt werden, das als Intermediär zwischen die Parteien tritt. So sollen zum einen Ausfallrisiken verkleinert und zum anderen die Transparenz dieser Geschäfte erhöht werden. Mit dieser heilenden Wirkung gehen aber auch Risiken einher. Als Risikoregulationsinstrument hat die Finanzmarktinfrastruktur einen pharmakologischen Charakter. Denn durch die Abwicklung über zentrale *clearing*-Stellen werden zugleich obligatorische Passagepunkte geschaffen, deren fortgesetztes Operieren systemwichtig ist. So wird in den *High-Level*

---

222 So soll das *settlement*-Risiko, dass eine Partei ihre Zahlungen etwa auf Grund einer Insolvenz nicht mehr leisten kann, obwohl sie bereits die Zahlungen der Gegenpartei erhalten hat, in einem *netting*-System dadurch vermieden werden, dass ausstehende Zahlungen an eine insolvente Institution an deren Schuldner übermittelt werden können. Sehr vereinfacht ausgedrückt: wenn Harry Peter 5 Euro schuldet und nicht bezahlen kann, zugleich aber von Frank noch 5 Euro bekommen kann, dann kann auch einfach Frank Peter bezahlen. In einem RTGS-System sollen *settlement*-Risiken dadurch verhindert werden, dass alle Zahlungen unmittelbar vollzogen werden und dadurch die Zeitdifferenzen vermieden werden sollen. Hintergrund für die Besorgnis um *settlement*-Risiken ist der Fall des deutschen Bankhauses Herrstatt, weshalb *settlement*-Risiken bis heute auch als »Herrstatt risk« bekannt sind. Im Jahr 1974 ging das Bankhaus Herrstatt insolvent. Die damals zuständige Bundesbank hat Herrstatt ihren Regularien entsprechend am Ende eines Handelstages um 16 Uhr deutscher Zeit geschlossen. Das führte aber dazu, dass die ausstehenden Zahlungen von Herrstatt an US-amerikanische Banken aufgrund der Zeitverschiebung nicht mehr vollzogen werden konnten, obwohl die Bank die Gegenleistungen bereits erhalten hatte. Dieser Zahlungsausfall führte zu einer Kettenreaktion, die beinahe eine Finanzkrise ausgelöst hätte. Was dieser Fall deutlich machte, war, dass *settlement*-Risiken mit systembedrohender Potenzialität durch die willkürlichen Vorgaben der Betreiber der Zahlungssysteme (der Zentralbanken) entstehen können. In Reaktion auf diese Krise hat sich die Bank for International Settlements mit Sitz in Basel gegründet, die als »Superzentralbank« die Arbeit der nationalen Zentralbanken besser koordinieren soll. *Settlement*-Risiken sind eine mögliche Ursache von Systemrisiken und standen als solche bereits im Fokus regulatorischer Aufmerksamkeit, lange bevor die *systemic risks* des Finanzmarktes in aller Munde waren.

*Principles for Business Continuity* der BIS die »concentration of clearing and settlement processes in most financial systems« (Joint-Forum 2006, 5) als entscheidender Hintergrund für die Notwendigkeit von Schutzvorkehrungen für die finanzielle Infrastruktur durch *Business Continuity*-Maßnahmen betont. »Disruptions of these processes can have material adverse consequences for a financial system and prevent significant market participants from completing transactions and meeting their obligations.« (Joint-Forum 2006, 5)

Im Brennpunkt der Sorge um die Integrität der Zahlungsinfrastrukturen des Finanzmarktes stehen dabei insbesondere die *Systemically Important Payment Systems* (SIPS). Bereits im Jahr 2001 veröffentlichte die Bank for International Settlements die *Core Principles for SIPS*, die einheitliche, internationale Standards für diese systemwichtigen Systeme etablieren sollten. SIPS werden definiert als »systems which could trigger or transmit systemic disruptions in the financial area because of the size or nature of individual payments which they handle or because of the aggregate value of the payments processed« (BIS 2001, 5).<sup>223</sup> Die EZB weist mittlerweile vier Zahlungssystemen in ihrem Regulationsbereich systemwichtige Bedeutung zu: TARGET2, EURO1, STEP2-T und CORE(FR).<sup>224</sup> »[S]ystemic disruptions«, die von diesen systemwichtigen Zahlungssystemen ausgehen können, stellen eine distinkte Quelle von *systemic risks* dar.

»[I]n the context of payment systems this [systemic risk, A.F.] is the risk that the inability of one of the participants to meet its obligations, or a disruption in the system itself, could result in the inability of other system participants or of financial institutions in other parts of the financial system to meet their obligations as they become due. Such a failure could cause widespread liquidity or credit problems

<sup>223</sup> In einem Papier der EZB aus dem Jahr 2003 zur Regulation von *Retail Payment Systems* wird deutlich, was die Systemwichtigkeit eines Zahlungssystems konstituiert. Das Papier nennt drei Kriterien für Systemwichtigkeit: »market penetration«, »aggregate financial risk« und »domino effects« (ECB 2003, 2). Letztere können vor allem in *netting*-Systemen auftreten. Deutlich wird hier, dass eigentlich nur *Large Value Payment Systems* – die Zahlungssysteme des Finanzmarkts – systemwichtige Bedeutung erlangen können, während die *Retail Payment Systems*, die hauptsächlich die *real economy* betreffen, bestenfalls »prominente« Bedeutung haben können.

<sup>224</sup> Dabei wird TARGET2 vom Eurosystem, also von den Zentralbanken im Euroraum betrieben. Zwar hat TARGET2 eine einheitliche technische Basis, aber die Betreiber sind letztlich immer noch nationale Zentralbanken wie die deutsche Bundesbank. EURO1 und STEP2-T werden dagegen von EBA Clearing betrieben, einem Zusammenschluss der an diesem Zahlungssystem beteiligten Banken. Sowohl öffentliche als auch privatwirtschaftliche Zahlungssysteme haben also eine systemwichtige Bedeutung.

and, as a result, could threaten the stability of the system or of financial markets.« (BIS 2001, 5)

Auf den ersten Blick enthält diese Definition von systemischen Risiken keine Neuigkeit: Fortgesetzte Zahlungsausfälle führen zu Liquiditätsengpässen, zu einer gefährlichen Stockung des Zahlungsflusses. Bemerkenswert sind aber kleine Details der Definition. Zum einen werden als mögliche Ursache für ein Risiko nicht nur der Ausfall eines »participants« wie etwa einer Bank, sondern auch die »disruptions« des Systems selbst genannt, also der intermediären Infrastruktur der Zahlungsprozession. Zudem signalisiert das kleine Wort »due« die zeitkritische Komponente systemischer Gefährdungen in Zahlungssystemen. Systemische Risiken entstehen also auch durch die Imperative der Taktung und die mehr oder weniger willkürlich vorgegebenen Termine der Betreiber der Systeme. Im Grunde handelt es sich bei all dem um eine bestimmte Form von *settlement*-Risiken, die sich zu systemischen Risiken ausweiten können. *Settlement*-Risiken, wie beim Fall der Bank Herstatt, können durch die Unterbrechungen in Zahlungssystemen entstehen und sich schnell fortsetzen: »disruptions spread quickly and widely« (BIS 2008). Letztlich könnte es dadurch – auch in einer ansonsten stabilen Marktsituation – zu einem kaskadierenden Zahlungsausfall kommen.

Vor diesem Hintergrund wird verständlich, warum die Gewährleistung kontinuierlicher Operationsfähigkeit der Zahlungssysteme von entscheidender Bedeutung für die Vermeidung systemischer Risiken ist. Denn schon eine kurze, temporäre Stockung der Operationen einer Zahlungsinfrastruktur kann verheerende Folgen haben, wenn dadurch wichtige Transaktionen nicht oder nicht rechtzeitig beglichen werden können. Entsprechend lautet ein Prinzip der insgesamt zehn »core principles«: »The system should ensure a high degree of security and operational reliability and should have contingency arrangements for timely completion of daily processing.« (BIS 2001, 8) Aufbauend auf diesem Prinzip hat die EZB im Jahr 2006 die *Business Continuity Oversight Expectations for Systemically Important Payment Systems (SIPS)* herausgegeben. Diese strengen BCM-Vorgaben unterstreichen vor allem die Zeitkritikalität der systemwichtigen Zahlungssysteme. So heißt es: »Business continuity objectives for SIPS should aim at the recovery and resumption of critical functions within the same settlement day.« (ECB 2006, 3) Und, noch anspruchsvoller: »Under the emerging and more demanding »good practice«, it is recommended that SIPS should aim to recover and resume critical functions or services (in-

cluding critical services outsourced to third party providers) no later than two hours after the occurrence of a disruption.« (ECB 2006, 5) Diese zwei Stunden-Regel ist mittlerweile zur *benchmark* für BCM von Zahlungssystemen geworden. In den 2012 von der BIS (mit)herausgegebenen Prinzipien für *Financial Market Infrastructures* (FMIs)<sup>225</sup> wird das bestätigt und zudem eine unmittelbare Fortsetzung der Tätigkeit der Infrastruktur durch backup-Systeme empfohlen. »An FMI should aim to be able to resume operations within two hours following disruptive events; however, backup systems ideally should commence processing immediately.« (BIS und IOSCO 2012, 98)

Neben diesen systemwichtigen Zahlungssystemen gibt es aber auch eine Reihe von »critical services« (Joint-Forum 2006, 9), die ihrerseits für die Zahlungsinfrastruktur des Finanzsystems systemwichtige Bedeutung haben. Hierbei sticht der Telekommunikationsdienst SWIFT heraus. SWIFT steht für *Society for Worldwide Interbank Financial Telecommunications*, besteht seit 1973, hat seinen Sitz in Belgien und operiert weltweit. SWIFT ist nicht selbst ein Zahlungssystem, sondern stellt die Telekommunikationsinfrastruktur für die Übermittlung von Transaktionen zwischen Banken bereit und ist hier nahezu konkurrenzlos. Die Zahlen sind beeindruckend: 2013 übermittelte SWIFT täglich 20 Millionen Nachrichten mit einem Gesamtwertvolumen von 7,5 Billionen Euro. Der seltsame Status von SWIFT – kein Zahlungssystem, aber doch ein entscheidender Service für Zahlungssysteme – gestaltet seine Regulation sehr schwierig. »SWIFT is not itself a payment system, but a messaging services provider to such systems, so that many of the Core Principles (for the regulation of systemically important payment systems) do not apply to SWIFT or have only partial relevance.« (NBB 2007, 96) Aber nicht nur sind die existierenden Regeln schwer auf SWIFT zu übertragen, sie sind vor allem auch nicht bindend. Entsprechend bemerkt die Belgische Nationalbank: »The major instrument for the oversight of SWIFT is moral suasion.« (NBB 2007, 92) Regulati-

---

225 Die Regulierung für SIPS ist mittlerweile in der umfassenderen Regulierung für FMIs (*Financial Market Infrastructures*) aufgegangen. Der Hintergrund hierfür ist die oben erwähnte Aufmerksamkeit für Marktinfrastrukturen als Instrument und Problem für die Regulation des Finanzmarktes. Zu FMIs gehören nicht nur *Large Value Payment Systems*, sondern auch andere Infrastrukturen, die spezielle Finanztransaktionen vollziehen. Hierzu gehören etwa »central securities depositories (CSDs), securities settlement systems (SSSs), and central counterparties (CCPs)« (BIS und IOSCO 2012, 5). Die EU hat diese Prinzipien für die Regulierung der Zahlungssysteme in ihrer Jurisdikation mittlerweile übernommen (EZB 2014).

onsinstanzen können also SWIFT nur gut zureden, obwohl die Gefährdungen, die gerade von der operationellen Verwundbarkeit von SWIFT ausgehen (also Unterbrechungen im Betrieb des sozio-technischen *mesaging services*) durchaus systemwichtige Relevanz haben können. »Overseers recognized that their main focus when overseeing SWIFT should be on operational risk, as this is believed to be the primary risk category through which SWIFT could pose systemic risk to the global financial system.« (NBB 2007, 96) Dementsprechend messen die fünf *High Level Expectations for the Oversight of SWIFT* der »reliability und resilience« einen hohen Stellenwert bei und fordern Maßnahmen zu »disaster recovery« und »business continuity management« (NBB 2007, 97).

Das Beispiel von SWIFT unterstreicht, wie schwierig die Regulierung und Sicherung der Infrastrukturen des Finanzwesens ist. Gerade weil die Infrastrukturen des Zahlungsverkehrs die Operationen eines globalen Marktgeschehens ermöglichen und unterstützen sollen, entgehen sie systematisch Regulierungen auf nationaler Ebene. Es entstehen globale Gefüge der Sicherheit, die bisweilen ebenso verschachtelt wirken wie die Materie, die sie zu regulieren versuchen. Die Komplexität der unterschiedlichen Ebenen und Bestandteile der Zahlungsinfrastruktur macht es schwer, überhaupt auszumachen, was innerhalb dieser sozio-technischen Netzwerke voneinander abhängt und was genau kritisch ist. Eine Ahnung davon, wie kritisch diese Netzwerke tatsächlich sind, bekommt man gleichwohl, wenn man die beachtlichen Summen bedenkt, die täglich durch ihre Kanäle laufen. Sie bilden das Kanalsystem für die Zahlungsflüsse des Finanzwesens. Die Bedeutung dieser Zahlungsflüsse und der dauerhaften Liquidität des Finanzsystems wurde in den jüngsten Finanzkrisen schmerzhaft bewusst, als der Zahlungsverkehr zwischen den Banken stockte (*credit crunch*) und das Finanzsystem nur durch massiven externen Geldzufluss wieder zum Laufen gebracht werden konnte (siehe Kapitel 2.5.2.). Das ist der Grund, warum Zahlungssysteme ein »boundary object« darstellen, in dem die Vorsorge gegen operationelle Risiken und die Regulation von systemischen Risiken auf Finanzmärkten zusammenlaufen. Hier weisen die Sicherheitstechnologien zum Schutz Kritischer Infrastrukturen bzw. operativer Reliabilität der Banken und der Regulation systemischer Finanzrisiken nicht nur Familienähnlichkeiten auf (zu diesen Analogien siehe Kapitel 2.5.), sondern stützen sich – wengleich mit unterschiedlichen Maßnahmen – auf dasselbe *matter of concern*: die Finanzmarktinfrastuktur. Während mit Regulationen wie der EMIR versucht wurde, die Resilienz des Finanzsys-



tems durch ein verändertes Systemdesign zu erhöhen, sorgt sich das Kontinuitätsmanagement um die sozio-technische Grundlage dieses Systems.

#### 4.4. Management der Kontinuität, Politik des Ereignisses

Eine Orientierung an Ereignissen ist den Sozialwissenschaften traditionell suspekt. Es geht ihnen schließlich eher um »continuity and structure« als um »breaks and ruptures« (Guggenheim 2014, 2). Diese Haltung ist, wie Michael Guggenheim (2014, 3) bemerkt, selbst in der Katastrophensoziologie weit verbreitet. Tatsächlich neigen sozialwissenschaftliche Studien über Katastrophen dazu, die strukturell angelegten sozialen Vulnerabilitäten (die latenten Katastrophen von Armut, Exklusion und sozialer Ungleichheit) zu betonen, die ein bestimmtes Naturereignis erst zur Katastrophe machen – eine Methode, die Eric Klinenberg (2003) als »soziale Autopsie« der Katastrophe bezeichnet hat. In der Aufdeckung der Strukturen, die eine Krise erst möglich gemacht haben, wurde traditionellerweise das kritische Potenzial der Soziologie gesehen. Und auch wenn diese Arbeit eine andere Kritik- und Analysestrategie verfolgt, so hat sie sich doch bisher vornehmlich darauf konzentriert, zu zeigen, wie Sicherheitstechnologien sich in längeren Zeitabschnitten gebildet und umgebildet haben, anstatt einzelne Katastrophenereignisse in den Blick zu nehmen.

Zum Abschluss der Arbeit werde ich jedoch mit dieser Gewohnheit brechen und doch auf einige Unterbrechungsereignisse eingehen, die für das BCM von Banken relevant sind. Für die Analytik des Sicherheitsdispositivs der Resilienz ist der Blick auf das Ereignis vor allem deshalb interessant, weil sich hier »ad hoc assemblage[s]« (Braun 2014, 51) bilden, die durchaus typisch für die gegenwärtige Regierung der Katastrophe sind. Ereignisse sind die Orte, an denen sich unterschiedliche Akteure und Sicherheitsrationalitäten treffen, die von der normativen Kraft des Geschehnisses zusammengebracht werden. Wie sich im Anschluss an Debatten des Neuen Materialismus argumentieren ließe, ist der Fokus auf Ereignisse aber auch attraktiv, weil hier soziale und nicht-soziale Komponenten in Konjunktion treten und das Potenzial haben, gewohnte soziale Verlaufsmuster zu stören (Althusser 2010, Connolly 2013, Folkers 2013b). Materielle Unterbrechungsereignisse liefern so gewissermaßen die Substanz für politische, wissenschaftliche sowie öffentliche Debatten und Problemati-

sierungen (Marres 2007), insofern sie dazu nötigen, unhinterfragt angenommene Tatsachen in »matters of concern« (Latour 2004) zu verwandeln. Materielle Ereignisse haben also das Potenzial, eine Politik des Ereignisses zu katalysieren. Auf diese Weise machen Ereignisse BCM, das für gewöhnlich im Verborgenen operiert, sichtbar und damit auch kritisierbar – und zwar nicht nur für soziologische Expert\_innen, sondern auch für eine politische Öffentlichkeit, die auf die eine oder andere Weise vom BCM betroffen ist.

Im Folgenden werde ich zunächst darauf eingehen, welche Rolle konkrete Unterbrechungsereignisse für die Ausarbeitung des generischen Kontinuitätsmanagements spielen. (4.4.1.). Anschließend werde ich auf zwei BCM-relevante Ereignisse aus der jüngeren Vergangenheit eingehen. Einmal die Ereignisse rund um den *Hurricane Sandy* in New York (4.4.2.) und zum anderen die Konfrontation zwischen Kontinuitätsmanagement und der Unterbrechungspolitik der Blockupy-Bewegung in Frankfurt am Main (4.4.3.). Dabei werde ich auch die Kritik an bestimmten Ausformungen der Sicherheit beleuchten, die im Verlauf dieser Ereignisse artikuliert wurde.

#### 4.4.1. Krise, Kritik und Kontinuität: Ereignisse im Raster des BCM

Die generischen Maßnahmen zur Gewährleistung der Kontinuität der Operationen des Finanzwesens unterscheiden sich auf den ersten Blick nur wenig von denjenigen in anderen Bereichen. Die Besonderheiten der BCM-Maßnahmen im Finanzwesen liegen weniger in einem prinzipiellen Unterschied zu anderen Kontinuitätsprojekten als vielmehr in der Intensität und dem hohen Anspruch an ununterbrochene Geschäftstätigkeit. Gerade die systemwichtigen Zahlungssysteme dürfen sich nur sehr kurze Unterbrechungszeiten leisten, wie durch die immer wiederkehrende zwei Stunden-Regel deutlich wird (ECB 2006, 3, BIS und IOSCO 2012, 98). Eigene Ausweichstandorte werden vorgeschrieben und selbst die Etablierung einer »third site« (BIS und IOSCO 2012, 98) wird angeregt. Die starke Angewiesenheit auf das Funktionieren der technischen Infrastrukturen lässt zudem Überlegungen entstehen, auf altbewährte analoge Techniken zurückzugreifen. »An FMI should also consider alternative arrangements (for example, manual paper-based procedures) to allow for the processing of time critical transactions.« (BIS und IOSCO 2012, 98) Aber auch Personalausfälle stehen im Fokus der Kontinuitätspläne. Hier wirft vor allem der 11. September noch immer seinen langen Schatten (ECB 2006, 5f.). Nicht

nur redundante Infrastrukturen, sondern auch redundante Personalressourcen sind zur Fortsetzung des Geschäftsbetriebs notwendig. »Steps should be taken to ensure that not all operational [...] staff identified as critical [...] are in the same place at the same time.« (ECB 2006, 7) Zudem ist die bereits angesprochene globale Vernetzung ein besonderes Charakteristikum des BCM im Finanzwesen. Die Beschwörungen der Bedeutung von »cross-border communications« (Joint-Forum 2006, 11) und die Empfehlung, »joint-exercises« (Joint-Forum 2006, 10) durchzuführen und gemeinsame Strategien zu entwickeln (siehe: Joint-Forum 2006, 13), ist zwar prinzipiell typisch für den Schutz vor Katastrophen, die »keine Grenzen kennen«, aber nicht selbstverständlich für das BCM, dem es zunächst einmal um den Schutz einzelner Unternehmen bzw. Institutionen geht. Hier wird erneut deutlich, dass es beim BCM im Finanzwesen nicht nur um den Schutz einzelner Finanzinstitutionen oder Standorte geht, sondern um die Verhinderung systemischer Risiken in einem exzessiv vernetzten Geschäftsbereich.

Trotz dieser Besonderheiten sind die Pläne für das Kontinuitätsmanagement bei Banken auf generische Maßnahmen ausgerichtet. »Also man versucht möglichst generisch zu bleiben, um möglichst breite Abdeckung zu haben.« (Interview 4) Gleichwohl gibt es doch eine zumindest rudimentäre Reflexion über die Spezifität einzelner Fälle. So enthalten die *High Level Principles for Business Continuity* der *Bank for International Settlements* im Anhang eine Reihe von »case studies« zu konkreten BCM-relevanten Vorfällen seit dem 11. September: der Stromausfall an der amerikanischen Ostküste im August 2003, der die kanadische und US-amerikanische Finanzindustrie betroffen hat, der Ausbruch von SARS 2003 in Hongkong mit Auswirkungen auf den wichtigsten chinesischen Finanzplatz, lokale SARS-Fälle in Toronto, das Nügata Chuetsu-Erdbeben in Japan im Jahr 2004 und die verheerenden Terroranschläge in London 2005 (Joint-Forum 2006, 19–35). Schon diese Liste lässt sowohl ein ortsspezifisches Risikoprofil erkennen (etwa Erdbebenrisiken in Japan) als auch die Bandbreite von möglichen, die Kontinuität der Finanzoperationen bedrohenden Ereignissen deutlich werden (von Terror bis Pandemie). Allerdings werden auch in der Analyse solcher konkreten Fälle eher die Vorzüge eines generischen Ansatzes betont: »It appears that business continuity planning in many financial institutions is focused upon impact and decision-making processes rather than on the nature of the disruption. [...] This generic impact-based approach worked particularly well.« (Joint-

Forum 2006, 33) Gleichwohl fällt auf, wie sehr sich die Maßnahmen gegen beispielsweise einen Stromausfall und eine Pandemie voneinander unterscheiden. Während beim Stromausfall in den USA und Kanada 2003 die Notstromaggregate der Banken zum Einsatz gebracht werden mussten (Joint-Forum 2006, 19ff.), bestand die Herausforderung des SARS-Ausbruches vor allem darin, die Ausbreitung der Krankheit unter den Beschäftigten des Finanzsektors einzudämmen. Dafür wurden Gesichtsmasken verteilt, Mitarbeiter\_innen sollten von zu Hause aus arbeiten und durch Telefonkonferenzen miteinander kommunizieren (Joint-Forum 2006, 24). Spezielle »clean teams« (Joint-Forum 2006, 28) wurden eingerichtet, um die Hygiene der Arbeitsorte zu gewährleisten.

Letztlich ist die Struktur der »case studies« jedoch weit aufschlussreicher als ihr Inhalt. Einer knappen Schilderung des *events* folgt jeweils die Beschreibung von dessen *impact* und der sicherheitstechnischen *response*. Den Abschluss der kurzen Berichte bildet stets ein Teil zu den *lessons learned*. Diese Struktur ist ein Indiz für die erfolgreiche Etablierung eines für ein Sicherheitsdispositiv entscheidenden Rahmens, bei dem es weniger darum geht, dass alle Gefahren perfekt bewältigt werden, sondern darum, dass es gelingt, eine Matrix für den routinierten Umgang mit Ereignissen zu etablieren und auch Fehlschläge oder Mängel der Sicherheitstechniken vor dem Hintergrund dieser Matrix adressieren zu können. Wie gesehen (insbesondere in Kapitel 2.3.2.) geschieht dies durch den Aufbau von epistemischen, technischen und praktischen Kapazitäten zur Antizipation von und zum Umgang mit Katastrophen. Aber auch durch strukturierte Berichtsformate – *event, impact, response, lessons learned* – und andere ritualisierte Formen der nachträglichen Evaluation werden Ereignisse auf eine bestimmte Art serialisiert und handhabbar gemacht. Dass diese Handhabbarkeit nicht gleichbedeutend mit perfekter Kontrolle ist, versteht sich von selbst. Defizite und Lücken in den Netzen der Sicherheit haben unter dem Punkt *lessons learned* ihren eigenen Ort. Hier findet Platz, was nicht wie geplant gelaufen ist, was die Sicherheitsexpert\_innen überrascht oder überwältigt hat und für die Zukunft größere Aufmerksamkeit erheischt. Auf diese Weise macht das Sicherheitsdispositiv auch aus seinem Scheitern einen Grund für seine Ausweitung, Intensivierung und punktuelle Modifikation. Das gilt insbesondere für das Sicherheitsdispositiv der Resilienz, dessen innere Logik verlangt, dass Irritationen und Störungen wahrgenommen werden, um sich dadurch immer besser an sich ständig verändernde Umweltbedingungen anzupassen. Sicherheit ist hier kein Zustand,

sondern ein prinzipiell unabschließbares Projekt, das auch sein Scheitern als Chance und damit Teil des Projekts begreift und das deshalb nur dann erfolgreich sein kann, wenn der Zustand der Sicherheit immer wieder gestört wird.

Aus diesem Grund ist die Auswertung des Katastropheneignisses, seine »Autopsie«, auch eine so entscheidende Veridiktionsform des Sicherheitsdispositivs der Resilienz – mindestens so bedeutend wie die in der Forschung viel ausführlicher diskutierte Rationalität der Antizipation (zur Antizipation siehe u.a.: Grusin 2004, de Goede 2008, Massumi 2010a, Adey und Anderson 2012). Das Störungsereignis wird hier mobilisiert, um als Richterin über die Güte der Sicherheitsmaßnahmen zu urteilen, es dient als »revelatory moment« (Roitman 2013, 4), in dem das zuvor Geschätzte, Vermutete, Geübte und Inszenierte auf einen Prüfstein trifft und bisweilen an diesem zerschellt. Gleichwohl soll durch den Prüfstein der eingetretenen Krise nicht über Maßnahmen geurteilt werden wie im Jüngsten Gericht nach der Apokalypse. Vielmehr soll die Krise wie ein Experiment fungieren, aus dem lehrreiche Schlüsse zu ziehen sind. Jede Krise bietet Lernmöglichkeiten, indem sie »Änderungstrigger« (BSI 2008, 92) setzt und so eine bessere Anpassung an künftige Bedrohungen ermöglicht. Nur so kann eine immer wieder eingeforderte »kontinuierliche Verbesserung des Notfallmanagements« (BSI 2008, 60) gelingen. Dafür muss die Krise genau dokumentiert werden. »Die Dokumentation dient der Lagebeurteilung, aber vor allem auch der Nachbereitung des Notfalls bzw. der Krise für die Beurteilung und Verbesserung des Notfallbewältigungsprozesses.« (BSI 2008, 74) Zudem ist die Dokumentation natürlich aus organisationsinternen Gründen notwendig, weil nur so das BCM von den Vorgesetzten evaluierbar und von Wirtschaftsprüfern überprüfbar wird. »A BCMS [Business Continuity Management System, A.F.] [...] includes [...] a set of documentation providing auditable evidence.« (ISO 2012a, vi)<sup>226</sup>

Durch die Dokumentations- und Evaluationsverpflichtung wird jedoch tatsächlich ein bestimmter Zusammenhang von Krise und Kritik gestiftet. Dabei soll allerdings negative und »unproduktive« Kritik unbedingt vermieden werden. Kritik soll zukunftsgerichtet sein, nicht voll des Ressentiments für vergangene Fehler. »Nicht: was ist schlecht gelaufen, sondern was können wir besser machen. Das interessiert uns nachher, in der Nachbetrachtung.« (Interview 5) Kritik soll hier von vornherein in einen geregelt-

---

<sup>226</sup> Siehe auch die ausführlichen Spezifizierungen der Erfordernisse der Dokumentation laut ISO-Standard (2012a, 20–23).

ten Prozess eingebracht werden, der auch als »Änderungsmanagement« (BSI 2008, 90) bezeichnet wird. *Business Continuity Management* ist in diesem Sinne nicht nur ein vorsorgliches »taming of chance« (Hacking 1990), sondern auch eine nachträgliches *taming of change*. In der Kultur der Resilienz sind begangene Fehler kein Stigma, sondern vielmehr ein Qualitätsmerkmal.

»Da sage ich, nichts Besseres als jemand, der schon einmal eine Krise hatte. Egal, ob er die jetzt wirklich super toll umgesetzt hat oder weniger toll. Wenn er die Lernkurve natürlich mitgemacht hat, um zu sagen, diese Fehler mache ich nicht mehr.« (Interview 6)

Vor diesem Hintergrund erscheint es wenig sinnvoll, bei der Analyse konkreter Ereignisse eine evaluative Bilanz dessen aufzustellen, was geklappt hat und was schief gegangen ist, ob die Programme aufgegangen oder gescheitert sind. Schließlich ist diese Art der Überprüfung selbst ein Teil der Funktionslogik des BCM. Stattdessen will ich im Folgenden auf Formen der Kritik im Zuge von zwei BCM-relevanten Ereignissen eingehen, gegen die das BCM sich noch nicht immunisiert hat, die es noch nicht in die Strategie erhöhter Resilienz einspeisen kann.

#### 4.4.2. Ein Sturm im Finanzdistrikt: Hurricane Sandy in New York

Tropenstürme wie Hurricane Sandy, der im Oktober 2012 die Ostküste der USA und die Karibik heimsuchte, sind Resonanzphänomene. Rückkopplungen und wechselseitige Verstärkungen von Temperaturen, Luftdruck und Luftfeuchtigkeit, Windgeschwindigkeiten und Windrichtungen können sich zu einem geschlossenen Sturmsystem aufschaukeln. Aber nicht nur die Ursachen eines Sturms, sondern auch seine Effekte ergeben sich aus Resonanzen, aus den Schwingungen zwischen natürlichen, technischen und sozialen Elementen. Die Verwüstungen, die Hurricane Sandy an der Ostküste der USA und in zahlreichen Ländern in Mittelamerika verursacht hat, sind gewiss nicht auf den Effekt einer von außen hereinbrechenden Naturkatastrophe zu reduzieren. Sie sind aber ebenso wenig nur die Folge sozialer Verwundbarkeiten, politischer Entscheidungen und ökonomischer Macht, sondern eine komplexe Vermengung von Naturereignis und gesellschaftlichen Prozessen. Es bildete sich ein temporäres Katastrophengefüge, in dem etwas zusammenkam – Wasserfluten und U-Bahntunnel, Handelsalgorithmen und Wirbelstürme, Stromausfälle und eine Stadt, die

niemals schläft, Politiker und Gummistiefel – was für gewöhnlich getrennt voneinander existiert, aber in der Katastrophensituation doch systematisch zusammenwirkt. Deshalb ist Sandy kein lediglich sozialer Gegenstand, den man nur mit Sozialem erklären kann, sondern »mehr als sozial«, nicht inhuman oder posthuman, sondern »more than human« (Whatmore 2006). Die Begegnung von Sandy mit dem Gefüge namens New York City am 29. Oktober 2012, um die es im Folgenden gehen soll, ist ein solches »mehr als soziales« Ereignis.

Als der Sturm New York erreichte, waren die Vorbereitungsmaßnahmen bereits getroffen. *preparedness*-Pläne wurden aus der Schublade geholt, Sandsäcke gefüllt und tiefliegende Teile von Manhattan und Brooklyn evakuiert. Schließlich war die Sensibilität für die Gefahren katastrophischer Ereignisse in New York seit dem 11. September besonders präsent. *Hurricane Katrina*, der im Jahr 2005 New Orleans verwüstete, hatte die Aufmerksamkeit nicht nur für Naturkatastrophen, sondern auch für das politische Management von Katastrophen in der US-amerikanischen Öffentlichkeit zusätzlich geschärft.

Die Geschichte Katrinas war die Geschichte sozialer Verwundbarkeit, die durch das Naturereignis intensiviert und sichtbar wurde. Der Wasserdruck der Überflutungen folgte dem Weg des geringsten Widerstands in die niedrig gelegenen Teile von New Orleans. Und es ist kein Zufall, dass diese Bassins der Verwundbarkeit hauptsächlich von der armen und zu meist Schwarzen Bevölkerung bewohnt waren. Wasserdruck und der Druck sozialer Schichtung und sozialräumlicher Segregation gingen Hand in Hand, so dass die Naturkatastrophe bruchlos in eine soziale Katastrophe überging. *Katrina* war wie ein Lehrstück zu Georg Simmels Theorie sozialer Druckübertragung. In der Gesellschaft

»bewegt sich ein neuer Druck [...] längs der Linie des geringsten Widerstandes, welche schließlich [...] die nach unten laufende zu sein pflegt. Das ist die Tragödie des Tiefsten in jeder sozialen Ordnung. Er hat nicht nur unter den Entbehungen, Anstrengungen und Zurückhaltungen zu leiden, deren Summe eben seine Stellung charakterisiert, sondern jeder neue Druck [...] wird [...] nach unten weitergegeben und macht erst an ihm Halt.« (Simmel 1992, 215)

Die Geschichte von Sandy in New York ist komplexer, weil im Big Apple, anders als in The Big Easy, nicht vornehmlich arme Leute vom Sturm betroffen waren. Sandy hat auch die reichen und mächtigen Bewohner\_innen Manhattans – Firmen wie Privatleute – betroffen. Die Folgen des Sturms haben sich daher nicht so deutlich von oben nach unten, son-

dern eher netzwerkartig über die Stadt und quer durch soziale Schichten hindurch ausgebreitet. Warum dennoch differenziell ausgeprägte Verwundbarkeiten zum Vorschein gekommen sind und zu öffentlicher Kritik geführt haben, liegt nicht unwesentlich am BCM bei Banken.

Aber der Reihe nach: Sandy traf am 29. Oktober 2012 auf New York, kostete 53 Menschen das Leben und verursachte einen Sachschaden in Höhe von 18 Milliarden US-Dollar. Vor allem die Schäden an der Infrastruktur New Yorks waren signifikant. Die Folgen von Sandy haben den Sicherheitsexpert\_innen Recht gegeben, die schon lange vor der erhöhten Verwundbarkeit komplexer Infrastrukturen gegenüber Naturereignissen gewarnt haben. Das U-Bahn System der Stadt fiel aus, weil die U-Bahnschächte massenhaft unter Wasser standen. Auch die Tunnel, die die Halbinsel Manhattan mit ihrer Umgebung verbinden, waren größtenteils von Überflutung betroffen. Der gravierendste Schaden an der Infrastruktur war der durch eine Explosion in einem Umspannwerk ausgelöste Stromausfall, der 250.000 Bewohner Manhattans teilweise für Tage von der Elektrizitätsversorgung abgeschnitten hat. Diese Schäden der Infrastruktur machten die Folgen des Sturms erst so verheerend und offenbarten eine genuin sozio-technische Verletzlichkeit. Selbst der *Financial District* an der Südspitze Manhattans war vom Stromausfall betroffen, wie die berühmten Luftbildaufnahmen offenbarten, die das zur Hälfte verdunkelte New York unter düsteren Gewitterwolken zeigten. Trotz dieser eher transversalen als vertikalen Verteilung der Sturmschäden war Sandy aber auch kein »demokratisches« Risikoereignis im Sinne von Becks Risikogesellschafts-These, nach der die Risiken der zweiten Moderne die Gesellschaft gleichmäßig »jenseits von Stand und Klasse« betreffen (Beck 1986). Denn wie der lokalen, im Dunkeln nach Orientierung suchenden Bevölkerung schnell auffiel, brannte in einigen wenigen Gebäuden in Lower Manhattan doch noch Licht. Besonders hell erleuchtet war ausgerechnet der Firmensitz der Investmentbank Goldman Sachs. Zwar konnte auch Goldman keinen Strom mehr aus dem zusammengebrochenen Netz beziehen, aber ihr *backup*-Stromsystem lieferte weiter Elektrizität. Das *Business Continuity Management* hatte ganze Arbeit geleistet. Nicht nur funktionierte das *backup*-Stromsystem einwandfrei. Zudem war das Hauptgebäude von Goldman auch von einem Wall aus Sandsäcken umgeben. Diese goldschimmernde Demonstration der operationellen Resilienz des Finanzsektors inmitten des ansonsten düsteren Lower Manhattan hat nicht nur die Katastrophenschutzmaßnahmen von Banken, sondern auch die Ungleichheiten des



Schutzes Kritischer Infrastrukturen im Wortsinne beleuchtet. Die erleuchtete Goldman-Zentrale wurde zum Symbol für die ungleiche Verteilung der Sicherheit. Zum besonderen Ärger trug bei, dass, während bei Goldman noch die Lichter brannten, im NYU Langone Medical Center alle Patient\_innen evakuiert werden mussten, nachdem dort auch die Notstromversorgung ausgefallen war. Ein tausendfach geteilter *tweet*, der beide Sachverhalte zusammenbrachte, schien nicht nur vielen New Yorkern aus der Seele zu sprechen: »The fact that the NYU hospital is dark but Goldman Sachs is well-lit is everything that's wrong with this country.«<sup>227</sup>

Der Schein der beleuchteten Goldman-Zentrale ist gleichwohl trügerisch. Denn das Finanzsystem konnte keineswegs ohne Unterbrechungen weiteroperieren. Ein erster Grund hierfür war die heiß diskutierte Entscheidung, die New Yorker Börse (NYSE) für zwei Tage zu schließen, was seit dem 11. September nicht mehr vorgekommen war. Dabei sah es zunächst danach aus, als ob die Geschäfte an der NYSE trotz Sturm größtenteils weiterlaufen könnten. Schließlich sind Börsen schon lange nicht mehr durch Parketthandel geprägt, bei dem schwitzende Händler\_innen Kauf- und Verkaufsgesuche durch den Saal brüllen. Die Automatisierung des Handels hat die abseits gelegenen Rechenzentren zum eigentlichen Schauplatz des Finanzgeschehens werden lassen. So sollte in New York zunächst der automatische Handel weiterlaufen und nur der übrige Parketthandel geschlossen werden. Je näher der Sturm rückte, desto größer wurden jedoch die Zweifel bei den Entscheidungsträger\_innen. Konnte man wirklich ausgerechnet zu einem Zeitpunkt, an dem ein schwerer Sturm die Märkte ohnehin verunsichert, den Handelsmaschinen, die sich immer wieder als störungssensibel und fehleranfällig erwiesen hatten,<sup>228</sup> das Feld überlassen? In einem Bericht des privaten Finanzforschungsinstituts IDC mit dem vielsagenden Titel *Sandy Surfaces the Importance of the Human Machine on Wall Street* heißt es dazu:

»Keeping the market open on a purely electronic basis, having never operated this way even under perfect conditions, would only increase the chances of any minor malfunction to a high frequency trading algorithm causing potentially great disruption.« (Sauer und Versace 2012).

227 Siehe: <https://twitter.com/kenshadford/status/263115191674368001>.

228 So etwa im sogenannten flash crash von 2010, bei dem massive Kursschwankungen durch Fehler der automatischen Handelsmaschinen ausgelöst wurden. Siehe dazu: MacKenzie (2011).

Nicht die Angst vor technischen Unterbrechungen durch den Sturm, sondern das mangelnde Vertrauen in die Sicherheit der Algorithmen und *high frequency trading bots* führte also zur Schließung der NYSE. Ein fehlerhafter Algorithmus könnte zu massiven Störungen und Krisenphänomenen führen und wäre dann möglicherweise nur schwer durch menschliche Intervention zu beheben. Zudem hätten Handelsmaschinen mögliche Turbulenzen, die sich gleichsam vom Wetter auf den Finanzmarkt übertragen, noch weiter verstärken können.

»As technology advances it is clear that regulators and financial institutions need to have long and hard discussions about what can and cannot be done in the event of such scenarios. While a number of banks may well provide traders the ability to access its security network and trade electronically from home or satellite offices, this functionality is rendered meaningless if regulators are not comfortable or do not have the risk infrastructure or capability necessary to police markets that are already increasingly moving away from the physical trading floor.« (Sauer und Versace 2012)

Nicht nur die Schließung der NYSE, auch weitere Ereignisse »have made it abundantly clear that the markets cannot and must not operate without the fully functioning human »machine.« (Sauer und Versace 2012) Im Interview wurde als größte Schwierigkeit für das BCM der Bank weniger der Stromausfall, sondern vielmehr die Unterbrechung der Verkehrsinfrastruktur thematisiert. Schließlich wohnt ein Großteil der Bankangestellten nicht in Manhattan selbst, sondern in New Jersey oder Long Island und ist darauf angewiesen, mit der U-Bahn oder durch Tunnel für den Autoverkehr zur Arbeit zu gelangen, was aufgrund der Überschwemmungen nach Sandy unmöglich geworden war. So war plötzlich die physische Geographie New Yorks, die angeblich im ortslosen Finanzkapitalismus keine Bedeutung mehr hat, zu einer entscheidenden Größe geworden.

Nur scheinbar können sich Banken wie Goldmann von diesen materiellen und infrastrukturellen Bedingungen abkoppeln. Die Vorhaltung von Notstromaggregaten bei Banken kann zwar als typisches Phänomen eines »splintering urbanism« (Graham und Marvin 2001) verstanden werden, bei dem sich Unternehmen oder sehr wohlhabende Stadtbewohner\_innen privatisierte infrastrukturelle Versorgungsinseln sichern, die in puncto Sicherheit, Schnelligkeit oder Servicequalität über dem kommunalen Durchschnittsniveau liegen. Gleichwohl ist die Angewiesenheit auf eine funktionierende öffentliche Nahverkehrsinfrastruktur erhalten geblieben. Die Finanzmärkte sind möglicherweise nicht sozial *embedded*, aber sie sind

doch technisch *connected*, an eine Vielzahl öffentlicher und kollektiv genutzter infrastruktureller Leistungen angeschlossen.<sup>229</sup>

Ein weiterer Grund für die Beschränktheit der Effektivität der Kontinuitätsmaßnahmen liegt im Versagen der Planungen für Ersatzinfrastrukturen bei etlichen Banken. In der Folge von Sandy haben nahezu alle Banken, die in New York operieren – und das sind viele – die von ihren Vertragspartnern (zumeist die Firma Sungard) für solche Fälle betriebenen Ersatzstandorte nachgefragt. Nahe gelegene Ausweichstandorte wurden deshalb schnell knapp, so dass nur wenige Banken, die sich besondere Vorzugsrechte bei Sungard gesichert hatten, einen Ersatzstandort in der Nähe beziehen konnten. Im Fall der von mir untersuchten deutschen Bank wurde auf die Inanspruchnahme eines mehrere Flugstunden entfernten Ausweichstandorts verzichtet. Die notwendigsten Operationen wurden stattdessen von einem eilig angemieteten Hotelzimmer aus in die Wege geleitet. Im Interview wurde diese Situation schnell als Heldengeschichte interpretiert. Die Rede war von übernächtigten »Musketieren« der Bank, die auf engstem Raum im Hotel mit ungewaschenen Socken, dafür aber umso gefestigterem Teamgeist die Geschäfte am Laufen hielten. Solche Geschichten können nicht darüber hinwegtäuschen, dass offensichtlich die laut Standards und Regulationen vorgeschriebenen und von den Banken für gewöhnlich durchgeführten BCM-Maßnahmen nur dann helfen können, wenn eine einzelne Bank durch einen Störfall betroffen ist und ihre Geschäfte kurzfristig an einen anderen Standort verlegen muss. Bei einem großflächigen und langanhaltenden Katastrophenfall dagegen scheinen die Maßnahmen kaum zu helfen: Weder Ausweichstandorte noch Notstromversorgung haben den Banken viel genützt. So scheint es, dass der Rahmen des BCM, der vornehmlich auf eine einzelne Institution fokussiert, zu eng gefasst ist und allzu leicht von einer Reihe von Externalitäten (mitunter im Wortsinne) überflutet wird. Sowohl die Vernetzung mit der städtischen

---

229 Die Frage der Eingebettetheit von Märkten ist bekanntlich seit Polanyi (1957) Thema der Soziologie, das auch in neueren Debatten der ökonomischen Soziologie viel Aufmerksamkeit erhalten hat (siehe dazu den Überblick von: Fligstein und Dauter 2007). Während dabei zumeist die soziale Einbettung etwa durch moralische Konventionen und rechtlich-Institutionelle Settings betont wurde, hat Michel Callon (1998b) argumentiert, dass die Ökonomie in die Ökonomik, also in ökonomische Wissensformen, eingebettet ist. Hier möchte ich aber einen noch einmal anderen Sinn von Einbettung, nämlich als Anschluss an sozio-technische Netze und öffentliche Infrastrukturen, zur Geltung bringen, der sich als Beitrag zum soeben skizzierten *material turn* in den SSF versteht.

Infrastruktur als auch die Resonanzen zwischen den Kontinuitätsplanungen der Banken haben zu massiven Schwierigkeiten geführt. In letzterem Fall nicht trotz, sondern gerade weil alle Banken vorschriftsmäßig vorgesorgt hatten. Diese Erfahrung steht im Kontrast zur Betonung von Interdependenzen in BCM-Standards und zum Anspruch des Kontinuitätsmanagements, zur Sicherheit größerer Systemzusammenhänge beizutragen. »Business Continuity contributes to a more resilient society. The wider community and the organization's environment impact on the organization and therefore other organizations may need to be involved.« (ISO 2012a, vi) Es war aber gerade das Gemeinschaftsereignis Sandy – die kollektive Betroffenheit von den Folgen des Sturms, vermittelt und verstärkt durch die kollektive Infrastruktur –, durch die das BCM der Banken scheiterte.

Die *spillovers* des Gemeinschaftsereignisses Sandy hatten aber auch den Effekt, dass sie das sonst im Verborgenen arbeitende *disaster preparedness* der Finanzbranche sichtbar und dadurch kritisierbar gemacht haben. Es bedurfte keiner besonderen Phantasie, keiner Entlarvung, keines Blickes hinter die Kulissen, um die Sicherheitslogik der *vital systems security*, wie sie sich in New York gezeigt hatte, zu kritisieren. Alles war genau so, wie es (auf Manhattan blickend) auch schien: Eine große Investmentbank und ein wesentlicher Verursacher der Finanzkrise hatte noch Strom, während 250.000 New Yorker im Dunkeln saßen und selbst ein Krankenhaus evakuiert werden musste. Ein weiteres Mal schien die fatale *too big to fail*-Logik am Werke zu sein, die schon während der Finanzkrise 2008 zu Ungerechtigkeiten geführt hatte, als unzählige verschuldete Hausbesitzer\_innen geräumt wurden, während die Verursacher der Krise – nicht zuletzt Goldman Sachs – mit milliardenschweren Rettungspaketen unterstützt wurden. Damals wie jetzt bei Sandy gingen in den Wohnhäusern die Lichter aus. Auch wenn der Staat diesmal nur mittelbar dafür verantwortlich war, dass Goldman noch Strom hatte – das hell erleuchtete Hauptquartier der Investmentbank wirkte wie ein ausgestreckter Mittelfinger an die von Finanzkrise und schlechtem Katastrophenmanagement gebeutelten New Yorker. Die Frage drängte sich auf: Wer ist eigentlich »kritisch« und was ist »vital«? Durch die Gegenüberstellung von erleuchteter Goldman-Zentrale und evakuiertem NYU Medical Center durch den häufig geteilten *tweet* (s.o.) wird die faktische Hierarchie der Kritikalität und damit die ungleiche Verteilung der *vital systems security* in Frage gestellt. Gleichwohl wird deren prinzipielle Idee, nämlich den Schutz der Bevölkerung an den Betrieb und

das kontinuierliche Funktionieren einer Reihe von kritischen bzw. vitalen Infrastrukturen und Systemen zu koppeln, durchaus bestätigt.

#### 4.4.3. Disruptive Demokratie: Blockupy in Frankfurt

Frankfurt liegt in Europa, aber Europa liegt auch in Frankfurt. Um diese paradoxe topologische Konstellation zu verstehen, braucht es keine elaborierte mathematische Theorie, sondern lediglich einen kleinen Ausflug in die Geschichte der Europäischen Zentralbank (EZB).<sup>230</sup> Seit ihrer Gründung im Jahr 1998 hat die EZB ihren Sitz in Frankfurt am Main – zunächst im »Eurotower« mitten im Frankfurter Bankenviertel, seit 2014 vornehmlich im neugebauten EZB-Turm im Frankfurter Ostend. Als EU-Institution besitzt die EZB einen »extra-territorialen« Status. Sie etabliert zwar kein eigenes souveränes Territorium mit eigenen Gesetzen, genießt aber eine Vielzahl rechtlicher Privilegien und Immunitäten. In der EZB-Zentrale befindet man sich genau genommen nicht auf deutschem Boden, sondern in der EU – also nicht in der EU *und* in Deutschland, sondern *nur* in der EU, in *Europe sans phrase*. Wie die Juristen Gruber und Benisch (2007) in einem Gutachten für die EZB darlegen, ist der Status der Bank mit dem einer Botschaft zu vergleichen, ist aber noch umfangreicher. Die EZB genießt nicht nur Immunität gegenüber der Durchsetzung deutschen Rechts, sondern ist zudem von einer Reihe rechtlicher Regelungen ausgenommen. Laut Artikel 291 der europäischen Verträge ist die EZB etwa vom deutschen Steuerrecht und Arbeitsrecht ausgenommen. Zugleich geht der Sonderstatus der EZB aber auch mit Schutzansprüchen gegenüber dem deutschen Staat und der Stadt Frankfurt einher. Einerseits dürfen öffentliche deutsche Autoritäten die EZB nicht ohne Genehmigung betreten (EZB und BRD 1998, 3). Andererseits soll der deutsche Staat die Gebäude der EZB und ihre territoriale Integrität nicht nur achten, sondern aktiv schützen, um so ihre Operationsfähigkeit zu gewährleisten. Deutschland, so heißt es, habe die EZB »against any intrusion or damage and any other impairment of its operations« (EZB und BRD 1998, 5) zu schützen.

Diese komplexe rechtliche Sonderstellung der EZB »in« Deutschland und »außerhalb« Deutschlands nimmt in der Architektur und den Sicherungsmaßnahmen des neu errichteten EZB-Sitzes materielle Gestalt an. So

---

<sup>230</sup> Wesentliche Informationen und Inspirationen zum Status der EZB in Frankfurt verdanke ich: (Stenmanns 2014).

ist die Bank von insgesamt vier Absperrungsringen umgeben, die potenzielle Eindringlinge abhalten sollen. Selbst die FAZ sprach daher vom Neubau als der neuen »Burg« der EZB (Nienhaus 2014). Ebenso gut hätte man auch von »Europas Festung« sprechen können. Allzusehr erinnert die Abriegelung der Zentralbank an die »Festung Europa«, die Synonym geworden ist für die Abschottung der Außengrenzen der Europäischen Union. Hier wie dort soll ein System von Grenzen und Schutzringen (teilweise noch vor der eigentlichen EU-Grenze) »Eindringlinge« vor Betreten der Union schützen, um ihre territoriale Integrität zu sichern.

Gleichzeitig ist die EZB aber auch der Schauplatz eines anderen Sicherheitsprojekts, dem es weniger um die Sicherung von Grenzen und um territoriale Integrität als um die Sicherstellung von *flows* bzw. um die Kontinuität von Finanztransaktionen geht. Der Neubau der EZB inkorporiert Teile der ehemaligen Frankfurter Großmarkthalle. Die 1928 eröffnete Großmarkthalle war ein Umschlagsplatz für Waren und Güterströme, die über den Main nach Frankfurt geliefert wurden. Dadurch war die Markthalle so etwas wie ein obligatorischer Passagepunkt für die materiellen Güterströme des Handelskapitalismus. Mit der EZB ist derselbe Ort heute ein Knotenpunkt virtueller Finanzströme. Kaum eine Finanztransaktion in Europa, die nicht durch die Zahlungssysteme der EZB (SEPA, das *Retail Payment System* und TARGET2, das *Large Value Payment System*) geschleust wird. Die Etablierung, der Betrieb und die Sicherung dieser Zahlungssysteme stehen nicht für die souverän-territoriale Abschottung des europäischen Staatsgebietes, sondern vielmehr für die Gewährleistung des freien, ungehinderten und kontinuierlichen Geldflusses innerhalb des europäischen Binnenmarktes: Europa als *Single Euro Payment Area* (SEPA). Die Sicherung der Zahlungsströme wird aber nicht zuletzt mithilfe der territorialen Sicherung der extra-territorialen EZB ermöglicht. Um als Herrin über die Ströme zu wachen, hat sich die EZB inselhaft abgesetzt und genießt die Vorzüge ihrer Extra-Territorialität, die dazu beitragen sollen, den kontinuierlichen Betrieb systemwichtiger Operationen zu ermöglichen. Die Sicherung des Territoriums ist hier ein Mittel zur biopolitischen Sicherung von Zirkulationen. Ihr territorialer Sonderstatus macht die EZB zu einer »Heterotopie der Zirkulation« (Opitz und Tellmann 2012).

In der Folge einer Demonstration gegen die europäische Krisenpolitik am 15. Oktober 2011 hatte sich unmittelbar vor der EZB zwischenzeitlich aber noch eine andere Heterotopie in der Frankfurter Innenstadt etabliert: ein Camp der Occupy-Bewegung. Die Occupy-Bewegung hatte diesen Ort

nicht zufällig gewählt, schließlich verstand sie sich gegenüber der Frankfurter Bankenwelt und deren Aufseherin als »Gegenort« (Foucault 2005h, 935). Wie ihr US-amerikanisches Vorbild, die Occupy Wall Street-Bewegung, wollten auch die Frankfurter Occupisten den häufig diffusen Widerstand gegen den Finanzkapitalismus an den Orten seiner konkreten Praxis sichtbar und dauerhaft machen, indem sie Zelte inmitten der Handelszentren aufschlugen.

Die sogenannte Blockupy-Bewegung hat diesen Ansatz weiterentwickelt. Ihr geht es nicht nur darum, den Widerstand an zentralen Orten und Drehscheiben der Finanzökonomie und Politik symbolisch sichtbar zu machen, sondern praktisch zu intervenieren, indem sie diese Orte blockiert. Mit Parolen wie »Frankfurt fluten« hatte das Blockupy-Netzwerk, bestehend aus unterschiedlichen linkspolitischen Gruppierungen, das erste Mal für den 16. bis 19. Mai 2012 nach Frankfurt bzw. »ins Herz des europäischen Krisenregimes« mobilisiert, um gegen die Politik der Troika (IWF, EU und EZB) zu demonstrieren. Dabei sollte unter anderem versucht werden, für einen Tag das Frankfurter Bankenviertel »lahmzulegen« und insbesondere die Europäische Zentralbank zu blockieren. Im Aufruf der Blockupy-Bewegung heißt es:

»Wir werden gegen die Politik von EU und Troika demonstrieren, die EZB blockieren und die öffentlichen Plätze im Frankfurter Finanzzentrum okkupieren [...]. Wir werden am 18. Mai den Geschäftsbetrieb der Banken in Frankfurt blockieren, um unsere Wut über die Troika-Politik konkret werden zu lassen.« (Blockupy 2012)

Vor dem Hintergrund der massiven Sicherheitsmaßnahmen und der Schutzpflichten seitens der Stadt gegenüber der EZB sowie der Sorge um Unterbrechungen des »Geschäftsbetriebes« bei Banken ist es wenig verwunderlich, dass die Drohgebärden der Blockadebewegung massive Reaktionen hervorgerufen haben. Angesichts der bevorstehenden Demonstration wurden die BCM-Pläne der Banken aktiviert und einige Filialen teilweise ganz geschlossen, Mitarbeiter\_innen wurden dazu aufgefordert, von zu Hause aus oder an einem Ausweichstandort zu arbeiten und, sofern sie doch einen der Bankentürme aufsuchen mussten, dies nur in unauffälliger »Freizeitkleidung« zu tun. Zudem wurde das Bankenviertel weiträumig von der Polizei abgesperrt, U- und S-Bahnhaltestellen in der Nähe der

EZB und des deutschen Bankgebäudes (Willy-Brandt-Platz und Taunusanlage) wurden nicht mehr angefahren.<sup>231</sup>

Nicht nur das Ausmaß der Sicherheitsmaßnahmen, sondern auch die Konsequenz und Gründlichkeit, mit der die von den Demonstrant\_innen angeordnete Blockade des Bankenviertels nun de facto hoheitlich von der Polizei exekutiert wurde, sorgte bei vielen Beobachter\_innen für Irritationen. Nicht zuletzt die Protestbewegung, die wohl selbst überrascht war, welche Prozesse sie mit ihren Blockadevorhaben ausgelöst hatte, griff die offensichtlich gewordene Sicherheitsparadoxie genüsslich auf und verbuchte sie als Erfolg. Auf einer vorsorglich aus der Innenstadt verbannten Diskussionsveranstaltung mit David Graeber und Michael Hardt im Frankfurter Studierendenhaus gab letzterer dieser weit verbreiteten Stimmung Ausdruck: »Something remarkable, indeed magical happened today. The protest was successful before it even started.«<sup>232</sup> Tatsächlich waren die relevanten Expert\_innen der Sicherheit mit der klassischen Problematik liberaler Sicherheitsdispositive konfrontiert: Wie kann man eine »Flut« (in diesem Fall von Demonstrant\_innen) aufhalten, ohne gleichzeitig die vitalen *flows* zu unterbinden?

Aus der Perspektive der Kontinuitätsmanager\_innen der Banken stellte sich die Lage naturgemäß anders dar. So betonte ein von mir interviewter BC-Manager immer wieder die Gefahr, die von Blockupy für das Frankfurter Bankwesen ausgegangen sei. Blockupy habe das spezifische »Gefährdungspotenzial« des Frankfurter Bankenviertels deutlich werden lassen:

»Also ich kann in Frankfurt mit wenigen Maßnahmen den Financial District blockieren, indem ich einfach ein paar wenige U-Bahnstationen blockiere. Ein Großteil der Mitarbeiter kommt über öffentliche Verkehrsmittel nach Frankfurt rein. Wenn ich hier die Hauptwache blockiere - das haben die Blockupy-Aktivisten ja auch schnell erkannt - wenn ich da zwei, drei U-Bahnstationen blockiere, dann geht in Frankfurt nicht mehr allzu viel. Das ist natürlich eine Konzentration, das ist immer ein Risiko.« (Interview 4)

Entsprechend habe Blockupy eine »Awareness bis ganz hoch zum Management« erzeugt »wo viele Banken hier für einen Tag ihre Bürotürme komplett geräumt haben« (Interview 4), und ein weltweit bisher einzigartiges, BCM-relevantes Ereignis im Finanzsektor dargestellt. »Also das ist

---

231 Auch die Goethe-Universität und der beliebte Ebbelwei-Express haben ihren Betrieb aufgrund der anstehenden Demonstrationen eingestellt. Kritische Infrastrukturen sind beide Institutionen jedoch nicht.

232 Reproduziert nach Beobachtungsprotokoll von entsprechender Veranstaltung.



bisher einmalig gewesen in der Bankengeschichte. Ich kenne es nicht, dass fast alle Banken ihre Bürotürme geräumt haben, gemeinschaftlich.« (Interview 4) Auch die internationale Kontinuitätsmanagement-Szene wurde durch Protestformen wie die von Blockupy auf eine neue Gefährdungsgattung aufmerksam. Nur wenige Monate nach Blockupy erschien im Magazin *Resilience. Winning with Risk* der Beratungsfirma PWC ein Bericht mit dem Titel *Gearing up for protests*.

»Popular protests against cuts and austerity are gathering momentum across Europe. These are a foretaste of what may lie ahead. If there are exits or the currency collapses [...] ensuing unrest may be difficult to contain. Incident management and business continuity planning are generally associated with issues related to natural disasters. But they may need to be broadened to incorporate the repercussions of economic meltdown.« (Hepburn 2012, 12)

Die Demonstrationen in Frankfurt werden aus der Perspektive des Kontinuitätsmanagements als ein Störimpuls angesehen, der, sofern die richtigen Schlüsse aus ihm gezogen werden, zu einer Erweiterung des Anwendungsfeldes der Sicherheitstechnologie des BCM führen und so zu einer Steigerung betrieblicher Resilienz beitragen kann.

Gleichwohl sind den Akteuren des BCM auch die autoimmunen Effekte der eigenen Sicherheitsmaßnahmen nicht entgangen.

»Natürlich kam das so ein Stück weit zu einer Selbstblockade. Auf der anderen Seite muss man auch mal sehen, dass es auch eine sehr gute Gelegenheit war, für Frankfurt genau so ein Szenario mal zu beüben, gemeinschaftlich ne. Also viele haben die Situation auch als Übung verstanden und gefahren. Und dann macht es auch großen Sinn, weil man eine Übung in dem Ausmaß im Normalbetrieb gar nicht planen kann. Das würde keiner akzeptieren, dass man einen gesamten Bankenturm leerräumt. Aber hier war das adäquat und angemessen. Da konnte man das auch mal beüben. Wie arbeiten jetzt tausende von Mitarbeitern remote von Zuhause oder von einem Ausweich-Arbeitsplatz, funktioniert das dann?« (Interview 4)

Sicherheitsexpert\_innen wie der interviewte Kontinuitätsmanager wissen, dass sie sich für ihre Maßnahmen und Entscheidungen im Nachhinein rechtfertigen müssen. Deshalb wissen sie auch (zumindest implizit), dass Risiko nicht nur in einer jeweils äußeren Gefährdung, sondern vor allem auch in ihren Entscheidungen für oder gegen eine bestimmte Sicherheitsmaßnahme liegt. Die Rechtfertigungen vergangener Entscheidungen gehört ebenso zum Beruf des Krisenmanagers wie die vorsorgliche Erwägung von Schutzmaßnahmen. Besonders aufschlussreich ist zudem der

Bezug auf die Logik der Übung. Er zeigt, dass BCM nicht erst in konkreten Einsatzsituationen mit Paradoxien der Sicherheit konfrontiert ist. Denn einerseits sollen Geschäftsunterbrechungen vermieden werden, andererseits ist aber schon die bloße Existenz eines *Business Continuity Managements* ein potenzieller Störfaktor, weil Übungen als intrinsischer Bestandteil einer jeden Kontinuitätsstrategie notwendigerweise selber Friktionen bis hin zu Geschäftsunterbrechungen darstellen. Die Grenzen zwischen Übung und Störfall verschwimmen. Nicht nur ist jeder Ernstfall eine Übung, die neue Erkenntnisse generiert und Anpassungszwänge an neue Gefährdungslagen aufzeigt. Umgekehrt ist auch jede Übung ein Unterbrechungsereignis.

Wie selbst der Kontinuitätsmanager zugestanden hat, konnte die Blockupy-Bewegung den Sicherheitsapparat nicht nur zu einer Selbstblockade nötigen, sondern diese Selbstblockade zugleich auch als Paradoxie der Sicherheit sichtbar machen. Die Kritik von Blockupy geht freilich über die Konstatierung solcher Paradoxien hinaus. Der in ihren Aktionsformen – »Blockierung des Geschäftsbetriebes der Banken« – eingelagerte praktische Widerstand läuft schließlich auf eine grundsätzliche Konfrontation mit dem Kontinuitätsmanagement hinaus. Es gibt aufgrund der Heterogenität der Bewegung unterschiedliche Möglichkeiten, diese den Aktionsformen implizite Kritik zu explizieren. Äußerungen wie die im Demonstrationsschrei – »Wir werden am 18. Mai den Geschäftsbetrieb der Banken in Frankfurt blockieren, um unsere Wut über die Troika-Politik konkret werden zu lassen« (Blockupy 2012) – lassen erst einmal nur auf ein diffuses Unbehagen schließen. Mit ihren massiven Sicherheitsmaßnahmen hat die Polizei suggeriert, den Demonstrant\_innen gehe es um eine substantielle *Sabotage* der »finanzkapitalistischen Maschine«. Dies war jedoch faktisch nicht der Fall. Insofern scheint eine angemessenere Interpretation zu sein, dass es Blockupy weniger um Zerstörung der Maschine als um ein temporäres Bremsen und Blockieren des Arbeitsalltags im Frankfurter Bankenviertel ging, um ihrer Kritik Gehör und Geltung zu verschaffen. Es ging darum, durch die Unterbrechung der Routinen des Geschäftsbetriebs zugleich die Routinen einer Politik zu hinterfragen, in der grundsätzliche Kritik an den Maßnahmen der Bankenrettung, Finanzregulation und Austeritätspolitik zumeist überhört wurde.

In diesem Sinne lässt sich Blockupy als Bewegung der Disruptiven Demokratie verstehen. Mit dem Begriff der Disruptiven Demokratie bezeichne ich eine Reihe von politischen Bewegungen, die ihre politische Macht dadurch manifestieren, dass sie Unterbrechungen sozio-

ökonomischer Funktionsvollzüge erzeugen. Beispiele für solche Bewegungen sind die westeuropäischen Arbeiter\_innen der Kohleindustrie, die um die Wende vom 19. zum 20. Jahrhundert durch die Blockade des Energieflusses der industriellen Welt zu entscheidenden Protagonist\_innen der Etablierung wohlfahrtsstaatlicher Massendemokratien geworden sind (Mitchell 2011, 18–31). Die Streiks der Kohlearbeiter\_innen haben aufgrund der Kohleabhängigkeit der gesamten Industrie nicht nur entscheidend dazu beigetragen, ihren Forderungen Nachdruck zu verleihen, sondern auch eine Vernetzung mit Arbeiter\_innen in anderen ebenfalls lahmliegenden Teilen der Industrie ermöglicht. »What was missing was [...] not a repertoire of demands, but an effective way of forcing the powerful to listen to those demands. The flow and concentration of energy made it possible to connect the demands of miners to those of others, and give their arguments a technical force that could not easily be ignored.« (Mitchell 2011, 21) Auch der zivile Ungehorsam gegen die Castor-Transporte, mit denen die deutsche Ökobewegung gegen Kernenergie und den Atomstaat protestierte, sind ein Beispiel, bei dem Bewegungen die infrastrukturelle Verwundbarkeit eines techno-ökonomischen Systems genutzt haben, um ihrem Protest Nachdruck zu verleihen (Folkers 2017d, siehe auch Kapitel 3.3.2.). Jeweils waren die Interdependenzen und Konzentrationen des Energiesystems, die von Sicherheitsexpert\_innen so gefürchtet werden, zugleich die infrastrukturellen Voraussetzungen für effektiven Widerstand. Nicht zufällig sorgen in jüngerer Zeit immer wieder Proteste von Transport- und Hafentarbeiter\_innen für Aufmerksamkeit. Aufgrund ihrer Stellung im kapitalistischen Produktions- und Zirkulationsprozess haben sie seit jeher eine besondere Affinität zu Formen des logistischen Widerstands. In der Gegenwart haben diese Widerstände sogar noch an Bedeutung gewonnen. So geht die Verlagerung von Produktionsstandorten in Niedriglohnländer im Zuge kapitalistischer Globalisierungsbewegungen mit einem intensivierten Waren- und Güterverkehr einher, der seinerseits überhaupt nur durch die logistische Revolution seit dem Zweiten Weltkrieg möglich geworden ist (Cowen 2014, 23–52). In Anbetracht der wachsenden Bedeutung von Waren und Lieferketten hat Anna Tsing das gegenwärtige Regime kapitalistischer Wertschöpfung gar als »supply chain capitalism« (Tsing 2009, 148) bezeichnet. Mit dem Aufstieg des globalen Lieferkettenkapitalismus haben sich veränderte Konfliktmuster zwischen Arbeit und Kapital eingespielt. So hat Beverly Silver (2005) gezeigt, dass die Arbeiter\_innenmacht durch die Globalisierung zwar geschwächt

wurde, weil Unternehmen durch Verlagerung von Produktionsstandorten Druck auf Regierungen und Arbeitnehmer\_innen ausüben können. Gleichzeitig eröffnet die große Abhängigkeit von störungsfreien, weltweit verteilten Versorgungsnetzwerken neue Protestmöglichkeiten, in deren Zentrum Logistikerarbeiter\_innen stehen. In Bezug auf eine alte Marx'sche Unterscheidung (Marx 1968) ließe sich – gewiss etwas zugespitzt – argumentieren, dass nicht mehr die Produktionssphäre der Fabrik, sondern die Zirkulationssphäre der Lieferketten und logistischen Versorgungsnetzwerke zum entscheidenden Ort des Widerstands gegen den Kapitalismus geworden ist.

Das gilt in gewisser Weise auch für die Blockupy-Bewegung, deren Widerstand sich auch gegen eine bestimmte Form des »circulatory capitalism« (Lee und LiPuma 2004, 15) richtet,<sup>233</sup> indem sie versucht, die Operationen des Finanzwesens zu unterbrechen. Darin liegt die Ähnlichkeit von Blockupy zu einem anderen Ableger der Occupy-Bewegung, Occupy Oakland. In einem Bündnis mit den Hafendarbeiter\_innen ist es der Occupy-Bewegung hier im Winter 2011 gelungen, den Hafen der kalifornischen Stadt Oakland – einer der bedeutendsten Häfen der US-Westküste – für mehrere Tage lahmzulegen (siehe dazu: Cowen 2014, 194). Wenn all diese Bewegungen versuchen, den reibungslosen Fluss von Energie, Geld oder Waren zu stören, geht es nicht um die Zerstörung der angegriffenen Systeme und Netzwerke, sondern darum, politische und ökonomische Forderungen mal begrenzter, mal weitreichender Natur durchzusetzen. Die Unterbrechungen sind Mittel, keine Zwecke der Politik und der Politisierung von nur scheinbar rein funktional-technischen Prozessen.

Die genannten Bewegungen eint aber nicht nur ein bestimmtes Set an Aktionsformen, sondern auch ihre schwierige Position in einem Dispositiv der Sicherheit, das in der Sicherstellung von Zirkulationen und dem Schutz vitaler Systeme seine vornehmste Aufgabe sieht. Jeweils sind die Disruptiven Demokratiebewegungen nämlich nicht nur mit bestimmten Konfigurationen ökonomischer und sozialer Macht konfrontiert, sondern zudem mit Sicherheitsprojekten, die einen flüssigen und kontinuierlichen Strom der

---

233 Benjamin Lee und Edward LiPuma (2004, 8) argumentieren, dass der gegenwärtige Kapitalismus durch ein »circulation centred paradigm« gekennzeichnet ist, wobei sie weniger die Logistik, sondern vielmehr das Finanzwesen für diese Entwicklung verantwortlich machen: »circulation is rapidly becoming the principle means of generating profit, absorbing the capital formerly directed towards production.« (Lee und LiPuma 2004, 8f.)

vitalen Güter und Ressourcen organisieren sollen. Die Reorganisierung der Energieversorgung durch das flexibler und dadurch sicherer zu transportierende Öl (Mitchell 2011, 36–39), das »Supply Chain Risk Management« (Cowen 2014, 76–79), aber auch das *Business Continuity Management* bei Banken sind Projekte der Sicherstellung kapitalistischer Kontinuität, die den Bestrebungen der Disruptiven Demokratisierung diametral entgegenstehen. Auf den ersten Blick wirken beide Bewegungen – Disruptive Demokratie und die Apparate zur Sicherung vitaler Operationen – wie Spiegelbilder. So verfügen beide über ein ähnliches Wissen über Verwundbarkeiten und *bottle necks* in der Infrastruktur. »Wenn ich hier die Hauptwache blockiere – das haben die Blockupy-Aktivist\*innen ja auch schnell erkannt – wenn ich da zwei, drei U-Bahnstationen blockiere, dann geht in Frankfurt nicht mehr allzu viel.« (Interview 4) Was dabei jeweils die Infrastruktur ausmacht, unterscheidet sich jedoch grundsätzlich. Während in einem Fall die Infrastruktur »kritisch« ist, weil vitale Funktionen von ihr abhängen, ist sie im anderen Fall »kritisch«, weil sie ein Werkzeug für kritische Widerstandspraktiken ist. Welten trennen beide Bewegungen, weil sie tatsächlich unterschiedliche Ontologien der Infrastrukturen voraus- und einsetzen: einmal Infrastruktur als Schutzobjekt, einmal als Terrain für politische Kämpfe, einmal Kritische Infrastrukturen, einmal Infrastrukturen der Kritik. Dass sich beide ontologisch inkommensurable Welten dennoch überlagern und aneinander reiben, führt zu Erschütterungen bei ihrem Aufeinandertreffen, zu ontologischen Konflikten bzw. »Seinsbeben« (zum Konzept des Seinsbebens siehe: Folkers 2017b). Denn von der Warte der Ontologie der Sicherheit aus muss Widerstand als Unterbrechungsrisiko verstanden und deshalb unterbunden werden.

»If it is the security of efficient trade flows that animates [...] security today, then the interference that comes from »inefficiencies« like democracy, and the actors that demand it, might themselves be construed as security threats.« (Cowen 2010, 17)

Tatsächlich ist die jüngere Vergangenheit voll von Beispielen, etwa Streiks von Arbeiter\_innen im Logistik- oder Transportbereich, die empfindliche Reaktionen des Sicherheitsapparats hervorgerufen haben.<sup>234</sup> Umgekehrt

---

<sup>234</sup> Aufsehenerregend war die Reaktion der spanischen Regierung auf einen Fluglotsenstreik im Jahr 2010, auf den sie durch die Verhängung des Ausnahmezustands reagierte und den Streik mit Militärgewalt beendete. Für eine Übersicht über diesen und andere ähnlich gelagerte Fälle siehe: Bewernitz (2010). Auch im Zuge der Lokführerstreiks der Bahngewerkschaft GDL ist in Deutschland eine Debatte über die Grenzen des Streikrechts in Bereichen der Daseinsvorsorge ausgebrochen. Auf Grundlage eines Rechtsgut-

muss aus der Perspektive der Disruptiven Demokratie die Sicherung vitaler Systeme als *counterinsurgency* erscheinen.

Auch in Frankfurt schien die Sicherheit der Kritischen Infrastrukturen des Finanzwesens wichtiger zu sein als das Recht auf kritische Meinungsäußerung; das war zumindest das Bild, das sich angesichts des Verbots von nahezu allen Veranstaltungen von Blockupy, des massiven Sicherheitsaufgebots und der Aktivierung der Katastrophenpläne bei den Banken einstellte. Allerdings ging das Verbot der Protestveranstaltungen nicht vom BCM der Banken selbst aus. Das massive Polizeiaufgebot war zwar Teil einer »gemeinschaftlichen« Sicherheitsstrategie Frankfurts, aber nicht alleiniger Ausdruck der Programmatik des Kontinuitätsmanagements. Vielmehr kam es zu einer Vermischung von *vital systems security* und dem Sicherheitsapparat der souveränen Staatsmacht. Gleichwohl gehören in der »generischen« Logik des *Continuity Managements* Phänomene wie Proteste, Streiks und ziviler Ungehorsam in dieselbe Serie von Ereignissen wie Naturkatastrophen, Terror und Epidemien, insofern sie zu Geschäftsunterbrechungen führen können. »Deshalb wäre für mich Streik und Pandemie mit dem Effekt, beide Male sind die Menschen nicht da, gleich zu bewerten.« (Interview 6) Dadurch ist die Logik des BCM zumindest anschlussfähig an repressive Maßnahmen gegen Disruptive Demokratiebewegungen.

Blockupy hat keine substantielle Unterbrechung des Finanzbetriebs bewirkt. Die Folge der Blockupy-Aktionen – und wenn man will auch ihr Erfolg – bestand vielmehr darin, dass sie eine Reihe von Sachverhalten und Machtbeziehungen sichtbar gemacht haben. Das massive Sicherheitsaufgebot und die Implementierung von BCM-Plänen bei Banken, die auch ein Thema in der Presse waren, haben die Verwundbarkeit des globalen Finanzkapitalismus unterstrichen – und zwar nicht nur für Sicherheitsexpert\_innen, sondern auch für eine kritische Öffentlichkeit. Das ist wichtig, nicht weil es Möglichkeiten für die Sabotage der Finanzmaschine anzeigt, sondern weil es einen Anhaltspunkt für die Sinnfälligkeit politischer Proteste an den konkreten Orten des häufig als anonym, ortlos und abstrakt beschriebenen Finanzkapitalismus ergibt. Der Finanzkapitalismus kann nur

---

achtens mit dem Titel *Arbeitskampf in der Daseinsvorsorge* (Franzen, Thüsing und Waldhoff 2012) hat der Parteivorstand der CSU 2015 in einem Papier gefordert, das »Streikrecht in Bezug auf die Daseinsvorsorge den Anforderungen einer vernetzten Lebenswirklichkeit anzupassen« (CSU 2015, 1). Das Papier sieht unter anderem staatlich verordnete Schlichtungsverfahren vor und bezieht sich dabei auf das Konzept der Kritischen Infrastruktur (CSU 2015, 1, 3).

global sein, weil er mundan ist, weil er an konkreten Orten, über materielle Infrastrukturen und mit identifizierbaren Personen operiert. Das macht ihn verwundbar, aber vor allem macht es ihn auch für Kritik adressierbar.

### Exkurs zur Zeit: »dass es so weitergeht...«

Sicherheit wird im BCM als Kontinuität konzeptualisiert und als Kontinuitätsmanagement praktiziert. Diese Artikulation von Sicherheit erlaubt einen vertieften Blick auf die zeitliche Ordnung des Sicherheitsdispositivs der Resilienz. Gerade hier wird nämlich deutlich, dass Technologien der Resilienz nicht nur im Davor, sondern ebenso im Dazwischen und Danach der Katastrophe operieren. Die Regierung der Katastrophe beginnt mit den Fragen: »Was kann passieren?« und: »Sind wir vorbereitet?« Die Antizipation möglicher Katastrophenereignisse und die Analyse systemischer Verwundbarkeiten soll die Kontingenz der Zukunft in den Bereich des Planbaren holen und es so ermöglichen, Katastrophenvorbereitungsmaßnahmen zu treffen (siehe insbesondere Kapitel 2.3.). Die Fragen nach der Antizipation von ebenso unwahrscheinlichen wie unvermeidlichen Katastrophen durch diverse Formen des »enactment based knowledge« (Collier 2008, 225f.) und des »vulnerability mappings« (Collier und Lakoff 2008, 8f.) sowie Maßnahmen der Katastrophenvorbereitung (*preparedness*), die die systemische Resilienz durch den Aufbau von Puffern und veränderte Systemdesigns erhöhen sollen, dominieren die Debatten zur Regierung der Katastrophe.

Darüber wurde allzu häufig die Bedeutung von Sicherheitstechnologien zur Bewältigung schwerwiegender Schadenslagen im »Intervall« (Adey und Anderson 2011, 2879) der Katastrophe übersehen. Das kritische Dazwischen bzw. das Milieu der Katastrophe (siehe zu diesem Sinn von Milieu Kapitel 2.3.3.) ist weniger durch die ungewisse Zukunft, sondern durch die komprimierte Prozess- und Ereigniszeit einer sich von Gegenwartspunkt zu Gegenwartspunkt entfaltenden Krisensituation gekennzeichnet. In der eskalierenden Notfallsituation ist keine Zeit für vorsorgende Planung. Vielmehr erfordert sie blitzschnelle Reaktionen (*rapid response*) des Krisen- und Lagemanagements. Nicht »Was kann passieren? Sind wir vorbereitet?«, sondern »Was muss prioritär bearbeitet werden? Was ist als nächstes zu tun?« sind die entscheidenden Fragen. Zwar werden auch Notfalleinsätze

vorbereitend geplant und geübt. Es kommen hier aber andere Wissens- und Interventionsformen zum Einsatz als vor der Katastrophe. Notfallpläne, Entscheidungsprotokolle oder medizinische Behandlungsalgorithmen sollen im Zeitdruck der Situation helfen, die richtigen Notfallmaßnahmen zu ergreifen (siehe Kapitel 4.2.2.). Im Idealfall kann das Krisenmanagement vor Ort durch ein zentrales Lagemanagement unterstützen (siehe zum Lagezentrum Kapitel 2.2.2., zum Lagemanagement Kapitel 2.3.3.). Zusammengefasst stehen diese Vorrichtungen und Maßnahmen im Dienste der operativen Resilienz.

Nach der Katastrophe schlägt zunächst einmal die Stunde der Überprüfung. Die möglichst schon während des Ereignisses erfolgte Dokumentation des Krisenmanagements soll dessen nachträgliche Evaluation ermöglichen. Diese Autopsie der Krise ist dabei schon allein deshalb eine so wichtige Wissenstechnik, weil sie es im Gegensatz zu Szenarien und Notfallprotokollen erlaubt, sich auf Evidenzen und nicht bloß auf Optionen und Wahrscheinlichkeiten zu stützen. Damit sind diese Verfahren zugleich die Voraussetzung für eine Wiederherstellung (*recovery*) des Systems, das dieses besser für zukünftige Zwischenfälle wappnet. In diesem Sinne verschreiben sich die Prozeduren der Evaluation, Nachbereitung und des *recovery* dem Prozessgeschehen evolutionärer Resilienz. »Was können wir aus dem Geschehen lernen, wie können wir uns besser auf derartige Situationen einstellen?« Aus vergangenen Ereignissen soll gelernt werden, um sich besser an zukünftige Gefährdungslagen anzupassen. Der relevante Zeithorizont ist eine evolutionäre Zeit der ständig erneuerten Anpassung an neue Gefahrensituationen, die aber nicht unbedingt antizipatorisch vorweggenommen werden kann. Evolution kehrt der Zukunft den Rücken zu und lernt mit Blick auf das Erlebte, um gerade dadurch für das Komende gewappnet zu sein.

Es gilt also: Nach der Katastrophe ist vor der Katastrophe. So schließt sich der Kreis. Davor, Dazwischen und Danach sind keine unabhängigen und für sich stehenden Zeitabschnitte, sondern stellen vielmehr ein zusammenhängendes Ablaufgeschehen dar, das die zeitliche Ordnung des Sicherheitsdispositivs der Resilienz kennzeichnet. Resilienz ist somit kein Zustand, sondern ein zyklischer und zeitlich ausgedehnter Prozess der ständigen Neuordnung und Anpassung. Dafür steht bei Holling der sogenannte »adaptive cycle« (Holling 2001, 394), eine an ein Möbiusband erinnernde Schleife mit vier aufeinanderfolgenden Phasen – *exploitation, conservation, release, reorganization* –, die ein resilientes System durchläuft. Der



*adaptive cycle* evoziert und transportiert ein bestimmtes Konzept von Kontinuität, das evolutionär und nicht statisch-linear gedacht ist. Kontinuität kann so als übergreifender Horizont der unterschiedlichen Temporalitäten der Resilienz verstanden werden. Nur so ist es möglich, auf den ersten Blick radikal unerwartete und disruptive Ereignisse in eine kohärente Serie von Ereignissen zu überführen.

Aspekt	Davor	Dazwischen	Danach
Wissen	Risikoabschätzung/ Antizipation: - <i>enactment based knowledge</i> (Szenario, Übung), - Verwundbarkeits- kartierung bzw. Impact- Analyse	Notfallplan, Entscheidungs- protokolle, Medizinische Behandlungs- algorithmen, Triagestufen	Dokumentation, Überprüfung ( <i>auditing</i> )
Intervention	Katastrophenvorbereitung ( <i>preparedness</i> )	Krisenmanagement, Lagemanagement ( <i>rapid response</i> )	Evaluation, Nachbereitung, Reaktion auf Probleme, Wiederherstellung ( <i>recovery</i> )
Form der Resilienz	systemische bzw. strukturelle Resilienz: - Aufbau von Puffern, Redundanzen - Veränderung der Systemarchitektur	operative Resilienz: - Aufbau und Training von Notfallteams - situationsgerechte Krisenbearbeitung	evolutionäre Resilienz: - Lernen aus vergangenen Katastrophen - Anpassung an zukünftige Gefährdungen

Table 6: Die Temporalitäten der Resilienz

Resilienz nimmt damit offensichtlich Denkfiguren auf, die bereits in der Biologie des 19. Jahrhunderts entwickelt wurden. Mit dem Aufkommen eines Denkens des Lebens als Kollektivsingular seit Beginn des 19. Jahrhunderts (Foucault 1974, 322–341) und spätestens mit der Darwin'schen Evolutionsbiologie in der zweiten Hälfte des 19. Jahrhunderts ist eine neue Konzeption von Kontinuität möglich geworden. Jenseits der begrenzten Kontinuität des Einzellebewesens konnte jetzt eine erweiterte Kontinuität der Gattung, die stets die Diskontinuität, also das Verenden des Einzellebens, voraussetzt, biologisch gedacht werden. Die individuelle Lebenszeit und die Zeit des Lebens sind auseinandergetreten. Zudem konnte ein größerer Zusammenhang *des Lebens selbst* angenommen werden, der die phä-

nomenalen Gattungsunterschiede mit Blick auf den Prozess der Evolution relativierte. Henri Bergsons philosophischer Vitalismus und sein Konzept der Zeit als Dauer, *durée*, hat dieses Denken der Zeit des Lebens aufgegriffen und damit die scheinbar widersprüchlichen Konzepte von Kontinuität und Wandel, Beständigkeit und Flüssigkeit, Dauerhaftigkeit und Beweglichkeit zusammengedacht. Im Gegensatz zum Prinzip des Raums, der Diskontinuität, also der Diskretheit materieller Wirklichkeitsstücke, ist das Prinzip der Zeit die Kontinuität, der ungeteilte Prozess, der letztlich alles Seiende zusammenhält. Diese Zeit ist für Bergson die Zeit des Lebens und der schöpferischen Evolution. Die intensive Kontinuität der Zeit steht für das beständige Werden des Lebendigen, das in diesem Werden das Prinzip seiner Konsistenz (*élan vital*) findet. »Es ist gerade diese unteilbare Kontinuität von Veränderungen, die die wahre Dauer ausmacht.« (Bergson 2013, 28)<sup>235</sup> Auch Holling versucht mit seinem Konzept von Resilienz Wandel und Kontinuität zusammenzudenken und »learning with continuity« (Holling 2001, 399) zu verbinden. Das heißt aber auch, dass das Leben von Einzellebewesen bzw. Systemelementen dem Systemganzen untergeordnet und damit die zeitliche Dimension existenzieller Endlichkeit ausgeblendet wird. Gleichzeitig dichtet sich das resiliente System gegen alle tatsächlichen Diskontinuitäten und gegen grundlegenden, qualitativen Wandel ab. Das einzelne Ereignis verliert seinen Schrecken in dem Maße, in dem es zum Teil eines umfassenden Prozesses gemacht wird. Nur das Ereignis eines grundlegenden *phase change* des Systems muss noch gefürchtet werden. Das ist aus zweierlei Gründen beunruhigend. Zum einen scheint es so gar nicht mehr um je meine Sicherheit zu gehen, sondern bloß noch um die Funkti-

---

235 Nicht nur Martin Heidegger (2006) hat die Bergson'sche Konzeption der Zeit kritisiert, weil sie den Tod und damit die Endlichkeit vergisst. Auch bei der Kritischen Theorie der Frankfurter Schule findet sich diese Kritik, die hier weniger existenzialphilosophisch, sondern geschichtsphilosophisch aufgeladen ist. Max Horkheimer (1988, 187f.) bemerkt: »Die Betätigung der Zeit an jedem Sein bedeutet, daß es altert und vergeht – nicht bloß, daß es wechselt. [...] Durch diese überirdische und darum schiefe Blickrichtung wird er [Bergson] dazu verführt, das Ende der gelebten Zeit durch die Idee des Wechsels auszulöschen, während doch die Menschen aus der Unaufhebbarkeit, der unbedingten Endgültigkeit des eigenen und fremden Todes die verzweifelten Kräfte schöpfen müssen, deren sie bei ihrer geschichtlichen Tätigkeit bedürfen.« Wie Horkheimer sieht Walter Benjamin in diesem Übersehen des Todes nicht bloß eine philosophische Nachlässigkeit, sondern eine Ideologie, welche der »geschichtlichen Tätigkeit« keine Rechnung tragen kann, also den Praktiken, die auf historische Veränderung im emphatischen Sinne zielen. »Daß in Bergsons *durée* der Tod ausfällt, dichtet sie gegen die geschichtliche [...] Ordnung ab.« (Benjamin 1991a, 643)

on von Systemen. Zum anderen scheint eine Sicherung der Kontinuität komplexer Prozesse, die ständigen Wandel und Anpassung einschließt, zugleich eine grundsätzliche Umgestaltung dieser Prozesse zu verunmöglichen. Ja, in dem Maße, in dem individuelle Endlichkeit ausgeblendet wird, verschwindet auch die Perspektive auf den Wandel des Systems.

Gegen diese ununterbrochene Prozesszeit der Kontinuität scheint kein apokalyptisches Kraut gewachsen zu sein. Obwohl Vorbereitungen auf die kommende Katastrophe stattfinden, der Ausnahmezustand geübt und mit dem Schlimmsten gerechnet wird, bleibt der zeitliche Horizont doch vom Imperativ des »immer weiter« zugenäht. Das unterscheidet die Temporalität der gegenwärtigen Regierung von Katastrophen und Ausnahmezuständen radikal von vergleichbaren Projekten in vorkapitalistischen Zeiten. Eine genealogische Verortung des Kontinuitätsmanagements in der Geschichte des Ausnahmerechts seit der römischen Antike kommt – wie in Kapitel 4.1.1. gezeigt – zu dem Schluss einer radikalen Differenz zwischen römischem *iustitium*, bei dem alle Geschäfte für die Zeit der Ausnahmesituation ausgesetzt wurden, und gegenwärtigem *state of emergency*, bei dem die Operationen von vitalen Systemen unbedingt fortgesetzt werden müssen (siehe: Bussolini 2014). Resilienz ist keine Technik der Souveränität, sondern steht eher mit Machtformen in Zusammenhang, die Deleuze als Kontrolle beschrieben hat. »Die Kontrolle ist kurzfristig und auf schnellen Umsatz gerichtet, aber auch kontinuierlich und unbegrenzt« (Deleuze 1993, 260). Kontrolle ist nicht mehr durch fixe, abgrenzbare Identitäten und vorgeschriebene Normen, sondern durch »permanente [...] Metastabilität« und »tiefgreifende [...] Modulation« (Deleuze 1993, 256) gekennzeichnet. Deleuze vergleicht die Kontrollmacht mit einer »sich selbst verformenden Gußform, die sich von einem Moment zum anderen verändert« (Deleuze 1993, 256), und liefert damit – so können wir am Ende dieser Analyse sagen – zugleich eine Metapher für die normative Ordnung der Resilienz.

Das heißt aber auch, dass es nicht reicht, die Macht der Kontrolle und das Sicherheitsdispositiv der Resilienz dafür zu kritisieren, dass sie Veränderungen verunmöglichen und das soziale Geschehen stillstellen. Das Problem besteht eher darin, dass die permanenten Transformationen, Mutationen und Evolutionen der »Systeme« nicht mit dem einhergehen, was einmal als revolutionäre Veränderungen der »Gesellschaft« verstanden

wurde und einst den gesellschaftlichen Erwartungshorizont bestimmte.<sup>236</sup> Die Konjunktur des Sicherheitsdispositivs der Resilienz und des Kontinuitätsmanagements als »Änderungsmanagement« (BSI 2008, 12) evoziert vielmehr das Bild des »rasenden Stillstands« (Virilio 2002). Seit Virilio diese Formel geprägt hat, wurde sie in kulturkritischen Analysen immer wieder genutzt, um die Diskrepanz zwischen der ständigen und immer noch beschleunigten Veränderung des sozialen Lebens und der gleichzeitigen Versiegelung der grundlegenden Mechanismen, Motoren und Motive dieser akzelerierten Transformation zu beschreiben. Hartmut Rosa, der sich ebenfalls dieses Motivs bedient, bemerkt: »[T]he sense of a directed movement of history has given way to a sense of directionless, frantic change.« (Rosa 2003, 22) Trotz oder gerade wegen der vertieften Aufmerksamkeit für temporale Prozesse, Zeitknappheit, schnelle Taktungen und Anschlussimperative, wie es gerade für das BCM typisch ist, verschwinden zentrale Charakteristiken des Zeitlichen. Das Ergebnis ist, wie Jonathan Crary (2013, 29) formuliert, eine »time without time, a time extracted from any material or identifiable demarcations [...] it celebrates a hallucination of presence, of an unalterable permanence composed of incessant, frictionless operations.«

Der Denker, der derartige Motive als erster und wohl am konsequentesten entwickelt hat, ist Walter Benjamin. Nicht zuletzt hat er dabei auch ein alternatives Verständnis der Katastrophe entwickelt, das im scharfen Gegensatz zur Figur der Katastrophe als Unterbrechung eines reibungslosen Prozessverlaufs steht. Apodiktisch stellt Benjamin fest: »Der Begriff des Fortschritts ist in der Idee der Katastrophe zu fundieren. Daß es »so weiter« geht, ist die Katastrophe. Sie ist nicht das jeweils Bevorstehende, sondern das jeweils Gegebene.« (Benjamin 1991c, 592) Und an anderer Stelle: »Fortschritt ist nicht in der Kontinuität des Zeitverlaufs, sondern in seinen Interferenzen zu Hause: dort, wo ein wahrhaft Neues zum ersten Mal mit der Nüchternheit der Frühe sich fühlbar macht.« (Benjamin 1991c, 593) Entsprechend besteht für Benjamin die revolutionäre Tat nicht mehr im Vorwärtstreiben der Geschichte oder in der Zuspitzung historischer

---

236 Paul Virilio hat argumentiert, dass der revolutionäre Erwartungshorizont im 20. Jahrhundert zunächst vom Krieg und dann vom katastrophischen Unfall verdrängt wurde. »Das Gefühl der Unsicherheit [...] scheint das Symptom eines neuen *Erwartungshorizonts* zu sein, des dritten seiner Art nach der »Revolution« und dem »Krieg« [...] ich spreche von der Erwartung des *vollständigen Unfalls*« (Virilio 2009, 53 – Hervorhebung im Original)

Tendenzen, sondern in der Unterbrechung und Stillstellung des historischen Verlaufs. »Marx sagt, die Revolutionen sind die Lokomotive der Weltgeschichte. Aber vielleicht ist dem gänzlich anders. Vielleicht sind die Revolutionen der Griff [...] nach der Notbremse.« (Benjamin 1991b, 1232)

Stimmt man dieser Diagnose zu – echter Fortschritt kann, scheinbar paradox, nur noch als katastrophische Unterbrechung bewirkt werden – und hat zudem revolutionäre Veränderung im Sinn, dann ist es wohl allzu verführerisch, sich als Agent\_in der Apokalypse zu inszenieren. Die gegenwärtig prominenteste Variante solch eines revolutionären Katastrophismus findet sich bei der französischen Intellektuellen- und Aktivist\_innengruppe *Comité Invisible*. In einem Echo auf Benjamins Geschichtskritik stellen sie fest: »The catastrophe is not coming, it is here.« (Comité Invisible 2009, 96)

»The normal functioning of the world serves to hide our state of truly catastrophic dispossession. What is called ›catastrophe‹ is no more than the forced suspension of this state [...]. Any loss of control would be preferable to all the crisis management scenarios they envision.« (Comité Invisible 2009, 81)

Gegen die Katastrophe der bzw. in Permanenz stellen sie eine Politik des Ereignisses und der Unterbrechung. Dabei haben sie es vor allem auf die Sabotage der kontinuierlichen Operationen der Systeme der Macht und ihrer Infrastrukturen abgesehen: »Every network has its weak points, the nodes that must be undone in order to interrupt circulation. [...] In order for something to rise up in the midst of the metropolis and open up other possibilities, the first act must be to interrupt its *perpetuum mobile*.« (Comité Invisible 2009, 60f.) Parallel zur Sabotage metropolitaner Infrastrukturen sollen alternative Versorgungsnetze aufgebaut werden, um auf die revolutionäre Katastrophe vorbereitet zu sein: *be prepared!* lautet auch die Parole des unsichtbaren Insurrektionalismus (Comité Invisible 2009, 107) Fredric Jameson (2003) hat einmal bemerkt, es sei mittlerweile leichter, sich das Ende der Welt vorzustellen als das Ende des Kapitalismus. Wohl deshalb imaginiert der Katastrophismus des Unsichtbaren Komitees das Ende des Kapitalismus kurzerhand als Ende der Welt. Die revolutionäre Vorhut fährt hier nicht mehr mit Marx in der Lokomotive der Geschichte, sondern galoppiert mit den Reitern der Apokalypse – zum Ende der Geschichte.<sup>237</sup>

---

237 Für eine Kritik des Comité's, die ebenfalls die Bedeutung von logistischen Widerständen im gegenwärtigen Kapitalismus betont siehe: Toscano (2011).

Ähnlich gelagert, wenngleich in Ton und Absicht weit weniger apokalyptisch, ist das Konzept der »counter-operations«, das Brett Neilson und Sandro Mezzadra (2013) im kritischen Anschluss an Agambens Konzept der Inoperabilität<sup>238</sup> entwickelt haben. Die Politik der *counter-operations* bezeichnet die Praxis von bestimmten antikapitalistischen Bewegungen. »It is through this suspension [of operations] that other ways of fabricating the world become theoretically visible and the politics of operation can give way to the forging of »counter-operations.« (Mezzadra und Neilson 2013, 16) *Counter-operations* unterbrechen also temporär die gängigen sozio-ökonomischen Operationen – etwa der Logistik – und lassen dadurch alternative Handlungsmöglichkeiten erscheinen. Dabei sind, wie die Autoren sich bemühen festzustellen, diese *counter-operations* mehr als bloße Sabotageakte (Mezzadra und Neilson 2013, 17). Auch den Bewegungen, die ich mit dem Begriff der Disruptiven Demokratie bezeichnet habe, geht es nicht um eine Zerstörung der Systeme, sondern um eine temporäre Unterbrechung systemischer Operationen, um eine Situation zu erzeugen, in der die Kritik und der Protest der Bewegung nicht mehr einfach überhört werden können. »Die Temporalität der Kritik ist die Zeit der Inoperabilität.« (Opitz 2013, 61) Die gegenwärtige Proliferation von Widerstandspraktiken der Unterbrechung sagt in gewisser Hinsicht mehr über die Selbstverständlichkeiten des Sicherheitsdispositivs der Resilienz aus als die Flut seiner eigenen Stellungnahmen und Positionierungen. Denn wenn eine widerständige Praxis und ein emanzipatorisches Imaginäres die Unterbrechung und den Stillstand betonen, dann artikulieren sie damit auch ein Unbehagen gegenüber der Kontinuitätszeit der Resilienz. Das Ausblenden von Diskontinuität und existenzieller Endlichkeit scheint nämlich auch das radikale Neuanfangen zu kompromittieren, das für Hannah Arendt (2007, 215ff.) den Kern politischen Handelns ausmacht.

Diese Darstellung der Zeit der Resilienz als Kontinuität ist gewiss überzeichnet. Es wäre falsch davon auszugehen, dass sich die Zeit der Sicherheit und die Zeit der Emanzipation *per se* widersprechen und Resilienz notwendig blind für endliche Phänomene ist. Ansätze für ein anderes Ver-

---

238 Giorgio Agamben (2011) entwickelt sein Konzept der Inoperabilität im Kontext seiner Überlegungen zur göttlichen Ökonomie. Agamben argumentiert, dass das Konzept der Inoperabilität bzw. *anapsis* im Judentum den Ruhetag Gottes bezeichnet, nachdem er die Welt erschaffen hat, wobei hier – anders als im Christentum – der ruhend-pausierende Gott höher steht als der schaffend-schöpferische. Dieses Motiv, so Agamben, findet sich im Judentum in Form des Sabbat institutionalisiert .

ständnisses von Resilienz finden sich etwa in Georges Canguilhem's Konzept der biologischen Normativität, das unverkennbar Züge dessen vorwegnimmt, was später als Resilienz bezeichnet werden sollte. Für Canguilhem gibt es biologische Normativität – also das Setzen von Vitalnormen durch das lebendige Wesen – nämlich überhaupt nur, weil das Leben stets vom Tod bedroht ist. Programmatisch heißt es bei Canguilhem:

»Heute [...] wage ich [...] den Versuch, durch eine philosophische Analyse des als Widerstand gegen die Trägheit und Indifferenz gefaßten Lebens die Grundbedeutung des Normalen zu fundieren. Das Leben sucht die Oberhand über den Tod zu gewinnen [...]. Das Leben spielt gegen die wachsende Entropie.« (Canguilhem 1977, 161)

Und ähnlich hat Holling 1973 gegen die Populationsökologie darauf beharrt, dass es bei der Resilienz nicht um Bestandszahlen, sondern um Fragen nach Sein oder Nicht-Sein gehen müsse. »Attention shifts, therefore, to the qualitative and to questions of existence or not.« (Holling 1973, 1) Dass davon in seinen späteren Veröffentlichungen zu Resilienz nichts mehr übrig geblieben ist, steht gewiss auch mit dem politischen Schicksal seines Konzepts in Verbindung.<sup>239</sup>

Schließlich erfordert der hier vorgeschlagene Blick auf die Zeit von Resilienz und Inoperabilität aber auch eine Reflexion auf die aktuelle Konjunktur der Zeit in der Soziologie. Die Ähnlichkeiten zwischen gewissen temporalisierten Sozialtheorien und dem Prozessdenken des Kontinuitätsmanagements sind frappierend. So ist im Zuge der »Temporalisierung des Sozialen« (Nassehi 2009, 234–241) auch das »soziale Band« verzeitlicht worden. Weniger die Integration des Individuums in einen größeren Gesellschaftsorganismus, sondern die Fortsetzung von sozialen Vollzügen (etwa: Kommunikationen, Praktiken, sozio-technische Operationen) ist zum entscheidenden Kriterium für sozialen Zusammenhalt geworden. Es erfolgt also eine Verschiebung von Integration zu Kontinuität. Besonders deutlich wird das in Luhmanns Theorie sozialer Systeme (Luhmann 1991b) und dessen Konzept der Autopoiesis. Die Gesellschaft ist für Luhmann ein hyperresilienter Prozesskomplex, der immer weiter macht, weil die Fortsetzung seiner Grundoperationen von Störungen, Irritationen und

---

239 Dieses Schicksal beleuchtet eindrucksvoll Sara Nelson (2014), indem sie zeigt, wie das anfangs progressive Konzept der Resilienz einer »neoliberal counter-revolution« zum Opfer gefallen ist.

Krisen eher angetrieben als gebremst wird. »Komplexe Systeme benötigen ein recht hohes Maß an Instabilität [...] und sie müssen diese Instabilität laufend reproduzieren« (Luhmann 1991b, 501). In Japps (2003) systemtheoretischer Katastrophensoziologie wird folgerichtig selbst das Desaster noch zum produktiven Impuls für soziale Operationen. Heinz Bude schließlich geht so weit, die Bedingung der Möglichkeit von Soziologie in der Weitermachtendenz der Gesellschaft zu verorten. So antwortet er auf die Frage »Wie ist Soziologie möglich?« mit der Bestimmung: »Weil sich Soziologie mit dem Phänomen beschäftigt, dass es immer weitergeht« (Bude, zitiert nach: Reemtsma 2010, 90). Zwar haben diese Ansätze die Soziologie gewiss bereichert. Aber gleichwohl werden vor dem Hintergrund der Ausführungen dieser Arbeit auch ihre Begrenzungen sichtbar. Dass es »immer weitergeht«, ist nämlich keineswegs selbstverständlich. Schließlich sollen Kontinuitätsmanager\_innen dieses Weitergehen sicherstellen, während Protestbewegungen versuchen, es zu stören. Hat man sich aber immer schon darauf festgelegt, dass es immer weiter geht, dann geraten die Momente der Inoperabilität und damit auch die Potenziale dafür, dass es *anders* weiter gehen könnte, aus dem Blick.



# Fazit

Die Gegenwart ist durch den Aufstieg einer neuen Art des Regierens geprägt, die sich der Vorbereitung auf Katastrophen und ihrer kontrollierenden Einhegung verschrieben hat. Dieser Regierungsmodus ist in der jüngeren Vergangenheit auch jenseits der Institutionen des Katastrophenschutzes so systematisch ausgearbeitet worden, dass sich darin die Emergenz eines neuen Sicherheitsdispositivs erkennen lässt, das in unterschiedlichen Gebieten mit isomorphen Technologien auf analoge Probleme reagiert und dem normativen Leitbild der Resilienz verpflichtet ist. Dieses Sicherheitsdispositiv der Resilienz unterscheidet sich von historisch konstituierten Formationen der Sicherheit, wie der souveränen Staatssicherheit und der normalisierenden Bevölkerungssicherheit, in Bezug auf seine zeitliche, räumliche, sachliche und normative Dimension.

Sicherheit operiert in einem neuen *zeitlichen* Gefahrenhorizont. Nicht mehr die Prävention von Schadensereignissen oder die Versicherung vor prognostizierbaren Risiken, sondern die Vorbereitung auf ebenso unwahrscheinliche und ungewisse wie verheerende Ereignisse gilt es zu organisieren. Dabei geht es nicht nur um singuläre Katastrophenereignisse, sondern ebenso um nicht-lineare Gefahrensituationen, die schon in ihrem Entstehen bekämpft werden müssen, um später nicht unkontrollierbar zu sein. Dafür müssen materielle, personelle und institutionelle Kapazitäten vorbereitend vorgehalten werden, die im Notfall schnell zum Einsatz kommen können.

Neue Technologien der Risikoanalyse und Gefahrenbewältigung zielen zudem auf Gefährdungen, die sich *räumlich* nicht mehr eindämmen lassen, die territoriale Grenzen und damit auch institutionelle Zuständigkeitsgrenzen überschreiten. In diesen »Katastrophenmilieus« müssen Sicherheitspraktiken die ansteckende Ausbreitung der Gefahr vermeiden, ohne die Mobilität und Beweglichkeit »offener«, globalisierter Gesellschaften einzuschränken. Dafür versuchen Sicherheitstechnologien ebenso vernetzt und

verstreut zu sein wie die Gefahren, auf die sie reagieren. Sie überwinden institutionelle Grenzen, zerlegen das Territorium in »Risikozonen« und unternehmen eine taktische Dislozierung von Schutzressourcen. Sicherheit schützt neuralgische Punkte und ist bestrebt, Versorgungsnetze zu dezentralisieren. Gerade im Angesicht ökologischer Gefährdungen ist die räumliche Reichweite von Sicherheitstechnologien geradezu planetarisch. Nicht mehr begrenzte historisch-natürliche Milieus wie im 19. Jahrhundert, sondern immer entgrenztere öko-technische Milieus gilt es zu sichern.

Das Sicherheitsdispositiv der Resilienz operiert im Rahmen einer Biopolitik vitaler Systeme, einer Politik des Lebens jenseits seiner selbst, die nicht unmittelbar auf den Körper des Einzelnen und der Gattung zielt, sondern versucht, deren Lebensbedingungen zu gestalten und zu sichern. Nicht nur die von Katastrophen bedrohte Bevölkerung, sondern auch Kritische Infrastrukturen und vitale Systeme sind zum entscheidenden *Gegenstand* von Sicherheitstechnologien aufgestiegen. Vitale Systeme sind zentrale Schutzobjekte, weil davon ausgegangen wird, dass das Leben der Gesellschaft in einem umfassenden Sinn von ihnen abhängt bzw. durch sie prozessiert wird. Sie gelten gleichzeitig aber auch als Gefahrenzusammenhang, weil ihre hohe interne Komplexität und die wuchernde Interdependenz zwischen ihnen als Quelle systemischer Risiken angesehen werden. Systemische Risiken bestehen aus Störungen und Unterbrechungen in Systemen, die sich schnell zu schwerwiegenden und weitreichenden Katastrophensituationen ausweiten können. Vorbereitender Katastrophenschutz versucht daher, die Anfälligkeit gegenüber externen Gefahren sowie das intrinsische Verwundbarkeits- und Gefährdungspotenzial vitaler Systeme zu reduzieren.

Das verweist bereits auf die Verschiebung des *normativen Leitbilds* der Sicherheit. Die Widerstandsfähigkeit der Gesellschaft und von »vitalen Systemen« gegenüber Katastrophen und systemischen Risiken soll gestärkt werden: operative Resilienz durch den Aufbau von Hilfskapazitäten sowie systemische Resilienz durch robustes Systemdesign und durch Vorhaltung von Ressourcen und Puffern, die Katastrophen abfedern können. Um dauerhafte Widerstandsfähigkeit gegenüber einer sich ständig verändernden Gefahrenumwelt zu gewährleisten, reicht es nicht mehr, nach Katastrophen schnell wieder zum *status quo ante* zurückzukehren, reicht also Normalisierung nicht mehr aus. Vielmehr geht Resilienz häufig mit einem Ethos des Lernens aus vergangenen und der dadurch verbesserten Anpassung an neue Gefährdungslagen einher. Evolutionärer Resilienz geht es

eher um die Gewährleistung der Normativität, der metastabilen Suche nach immer neuen Gleichgewichtspunkten, als darum, einer statistisch-statistischen Normalität näher zu kommen. Sicherheit ist hier weniger ein Zustand der Abwesenheit von Gefahr, sondern ein Prozess der flexiblen Anpassung an eine sich ständig verändernde Gefahrenumwelt.

Durch diese Absetzbewegung von klassischen Denk- und Operationsweisen der Sicherheit steht »Resilienz« nicht nur für ein neues Sicherheitsdispositiv, sondern ebenso für ein Problematisch-Werden bestimmter Ansprüche der Sicherheit. Gerade das Beharren auf vollständiger Sicherheit im Sinne von Gefahrenlosigkeit führe – so wird immer wieder betont – zu pathologischen Effekten, die häufig genau die Gefahren und Katastrophenpotenziale heraufbeschwören, die doch eigentlich verhindert werden sollten.

Sicherheitsdispositiv	Zeit	Raum	Gegenstand	Norm
Souveräne Staats-sicherheit	Souveräner Dezisionismus und Verhängung temporärer Ausnahmezustände	(nationales) Territorium extralegale Zonen (Lager)	Recht und Ordnung, Sicherung der territorialen Integrität des souveränen Staats	Juridische Norm, Gesetz, Standard → Normierung
Bevölkerungs-sicherheit	Prävention von bzw. Versicherung gegen statistisch kalkulierbare Risiken	Historisch-natürliches Milieu der Zirkulation	Bevölkerung	Statistische, empirische Normalität, Gleichgewicht → Normalisierung
Sicherheitsdispositiv der Resilienz	<i>Vorbereitung</i> auf Katastrophenereignisse	Milieu der Zirkulation, Risikozone	<i>Bevölkerung</i> (Schutz der Bevölkerung vor Katastrophen) <i>Vitale Systeme</i> (Reduktion der Verwundbarkeit durch systemische Risiken)	<i>Resilienz</i> – operationelle Resilienz – systemische Resilienz – evolutionäre Resilienz

Tabelle 7: Systematik der Sicherheitsdispositive

Aber was ist, jenseits der systematischen Abgrenzbarkeit von anderen Konstellationen der Sicherheit, wirklich »neu« am Sicherheitsdispositiv der Resilienz? Und wie setzt sich das Sicherheitsdispositiv der Resilienz konkret zusammen? Ist es bloß eine zu Forschungszwecken erstellte idealtypische Konstruktion, oder findet es in der Welt eine wirkliche und wirksame Entsprechung? Diesen Fragen möchte ich mich im nächsten Abschnitt des Fazits mit Rekurs auf die sachhaltigen Ergebnisse der Arbeit widmen (*Die Analytik des Sicherheitsdispositivs der Resilienz*). Anschließend möchte ich explizieren, inwiefern diese Arbeit nicht nur als Analytik, sondern auch als Kritik der Sicherheit verstanden werden kann (*Kritik der Sicherheit*).

### *Die Analytik des Sicherheitsdispositivs der Resilienz*

Folgt man Foucault (1978, 120), dann ist ein Dispositiv »das Netz, das zwischen [unterschiedlichen] Elementen geknüpft werden kann.« Die Arbeit hat insgesamt drei unterschiedliche Arten der Vernetzung untersucht, die das Dispositiv der Resilienz bilden und die seine Elemente zusammenhalten: gezielte Vernetzungsbemühungen von Akteuren (1), soziotechnische Netze, die Akteursbeziehungen ermöglichen und verstetigen (also Akteurs-Aktanten-Netzwerke) (2) und schließlich anonyme Beziehungsmuster wie genealogische Abstammungslinien und Familienähnlichkeiten zwischen unterschiedlichen Sicherheitstechnologien (3). Die Akteure sind gewissermaßen die selbstbewussten Monteur\_innen von Sicherheitsnetzen. So verstehen sich die Akteure der Sicherheitspolitik und Institutionen des Katastrophenschutzes bisweilen selbst als »Netzknoten« (siehe Kapitel 2.2.2), entwerfen Strategien »vernetzter Sicherheit« und bilden »Sicherheitspartnerschaften« (siehe Kapitel 3.3.4.). Sie erzeugen strategische Allianzen von Institutionen und verknüpfen, gerade beim Schutz Kritischer Infrastrukturen, private und öffentliche Institutionen miteinander (siehe Kapitel 3.1.3.). Mechanismen der Verknüpfung sind hier rechtliche Verpflichtungen, aber häufig auch nur das »Interessieren«, das Erzeugen von Aufmerksamkeit und Sensibilität für die eigenen Projekte und Probleme (zum Konzept des *interessement* siehe: Callon 2006a).

Doch die Monteur\_innen wären nichts ohne ihre Montagemittel, ohne den Klebstoff, der die Elemente zusammenbindet, und das Schmiermittel, das diese in Aktion hält. Mit Ansätzen aus den STS und der ANT wurden Mechanismen und Techniken der Netzbildung nachgewiesen, die heterogene Elemente durch »Aktanten« (Latour 2001b) bzw. »Quasi-Objekte«

(Serres 1981, 344–360) zu robusten Akteursnetzwerken verbinden. Unterschiedliche Hilfsorganisationen verständigen sich auf und durch »boundary objects« (Star und Griesemer 1989) und »boundary infrastructures« (Bowker und Star 2000, 285–317). Das Notfallinformationssystem deNIS etwa erzeugt eine digitale Plattform, auf der sich unterschiedliche Akteure einschreiben können und in Relation zu anderen auf »Lagekarten« verorten (siehe Kapitel 2.3.3.). Durch die Etablierung von »centres of calculation« (Latour 1987, 215–257) wie dem GMLZ können Akteure auf die gleichen Daten zugreifen und sich so koordinieren (siehe Kapitel 2.2.3.). Standardisierte Methoden der Risikoanalyse erzeugen verbindliche Risikoklassifikationen und etablieren einen geteilten Rahmen für die Wahrnehmung von Risiken und die Verteilung von institutionellen Zuständigkeiten (siehe Kapitel 2.3.1.). Weltweite Standards wie die ISO-Normen zum BCM oder die Identifikation systemrelevanter Banken durch das FSB bringen »global assemblages« (Ong und Collier 2005b) betrieblicher Sicherheitsstrategien hervor (siehe Kapitel 2.5. und Kapitel 4.3.2.). Die Notfallpläne, die nach den Vorgaben des ISO-Standards für BCM ausgearbeitet wurden, schaffen verbindliche Protokolle für den Einsatzfall und koordinieren so die »ad hoc assemblages« (Braun 2014, 51) des Notfallmanagements (siehe Kapitel 4.2.).

Allerdings ist ein Dispositiv mehr als ein Akteurs-Netzwerk. Es ist ein größerer und abstrakterer Zusammenhang, der »broader fields of significance and historical conditions of intelligibility« (Collier 2011, 28) beinhaltet und daher nicht vollständig durch die Analysewerkzeuge der ANT sichtbar gemacht werden kann. Deshalb ging es mir darum, jenseits der taktisch ausgerichteten Artikulationsarbeit von Akteuren und Aktanten auch die »großen anonymen Strategien, die, nahezu stumm, geschwätzige Taktiken koordinieren« (Foucault 1977, 116), zu untersuchen. Diese anonymen Strategien haben einen »implizite(n) Charakter« (Foucault 1977, 116), der das Spezifische eines Dispositivs jenseits von konkreten Akteurs-Netzwerken oder expliziten Strategien »vernetzter Sicherheit« ausmacht. Die nur impliziten Gemeinsamkeiten zwischen auf den ersten Blick disparaten Feldern wurden dadurch explizit gemacht, dass kontraintuitive Vergleiche gezogen wurden, etwa zwischen dem Vorhalten von Eigenkapital und der Schaffung von Erdölreserven als Resilienztechnologie (siehe Kapitel 2.5.2.) oder zwischen dem Infrastrukturschutz und der Bewahrung des Erdsystems als Biopolitik vitaler Systeme (siehe Kapitel 3.1. und 3.2.). Durch historische Analysen konnte geschichtlich Entferntes – die Regie-

rungsbunker des Kalten Kriegs und die *hot relocation sites* heutiger Banken – aneinander angenähert werden (siehe Kapitel 4.1). Ich habe Wahlverwandtschaften (Weber 1988b, 26) und genealogische Abstammungslinien von Denkrichtungen und Handlungsweisen diagnostiziert und so unerwartete »Familienportraits« erstellen können: Ökolog\_innen, die das Energiesystem dezentralisieren wollen, stehen in diesen Portraits neben Militärs, die Kritische Infrastrukturen durch eine Auflösung von verwundbaren *hubs* schützen wollen (siehe Kapitel 3.3.2.). Neoliberale Kritiker\_innen der Technokratie haben sich nicht mit Vertreter\_innen der Alternativbewegung abgesprochen, die das Amalgam von staatlicher und technischer Macht fürchteten, und wären vielleicht sogar schockiert über die Nähe ihrer Positionen gewesen (siehe Kapitel 3.2. und 3.3.). Dennoch konnte ich zeigen, dass ihre Kritik in eine ähnliche Richtung zielte und so zur Bildung »anonymer Strategien« beitrug.

Diese anonymen Strategien stellen einen genuinen Vernetzungsmodus des Sicherheitsdispositivs dar. Es handelt sich dabei gleichwohl nicht um Verbindungen, die in Form sozialer und institutioneller Beziehungen oder sozio-technischer Netze existieren. Vielmehr sind es »Kräfte«, die wie die Gravitation eine gemeinsame Ausrichtung verstreuter Technologien ermöglichen oder wie Fliehkräfte dafür sorgen, dass die Elemente eines Dispositivs gerade in ihrer und durch ihre Bewegung zusammenhalten. Die anonymen Strategien sind weder die Monteure noch die Kleb- und Schmiermittel, sondern der Treibstoff der dispositivhaften Regierungsapparaturen.

Der wichtigste Unterschied zwischen einem bloßen Akteurs-Netzwerk und einem Dispositiv ist vor allem die spezifische Historizität des letzteren. Dabei geht es nicht bloß darum, dass das Dispositiv auf diese oder jene Weise »in der Geschichte« verortbar ist. Vielmehr besteht die Geschichtlichkeit des Dispositivs darin, wie es selbst Geschichte versammelt, wie es sich in die längere Geschichte der Sicherheit einschreibt und sich zur Zukunft hin öffnet. Die Beachtung dieser Historizität erlaubt es besser zu verstehen, worin der Neuigkeitswert des Dispositivs der Resilienz besteht, wie es sich zu anderen historisch etablierten Sicherheitstechnologien verhält und welche Entwicklungsmöglichkeiten in ihm angelegt sind.

Denn was ist eigentlich neu am Sicherheitsdispositiv der Resilienz? Ist die Vorbereitung auf Katastrophen wirklich ein neuer Regierungsstil? Hat nicht schon der biblische Josef dem Pharao Vorbereitungsmaßnahmen für katastrophische Hungersnöte empfohlen, als er vorschlug, Kornlager anzu-

legen? Ist nicht schon Noahs Arche ein »Ausweichstandort« für den Katastrophenfall? Regierte nicht schon der Deichgraf die Katastrophe durch Vorbereitung? Haben sich Katastrophen- und Zivilschutz nicht schon lange mit vergleichbaren Strategien auf Unglücksfälle vorbereitet? Geht man nicht der Selbstrepräsentation deutscher Sicherheitspolitik als »neu« auf dem Leim, wenn man einen Paradigmenwechsel supponiert, den diese Sicherheitspolitik selbst ausruft? Neu ist nicht diese oder jene Institution, diese oder jene Sicherheitstechnik, diese oder jene Problemwahrnehmung, sondern die spezifische Konstellation, in die sie alle miteinander treten und durch die alle Einzelteile eine »neue« Ausrichtung, Position und Funktion erhalten: das Dispositiv der Sicherheit. Diese Arbeit verabschiedet sich vom modernistischen Verständnis des Neuen als das nie Dagewesene. Stattdessen orientiert sie sich an einem alternativen Verständnis von Neuigkeit als »zeitgenössisch« im Sinne von Paul Rabinows (2008, 24) Anthropologie des Zeitgenössischen: »The ethos of the contemporary contrasts with that of the modern; it is not fascinated with the new per se but concerned with the emergence and articulation of forms within which old and new elements takes on meaning and functions.« Das Sicherheitsdispositiv der Resilienz ist eine solche kontemporäre »Form«, deren Entstehen sich der Begegnung von sicherheitspolitischen Residuen und innovativen Sicherheitstechniken verdankt.

So habe ich gezeigt, dass sich seit dem 11. September in Deutschland tatsächlich eine Reihe neuer Elemente gebildet hat, die darauf zielen, Katastrophen und systemische Risiken zu regieren: neue politische Programmatiken, neue Institutionen, neue technische Systeme sowie neue Regeln, Gesetze und Standards. In etlichen neu aufgelegten *politischen Programmatiken* wurden neue Gefahrprofile identifiziert und Leitlinien für deren Regierung definiert: in der Neuen Strategie zum Schutz der Bevölkerung, dem nationalen Pandemieplan, der Cybersicherheitsstrategie (siehe Kapitel 2.5.5.) sowie der Deutschen Anpassungsstrategie an den Klimawandel (Kapitel 3.2.3.). Neue und neu ausgerichtete *Regierungsinstitutionen* sollen operativ und koordinierend die Regierung der Katastrophe übernehmen: Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Bundesamt für Sicherheit in der Informationstechnik (BSI) (Kapitel 2.2.), das *Financial Stability Board* (FSB) (Kapitel 2.5.). Innerhalb dieser Institutionen wurden neue *technische Katastropheninformations- und Überwachungssysteme* sowie Risikoanalysetechniken entwickelt: das Gemeinsame Melde- und Lagezentrum (GMLZ), das Katastrophen und Informations-

system deNiS, die bundeseinheitliche Risikomatrix sowie Stresstests für Banken (Kapitel 2.4.). Schließlich wurden eine Reihe von *Gesetzen* geändert und *Regulationswerke* verabschiedet: das Zivilschutzgesetz (Kapitel 2.2.1.), die Eigenkapitalverordnung Basel III (Kapitel 2.5.), der ISO-Standard 22301 zum *Business Continuity Management* (Kapitel 4.2.1.), das IT-Sicherheitsgesetz (2.5.4.).

Diese neuen Elemente wären aber hilf- und haltlos, könnten sie nicht auf alte Institutionen, Gesetze und materielle Vorrichtungen zurückgreifen. Ständige Institutionen der Bundesrepublik wie das Innenministerium und die Bundeswehr sind immer noch hauptverantwortliche Akteure des Schutzes der Bevölkerung, haben aber neue Aufgabenprofile entwickelt, die auf eine veränderte »Sicherheitslage« reagieren (Kapitel 2.1. und 2.2.). Relikte aus dem Kalten Krieg wie die strategische Erdölreserve und die Zivile Notfallreserve Getreide werden für neue Strategien zur Überbrückung großflächiger Infrastrukturausfälle mobilisiert, deren wahrscheinlichste Ursachen nicht mehr in sowjetischen Atomangriffen oder Ölembargos, sondern eher in Cyberangriffen liegen (Kapitel 3.3.5.). Selbst das während der NS-Zeit geprägte Konzept der Daseinsvorsorge informiert heutige Strategien des Infrastrukturschutzes und der Versorgungssicherheit, wenn auch im Rahmen des neuen Paradigmas des Gewährleistungsstaates (Kapitel 3.1.). Hilfsorganisationen wie das Rote Kreuz oder die Feuerwehr sind seit eh und je Expert\_innen des Notfalls, aber auch sie bleiben nicht unberührt von der Neuausrichtung des Katastrophenschutzes (Kapitel 2.1. und 2.2.). Die vorsorgliche Bildung von Vorräten ist eine alte Strategie, die Vorräte der Gegenwart – Information in riesigen Datenzentren (Kapitel 4.1.1.), Eigenkapital in Bilanzbögen (Kapitel 2.5.2.) – sind jedoch neu. Vorratsbildung zur Steigerung systemischer Resilienz ist zeitgenössisch, insofern hier eine alte Strategie auf neue Systeme und Probleme angewendet wird (Kapitel 2.5.).

Die Emergenz des Dispositivs folgt also nicht dem Entwicklungspfad der Erfindungen eines Renaissancegenies, sondern eher der mühsamen Konstruktionsarbeit der Automobilindustrie, die – wie Michel Serres festgestellt hat – aus technischen Einzelteilen, die auf hunderte, ja im Fall des Rads auf tausende Jahre alte Erfindungen zurückgehen, einen neuen Gegenstand zusammenschraubt: »Das Ensemble ist zeitgenössisch nur durch die Montage, das Design, die Verpackung, manchmal nur durch die Eitelkeit der Werbung.« (Serres 2008a, 70) In diesem Sinne ist auch das Dispositiv der Resilienz zeitgenössisch durch die spezifische Art, wie es Hetero-



genes versammelt, wie es Elemente aus unterschiedlichen Zeitschichten montiert und auf die Probleme der Gegenwart ausrichtet.

Als kontemporäre Konstellation schreibt sich das Sicherheitsdispositiv kritisch und reflexiv in die historische Landschaft der Sicherheit ein und verändert so »das Korrelationssystem« (Foucault 2004, 23) zwischen den historischen, etablierten Sicherheitsdispositiven der souveränen Staatssicherheit und der normalisierenden Bevölkerungssicherheit. Die historisch konstituierten Sicherheitsdispositive sind also nicht einfach linear hintereinander angeordnet oder durch definitive historische Brüche voneinander getrennt. Vielmehr überlagern sie sich und treten situationsabhängig in immer neue Konstellationen zueinander. Die Geschichte der Sicherheit ist topologisch und damit gewissermaßen gefaltet. Wie Serres (2008a, 93) argumentiert hat, gleicht in einem topologischen Verständnis Geschichte einem Taschentuch, durch dessen Faltungen neue Beziehungen von Nähe und Ferne etabliert werden. Die Machtdispositive können so gleichsam durch historische Wümlöcher miteinander in Beziehung treten.

Als eigenständiger Modus der Sicherheit etabliert sich Resilienz nicht zuletzt durch die Aufdeckung von Problemen der etablierten Sicherheitstechnologien. Strategien der Resilienz versuchen, die Freiheit und Freizügigkeit liberaler Gesellschaften und globaler Zirkulationen aufrechtzuerhalten und blicken daher argwöhnisch auf souveräne Sicherheitsmaßnahmen wie Grenzschießungen und extensive Kontrollen, die diese Zirkulationen behindern und einschränken (Kapitel 2.5.3. und Kapitel 4). Durch die Brille der Resilienz lässt sich der Preis klassischer Techniken der normalisierenden Bevölkerungssicherheit näher bestimmen. Der hohe Grad der Sicherheit der Lebensmittelversorgung geht mit unübersichtlichen Lebensmittelketten einher, in denen sich Gefahrenstoffe einnisten und ausbreiten können (Kapitel 2.4.3.). Die Bekämpfung von Krankheiten durch Antibiotika geht mit der Entstehung von multiresistenten Keimen einher (Kapitel 2.5.4.). Ökologische Kritiker\_innen der technologischen Hochmoderne betonen, dass die Entwicklung großer Infrastrukturnetzwerke im Rahmen der Daseinsvorsorge ökologische Folgeschäden erzeugt (Kapitel 3.2.). Schützer\_innen Kritischer Infrastrukturen betonen die endogenen Gefährdungen hochkomplexer Systeme (Kapitel 3.1.1.). Insbesondere das Festhalten am Leitbild der Normalität steht im Fadenkreuz der Kritik von Rationalitäten der Resilienz. Die Begradigung von Flüssen und die hydrologische Ingenieurskunst, die das natürliche Strömen des Wassers in technisch-kontrollierte Bahnen lenken sollte, steigert die Gefahr katastrophischer

schen Hochwassers (Kapitel 3.2.2.). Die normalistischen Annahmen der *efficient market hypothesis*, die den Technologien des Risikomanagements im Finanzwesen zugrunde liegen, haben zur Entstehung der weltweiten Finanzkrise beigetragen (Kapitel 2.4.4.). Die Normalisierung des Stromnetzes in Form von großen, weitläufigen Netzen, die eine erhöhte Effizienz erlauben, macht großflächige Stromausfälle möglich, die von Katastrophenschützer\_innen gefürchtet werden (Kapitel 3.3.5.). Statt dem unbedingten Beharren auf Dauernormalität und Sicherheit im Alltagsbetrieb, die mit katastrophischen Potenzialen erkaufte werden, setzt Resilienz auf fehlertolerante Designs, die Störungen des Normalfalls zulassen, um Katastrophen zu vermeiden. Diese Abkehr vom Willen zur vollständigen Risikovermeidung setzt die Resilienz bisweilen auch in einen Gegensatz zur Politik des Vorsorgeprinzips (Kapitel 3.2.1.) ebenso wie zu drastischen Maßnahmen der *preemption* (siehe Exkurs II), die versuchen, potenziell katastrophische Ereignisse vorbeugend zu verhindern.

Derartige Problematisierungsbewegungen schließen Kompromisse, Kombinationen und Hybridisierungen zwischen verschiedenen Formen der Sicherheit keineswegs aus. Klimaschutz – *precaution* – soll durch Klimawandelanpassung – *preparedness* – ergänzt, nicht ersetzt werden (Kapitel 3.2.3.). Souveräne Staatsmacht endet unter Bedingungen der Biopolitik vitaler Systeme nicht, sondern muss beginnen, sich selbst als vitales System zu beobachten und zu schützen (Kapitel 4.1.2.). Und natürlich gehören die Biopolitik der Bevölkerung und die Biopolitik vitaler Systeme aufs Engste zusammen (siehe Exkurs II). Dass normalisierende biopolitische Maßnahmen lebensnotwendig sind und dennoch eigene Risiken bergen, macht das zentrale Dilemma gegenwärtiger Sicherheitsdispositive aus. Das Sicherheitsdispositiv der Resilienz reagiert also nicht nur auf »neue« Sicherheitsprobleme – Terror, Pandemie, Cyberkriminalität –, sondern ebenso auf ein Problematisch-Werden der Sicherheit selbst. Deshalb fügt es der »historischen Landkarte« der Sicherheit nicht einfach nur ein neues Territorium hinzu, sondern faltet sie auf eine neuartige Weise, wodurch es zu »neuen« Kombinationen und Konfliktkonstellationen kommt.

Das Sicherheitsdispositiv schreibt sich aber nicht nur in eine längere Tradition des Schützens und Sicherns ein, sondern enthält auch spezifische Entwicklungspotenziale und latente Trajektorien. Es ist von Fluchtlinien und Tendenzen durchzogen, die über das Hier und Jetzt hinausgehen und dessen »Werden« gewährleisten (das Werden des Dispositivs betont vor allem: Deleuze 1991). Die mühevolle Entstehungsgeschichte des Disposi-

tivs bleibt als sein Gedächtnis präsent und spannt so ein Feld geteilter Problemlagen und konditionierter Möglichkeiten auf, das zukünftige Reaktionsbildungen nicht determiniert, aber mehr oder weniger wahrscheinlich macht.

Die Matrix der Risikoanalyse etabliert ein epistemisches Raster der Antizipation von Katastrophen, das nicht nur gegebene Notfälle registrierbar und bearbeitbar macht, sondern auch neue Problemfälle und Anwendungsbereiche identifiziert und damit Entwicklungs- und Erweiterungstendenzen von Sicherheitstechnologien ermöglicht (Kapitel 2.3.2.). Es scheint bisweilen so, als gäbe es nicht nur Ablaufprotokolle für den Notfall, sondern so etwas wie Phantomprotokolle, die von niemandem niedergeschrieben werden und dennoch *rapid responses* auf neue Situationen wahrscheinlich machen. Obwohl politischer Protest in keinem Programm, keinem Standard des BCM als Gefahrenquelle angesprochen wurde, konnten die Kontinuitätsmanager\_innen von Frankfurter Banken die Blockupy-Proteste schnell zum Anwendungsbereich betrieblicher Kontinuitätsstrategien machen und damit eine nur implizite Tendenz des Dispositivs entfalten (Kapitel 4.4.3.). Gerade die Verpflichtung darauf, keine konkreten Krisenszenarien auszumalen, sondern sich auf »generische« Katastrophen vorzubereiten, soll schließlich das paradoxe Unterfangen ermöglichen, das Unerwartete zu erwarten.

Diese relative Offenheit des Sicherheitsdispositivs macht auch verständlich, warum selbst offensichtliche »funktionale [...] Defizite« (Foucault 2004, 176) des Dispositivs kein »Scheitern« bedeuten müssen, sondern nicht selten durch »strategische Wiederauffüllung« (Foucault 1978, 121) zu Ausgangspunkten der Erschließung von neuen Funktionen und Anwendungsbereichen der Sicherheitstechnologien werden. Auch wenn die Stabilitätsmechanismen in der Eurozone nicht zur gewünschten Währungsstabilität und ökonomischen Prosperität der Euroländer geführt haben, erlauben sie es doch, die Krisenstaaten einer permanenten und kleinlichen fiskalpolitischen Kontrolle auszusetzen (Kapitel 2.5.2.). Für viele Sicherheitsexpert\_innen zeigt jede Katastrophe vor allem auf, dass »wir noch nicht genug vorbereitet sind«, dass wir »noch resilienter« werden müssen (Kapitel 4.4.1.). Widerstandskraft und Krisenfestigkeit können nur durch ständig erneuerte Anpassungen an eine sich ständig verändernde Gefahrenumwelt erreicht werden. Eingetretene Krisen, die Schwachstellen von Sicherheitsstrategien offen gelegt haben, bieten lehrreiche Einsichten für bessere Vorbereitung auf die kommende Katastrophe.

Die Analytik des Sicherheitsdispositivs der Resilienz leistet einen Beitrag zur soziologischen Gegenwartsdiagnose, indem sie nicht nur einen institutionellen bzw. gesellschaftlichen Teilbereich wie den Katastrophenschutz untersucht, sondern die Wirksamkeit analoger Sicherheitstechnologien quer durch die Gegenwartsgesellschaft aufgezeigt hat. Die Gesellschaftsdiagnose verfolgt jedoch keinen radikalen Anspruch, sondern geht transversal vor. Es ging also nicht um die Analyse eines integralen Prinzips, das die Gesellschaft als Ganze strukturiert (etwa Industriegesellschaft oder Risikogesellschaft), sondern darum, den rhizomatischen Verzweigungen eines bestimmten Typus der Versicherheitlichung durch unterschiedliche Bereiche zu folgen und ihre je spezifischen Effekte zu analysieren. Das Sicherheitsdispositiv durchzieht die Gegenwartsgesellschaft wie ein Straßennetz, das es erlaubt, viele zentrale Orte der Gegenwart anzusteuern, das aber keineswegs das gesamte Territorium des Sozialen abdeckt. Es ging weder darum, eine integrale Sicherheitsgesellschaft zum Vorschein zu bringen, noch die »Sicherheit der Gesellschaft« zu untersuchen und damit Sicherheit zu einem gesellschaftlichen Teilbereich eines größeren gesellschaftlichen Ganzen zu machen. Statt von einer fixen gesellschaftlichen Totalität auszugehen, wurde stattdessen gezeigt, welche Arten der Sozialität von den Netzen der Sicherheit selbst gesponnen werden. Das Sicherheitsdispositiv stützt sich nämlich auf eine ganz eigene Version des Gesellschaftlichen, die zu schützen es sich anschickt. Im reflexiven Blick auf gesellschaftliche Verwundbarkeiten wird Gesellschaft als interdependentes Netz sozio-materieller Anschlüsse erfahrbar, dessen zunehmende Komplexität zum Sicherheitsproblem geworden ist (Exkurs I). Dabei verschwimmen nicht nur die Grenzen zwischen sozialen Subsystemen, die alle als von der gleichen Infrastruktur abhängig betrachtet werden, sondern auch die Grenzen zwischen sozio-technischen Systemen und ihren natürlichen Umwelten. Die Externalitäten ersterer gefährden die Funktion letzterer, was wiederum die Umweltbedürftigkeit der Gesellschaft sichtbar und Ökosysteme selbst zu vitalen *life support systems* macht (Kapitel 3.2.4. und Exkurs II). Derartige Erfahrungen von Verwundbarkeit und Abhängigkeit transzendieren klassische Unterscheidungen zwischen sozialen Subsystemen, von Technik und Politik, Natur und Gesellschaft und verweisen damit auf die Grenzen der »Soziologie des Sozialen« (Latour 2007). Die Analytik der Sicherheit setzt an dieser Problemstellung an und nimmt sie ernst, versucht jedoch nicht sie schlicht für eine alternative Ontologie der Sozialität zu rekrutieren. Stattdessen habe ich ausgehend von den untersuchten Prob-

lemstellungen und Krisenerfahrungen versucht, eine Ontologie der Gegenwart herauszuarbeiten und ihr gegenüber eine kritische Distanz zu bewahren.

### *Kritik der Sicherheit*

Durch die Untersuchung vieler unterschiedlicher Anwendungsfälle und Einsatzbereiche des Sicherheitsdispositivs der Resilienz hat sich vor allem die Ambivalenz der beschriebenen Sicherheitsmaßnahmen gezeigt. So konnten auch die Vereinseitigungen und Pauschalisierungen der gängigen sozialwissenschaftlichen Kritik der Sicherheit und der Resilienz vermieden werden. Während etwa Filipa Lentzos und Nikolas Rose (2009, 243) argumentieren, dass Resilienz eine Alternative zum »big brother state« darstelle, sehen Melinda Cooper (2011) und Jeremy Walker (Cooper und Walker 2011) in Resilienz einen neoliberalen Katastrophismus, in dem Systeme fernab vom Gleichgewicht begrüßt und auch Störungen und Katastrophen noch als produktiv betrachtet werden. Während einige Autor\_innen die unabschließbare Ausweitung der Sicherheitsdispositive befürchten, weil man »nie sicher genug« sein kann (Bröckling 2012, 103), sehen andere in Resilienz eine Reduktion der Sicherheit durch einen Rückzug staatlicher Sicherheitspolitik, die nicht mehr vor Katastrophen schützen kann, sondern nur noch zur Vorbereitung auf das Unvermeidliche aufruft (Amin 2013). Diese Kritikpunkte und Einschätzungen sind nicht falsch, sie treffen aber jeweils nur gewisse Tendenzen des Sicherheitsdispositivs. Unangemessen werden sie, wenn sie diese Tendenzen generalisieren und damit die performative Flexibilität und Ambivalenz der untersuchten Sicherheitstechnologien unterschlagen.

Die Bankenrettung im Rahmen der *too big to fail*-Logik ist offensichtlich problematisch gewesen, weil sie die Verantwortlichen durch Verweis auf die Interdependenz und Komplexität des Finanzwesens nicht zur Rechenschaft gezogen hat. Die Ausarbeitung der Kategorie systemisches Risiko infolge der Finanzkrise hat allerdings Regulationsbemühungen des Finanzwesens ermöglicht, die Großbanken stärker in die Pflicht nehmen (Kapitel 2.5.2. und 2.5.3.). Eine konsequente Umsetzung der Rationalität der Resilienz bei der Finanzmarktregulation hat das Potenzial, gefährliche Effizienz- und Optimierungsphantasmen des Finanzwesens und der neoklassischen Wirtschaftstheorie hinter sich zu lassen (Kapitel 2.5.4.). Die Kritik an technischem Hochwasserschutz und staatlicher Flutversicherung

stellt Kernelemente staatlicher Katastrophenvorsorge in Frage. Sie artikuliert aber ebenso Anliegen des Umwelt- und Naturschutzes und tritt für einen anderen, ökologischen Hochwasserschutz ein (Kapitel 3.2.2.). Tatsächlich werden soziale Verwundbarkeiten bisweilen vernachlässigt, wenn der Fokus auf der Sicherung vitaler Systeme liegt. Meine Untersuchung zum Schutz Kritischer Infrastrukturen hat aber auch gezeigt, wie hier Unternehmen in die Pflicht genommen werden, einen Beitrag zur öffentlichen Sicherheit zu leisten (Kapitel 3.1.3.). Tatsächlich vollendet sich in der Logik vitaler Systeme bisweilen der kybernetische Traum, die Welt, das Leben als Ganzes unterschiedslos als System zu beschreiben, das unter technische Kontrolle gestellt werden kann und muss (Braun und Wakefield 2014a). Die Erdsystemforschung und Programme zur »grünen Infrastruktur« erlauben es aber auch, die anthropozentrischen Beschränkungen der Sicherheitspolitik zu überwinden und auch nicht-menschliches Leben als Objekt des Schutzes zu verstehen. Indem das »natürliche Kapital« von »Ökosystemdienstleistungen« betont wird, kommt es zu einer ökonomischen, aber auch sicherheitspolitischen Aufwertung der »Umwelt« (Kapitel 3.2.4.). Tatsächlich kann Resilienz und Katastrophenvorbereitung eine Alternative zu staatlicher Überwachung und Notstandspolitik darstellen. Im Namen der Resilienz vitaler Systeme kann aber auch politischer Protest unterbunden, können also demokratische Rechte eingeschränkt werden, wie das Beispiel Blockupy gezeigt hat (Kapitel 4.4.3.). Resilienz kann als Kritik der Sicherheit ins Spiel gebracht werden (Kapitel 2.5.4.), kann aber auch zur Immunisierung gegen Kritik beitragen, weil jedes Scheitern der Sicherheitsdispositive als Teil eines umfassenden Prozesses permanenter Adaption beschrieben werden kann (Kapitel 4.4.1.).

Die Ambivalenz von Sicherheitstechnologien der Resilienz ist groß, aber nicht beliebig. Das Sicherheitsdispositiv eröffnet eine spezifische »historische Ontologie« (Foucault 2005i, 702), ein Möglichkeitsfeld, in dem einige Optionen eröffnet und andere verschlossen werden. Diese Ontologie ist selbst nicht politisch im Sinne von links oder rechts, fortschrittlich oder konservativ, sondern bildet überhaupt erst eine Grundlage für politische Auseinandersetzungen (Marquardt 2016, 313). In diesem Sinne führt Sicherheit nicht zu einer Depolitisierung,<sup>240</sup> sondern ermöglicht politische Positionierungen, erzeugt Konfliktlinien und macht bestimmte Formen des Widerstandes und der Kritik wahrscheinlich. Eine wahrscheinliche und

---

240 So lautet etwa der Grundtenor von Mark Neocleous' (2008) einflussreicher *Critique of Security*.

gleichsam immanente Kritik besteht im Nachweis von Paradoxien der Sicherheit. Solche Formen der technischen Kritik der Sicherheit denunzieren etwa den *levee effect* im Hochwasserschutz (Kapitel 3.2.2.), die *moral hazards* bei der Regulation des Finanzmarktes (Kapitel 2.5.4.) oder weisen auf das Verwundbarkeitsparadoxon hin, mit dem Projekte zum Schutz Kritischer Infrastrukturen (Kapitel 3.1.3.) konfrontiert sind. Diese internen Kritiken haben eine aufschlussreiche Doppelrolle: Durch ihre Kritik reprogrammieren sie zugleich die Sicherheitspraktiken, etwa wenn Lovins und Lovins die »energy strategy« der USA mit Bezug auf einen sanften, resilienten Energiepfad kritisieren (Kapitel 3.3.2.). Wie gezeigt kann Resilienz nicht zuletzt selbst als Kritik überzogener Sicherheitsansprüche begriffen werden (2.5.4.).

Allerdings habe ich nicht nur Kritik »innerhalb« des Sicherheitsdispositives analysiert, sondern auch radikalere Infragestellungen aktueller Sicherheitpraktiken in den Blick genommen, die den von Resilienztechnologien gesetzten ontologischen Rahmen verlassen. Stellvertretend für andere Bewegungen Disruptiver Demokratie, die durch Unterbrechungen infrastruktureller Operationen Aufmerksamkeit für ihre Forderungen generieren, wurden die Protestaktionen des Blockupy-Bündnisses in Frankfurt untersucht (siehe Kapitel 4.4.3.). Weil die Blockupy-Demonstrant\_innen versucht haben, das Frankfurter Bankenviertel zu blockieren, wurden sie selbst als Unterbrechungsrisiko wahrgenommen. Die Proteste, Ziele und Forderungen von Bewegungen der Disruptiven Demokratie, die von streikenden Hafentarbeiter\_innen bis zu den Protesten gegen Castortransporte reichen (Kapitel 3.3.2.), evozieren eine alternative Ontologie von »Kritischen Infrastrukturen« und orientieren sich an einem anderen zeitlichen Horizont als das Sicherheitsdispositiv der Resilienz (Kapitel 4.3.3.). Infrastrukturen sind für diese Bewegungen nicht Objekte des Schutzes, sondern ein Terrain für politische Auseinandersetzungen. »Kritisch« sind die Infrastrukturen, weil sie von Protestgruppen bevölkert werden und nicht, weil davon ausgegangen wird, dass vitale gesellschaftliche Funktionen von ihnen abhängen. Bewegungen Disruptiver Demokratie verschreiben sich nicht der temporalen Logik der Kontinuität, um die Gegenwart vor einer bedrohlichen Zukunft zu schützen, sondern wollen Unterbrechungen und Diskontinuitäten erzeugen, um die Gegenwart für eine bessere Zukunft zu öffnen. Damit ruft dieser Protest eine über das gebannte Starren auf die Zukunft als Katastrophe allzu oft vergessene Perspektive wach: Es geht hier um Emanzipation und nicht um Sicherheit. Gefragt wird nicht: »Sind

wir vorbereitet, wie kann es weiter gehen?«, sondern: »Wie ist eine andere Welt möglich, wie kann es ganz anders weiter gehen?«

Indem ich Kritiken der Sicherheit zum Gegenstand der Analytik des Sicherheitsdispositivs der Resilienz gemacht habe, habe ich zugleich eine bestimmte Kritikstrategie verfolgt, die bis zu einem gewissen Grad Ähnlichkeiten mit dem Programm der »Soziologie der Kritik« (Boltanski und Thévenot 2007) hat, die versucht nicht nur aus der externen Beobachtungsperspektive Kritik zu üben, sondern »Kritik als soziale Praxis« (Celikates 2009) zu betrachten. Auf diese Weise lassen sich die Erfahrungen und Expertisen der Akteure angemessen würdigen und zudem als heuristisches Werkzeug mobilisieren. Die Untersuchung von Kritik hatte also nicht bloß das quasi forschungsethische Motiv, den Anliegen der Akteure gerecht zu werden, anstatt sie als bloßen Effekt verborgener Strukturen oder Mächte abzutun. Durch die Untersuchung von Auseinandersetzungen über und die Infragestellungen von Sicherheitstechnologien konnte gezeigt werden, wie die Ambivalenz von Sicherheitsmaßnahmen von unterschiedlichen Akteuren der Sicherheit performativ zur Geltung gebracht wird. Ambivalenzen und Paradoxien der Sicherheit wurden somit aus der Binnenperspektive rekonstruiert. Zudem wurden Kritik und »Widerstand als chemischer Katalysator« benutzt, um etwas an den Sicherheitstechnologien sichtbar werden zu lassen, was lediglich mit »Blick auf ihre innere Rationalität« (Foucault 2005f, 273) verdeckt geblieben wäre. Denn erst »über das Wechselspiel gegensätzlicher Strategien« (Foucault 2005f, 273) wird deutlich, dass Technologien der Sicherheit nicht bloß die quasi notwendige Reaktion auf externe Gefährdungen sind, sondern zugleich ein Machtverhältnis darstellen.

Aber was heißt es genau, Sicherheit als Machtverhältnis zu bestimmen, ohne den üblichen Fallstricken der Machtkritik zu erliegen? Wie kann man die Macht der Sicherheit kritisieren, ohne ihr einen geheimen Funktionalismus zu unterstellen und hinter den scheinbar »guten« Absichten der Sicherheit nur ebenso subtile wie perfide Strategien zu vermuten? Wie kann man Sicherheit als Macht kritisieren und das Verlangen nach und den Wert von Sicherheit dennoch ernst nehmen? Wie kann man »die Macht« also tatsächlich als Verhältnis von Kräften und nicht als monolithischen Block verstehen und kritisieren? Und natürlich: was ist das Spezifische des Machtverhältnisses der Sicherheit? Die zunehmende Versicherheitlichung der Existenz wird nicht erst in der Gegenwart mit Skepsis beobachtet. Darauf verweist etwa die aufschlussreiche Etymologie des englischen Wor-



tes *danger*, das sich vom normannischen *dan* für Schutzherr herleitet. »Being dependent on a dan, being in his power or indebted to him, was expressed as »being in danger.« (Dumm 1987, 7) Das spezifische Machtverhältnis der Sicherheit besteht demnach darin, dass sie zwar ein Schutzverhältnis, damit einhergehend aber auch eine Abhängigkeitsbeziehung zwischen Instanzen der Sicherheit und Ge- bzw. Versicherten etabliert. Durch diese Abhängigkeit stehen die Versicherten in der Schuld bzw. in der Macht der Schutzgewalten. Sie sind durch diese Macht in einem eminenten Sinne verwundet und ausbeutbar. Darum ist Sicherheit gefährlich.

Daran hat sich bis heute nichts grundlegend geändert. Ja, vielleicht ist die Ambivalenz der Sicherheitsbeziehung heute sogar noch intensiver geworden. Wir sind heute nicht mehr nur von Schutzherr\_innen abhängig, die uns vor der Gewalt anderer schützten, nicht mehr nur an einen Leviathan ausgeliefert, der bissige Wölfe voneinander fernhält. Vielmehr sind wir zusätzlich auf die zeitgenössischen Techniken der Sicherheit angewiesen, die nicht so sehr versuchen, die Teile eines hybriden Kollektivs durch Isolation voneinander zu schützen, sondern verhindern wollen, dass die Anschlüsse entkoppelt und die vitalen Flüsse unterbrochen werden (Exkurs I). Gerade biopolitisch-liberale Formen der Sicherheit sind keine bloß äußerlichen Sicherungen von territorialen Grenzen, souveränen Staaten und der »negativen Freiheit« bornierter Besitzindividualist\_innen. Es sind positive Formen der Sicherheit, die das Leben schützen und fördern und die liberale Freizügigkeit überhaupt erst ermöglichen, leb- und vollziehbar machen. Die Mittel dieser Sicherheit sind nicht bloß Mauer und Zaun, Schwert und Kanonenboot, sondern Straßenbau und Kanalisation, Impfstoff und Rettungshubschrauber. Die Deckungsreserve biopolitischer Sicherheitsdispositive sind nicht kasernierte Gewaltmittel, sondern Lebensmittel- und Rohstofflager für den Krisenfall. Durch diesen Positivierungs- und Materialisierungsprozess ist Sicherheit nicht länger bloß die Abwesenheit von Gefahr, sondern besteht in der dauerhaften Anwesenheit substanzialer Versorgungsgüter, auf die das Leben der Bevölkerung angewiesen ist (Kapitel 3.3.5.).

Das heißt nicht, dass das Überleben zuvor nicht auf derartige Versorgungsgüter – Nahrungsmittel, Trinkwasser, Energiequellen, medizinische Versorgung – angewiesen war. Aber erst im Verlauf der Moderne ist diese Versorgung zu einer öffentlichen Angelegenheit, zu einem politischen Anspruch und Projekt geworden, so dass heute das Leben auf die Unterstützung einer Reihe von Sicherungsinstanzen existenziell angewiesen ist.

Im Zuge dieser »Politisierung der Sicherheit« (Gros 2015), die mit einer umfassenden Politisierung des Lebens einhergeht, wurden Schritt für Schritt die Netze der Angewiesenheit expliziert und zu einem Sicherheitsprojekt gemacht: die Angewiesenheit der Stadtbewohner\_innen auf Nahrungsmittel, die Versorgung der Bevölkerung mit infrastrukturellen Leistungen (Kapitel 3.1.1.) und schließlich der Schutz der bedrohten Biosphäre (Kapitel 3.2.4.). Die Sicherheitsdispositive haben sich im Zuge dieses versicherheitlichenden Entfaltungsprozesses in einer zuvor kaum vorstellbaren Weise ausgeweitet. Sicherheit hat sich in unser Leben gefressen, in das Privateste, Intimste, Vitalste unserer Existenz hinein (in Form von Hygieneinfrastrukturen, *safer sex*, Atemschutzmasken gegen verpestete Luft) und sich zugleich an den gigantischsten Systemen (dem planetarischen Ökosystem, der Atomsphäre) festgemacht (Exkurs II). Damit ist nicht zuletzt auch der Schutz vor Katastrophen, die lange schlicht als »höhere Gewalt« dem menschlichen Einfluss entzogen schienen, zu einem politischen Anspruch geworden. Die Katastrophe ist zwar nicht vollständig beherrschbar, aber doch regierbar geworden. Gerade diese Fortschritte der Sicherheit, das »Anwachsen der Fähigkeiten« zum Schutz des Lebens, hat zugleich eine »Intensivierung der Machtbeziehungen« (Foucault 2005i, 705) bewirkt. Denn die Abhängigkeit des Lebens von Technologien der Sicherheit und funktionierenden Vitalsystemen ist immer größer geworden. Sicherheit schirmt vor Gefahren ab, setzt das geschützte Leben dadurch aber unweigerlich dem eigenen Zugriff aus. Durch ihr gesteigertes Sicherheitsbedürfnis und ihre gewachsene Schutzbedürftigkeit sind die Versicherten immer beherrschbarer geworden.

Die Spezifik des Machtverhältnisses »Sicherheit« – die Gleichzeitigkeit von Schutz und Abhängigkeit – macht Sicherheit zu einem schwierigen Gegenstand der Kritik. Schließlich muss man etwas kritisieren, was zumindest vorgibt, Schutz zu gewähren. Wie jede Kritik geht auch diese ein Risiko ein, weil sie sich gegen das wendet, was die eigene Lebensgrundlage gewährleistet. Man muss die Machtnetze angreifen, an deren Fäden das eigene Leben und Überleben hängt. Das heißt die Kritik kann nicht rein negativ bzw. subtraktiv vorgehen und einfach die »Abschaffung« der Sicherheit fordern. Die verheerenden Auswirkungen der Abwendung sichernder Mächte zeigen sich wohl am deutlichsten im Alltag der verwundbarsten und prekärsten Teile der Weltbevölkerung. Gerade hier wird deutlich, dass auch der Rückzug der Instanzen der Sicherheit gefährlich ist und auch die Entlassung in die Unsicherheit eine Machtbeziehung darstellt,

welche diejenigen im Bann hält, von denen sie sich abwendet.<sup>241</sup> Wenn aber die Kritik der Sicherheit deshalb unterbleibt oder gar – wie im Fall der Bewegungen der Disruptiven Demokratie – aus »Sicherheitsgründen« zurückgewiesen wird, wird das versichernde Machtverhältnis zu einem unent-rinnbaren *double-bind*.

Es ist deswegen kaum verwunderlich, dass Kritiker\_innen der Sicherheit immer wieder den Schutzpakt einseitig aufkündigen wollten und dabei zumeist die Freiheit gegen die Sicherheit ausspielen. Gerade bestimmte liberale, libertäre oder anarchistische Formen der Sicherheitskritik streben eine Limitierung oder gar vollständige Abschaffung der Mächte der Sicherheit an. Damit verkennen sie aber, dass liberale Sicherheitstechnologien diese Kritik bereits aufgenommen haben und stets bestrebt sind, eine bestimmte Form der Freiheit zu schützen und zu ermöglichen, die nicht fix und fertig da ist, sondern selbst das voraussetzungsreiche Produkt sozialer Prozesse. Indem sie diese Voraussetzungen der Freiheit übersieht, hat die libertäre Kritik der Sicherheit im Namen personaler Autonomie häufig einen souveränistischen Bias im doppelten Sinne: Sie imaginiert Sicherheit als souveräne Macht, die ebenso souveräne, autonome Subjekte äußerlich einschränkt. Statt von der personalen *Autonomie souveräner Subjekte* muss von der grundlegenden *Verwundbarkeit des Lebens* ausgegangen werden, wie sie vor allem von feministischen Autor\_innen wie Judith Butler (2009, 2004) und Donna Haraway (2014, 177) theoretisiert wird. Verwundbarkeit ist hier kein besonderer Zustand eines Lebens oder Systems, der sich durch mehr Sicherheit oder Resilienz reduzieren ließe, sondern eine Grundbedingung des Lebens überhaupt: »a generalized condition, it is, paradoxically, the condition of being conditioned« (Butler 2009, 23), »one's life is always in some sense in the hand of the other« (Butler 2009, 14). Verwundbarkeit ist damit eine grundlegende Eigenschaft des Lebens, aber nicht nur als »Leben selbst«, sondern als Leben-in-Beziehungen, als Leben jenseits seiner selbst: »in order to ›be, in the sense of ›persist, it must rely on what is

---

241 Giorgio Agamben (2002, 39) hat am konsequentesten Macht als Beziehung des Banns (im Sinne von Verbannung und unter das Banner der Macht gestellt sein) beschrieben. »Die originäre Beziehung des Gesetzes mit dem Leben ist nicht die Anwendung, sondern die *Verlassenheit* [...]. Die unüberbietbare Potenz des *nómos* [...] besteht darin, daß er das Leben in seinen Bann hält, indem er es verläßt.« (Hervorhebung im Original) Allerdings hat Agamben die Beziehung des Banns nur für souveräne Machtformen gedacht. Im Rahmen der Biopolitik vitaler Systeme besteht der Bann darin, das Leben zu entnetzen und es so einer »Zone infrastruktureller Entkopplung« (Marquardt 2017), im schlimmsten Fall dem Tod zu überlassen (Kapitel 3.1.1.).

outside itself« (Butler 2009, 33). Als eine solche Bedingung kann Verwundbarkeit niemals einfach vermieden werden, ohne zugleich die Offenheit des Lebens für andere und anderes zunichte zu machen. »Leben ist ein Fenster der Verwundbarkeit: es zu schließen, wäre ein Fehler.« (Haraway 2014, 177) In diesem Sinne ist Verwundbarkeit nicht bloß ein Makel, der zu Kraftlosigkeit und Passivität verdammen würde, sondern kann zur Grundlage der Bildung widerständiger politischer Kollektive werden (Butler, Gambetti und Sabsay 2016). Verwundbarkeit als *Bedingung der Bedingtheit* zu affirmieren, heißt deshalb auch nicht, *Zustände* der Verwundbarkeit oder gar Verwundungen und Beziehungen ausbeuterischer Abhängigkeit zu akzeptieren.

Die *Ethik der Verwundbarkeit* eröffnet die Grundlage für eine sowohl *kritische* als auch *affirmative Politik der Sicherheit*. Sicherheit wird nicht rundheraus abgelehnt oder anderen Werten gegenübergestellt, sondern als Recht und Lebensnotwendigkeit eingefordert und zugleich einer Kritik unterzogen, die vom Willen getragen ist, nicht *so* versichert zu werden! »[N]icht derartig, im Namen dieser Prinzipien da, zu solchen Zwecken und mit solchen Verfahren.« (Foucault 1992, 11) Nicht so, dass nur die Großen und Mächtigen geschützt werden und die Ungleichverteilung der Verwundbarkeit dadurch weiter wächst. Nicht um den Preis, dass effektiver Widerstand im Namen der Sicherheit verhindert wird. Nicht um den Preis, dass Sicherheit den politischen Horizont kolonisiert und die Frage, ob wir auf die kommende Katastrophe vorbereitet sind, Fragen nach einer anderen und besseren Zukunft gänzlich überblendet. Diese Kritik der Sicherheit entrichtet nicht länger das Schutzgeld an die Macht, sondern erstellt eine sicherheitspolitische Gegenkalkulation.

Diese Arbeit kann solche faktischen Kritiken der Sicherheit nicht ersetzen. Sie ist auch nicht kritisch im Sinne eines evaluativen Ratschlags über die Güte dieser oder jener Sicherheitstechnologie oder gar im Sinne einer pauschalen Denunziation des Resilienzdispositivs. Die Analyse des Sicherheitsdispositivs als wesentlicher Bestandteil der Ontologie unserer Gegenwart erlaubt es aber sehr wohl, in »der Kontingenz, die uns zu dem gemacht hat, was wir sind, [...] die Grenzen, die wir überschreiten können« (Foucault 2005i, 703), zu identifizieren. So kann die Arbeit helfen zu erkennen, was nicht (mehr) notwendig ist, was nicht so »vital« oder »kritisch« ist wie vorgegeben. Sie kann helfen, sicherheitspolitische Alternativen klarer zu sehen und die eigene Positionierung im Feld der Sicherheit zu reflek-

tieren. Und genau das kann einer Kritik an den intolerablen Formen der Sicherheit Gestalt geben.

# Abkürzungen

AKNZ	Akademie für Notfallplanung und Zivilschutz
ATF	Analytische Task Force
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BCM	Business Continuity Management
BIA	Business Impact Analyse
BImSchG	Bundesimmissionsschutzgesetz
BIS	Bank for International Settlements
BKA	Bundeskriminalamt
BMBF	Bundesministerium für Bildung und Forschung
BMELV	Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz
BMF	Bundesfinanzministerium
BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Inneren
BMU	Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit
BMWi	Bundesministerium für Wirtschaft und Technologie
BNetzA	Bundesnetzagentur
BS	British Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
BUND	Bund für Umwelt- und Naturschutz Deutschland e.V.
CBRN	Chemische, Biologische, Radiologische, Nukleare Gefahrenquellen
CRD	Capital Requirements Directive
DAS	Deutsche Anpassungsstrategie an den Klimawandel

deNIS	Deutsches Notfallinformationssystem
DHS	Department of Homeland Security
EFSF	European Financial Stability Facility
EKSE	Ethik-Kommission Sichere Energieversorgung
EMH	Efficient Market Hypothesis
EMIR	European Market Infrastructure Regulation
EnSiG	Gesetz zur Sicherung der Energieversorgung (Energiesicherungsgesetz)
EnWG	Gesetz zur Förderung der Energiewirtschaft (Energiewirtschaftsgesetz)
ESM	European Stability Mechanism
EZB	Europäische Zentralbank
FEMA	Federal Emergency Management Agency
FMI	Financial Market Infrastructure
FSB	Financial Stability Board
GI	Grüne Infrastruktur
GIS	Geographische Informationssysteme
GMLZ	Gemeinsames Melde- und Lagezentrum
GRASB	Szenariorientierte Grundlagen und innovative Methoden zur Reduzierung des Ausfallrisikos der Stromversorgung unter Berücksichtigung der Auswirkungen auf die Bevölkerung
IMK	Innenministerkonferenz
IOSCO	International Organization of Securities Commissions
IPCC	Intergovernmental Panel on Climate Change
ISO	International Organization for Standardization
KRITIS	Kritische Infrastrukturen
LCR	Liquidity Coverage Ratio
LÜKEX	Länderübergreifende Krisenmanagement-Übung/Exercise
MANV	Massenanfall von Verletzten
MTF	Medizinische Task Force
MRE	Multi-resistente Erreger

---

NBB	National Bank of Belgium
NHWSP	Nationales Hochwasserschutzprogramm
NSFR	Net Stable Funding Ratio
NYSE	New York Stock Exchange
Op. Risk	Operational Risk
OTC	Over the Counter
PCCP	President's Commission on Critical Infrastructure Protection
PIK	Potsdam Institut für Klimafolgenforschung
RKI	Robert Koch Institut
RSK	Reaktorschutzkommission
RTGS	Real Time Gross Settlement Systems
SEPA	Single European Payment Area
SIFI	Systemically Important Financial Institution
SIPS	Systemically Important Payment Systems
TAB	Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag
THW	Technisches Hilfswerk
UBA	Umweltbundesamt
ÜNB	Übertragungsnetzbetreiber
VDN	Verband Deutscher Netzbetreiber
WBGU	Wissenschaftlicher Beirat der Bundesregierung Globale Umweltveränderungen
WHO	World Health Organization (Weltgesundheitsorganisation)
Zös	Zukunftsforum öffentliche Sicherheit
ZSKG	Gesetz über den Zivilschutz und die Katastrophenhilfe des Bundes (Zivilschutz- und Katastrophenhilfegesetz)



# Interviews

Kürzel im Text	Jahr	Funktion
Interview 1	2012	Referatsleitung Kritische Infrastruktur BBK
Interview 2	2012	Arbeitsbereich Kritische Infrastruktur und Klimawandelanpassung BBK
Interview 3	2013	Arbeitsbereich Ausfallsicherheit der Stromversorgung BBK
Interview 4	2012	BCM in deutscher Bank. Internationaler Koordinator der Kontinuitätsplanung der Bank und Zuständiger für BCM der Niederlassung in Frankfurt
Interview 5	2013	Business Continuity Management und Operational Risk Management in der Niederlassung der deutschen Bank in New York
Interview 6	2012	Unternehmensberatung mit Schwerpunkt auf Prozessmanagement und Business Continuity Management

# Literatur

- Abrahamsson, Carl Christian (2013) On the genealogy of Lebensraum. *Geographica Helvetica*. 68 (1): 37–44.
- Adey, Peter und Ben Anderson (2011) Event and anticipation: UK Civil Contingencies and the space–times of decision. *Environment and Planning A*. 43 (12): 2878–2899.
- Adey, Peter und Ben Anderson (2012) Anticipating emergencies: Technologies of preparedness and the matter of security. *Security Dialogue*. 43 (2): 99–117.
- Agamben, Giorgio (2002) *Homo Sacer. Die souveräne Macht und das nackte Leben*. Frankfurt a.M.: Suhrkamp.
- Agamben, Giorgio (2004) *Ausnahmezustand*. Frankfurt a.M.: Suhrkamp.
- Agamben, Giorgio (2008) *Was ist ein Dispositiv?* Zürich: diaphanes.
- Agamben, Giorgio (2009) *Signatura rerum. Zur Methode*. Frankfurt a.M.: Suhrkamp.
- Agamben, Giorgio (2011) *The kingdom and the glory: For a theological genealogy of economy and government*. Stanford: Stanford University Press.
- AKNZ (2001) Kehren die Seuchen zurück? (Neue) Gefahren durch biologische Kampfstoffe. Bonn: Akademie für Notfallplanung und Zivilschutz.
- Akrich, Madeleine (2006) Die De-Skription technischer Objekte. In: *ANThology. Ein einführendes Handbuch zur Akteur Netzwerk Theorie*. Herausgegeben von: Andrea Belliger und David J. Krieger, 407–428. Bielefeld: transcript.
- Allianz (2008) Katastrophenschutz auf dem Prüfstand. Analysen, Prognosen und Empfehlungen für Deutschland. München: Allianz Versicherung.
- Althusser, Louis (2010) *Der Materialismus der Begegnung*. Zürich: diaphanes.
- Amin, Ash (2013) Surviving the turbulent future. *Environment and Planning D: Society and Space*. 31 (1): 140–156.
- Amoore, Louise und Marieke de Goede (2005) Governance, risk and dataveillance in the war on terror. *Crime, Law and Social Change*. 43 (2–3): 149–173.
- Anand, Nikhil (2011) Pressure: The politotechnics of water supply in Mumbai. *Cultural Anthropology*. 26 (4): 542–564.
- Anders, Günther (1980) *Die Antiquiertheit des Menschen: Über die Seele im Zeitalter der zweiten industriellen Revolution (Band 1)*. München: CH Beck Verlag.
- Anderson, Ben (2010) Preemption, precaution, preparedness: Anticipatory action and future geographies. *Progress in Human Geography*. 34 (6): 777–798.

- Anderson, Ben und Peter Adey (2012) Governing events and life: Emergency in UK Civil Contingencies. *Political Geography*. 31 (1): 24–33.
- Anderson, Ben, Peter Adey und Stephen Graham (2015) Special issue: Governing emergencies. *Theory, Culture & Society*. 32 (2).
- Appadurai, Arjun (1986) Commodities and the politics of value. In: *The social life of things. Commodities in cultural perspective*. Herausgegeben von: Arjun Appadurai, 3–63. Cambridge: Cambridge University Press.
- Aradau, Claudia (2007) Law transformed: Guantánamo and the »other« exception. *Third World Quarterly*. 28 (3): 489–501.
- Aradau, Claudia (2010) Security that matters: Critical infrastructure and objects of protection. *Security Dialogue*. 41 (5): 491–514.
- Aradau, Claudia und Rens van Munster (2007) Governing terrorism through risk: Taking precautions, (un)knowing the future. *European Journal of International Relations*. 13 (1): 89–115.
- Aradau, Claudia und Rens van Munster (2011) *Politics of catastrophe: Genealogies of the unknown*. London: Routledge.
- Arendt, Hannah (2007) *Vita Activa oder Vom tätigen Leben*. München: Piper.
- Arnoldi, Jakob (2009) *Alles Geld verdampft. Finanzkrise in der Weltrisikogesellschaft*. Frankfurt a.M.: Suhrkamp.
- Augstein, Rudolf (1977) Atomstaat oder Rechtsstaat. *Der Spiegel*. 28.02.1977.
- Bachelard, Gaston (1974) *Epistemologie. Ausgewählte Texte*. Frankfurt a.M., Berlin, Wien: Ullstein.
- Baecker, Dirk (1991) *Womit handeln Banken? Eine Untersuchung zur Risikoverarbeitung in der Wirtschaft*. Frankfurt a.M.: Suhrkamp.
- Baecker, Dirk (2011) *Organisation und Störung. Aufsätze*. Frankfurt a.M.: Suhrkamp.
- Bafin (2013) Bafin Journal. Mitteilungen der Bundesanstalt für Finanzdienstleistungsaufsicht. Bonn, Frankfurt a.M.: Bundesanstalt für Finanzdienstleistungsaufsicht.
- Baker, Tom und Jonathan Simon (Hg.) (2002) *Embracing risk. The changing culture of insurance and responsibility*. Chicago, London: University of Chicago Press.
- Barad, Karen (2012) *Agentieller Realismus: Über die Bedeutung materiell-diskursiver Praktiken*. Berlin: Suhrkamp.
- Barry, Andrew (2001) *Political machines: Governing a technological society*. London: Athlone Press.
- Barry, Andrew (2006) Technological zones. *European Journal of Social Theory*. 9 (2): 239–253.
- Barry, Andrew (2013) *Material politics: Disputes along the pipeline*. Malden, Oxford: Blackwell.
- Barry, Andrew, Thomas Osborne und Nikolas Rose (Hg.) (1996) *Foucault and political reason. Liberalism, neo-liberalism and rationalities of government*. Chicago, London: University of Chicago Press.
- Bateson, Gregory (1983) *Ökologie des Geistes. Anthropologische, psychologische, biologische und epistemologische Perspektiven*. Frankfurt a.M.: Suhrkamp.

- Bauman, Zygmunt (2000) *Liquid modernity*. Cambridge, Malden: Polity Press.
- Bauman, Zygmunt (2009) *Gemeinschaften: Auf der Suche nach Sicherheit in einer bedrohlichen Welt*. Berlin: Suhrkamp.
- BBK (2005a) 51. und 52. Jahrestagung der Schutzkommission beim Bundesminister des Innern. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.
- BBK (2005b) Schutz und Hilfe. Jahresbericht des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe 2005. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.
- BBK (2006a) Konzept zur überbehördlichen Hilfe bei MANV. Erneuerungen im Zivil-/Katastrophenschutz. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.
- BBK (2006b) Newsletter 8/2006 Wissenswertes aus dem Zentrum Krisenmanagement. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.
- BBK (2007a) Bevölkerungsschutz Magazin 3/2007. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.
- BBK (2007b) Partner im Bevölkerungsschutz. Jahresbericht des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe 2006. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.
- BBK (2008a) Global denken – Lokal handeln. Jahresbericht des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe 2007. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.
- BBK (2008b) Leitfaden für die Einrichtung und den Betrieb einer Notstromversorgung in Behörden und anderen wichtigen öffentlichen Einrichtungen. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.
- BBK (2009a) Anpassungsstrategien an den Klimawandel. Anforderungen an den Bevölkerungsschutz. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.
- BBK (2009b) Von Menschen für Menschen. Jahresbericht des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe 2008. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.
- BBK (2009c) Vulnerabilität Kritischer Infrastrukturen. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.
- BBK (2010a) Methode für die Risikoanalyse im Bevölkerungsschutz. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.
- BBK (2010b) Neue Strategie zum Schutz der Bevölkerung in Deutschland. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.
- BBK (2010c) Schutz von Kulturgut bei bewaffneten Konflikten. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.
- BBK (2010d) Zukunft vielfältig gestalten. Jahresbericht des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe 2009. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

- BBK (2011) Klimawandel – Herausforderungen für den Bevölkerungsschutz. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.
- BBK (2013a) Flyer: Länderübergreifende Krisenmanagement-Übung. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.
- BBK (2013b) Ratgeber für Notfallvorsorge und richtiges Handeln in Not-situationen. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.
- BBK (2014) Stromausfall. Grundlagen und Methoden zur Reduzierung des Ausfallrisikos der Stromversorgung. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.
- BBK und IM-BaWü (2010) Krisenmanagement Stromausfall. Krisenmanagement bei einer großflächigen Unterbrechung der Stromversorgung am Beispiel Baden-Württemberg. Kurzfassung. Heidelberg: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und Innenministerium Baden-Württemberg.
- BBK, AKNZ. (2005c) Problemstudie: Risiken in Deutschland. Gefahrenpotentiale für Staat, Wirtschaft und Gesellschaft aus Sicht des Bevölkerungsschutzes. Teil 1. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Akademie für Notfallplanung und Zivilschutz.
- BBK, AKNZ. (2006c) Problemstudie: Risiken in Deutschland. Gefahrenpotentiale für Staat, Wirtschaft und Gesellschaft aus Sicht des Bevölkerungsschutzes. Teil 2. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Akademie für Notfallplanung und Zivilschutz.
- BBK-Städtetag (2010) Drei Ebenen, ein Ziel: Bevölkerungsschutz. Gemeinsame Aufgabe von Bund, Ländern und Kommunen. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und Deutscher Städtetag.
- Beck, Ulrich (1986) *Risikogesellschaft. Auf dem Weg in eine andere Moderne*. Frankfurt a.M.: Suhrkamp.
- Beck, Ulrich (1988) *Die organisierte Unverantwortlichkeit*. Frankfurt a.M.: Suhrkamp.
- Beck, Ulrich (1993) *Die Erfindung des Politischen. Zu einer Theorie reflexiver Modernisierung*. Frankfurt a.M.: Suhrkamp.
- Beck, Ulrich (1996) *Das Zeitalter der Nebenfolgen und die Politisierung der Moderne*. Frankfurt a.M.: Suhrkamp.
- Beck, Ulrich (2008) *Weltrisikogesellschaft. Auf der Suche nach der verlorenen Sicherheit*. Frankfurt a.M.: Suhrkamp.
- Beck, Ulrich, Anthony Giddens und Scott Lash (1994) *Reflexive Modernisierung. Eine Kontroverse*. Frankfurt a.M.: Suhrkamp.
- Beck, Ulrich und Edgar Grande (2010) Jenseits des methodologischen Nationalismus: Außereuropäische und europäische Variationen der Zweiten Moderne. *Soziale Welt*. 61 (3–4): 187–216.
- Beck, Ulrich und Bruno Latour (2014) Die Apokalypse duldet keinen Sachzwang. *Frankfurter Allgemeine Zeitung*, 15.05.2014.
- Beck, Ulrich und Christoph Lau (2005) Second modernity as a research agenda: theoretical and empirical explorations in the »meta-change« of modern society. *The British Journal of Sociology*. 56 (4): 525–557.

- Beck, Ulrich und Peter Wehling (2012) The politics of non-knowing: An emerging area of social and political conflict in reflexive modernity. In: *The politics of knowledge*. Herausgegeben von: Fernando Domínguez Rubio und Patrick Baert, 33–57. Oxon, New York: Routledge.
- Beniger, James (1986) *The control revolution: Technological and economic origins of the information society*. Cambridge: Harvard University Press.
- Benjamin, Walter (1991a) *Abhandlungen, Gesammelte Schriften. Band I.2*. Frankfurt a.M.: Suhrkamp.
- Benjamin, Walter (1991b) *Anmerkungen zum Begriff der Geschichte, Gesammelte Schriften. Band I.3*. Frankfurt a.M.: Suhrkamp.
- Benjamin, Walter (1991c) *Das Passagen-Werk, Gesammelte Schriften. Band V.1*. Frankfurt a.M.: Suhrkamp.
- Bergson, Henri (2013) *Philosophie der Dauer: Textauswahl von Gilles Deleuze*. Hamburg: Meiner Verlag.
- Beunza, Daniel und David Stark (2003) The organization of responsiveness: Innovation and recovery in the trading rooms of Lower Manhattan. *Socio-Economic Review*. 1 (2): 135–164.
- Bevölkerungsschutzkongress (2012) 8. Europäischer Bevölkerungsschutzkongress. Fachkongress für Katastrophen- und Zivilschutz sowie zivilmilitärische Zusammenarbeit. Bonn, Berlin: Behörden Spiegel Gruppe.
- Bewernitz, Torsten (2010) Die Militarisierung des Arbeiterkampfes. *Direkte Aktion. November/Dezember*.
- Bigo, Didier (2001) Internal and external security(ies): The Möbius Ribbon. In: *Identities, Borders and Orders: Rethinking International Relations Theory*. Herausgegeben von: Mathias Albert, David Jacobson und Yosef Lapid, 91–136. Minneapolis: University of Minnesota Press.
- Bigo, Didier (2006) Internal and external aspects of security. *European Security*. 15 (4): 385–404.
- Bigo, Didier und Anastassia Tsoukala (Hg.) (2008) *Terror, insecurity and liberty: Illiberal practices of liberal regimes after 9/11*. London: Routledge.
- Bijker, Wiebe E. (2002) The Oosterschelde storm surge barrier: A test case for Dutch water technology, management, and politics. *Technology and Culture*. 43 (3): 569–584.
- Bijker, Wiebe E. (2007) Dikes and dams. Thick with politics. *Isis*. 98 (1): 109–123.
- BImSchG (1974) Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche Vorgänge (Bundesimmissionsschutzgesetz).
- BIS (2001) Core Principles for Systemically Important Payment Systems. Basel: Bank for International Settlements. Committee on Payment and Settlement Systems.
- BIS (2004) International Convergence of Capital Measurement and Capital Standards. A Revised Framework (Basel II). Basel: Bank for International Settlements. Basel Committee on Banking Supervision.

- BIS (2008) The interdependencies of payment and settlement systems. Basel: Bank for International Settlements. Committee on Payment and Settlement Systems.
- BIS (2010) Basel III: A global regulatory framework for more resilient banks and banking systems. Basel: Bank for International Settlements. Basel Committee on Banking Supervision.
- BIS (2013) Basel III: The Liquidity Coverage Ratio and liquidity risk monitoring tools. Basel: Bank for International Settlements, Basel Committee on Banking Supervision.
- BIS (2014) Basel III: The Net Stable Funding Ratio. Basel: Bank for International Settlements, Basel Committee on Banking Supervision.
- BIS und IOSCO (2012) Principles for financial market infrastructures. Basel: Bank for International Settlements und International Organization of Securities Commissions.
- Blackburn, Robin (2008) The Subprime Crisis. *New Left Review*. 50: 63–106.
- Blockupy (2012) Blockupy Frankfurt 16.–19. Mai. Europäische Aktionstage (Aufruf zur Demonstration). <http://2012.blockupy-frankfurt.org/de/aufruf/blockpyfrankfurt.html> (abgerufen am 23.03.2016).
- BMBF (2011) Forschung für die zivile Sicherheit. Sicherung der Warenketten. Berlin, Bonn: Bundesministerium für Bildung und Forschung.
- BMELV (2013) Strategien der Lebensmittelsicherheit. Berlin: Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz.
- BMF (2013a) Auf den Punkt. Informationen aus dem Bundesfinanzministerium: Europäische Stabilitätsmechanismen. Berlin: Bundesministerium der Finanzen.
- BMF (2013b) Auf den Punkt. Informationen aus dem Bundesfinanzministerium: Finanzmarktregulierung. Berlin: Bundesministerium der Finanzen.
- BMF (2013c) Auf den Punkt. Informationen aus dem Bundesfinanzministerium. Neue Haushaltspolitische Überwachung der EU. Berlin: Bundesministerium der Finanzen.
- BMG und RKI (2007) Nationaler Pandemieplan. Teil I: Überblick über die Maßnahmen. Berlin: Bundesministerium für Gesundheit und Robert Koch Institut.
- BMI (2005) Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen. Berlin: Bundesministerium des Inneren.
- BMI (2009) Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). Berlin: Bundesministerium des Inneren.
- BMI, BBK und BKA (2005) Schutz Kritischer Infrastrukturen: Basischutzkonzept. Empfehlungen für Unternehmen. Berlin: Bundesministerium des Inneren, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und Bundeskriminalamt.
- BMI, BBK (2011) Schutz Kritischer Infrastrukturen: Risiko und Krisenmanagement. Leitfaden für Behörden und Unternehmen. Bonn: Bundesministerium des Inneren und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.
- BMVg (1992) Verteidigungspolitische Richtlinien. Bonn: Bundesministerium der Verteidigung.

- BMVg (2006) Weißbuch zur Sicherheitspolitik Deutschlands und zur Zukunft der Bundeswehr. Berlin: Bundesministerium der Verteidigung.
- BMWi und BMU (2011) Der Weg zur Energie der Zukunft – sicher, bezahlbar und umweltfreundlich. Eckpunktepapier der Bundesregierung zur Energiewende. Berlin: Bundesministerium für Wirtschaft und Technologie und Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit.
- BNetzA (2006) Untersuchungsbericht über die Versorgungsstörungen im Netzgebiet des RWE im Münsterland vom 25.11.2005. Bonn: Bundesnetzagentur.
- BNetzA (2007) Bericht der BNetzA über die Systemstörung im deutschen und europäischen Verbundsystem am 4. November 2006. Bonn: Bundesnetzagentur.
- BNetzA (2011a) Auswirkungen des Kernkraftausstiegs auf die Übertragungsnetze und die Versorgungssicherheit. Bericht zur Notwendigkeit eines Reservekraftwerks im Sinne der Neuregelung des Atomgesetzes. Zusammenfassung. Bonn: Bundesnetzagentur.
- BNetzA (2011b) Auswirkungen des Kernkraftwerk-Moratoriums auf die Übertragungsnetze und die Versorgungssicherheit. Bonn: Bundesnetzagentur.
- BNetzA (2011c) Smart Grid und Smart Market: Eckpunktepapier der Bundesnetzagentur zu den Aspekten des sich verändernden Energieversorgungssystems. Bonn: Bundesnetzagentur.
- BNetzA (2012) Bericht zum Zustand der leitungsgebundenen Energieversorgung im Winter 2011/12. Bonn: Bundesnetzagentur.
- Boehmer-Christiansen, Sonja (1994) The precautionary principle in Germany. Enabling government. In: *Interpreting the precautionary principle*. Herausgegeben von: Timothy O’Riordan und James Cameron, 31–60. London: Earthscan Publications.
- Bogner, Alexander und Wolfgang Menz (2009) Das theoriegenerierende Experteninterview: Erkenntnisinteresse, Wissensformen, Interaktion. In: *Experteninterviews. Theorien, Methoden, Anwendungsfelder*. Herausgegeben von: Alexander Bogner, Beate Littig und Wolfgang Menz, 61–98. Wiesbaden: VS-Verlag.
- Boltanski, Luc und Laurent Thévenot (2007) *Über die Rechtfertigung. Eine Soziologie der kritischen Urteilskraft*. Hamburg: Hamburger Edition.
- Bond, David (2013) Governing disaster: The political life of the environment during the BP oil spill. *Cultural Anthropology*. 28 (4): 694–715.
- Bonß, Wolfgang (1995) *Vom Risiko: Unsicherheit und Ungewißheit in der Moderne*. Hamburg: Hamburger Edition.
- Bougen, Philip (2003) Catastrophe Risk. *Economy and Society*. 32 (2): 253–274.
- Bourdieu, Pierre (1992) *Rede und Antwort*. Frankfurt a.M.: Suhrkamp.
- Bourdieu, Pierre (1998) *Praktische Vernunft. Zur Theorie des Handelns*. Frankfurt a.M.: Suhrkamp.
- Bowker, Geoffrey C und Susan Leigh Star (2000) *Sorting things out: Classification and its consequences*. Cambridge: MIT press.
- Boy, Nina (2015) Sovereign safety. *Security Dialogue*. 46 (6): 530–547.



- Braun, Bruce P. (2008) Thinking the city through SARS: Bodies, topologies, politics. In: *Networked disease: Emerging infections in the global city*. Herausgegeben von: S. Harris Ali und Roger Keil, 250–266. Malden, Oxford: Blackwell.
- Braun, Bruce P. (2014) A new urban dispositif? Governing life in an age of climate change. *Environment and Planning D: Society and Space*. 32 (1): 49–64.
- Braun, Bruce P. und Stephanie Wakefield (2014a) Guest Editorial. *Environment and Planning D: Society and Space*. 32 (1): 4–11.
- Braun, Bruce P. und Stephanie Wakefield (2014b) Inhabiting the Post-Apocalyptic City. <http://societyandspace.org/2014/02/11/inhabiting-the-postapocalyptic-city-bruce-braun-and-stephanie-wakefield/> (abgerufen am 23.03.2016).
- Bröckling, Ulrich (2007) *Das unternehmerische Selbst. Soziologie einer Subjektivierungsform*. Frankfurt a.M.: Suhrkamp.
- Bröckling, Ulrich (2012) Dispositive der Vorbeugung: Gefahrenabwehr, Resilienz, Precaution. In: *Sicherheitskulturen. Soziale und politische Praktiken der Gefahrenabwehr*. Herausgegeben von: Christopher Daase, Philipp Offermann und Valentin Rauer, 93–108. Frankfurt a.M.: Campus.
- Bröckling, Ulrich und Susanne Krasmann (2010) Ni méthode, ni approche. Zur Forschungsperspektive der Gouvernementalitätsstudien - mit einem Seitenblick auf Konvergenzen und Divergenzen zur Diskursforschung. In: *Diskursanalyse meets Gouvernementalitätsforschung. Perspektiven auf das Verhältnis von Subjekt, Sprache, Macht und Wissen*. Herausgegeben von: Johannes Angermüller und Silke van Dyk, 23–42. Frankfurt a.M.: Campus.
- Bröckling, Ulrich, Susanne Krasmann und Thomas Lemke (Hg.) (2011) *Governmentality. Current Issues and Future Challenges*. Oxon: Routledge.
- Brückner, Fabian und Stephan Wolf (2014) Die Produktion von Unsicherheit. Nicht-intendierte Folgen des operationellen Risikomanagements in Banken. In: *Organisation und Unsicherheit*. Herausgegeben von: Maja Apelt und Konstanze Senge, 139–158. Wiesbaden: VS-Verlag.
- BS (2006) BS 25999-1:2006. Business Continuity Management – Code of Practice. Herausgegeben von British Standard. London.
- BSI (2008) BSI-Standard 100-4. Notfallmanagement. Bonn: Bundesamt für Sicherheit in der Informationstechnik.
- BSI (2017) Schutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS. Bonn: Bundesamt für Sicherheit in der Informationstechnik.
- Bühmann, Andrea und Werner Schneider (2007) Mehr als nur diskursive Praxis? Konzeptionelle Grundlagen und methodische Aspekte der Dispositivanalyse. *Forum Qualitative Sozialforschung*, 8 (2).
- BUND (2002) Ökologischer Hochwasserschutz. Raum für naturnahe Gewässer, Auen und Feuchtgebiete – Schutz für die Menschen. Berlin: Bund für Umwelt und Naturschutz Deutschland e.V.
- Bundesregierung (2003) Entwurf eines Gesetzes über die Errichtung des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe. Berlin: Bundesregierung der Bundesrepublik Deutschland.

- Bundesregierung (2008) Deutsche Anpassungsstrategie an den Klimawandel. Vom Bundeskabinett am 17. Dezember 2008 beschlossen. Berlin: Bundesregierung der Bundesrepublik Deutschland.
- Bundesregierung (2011) Aktionsplan Anpassung der Deutschen Anpassungsstrategie an den Klimawandel. Vom Bundeskabinett am 31. August 2011 beschlossen. Berlin: Bundesregierung der Bundesrepublik Deutschland.
- Bundesregierung (2015) Überführung von Braunkohlekraftwerksblöcken in die Sicherheitsbereitschaft. Berlin: Bundesregierung der Bundesrepublik Deutschland, Mitteldeutsche Braunkohlegesellschaft mbH und Helmstedter Revier GmbH.
- Bundestag (2004) Planarprotokoll 15/94. Sitzung vom Donnerstag 4. März 2004. Berlin: Deutscher Bundestag.
- Bundestag (2010) Bericht über die Methode zur Risikoanalyse im Bevölkerungsschutz 2010. Unterrichtung durch die Bundesregierung. Berlin: Deutscher Bundestag.
- Bundestag (2011a) Bericht zur Risikoanalyse im Bevölkerungsschutz 2011. Unterrichtung durch die Bundesregierung. Berlin: Deutscher Bundestag.
- Bundestag (2011b) Plenarprotokoll 17/96. Berlin: Deutscher Bundestag.
- Bundestag (2012) Bericht zur Risikoanalyse im Bevölkerungsschutz 2012. Unterrichtung durch die Bundesregierung. Berlin: Deutscher Bundestag.
- Bundestag (2013) Bericht zur Risikoanalyse im Bevölkerungsschutz 2013. Unterrichtung durch die Bundesregierung. Berlin: Deutscher Bundestag.
- Burchell, Graham, Collin Gordon und Peter Miller (Hg.) (1991) *The Foucault Effect. Studies in Governmentality*. Chicago: University of Chicago Press.
- Bussolini, Jeffrey (2010) What is a Dispositive? *Foucault Studies*. 10: 85–107.
- Bussolini, Jeffrey (2014) Nuclear state of exception: Nuclear weapons, sovereignty, and geopolitics/biopolitics. (Unveröffentlichtes Manuskript).
- Butler, Judith (2001) What is Critique? An Essay on Foucault's Virtue. <http://transform.eipcp.net/transversal/0806/butler/en> (abgerufen am 23.03.2016).
- Butler, Judith (2004) *Precarious life. The power of mourning and violence*. London: Verso.
- Butler, Judith (2009) *Frames of war. When is life grievable?* London: Verso.
- Butler, Judith, Zeynep Gambetti und Leticia Sabsay (Hg.) (2016) *Vulnerability in resistance*. Durham: Duke University Press.
- Buzan, Barry, Ole Wæver und Jaap De Wilde (1998) *Security: a new framework for analysis*. Boulder: Lynne Rienner Publishers.
- Calhoun, Craig (2004) A world of emergencies: Fear, intervention, and the limits of cosmopolitan order. *Canadian Review of Sociology and Anthropology*. 41 (4): 373–395.
- Callon, Michel (1998a) An essay on framing and overflowing: Economic externalities revisited by sociology. *The Sociological Review*. 46 (S1): 244–269.
- Callon, Michel (1998b) Introduction: The embeddedness of economic markets in economics. *The Sociological Review*. 46 (S1): 1–57.
- Callon, Michel (Hg.) (1998c) *The Laws of the Markets*. Oxford: Blackwell.

- Callon, Michel (2006a) Die Sozio-Logik der Übersetzung: Auseinandersetzungen und Verhandlungen zur Bestimmung von Problematischem und Unproblematischem. In: *ANThology. Ein einführendes Handbuch in die Akteur-Netzwerk-Theorie*. Herausgegeben von: Andrea Belliger und David J. Krieger, 51–74. Bielefeld: transcript.
- Callon, Michel (2006b) Einige Elemente einer Soziologie der Übersetzung: Die Domestikation der Kammuscheln und der Fischer der St. Brieuc-Bucht. In: *ANThology. Ein einführendes Handbuch in die Akteur-Netzwerk-Theorie*. Herausgegeben von: Andrea Belliger und David J. Krieger, 135–147. Bielefeld: transcript.
- Callon, Michel, Pierre Lascoumes und Yannick Barthe (2009) *Acting in an Uncertain World. An Essay on Technological Democracy*. Cambridge: MIT Press.
- Callon, Michel und Bruno Latour (2006) Die Demontage des großen Leviathans: Wie Akteure die Makrostruktur der Realität bestimmen und Soziologen ihnen dabei helfen. In: *ANThology. Ein einführendes Handbuch in die Akteur-Netzwerk-Theorie*. Herausgegeben von: Andrea Belliger und David J. Krieger, 75–134. Bielefeld: transcript.
- Callon, Michel und Fabian Muniesa (2005) Peripheral vision: Economic markets as calculative collective devices. *Organization Studies*. 26 (8): 1229–1250.
- Canguilhem, Georges (1977) *Das Normale und das Pathologische*. Frankfurt a.M., Berlin, Wien: Ullstein.
- Canguilhem, Georges (1979) *Wissenschaftsgeschichte und Epistemologie. Gesammelte Aufsätze*. Frankfurt a.M.: Suhrkamp.
- Canguilhem, Georges (2008) *Knowledge of Life*. New York: Fordham University Press.
- Carse, Ashley (2012) Nature as infrastructure: Making and managing the Panama Canal watershed. *Social Studies of Science*. 42 (4): 539–563.
- Castel, Robert (2000) *Metamorphosen der sozialen Frage. Eine Chronik der Lohnarbeit*. Konstanz: UVK.
- Castel, Robert und Klaus Dörre (Hg.) (2009) *Prekarität, Abstieg, Ausgrenzung: Die soziale Frage am Beginn des 21. Jahrhunderts*. Frankfurt a.M.: Campus.
- Castells, Manuel (2010) *The rise of the network society. The information age: Economy, society, and culture*. Malden, Oxford: Blackwell.
- Celikates, Robin (2009) *Kritik als soziale Praxis: gesellschaftliche Selbstverständigung und kritische Theorie*. Frankfurt a.M.: Campus.
- Chakrabarty, Dipesh (2009) The climate of history: Four theses. *Critical Inquiry*. 35 (2): 197–222.
- Choy, Timothy K. (2011) *Ecologies of comparison: An ethnography of endangerment in Hong Kong*. Durham: Duke University Press.
- Clarke, Lee (1999) *Mission improbable: Using fantasy documents to tame disaster*. Chicago: University of Chicago Press.
- Clausen, Lars, Elke M. Geenen und Elísio Macamo (Hg.) (2003) *Entsetzliche soziale Prozesse. Theorie und Empirie der Katastrophen*. Münster: Lit-Verlag.

- Collier, Stephen J. (2005) Budgets and biopolitics. In: *Global assemblages: Technology, politics, and ethics as anthropological problems*. Herausgegeben von: Stephen J. Collier und Aihwa Ong, 373–390. Malden, Oxford: Blackwell.
- Collier, Stephen J. (2008) Enacting catastrophe: preparedness, insurance, budgetary rationalization. *Economy and Society*. 37 (2): 224–250.
- Collier, Stephen J. (2011) *Post-soviet social: Neoliberalism, social modernity, biopolitics*. Princeton: Princeton University Press.
- Collier, Stephen J. (2014) Neoliberalism and natural disaster: Insurance as political technology of catastrophe. *Journal of Cultural Economy*. 7 (3): 273–290.
- Collier, Stephen J. und Andrew Lakoff (2008) Distributed preparedness: The spatial logic of domestic security in the United States. *Environment and Planning D: Society and Space*. 26 (1): 7–28.
- Collier, Stephen J. und Andrew Lakoff (2015) Vital systems security: Reflexive biopolitics and the government of emergency. *Theory, Culture & Society*. 32 (2): 19–51.
- Collier, Stephen J., Andrew Lakoff und Christopher M. Kelty (Hg.) (2011) Systemic Risk. *limn*. 1 (1).
- Comité Invisible (2009) *The coming insurrection*. Los Angeles: semiotext(e).
- Comité Invisible (2015) *An unsere Freunde*. Hamburg: Edition Nautilus.
- Conaty, Matthew L. (2010) Atomic midwife: The Eisenhower Administration's continuity-of-government plans and the legacy of »constitutional dictatorship«. *Rutgers Law Review*. 62 (3): 627–685.
- Connolly, William E. (2011) *A world of becoming*. Durham, London: Duke University Press.
- Connolly, William E. (2013) The »New Materialism« and the fragility of things. *Millennium. Journal of International Studies*. 41 (3): 399–412.
- Conze, Eckart (2005) Sicherheit als Kultur. Überlegungen zu einer »modernen Politikgeschichte« der Bundesrepublik Deutschland. *Vierteljahreshefte für Zeitgeschichte*. 53 (3): 357–380.
- Conze, Werner (1982) Sicherheit, Schutz. In: *Geschichtliche Grundbegriffe: Historisches Lexikon zur politisch-sozialen Sprache in Deutschland* Herausgegeben von: Otto Brunner, Werner Conze und Reinhart Koselleck, 831–862. Stuttgart: Klett-Cotta.
- Cookson, Clive, Gillian Tett und Chris Cook (2009) Eco-economics. Could biology explain the recession? <http://giffenman-miscellanea.blogspot.de/2009/11/eco-economics-could-biology-explain.html> (abgerufen am 23.03.2016).
- Cooper, Melinda (2006) Pre-empting emergence: The biological turn in the war on terror. *Theory, Culture & Society*. 23 (4): 113–135.
- Cooper, Melinda (2008) *Life as Surplus. Biotechnology and Capitalism in the Neoliberal Era*. Seattle: University of Washington Press.
- Cooper, Melinda (2010) Turbulent worlds: Financial markets and environmental crisis. *Theory, Culture & Society*. 27 (2–3): 167–190.

- Cooper, Melinda (2011) Complexity theory after the financial crisis. The end of neoliberalism or the triumph of Hayek. *Journal of Cultural Economy*. 4 (4): 371–385.
- Cooper, Melinda und Jeremy Walker (2011) Genealogies of resilience. From systems ecology to the political economy of crisis adaptation. *Security Dialogue*. 42 (2): 143–160.
- Corry, Olaf (2014) From defense to resilience: Environmental security beyond neoliberalism. *International Political Sociology*. 8 (3): 256–274.
- Cowen, Deborah (2010) A geography of logistics: Market authority and the security of supply chains. *Annals of the Association of American Geographers*. 100 (3): 600–620.
- Cowen, Deborah (2014) *The deadly life of logistics: Mapping violence in global trade*. Minneapolis: University of Minnesota Press.
- Cowen, Deborah und Neil Smith (2009) After geopolitics? From the geopolitical social to geoeconomics. *Antipode*. 41 (1): 22–48.
- Crary, Jonathan (2013) *24/7: Late capitalism and the ends of sleep*. London: Verso.
- Crockett, Andrew (2000) Marrying the micro-and macro-prudential dimensions of financial stability. Herausgegeben von der Bank for International Settlements. Basel: BIS Speeches.
- Cruikshank, Barbara (1999) *The will to empower. Democratic citizens and other subjects*. Ithaca, London: Cornell University Press.
- Crutzen, Paul J. (2002) Geology of mankind. *Nature*. 415 (6867): 23.
- CSU (2015) Für ein modernes Streikrecht. Koalitionsfreiheit achten – Daseinsvorsorge sicherstellen. München: Parteivorstand der Christlich Sozialen Union.
- Daase, Christopher (2010) Der erweiterte Sicherheitsbegriff. *Sicherheitskultur im Wandel. Working Paper*. 2010: 1–24.
- Daase, Christopher und Oliver Kessler (2007) Knowns and unknowns in the war on terror: Uncertainty and the political construction of danger. *Security Dialogue*. 38 (4): 411–434.
- Dalby, Simon (2017) Anthropocene formations: Environmental security, geopolitics and disaster. *Theory, Culture & Society*. 34 (2-3): 233–252.
- Danielsson, Jon, Hyun Song Shin und Jean-Pierre Zigrand (2012) Endogenous and systemic risk. In: *Quantifying Systemic Risk*. Herausgegeben von: Joseph G. Haubrich und Andrew W. Lo, 73–94. Chicago: University of Chicago Press.
- Daston, Lorraine (1987) The domestication of risk: Mathematical probability and insurance 1650–1830. In: *The Probabilistic Revolution. 1*. Herausgegeben von: Lorenz Krüger, Lorraine Daston und Michael Heidelberger, 237–260. Cambridge, London: MIT Press.
- de Goede, Marieke (2008) Beyond risk: Premediation and the post-9/11 security imagination. *Security Dialogue*. 39 (2–3): 155–176.
- de Goede, Marieke (2012) Fighting the network: a critique of the network as a security technology. *Distinktion: Scandinavian Journal of Social Theory*. 13 (3): 215–232.

- Dean, Mitchell (1995) Governing the unemployed self in an active society. *Economy and Society*. 24 (4): 559–583.
- Defert, Daniel (1991) »Popular life« and insurance technology. In: *The Foucault Effect. Studies in Governmentality*. Herausgegeben von: Graham Burchell, Collin Gordon und Peter Miller, 211–233. London, Toronto, Sydney, Tokio, Singapore: Harvester Wheatsheaf.
- DeLanda, Manuel (1991) *War in the age of intelligent machines*. New York: Zone Books.
- Deleuze, Gilles (1989) *Henri Bergson zur Einführung*. Hamburg: Junius.
- Deleuze, Gilles (1991) Was ist ein Dispositiv? In: *Spiele der Wahrheit. Michel Foucaults Denken*. Herausgegeben von: François Ewald und Bernhard Waldenfels, 153–162. Frankfurt a.M.: Suhrkamp.
- Deleuze, Gilles (1993) Postskriptum über die Kontrollgesellschaften. In: *Unterhandlungen 1972–1990*, 254–262. Frankfurt a.M.: Suhrkamp.
- Deleuze, Gilles und Felix Guattari (1997) *Tausend Plateaus. Kapitalismus und Schizophrenie*. Berlin: Merve.
- Demeritt, David (2006) Science studies, climate change and the prospects for constructivist critique. *Economy and Society*. 35 (3): 453–479.
- Der Derian, James und Jesse Finkelstein (2008) Critical Infrastructures and network pathologies. The semiotics and biopolitics of heteropolarity. In: *Securing »the Homeland«. Critical Infrastructure, Risk and (In)security*. Herausgegeben von: Myriam Dunn Cavelty und Kristian Soby Kristensen, 84–105. Oxon: Routledge.
- Derrida, Jacques (1998) *Gesetzeskraft. Der mystische Grund der Autorität*. Frankfurt a.M.: Suhrkamp.
- Derrida, Jacques (2003) *Schurken. Zwei Essays über die Vernunft*. Frankfurt a.M.: Suhrkamp.
- Derrida, Jacques und Jürgen Habermas (2004) *Philosophie in Zeiten des Terrors. Zwei Gespräche, geführt, eingeleitet und kommentiert von Giovanna Borradori*. Berlin: Philo.
- Deville, Joe, Michael Guggenheim und Zuzana Hrdličková (2014) Concrete governmentality: shelters and the transformations of preparedness. *The Sociological Review*. 62 (S1): 183–210.
- DHS (2007) National Strategy for Homeland Security. Washington: Homeland Security Council.
- Diaz-Bone, Rainer (2005a) Die »interpretative Analytik« als rekonstruktiv-strukturalistische Methodologie. Bemerkungen zur Eigenlogik und strukturalistischen Öffnung der Foucaultschen Diskursanalyse. In: *Die diskursive Konstruktion von Wirklichkeit. Zum Verhältnis von Wissenssoziologie und Diskursforschung*. Herausgegeben von: Reiner Keller, Andreas Hirsland, Werner Schneider und Willy Viehöver, 179–197. Konstanz: UVK.
- Diaz-Bone, Rainer (2005b) Zur Methodologisierung der Foucaultschen Diskursanalyse. *Forum Qualitative Sozialforschung*. 7 (1).

- Diaz-Bone, Rainer (2006) Die interpretative Analytik als methodologische Position. In: *Foucault: Diskursanalyse der Politik*. Herausgegeben von: Brigitte Kerchner und Silke Schneider, 68–84. Wiesbaden: VS-Verlag.
- Dillon, Michael und Luis Lobo-Guerrero (2008) Biopolitics of security in the 21st century: an introduction. *Review of International Studies*. 34: 265–292.
- Dittmar, Norbert (2004) *Transkription. Ein Leitfaden mit Aufgaben für Studenten, Forscher und Laien*. Wiesbaden: VS Verlag.
- Dombrowsky, Wolf (1989) *Katastrophe und Katastrophenschutz. Eine soziologische Analyse*. Wiesbaden: Deutscher Universitäts-Verlag.
- Dombrowsky, Wolf (2013) Der Mensch als Risiko – oder: Geht alle Gefahr vom Volke aus? In: *Aufbruch ins Unversicherbare. Zum Katastrophendiskurs der Gegenwart*. Herausgegeben von: Leon Hempel, Marie Bartels und Thomas Markwart, 29–52. Bielefeld: transcript.
- Dombrowsky, Wolf, Jörg Horenczuk und Willi Streitz (2003) Erstellung eines Schutzdatenatlas. Bonn: Schriftenreihe der Schutzkommission beim Bundesminister des Inneren.
- Donzelot, Jacques (1988) The promotion of the social. *Economy and Society*. 17 (3): 395–427.
- Donzelot, Jacques (1991) The mobilization of society. In: *The Foucault effect. Studies in governmentality*. Herausgegeben von: Graham Burchell, Collin Gordon und Peter Miller, 196–180. Hempstead: Harvester Wheatsheaf.
- Douglas, Mary und Aaron B. Wildavsky (1982) *Risk and culture. An essay on the selection of technical and environmental dangers*. Berkely, Los Angeles, London: University of California Press.
- DPA (2013) Juni-Hochwasser: Merkel verspricht Flutopfern Geld noch im August. *Spiegel Online*. <http://www.spiegel.de/politik/deutschland/juni-hochwasser-merkel-besucht-flutopfer-a-912644.html> (abgerufen am 23.06.2016).
- Dreyfus, Hubert L. und Paul Rabinow (1983) *Michel Foucault: Beyond structuralism and hermeneutics*. Chicago: University of Chicago Press.
- Dreyfus, Hubert L. und Paul Rabinow (1994) *Michel Foucault. Jenseits von Strukturalismus und Hermeneutik*. Weinheim: Beltz-Athenaeum.
- Dumm, Thomas L. (1987) *Democracy and punishment: Disciplinary origins of the United States*. Madison: University of Wisconsin Press.
- Dunn Cavely, Myriam (2008) Like a phoenix from the ashes: The reinvention of Critical Infrastructure Protection as distributed security. In: *Securing »the Homeland«. Critical Infrastructure, risk and (in)security*. Herausgegeben von: Myriam Dunn Cavely und Kristian Soby Kristensen, 40–62. Oxon: Routledge.
- Durkheim, Emile (1988) *Über soziale Arbeitsteilung. Studie über die Organisation höherer Gesellschaften*. Frankfurt a.M.: Suhrkamp.
- Easterling, Keller (2014) *Extrastatecraft. The power of infrastructure space*. London, New York: Verso.
- ECB (2003) Oversight standards for Euro retail payment systems. Frankfurt a.M.: Europäische Zentralbank.

- ECB (2006) Business Continuity oversight expectations for Systemically Important Payment Systems (SIPS). Frankfurt a.M.: Europäische Zentralbank.
- Eckardt, Nikolaus, Margitta Meinerzhagen und Ulrich Jochimsen (1985) *Die Stromdiktatur: Von Hitler ermächtigt, bis heute ungebrochen*. Hamburg: Rasch und Rohring.
- Edwards, Paul N. (1997) *The closed world: Computers and the politics of discourse in Cold War America*. Cambridge: MIT Press.
- Edwards, Paul N. (2003) Infrastructure and modernity: Force, time, and social organization in the history of sociotechnical systems. In: *Modernity and technology*. Herausgegeben von: Thomas J. Misa, Philip Brey und Andrew Feenberg, 185–225. Cambridge: MIT Press.
- Edwards, Paul N. (2010) *A vast machine: Computer models, climate data, and the politics of global warming*. Cambridge: MIT Press.
- Edwards, Paul N. und Gabrielle Hecht (2010) History and the technopolitics of identity: The case of Apartheid South Africa. *Journal of Southern African Studies*. 36 (3): 619–639.
- EKSE (2011) Deutschlands Energiewende. Ein Gemeinschaftswerk für die Zukunft. Berlin: Ethik-Kommission Sichere Energieversorgung.
- Elbe, Stefan, Anne Roemer-Mahler und Christopher Long (2014) Securing circulation pharmaceutically: Antiviral stockpiling and pandemic preparedness in the European Union. *Security Dialogue*. 45 (5): 440–457.
- Elden, Stuart (2007) Governmentality, calculation, territory. *Environment and Planning D: Society and Space*. 25 (3): 562–580.
- Ellebrecht, Nils (2009) Triage. Charakteristika und Gegenwart eines ordnungsstiftenden Verfahrens. *Sociologia Internationalis*. 47 (2): 229–257.
- Ellebrecht, Nils, Markus Jenki und Stefan Kaufmann (2013) Inszenierte Katastrophen: Zur Genese der Übung im Bevölkerungsschutz und ihre gegenwärtigen Formen. In: *Aufbruch ins Unversicherbare. Zum Katastrophendiskurs der Gegenwart*. Herausgegeben von: Leon Hempel, Marie Bartels und Thomas Markwart, 235–277. Bielefeld: transcript.
- Endreß, Martin und Andrea Maurer (2014) *Resilienz im Sozialen: theoretische und empirische Analysen*. Wiesbaden: VS-Verlag.
- EnSiG (1975) Gesetz zur Sicherung der Energieversorgung (Energiesicherungsgesetz).
- EnWG (1935) Gesetz zur Förderung der Energiewirtschaft (Energiewirtschaftsgesetz).
- EnWG (2005) Energiewirtschaftsgesetz. Gesetz über die Elektrizitäts- und Gasversorgung.
- Ericson, Richard (2005) Governing through risk and uncertainty. *Economy and Society*. 34 (4): 659–672.
- Ericson, Richard und Aron Doyle (2004) Catastrophe risk, insurance and terrorism. *Economy and Society*. 33 (2): 135–173.



- Erturk, Ismail, Julie Froud, Adam Leaver, Michael Moran und Karel Williams (2011) Haldane's gambit: Political arithmetic and/or a new metaphor. *Journal of Cultural Economy*. 4 (4): 387–404.
- Esposito, Elena (2007) *Die Fiktion der wahrscheinlichen Realität*. Frankfurt a.M.: Suhrkamp.
- Esposito, Elena (2011) *The future of futures: The time of money in financing and society*. Cheltenham: Edward Elgar Publishing.
- Esposito, Elena (2013) The structures of uncertainty: performativity and unpredictability in economic operations. *Economy and Society*. 42 (1): 102–129.
- Esposito, Roberto (2004) *Immunitas. Schutz und Negation des Lebens*. Berlin, Zürich: diaphanes.
- Esposito, Roberto (2014) Das Paradigma der Immunisierung. In: *Biopolitik. Ein Reader*. Herausgegeben von: Andreas Folkers und Thomas Lemke, 337–382. Berlin: Suhrkamp.
- EU (2005) Grünbuch über ein europäisches Programm für den Schutz Kritischer Infrastrukturen. Brüssel: Kommission der europäischen Gemeinschaften.
- EU (2006) Communication from the Commission on a european programme for Critical Infrastructure Protection. Brüssel: Kommission der europäischen Gemeinschaften.
- EU (2008) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Brüssel: Rat der Europäischen Union.
- EU (2009) Anpassung an den Klimawandel: Ein europäischer Aktionsrahmen. Brüssel: Kommission der Europäischen Gemeinschaften.
- EU (2013) Grüne Infrastruktur (GI) – Aufwertung des europäischen Naturkapitals. Brüssel: Europäische Kommission.
- EU (2014) Eine Grüne Infrastruktur für Europa. Luxemburg: Europäische Kommission.
- Ewald, François (1993) *Der Vorsorgestaat*. Frankfurt a.M.: Suhrkamp.
- Ewald, François (2002) The return of Descarte's malicious demon: An outline of a philosophy of precaution. In: *Embracing risk. The changing culture of insurance and responsibility*. Herausgegeben von: Tom Baker und Jonathan Simon, 273–301. Chicago, London: The University of Chicago Press.
- Ewald, François (2011) Situation in France: The principle of precaution. In: *Nanoethics and Nanotoxicology*. Herausgegeben von: Philippe Houdy, Marcel Lahmani und Francelyne Marano, 483–494. Heidelberg, London, New York: Springer.
- EZB (2013) TARGET2 – A single Europe for individual payments. Frankfurt a.M.: Europäische Zentralbank. Department Payment and Settlement Systems.
- EZB (2014) Regulation of the European Central Bank (EU) No 795/2014 on oversight requirements for systemically important payment systems. Frankfurt a.M.: Europäische Zentralbank.

- EZB und BRD (1998) Headquarters Agreement between the European Central Bank and the Government of the Federal Republic of Germany concerning the seat of the European Central Bank. Frankfurt a.M.: Europäische Zentralbank, Bundesrepublik Deutschland.
- Fassin, Didier (2012) *Humanitarian reason: A moral history of the present*. Berkeley, Los Angeles, London: University of California Press.
- Fassin, Didier und Mariella Pandolfi (2010) *Contemporary states of emergency: the politics of military and humanitarian interventions*. New York: Zone Books.
- Fearnley, Lyle (2008) Signals come and go: syndromic surveillance and styles of biosecurity. *Environment and Planning A*. 40 (7): 1615–1632.
- Felgentreff, Carsten und Wolf Dombrowsky (2008) Hazard-, Risiko- und Katastrophenforschung. In: *Naturrisiken und Sozialkatastrophen*. Herausgegeben von: Carsten Felgentreff und Thomas Glade, 13–29. Berlin: Spektrum Akademischer Verlag.
- Feustel, Robert und Maximilian Schochow (Hg.) (2010) *Zwischen Sprachspiel und Methode. Perspektiven der Diskursanalyse*. Bielefeld: transcript.
- Fleming, James Rodger (2006) The pathological history of weather and climate modification: Three cycles of promise and hype. *Historical Studies in the Physical and Biological Sciences*. 37 (1): 3–25.
- Flick, Uwe (1999) Leitfadeninterviews. In: *Qualitative Forschung. Theorie, Methoden, Anwendung in Psychologie und Sozialwissenschaften*, 94–114. Hamburg: Rowohlt.
- Fligstein, Neil und Luke Dauter (2007) The sociology of markets. *Annual Review of Sociology*. 33: 105–128.
- Flusser, Vilém (1999) *The shape of things. A philosophy of design*. London: Reaktion Books.
- Folkers, Andreas (2012) Kritische Infrastruktur. In: *Ortsregister. Ein Glossar zu Räumen der Gegenwart*. Herausgegeben von: Nadine Marquardt und Verena Schreiber, 154–159. Bielefeld: transcript.
- Folkers, Andreas (2013a) Von der Ironie der Normalisierung zur Autoimmunität. Der Subprime Mortgager und die Finanzkrise. *Soziale Systeme*. 19 (1): 85–109.
- Folkers, Andreas (2013b) Was ist neu am neuen Materialismus? Von der Praxis zum Ereignis. In: *Critical Matter. Diskussionen eines neuen Materialismus*. Herausgegeben von: Tobias Goll, Daniel Keil und Thomas Telios, 16–33. Münster: edition assemblage.
- Folkers, Andreas (2014) After virtù and fortuna: Foucault on the government of economic events. *Distinktion: Scandinavian Journal of Social Theory*. 15 (1): 88–104.
- Folkers, Andreas (2016) Daring the truth: Foucault, parrhesia and the genealogy of critique. *Theory, Culture & Society*. 33 (1): 3–28.
- Folkers, Andreas (2017a) Continuity and catastrophe: business continuity management and the security of financial operations. *Economy and Society*. 46 (1): 103–127.

- Folkers, Andreas (2017b) Die Onto-Topologie der Energiewende-Volatile Ströme, endliche Energien und die Sicherung des Bestandes. *Bebemoth. A Journal on Civilisation*. 10 (1): 29–56.
- Folkers, Andreas (2017c) Existential provisions: The technopolitics of public infrastructure. *Environment and Planning D: Society and Space*. 35 (5): 855–874.
- Folkers, Andreas (2017d) Nuclear states, renewable democracies? *limn*. 7: 83–88.
- Folkers, Andreas (2017e) Politik des Lebens jenseits seiner selbst. Für eine ökologische Lebenssoziologie mit Deleuze und Guattari. *Soziale Welt*. 68 (4): im Erscheinen.
- Folkers, Andreas und Thomas Lemke (Hg.) (2014) *Biopolitik. Ein Reader*. Berlin: Suhrkamp.
- Folkers, Andreas und Il-Tschung Lim (2014) Irrtum und Irritation. Für eine kleine Soziologie der Krise nach Foucault und Luhmann. *Bebemoth. A Journal on Civilisation*. 7 (1): 48–69.
- Folkers, Andreas und Nadine Marquardt (2016) Tent. In: *Making Things International 2. Catalysts and Reactions*. Herausgegeben von: Mark E. Salter, 63–78. Minneapolis: University of Minnesota Press.
- Forsthoﬀ, Ernst (1938) *Die Verwaltung als Leistungsträger*. Stuttgart, Berlin: Kohlhammer.
- Forsthoﬀ, Ernst (1941) *Grenzen des Rechts*. Königsberg: Gräfe & Unzer.
- Forsthoﬀ, Ernst (1950) *Lehrbuch des Verwaltungsrechts*. München: C.H. Beck.
- Forsthoﬀ, Ernst (1971) *Der Staat der Industriegesellschaft: Dargestellt am Beispiel der Bundesrepublik Deutschland*. München: C. H. Beck.
- Fortun, Kim (2001) *Advocacy after Bhopal: Environmentalism, disaster, new global orders*. Chicago: University of Chicago Press.
- Foucault, Michel (1974) *Die Ordnung der Dinge*. Frankfurt a.M.: Suhrkamp.
- Foucault, Michel (1976) *Überwachen und Strafen. Die Geburt des Gefängnisses*. Frankfurt a.M.: Suhrkamp.
- Foucault, Michel (1977) *Der Wille zum Wissen. Sexualität und Wahrheit 1*. Frankfurt a.M.: Suhrkamp.
- Foucault, Michel (1978) *Dispositive der Macht. Michel Foucault über Sexualität, Wissen und Wahrheit*. Berlin: Merve.
- Foucault, Michel (1981) *Archäologie des Wissens*. Frankfurt a.M.: Suhrkamp.
- Foucault, Michel (1989a) *Der Gebrauch der Lüste. Sexualität und Wahrheit 2*. Frankfurt a.M.: Suhrkamp.
- Foucault, Michel (1989b) *Die Sorge um sich. Sexualität und Wahrheit 3*. Frankfurt a.M.: Suhrkamp.
- Foucault, Michel (1992) *Was ist Kritik?* Berlin: Merve.
- Foucault, Michel (1996) *Diskurs und Wahrheit. Die Problematisierung der Parrhesia. Berkeley Vorlesungen 1983*. Berlin: Merve.
- Foucault, Michel (2001) *In Verteidigung der Gesellschaft. Vorlesungen am College de France, 1975–1976*. Frankfurt a.M.: Suhrkamp.

- Foucault, Michel (2003) Die Geburt der Sozialmedizin. In: *Michel Foucault. Dits et Ecrits. Schriften. Dritter Band*, 272–298. Frankfurt a.M.: Suhrkamp.
- Foucault, Michel (2004) *Sicherheit, Territorium, Bevölkerung (Geschichte der Gouvernementalität I). Vorlesungen am Collège de France, 1977–1978*. Frankfurt a.M.: Suhrkamp.
- Foucault, Michel (2005a) Die politische Technologie der Individuen. In: *Michel Foucault. Dits et Ecrits. Schriften. Vierter Band*, 999–1015. Frankfurt a.M.: Suhrkamp.
- Foucault, Michel (2005b) Die Sorge um die Wahrheit. In: *Michel Foucault. Dits et Ecrits. Schriften. Vierter Band*, 823–836. Frankfurt: Suhrkamp.
- Foucault, Michel (2005c) Diskussion vom 20. Mai 1978. In: *Michel Foucault. Dits et Ecrits. Schriften. Vierter Band*, 25–43. Frankfurt a.M.: Suhrkamp.
- Foucault, Michel (2005d) Ein endliches System angesichts einer unendlichen Nachfrage. In: *Michel Foucault. Dits et Ecrits. Schriften. Vierter Band*. Frankfurt a.M.: Suhrkamp.
- Foucault, Michel (2005e) Polemik, Politik und Problematisierung. In: *Michel Foucault. Dits et Ecrits. Schriften. Vierter Band*, 724–734. Frankfurt a.M.: Suhrkamp.
- Foucault, Michel (2005f) Subjekt und Macht. In: *Michel Foucault. Dits et Ecrits. Schriften. Vierter Band*, 269–294. Frankfurt a.M.: Suhrkamp.
- Foucault, Michel (2005g) Technologien des Selbst. In: *Michel Foucault. Dits et Ecrits. Schriften. Vierter Band*, 966–999. Frankfurt a.M.: Suhrkamp.
- Foucault, Michel (2005h) Von anderen Räumen. In: *Michel Foucault. Dits et Ecrits. Schriften. Vierter Band*, 931–942. Frankfurt a.M.: Suhrkamp.
- Foucault, Michel (2005i) Was ist Aufklärung? In: *Michel Foucault. Dits et Ecrits. Schriften. Vierter Band*, 687–707. Frankfurt a.M.: Suhrkamp.
- Foucault, Michel (2005j) Zur Genealogie der Ethik: Ein Überblick über die laufende Arbeit. In: *Michel Foucault. Dits et Ecrits. Schriften. Vierter Band*, 747–776. Frankfurt a.M.: Suhrkamp.
- Foucault, Michel (2006) *Die Geburt der Biopolitik (Geschichte der Gouvernementalität II). Vorlesungen am Collège de France, 1978–1979*. Frankfurt a.M.: Suhrkamp.
- Foucault, Michel (2009a) *Die Regierung des Selbst und der anderen. Vorlesungen am Collège de France, 1982–1983*. Frankfurt a.M.: Suhrkamp.
- Foucault, Michel (2009b) *Hermeneutik des Subjekts. Vorlesungen am Collège de France, 1981–1982*. Frankfurt a.M.: Suhrkamp.
- Foucault, Michel (2010) *Der Mut zur Wahrheit (Die Regierung des Selbst und der anderen II). Vorlesungen am Collège de France 1983–1984*. Berlin: Suhrkamp.
- Franzen, Martin, Gregor Thüsing und Christian Waldhoff (2012) *Arbeitskampf in der Daseinsvorsorge. Vorschläge zur Gesetzlichen Regelung von Streik und Aussperrung in Unternehmen der Daseinsvorsorge*. Berlin, Bonn, München: Carl Friedrich von Weizsäcker-Stiftung.
- Friedman, Thomas L (2006) *The world is flat: The globalized world in the twenty-first century*. London: Penguin.
- Friedrich, Alexander und Stefan Höhne (2014) Frischeregime. Biopolitik im Zeitalter der kryogenen Kultur. *Glocalism: Journal of Culture, Politics and Innovation*. 1–2: 1–44.

- FSB (2010) Reducing the moral hazard posed by systemically important financial institutions. FSB recommendations and Time Lines. Basel: Financial Stability Board.
- Füller, Henning (2012) Quarantäne. In: *Ortsregister. Ein Glossar zu Räumen der Gegenwart*. Herausgegeben von: Nadine Marquardt und Verena Schreiber, 224–230. Bielefeld: transcript.
- Galison, Peter (1996) Computer simulations and the trading zone. In: *The disunity of science. Boundaries, contexts, and power*. Herausgegeben von: Peter Galison und David J. Stump, 118–157. Stanford: Stanford University Press.
- Galison, Peter (2001) War against the Center. *Grey Room*. 4: 5–33.
- Galloway, Alexander (2004) *Protocol: How control exists after decentralization*. Cambridge: MIT-Press.
- Gandy, Matthew (2004) Rethinking urban metabolism: Water, space and the modern city. *City*. 8 (3): 363–379.
- Gandy, Matthew (2005) Cyborg urbanization: Complexity and monstrosity in the contemporary city. *International Journal of Urban and Regional Research*. 29 (1): 26–49.
- Gehring, Petra (2006) *Was ist Biomacht? Vom zweifelhaften Mehrwert des Lebens*. Frankfurt a.M.: Campus.
- Geis, Mathias und Tina Hildebrandt (2013) Die Frau, die alle abschöpft. *Zeit*. 13.06.2013.
- GG (Grundgesetz der Bundesrepublik Deutschland). Stand Januar 2016. Berlin: Deutscher Bundestag.
- Ghamari-Tabrizi, Sharon (2005) *The worlds of Herman Kahn. The intuitive science of thermonuclear war*. Cambridge: Harvard University Press.
- Glanz, James (2012) Power, pollution and the internet. The cloud factories. *New York Times*. 20.12.2014.
- Gleick, James (1990) *Chaos – die Ordnung des Universums. Vorstoß in die Grenzgebiete moderner Physik*. München: Knauer.
- Gordon, Collin (1991) Governmental Rationality: An Introduction. In: *The Foucault Effect. Studies in Governmentality*. Herausgegeben von: Graham Burchell, Collin Gordon und Peter Miller, 1–51. Chicago: University of Chicago Press.
- Graham, Stephen (2011) *Cities under siege: The new military urbanism*. London: Verso Books.
- Graham, Stephen und Simon Marvin (2001) *Splintering urbanism: Networked infrastructures, technological mobilities and the urban condition*. London, New York: Routledge.
- Gros, Frédéric (2015) *Die Politisierung der Sicherheit. Vom inneren Frieden zur äußeren Bedrohung*. Berlin: Matthes & Seitz.
- Gruber, Georg und Martin Benisch (2007) Privileges and immunities of the European Central Bank. *European Central Bank (ECB) Legal Working Paper 4*.
- Grusin, Richard (2004) Premediation. *Criticism*. 46 (1): 17–39.

- Guggenheim, Michael (2014) Introduction: disasters as politics–politics as disasters. *The Sociological Review*. 62 (S1): 1–16.
- Habermas, Jürgen (1973) *Legitimationskrise im Spätkapitalismus*. Frankfurt a.M.: Suhrkamp.
- Habermas, Jürgen (1981) *Theorie des kommunikativen Handelns*. 2 Bände. Frankfurt a.M.: Suhrkamp.
- Hacking, Ian (1990) *The taming of chance*. New York: Cambridge University Press.
- Hailey, Charlie (2009) *Camps: A guide to 21st-century space*. Cambridge: MIT Press.
- Haldane, Andrew (2009) Rethinking the Financial Network. *BIS Review*. 53: 1–26.
- Haldane, Andrew und Robert May (2011) Systemic risk in banking ecosystems. *Nature*. 469 (7330): 351–355.
- Haraway, Donna (1987) A manifesto for cyborgs: Science, technology, and socialist feminism in the 1980s. *Australian Feminist Studies*. 2 (4): 1–42.
- Haraway, Donna (1997) *Modest\_Witness@Second\_Millennium. FemaleMan\_Meets\_Onco Mouse: Feminism and Technoscience*. London: Routledge.
- Haraway, Donna (2014) Die Biopolitik postmoderner Körper. In: *Biopolitik. Ein Reader*. Herausgegeben von: Andreas Folkers und Thomas Lemke, 134–188. Berlin: Suhrkamp.
- Haraway, Donna (2015) Anthropocene, capitalocene, chthulucene: Staying with the trouble. *Environmental Humanities*. 6: 159–165.
- Hardt, Michael und Antonio Negri (2002) *Empire. Die neue Weltordnung*. Frankfurt, New York: Campus.
- Harman, Graham (2009) *Prince of networks: Bruno Latour and metaphysics*. Melbourne: Re. press.
- Harvey, Penelope (2012) The topological quality of infrastructural relation: An ethnographic approach. *Theory, Culture & Society*. 29 (4–5): 76–92.
- Hawken, Paul, Amory B. Lovins und L. Hunter Lovins (2013) *Natural capitalism: The next industrial revolution*. London: Routledge.
- Hayek, Friedrich August (1989) The pretence of knowledge. *The American Economic Review*. 79 (6): 3–7.
- Hayek, Friedrich August (2010) *Studies on the abuse and decline of reason: Text and documents*. Chicago: University of Chicago Press.
- Hayes, Denis (1979) *Alternative Energien*. Hamburg: Hoffmann und Campe.
- Hecht, Gabrielle (2009) *The radiance of France: Nuclear power and national identity after World War II*. Cambridge: MIT Press.
- Hegel, Georg Wilhelm Friedrich (1970) *Grundlinien der Philosophie des Rechts*. Frankfurt a.M.: Suhrkamp.
- Heidegger, Martin (1957) *Der Satz vom Grund*. Pfullingen: Günther Neske Verlag.
- Heidegger, Martin (1977) *The question concerning technology and other essays*. New York, London: Garland Publishing.
- Heidegger, Martin (2004) *Vorträge und Aufsätze*. Stuttgart: Klett-Cotta.
- Heidegger, Martin (2006) *Sein und Zeit*. Tübingen: Max Niemeyer.

- Helfferrich, Cornelia (2004) *Die Qualität qualitativer Daten. Manual für die Durchführung qualitativer Interviews*. Wiesbaden: VS Verlag.
- Hempel, Leon, Susanne Krasmann und Ulrich Bröckling (Hg.) (2010) *Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert*, *Leviathan Sonderheft 25*.
- Hepburn, Jamie (2012) Gearing up for protests. *Resilience. Winning with Risk (pwc)* (2): 12–13.
- Hirschman, Albert O. (1991) *The rhetoric of reaction: perversity, futility, jeopardy*. Cambridge: Harvard University Press.
- Hobbes, Thomas (1966) *Leviathan oder Stoff, Form und Gewalt eines bürgerlichen und kirchlichen Staates*. Frankfurt a.M., Berlin, Wien: Ullstein.
- Hobsbawm, Eric (1998) *Das Zeitalter der Extreme. Weltgeschichte des 20. Jahrhunderts*. München: Deutscher Taschenbuch Verlag.
- Hodson, Mike und Simon Marvin (2009) »Urban ecological security«: a new urban paradigm? *International Journal of Urban and Regional Research*. 33 (1): 193–215.
- Holling, Crawford S. (1973) Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*. 4: 1–23.
- Holling, Crawford S. (1996) Engineering resilience versus ecological resilience. In: *Engineering within ecological constraints*. Herausgegeben von: Peter Schulze, 31–44. Washington: National Academies Press.
- Holling, Crawford S. (2001) Understanding the complexity of economic, ecological, and social systems. *Ecosystems*. 4 (5): 390–405.
- Holzinger, Markus, Stefan May und Wiebke Pohler (2010) *Weltrisikogesellschaft als Ausnahmezustand*. Weilerswist: Velbrück.
- Honneth, Axel und Ferdinand Sutterlüty (2011) Normative Paradoxien der Gegenwart. Eine Forschungsperspektive. *WestEnd. Neue Zeitschrift für Sozialforschung*. 8 (1): 67–85.
- Horkheimer, Max (1967) *Zur Kritik der instrumentellen Vernunft*. Frankfurt a.M.: S. Fischer.
- Horkheimer, Max (1988) Zu Bergsons Metaphysik der Zeit. In: *Kritische Theorie. Eine Dokumentation*, 175–199. Frankfurt a.M.: Fischer.
- Horkheimer, Max und Theodor W. Adorno (2010) *Dialektik der Aufklärung: Philosophische Fragmente*. Frankfurt a.M.: Fischer.
- Hörl, Erich (2011) Die technologische Bedingung. Zur Einführung. In: *Die technologische Bedingung. Beiträge zur Beschreibung der technischen Welt*. Herausgegeben von: Erich Hörl, 7–53. Berlin: Suhrkamp.
- Horn, Eva (2014) *Zukunft als Katastrophe*. Frankfurt a.M.: Fischer.
- Hughes, Thomas Parke (1986) The seamless web: Technology, science, etcetera, etcetera. *Social Studies of Science*. 16 (2): 281–292.
- Hughes, Thomas Parke (1987) The evolution of large technical systems. In: *The social construction of technological systems: New directions in the sociology and history of technology*. Herausgegeben von: Trevor J. Pinch, Wiebe E. Bijker und Thomas Parke Hughes, 51–82. Cambridge, London: MIT Press.

- Hughes, Thomas Parke (1993) *Networks of power: Electrification in Western society, 1880–1930*. Baltimore, London: Johns Hopkins University Press.
- Hughes, Thomas Parke (2004) *Human-built world. How to think about technology and culture*. Chicago, London: University of Chicago Press.
- Husserl, Edmund (1982) *Die Krisis der europäischen Wissenschaften und die transzendente Philosophie*. Hamburg: Felix Meiner.
- IPCC (2001) Summary for Policymakers. Climate Change 2001: Impacts, Adaptation, and Vulnerability. A Report of Working Group II. Genf: Intergovernmental Panel on Climate Change.
- IPCC (2007a) Impacts, Adaptation and Vulnerability. Contribution of working group II to the fourth assessment report of the IPCC. Genf: Intergovernmental Panel on Climate Change.
- IPCC (2007b) IPCC: fourth assessment report. Genf: Intergovernmental Panel on Climate Change.
- IPCC (2012) Managing the risk of extreme events and disasters to advance climate change adaptation. Genf: Intergovernmental Panel on Climate Change.
- ISO (2012a) 22301: Societal security. Business continuity management systems. Guidance. Genf: International Organization for Standardization.
- ISO (2012b) 22301: Societal security. Business continuity management systems. Requirements. Genf: International Organization for Standardization.
- ISO (2015) 22317: Societal security. Business continuity management systems. Guidelines for business impact analysis (BIA). Genf: International Organization for Standardization.
- Jäger, Siegfried (2004) *Kritische Diskursanalyse. Eine Einführung*. Münster: Unrast.
- Jameson, Fredric (2003) Future city. *New Left Review*. 21 (May, June): 65–80.
- Japp, Klaus Peter (1990) Das Risiko der Rationalität für technisch-ökologische Systeme. In: *Risikante Entscheidungen und Katastrophenpotentiale*. Herausgegeben von: Klaus Peter Japp und Jost Halfmann, 34–60. Opladen: Westdeutscher Verlag.
- Japp, Klaus Peter (1992) Selbstverstärkungseffekte riskanter Entscheidungen: Zur Unterscheidung von Rationalität und Risiko. *Zeitschrift für Soziologie*. 21 (1): 31–48.
- Japp, Klaus Peter (2003) Zur Soziologie der Katastrophe. In: *Entsetzliche soziale Prozesse. Theorie und Empirie der Katastrophen*. Herausgegeben von: Lars Clausen, Elke M. Geenen und Elísio Macamo, 77–90. Münster: Lit-Verlag.
- Jasanoff, Sheila (2000) Commentary: Between risk and precaution. Reassessing the future of GM crops. *Journal of Risk Research*. 3 (3): 277–282.
- Jaspers, Karl (1999) *Die geistige Situation der Zeit*. Berlin, New York: Walter de Gruyter.
- Joerges, Bernward (1999) Do politics have artefacts? *Social Studies of Science*. 29 (3): 411–431.
- Joint-Forum (2006) High-level principles for business continuity. Basel: Basel Committee on Banking Supervision. Bank for International Settlements.



- Jonas, Hans (1989) *Das Prinzip Verantwortung: Versuch einer Ethik für die technologische Zivilisation*. Frankfurt a.M.: Suhrkamp.
- Joseph, Jonathan (2013) Resilience as embedded neoliberalism: A governmentality approach. *Resilience*. 1 (1): 38–52.
- Jungk, Robert (1977) *Der Atomstaat. Vom Fortschritt in die Unmenschlichkeit*. München: Kindler.
- Kalthoff, Herbert, Stefan Hirschauer und Gesa Lindemann (Hg.) (2008) *Theoretische Empirie: Zur Relevanz qualitativer Forschung*. Frankfurt a.M.: Suhrkamp.
- Kant, Immanuel (1968) Grundlegung zur Metaphysik der Sitten. In: *Werke Band 6*, 11–102. Darmstadt: Wissenschaftliche Buchgesellschaft Darmstadt.
- Kaube, Jürgen (2002) Die Vorsorgemaschine. *Frankfurter Allgemeine Zeitung*, 14.09.2002.
- Kaufman, George G. und Kenneth E. Scott (2003) What is systemic risk, and do bank regulators retard or contribute to it? *Independent Review*. 7 (3): 371–391.
- Kaufmann, Franz Xaver (1970) *Sicherheit als soziologisches und sozialpolitisches Problem. Untersuchungen zu einer Wertidee hochdifferenzierter Gesellschaften*. Stuttgart: Enke.
- Kaufmann, Stefan (2011) Zivile Sicherheit: Vom Aufstieg eines Topos. *Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert*. *Leviathan Sonderheft 25*. Herausgegeben von: Leon Hempel, Susanne Krasmann und Ulrich Bröckling, 101–123.
- Kaufmann, Stefan (2012) Resilienz als »Boundary Object«. In: *Sicherheitskultur. Soziale und politische Praktiken der Gefahrenabwehr*. Herausgegeben von: Christopher Daase, Philipp Offermann und Valentin Rauer, 109–131. Frankfurt a.M.: Campus.
- Kautzer, Chad (2007) Topographia Dominium: Property, divided sovereignty, and the spaces of rule. In: *Colonial and global interfacing: Imperial hegemonies and democratizing resistances*. Herausgegeben von: Gary Backhaus und John Murungi, 55–77. Cambridge: Cambridge Scholars Publishing.
- Kersten, Jens (2005) Die Entwicklung des Konzepts der Daseinsvorsorge im Werk von Ernst Forsthoff. *Der Staat*. 44 (4): 543–569.
- Kersten, Jens (2008) Mindestgewährleistungen im Infrastrukturrecht. *Informationen zur Raumentwicklung* (1/2): 1–15.
- Klinenberg, Eric (2003) *Heat wave: A social autopsy of disaster in Chicago*. Chicago: University of Chicago Press.
- Klinke, Andreas und Ortwin Renn (2002) A new approach to risk evaluation and management: Risk-based, precaution-based, and discourse-based strategies. *Risk Analysis*. 22 (6): 1071–1094.
- Klinke, Ian (2015) The bunker and the camp: Inside West Germany's nuclear tomb. *Environment and Planning D: Society and Space*. 33 (1): 154–168.
- Knorr Cetina, Karin und Urs Bruegger (2004) Traders' Engagement with Markets. A Postsocial Relationship. In: *The Blackwell Cultural Economy Reader*. Herausgegeben von: Nigel Thrift und Ash Amin, 121–142. Oxford: Blackwell.

- Knorr-Cetina, Karin (2003) From pipes to scopes: The flow architecture of financial markets. *Distinktion: Scandinavian Journal of Social Theory*. 4 (2): 7–23.
- Knorr-Cetina, Karin und Urs Bruegger (2002) Global microstructures: The virtual societies of financial markets. *American Journal of Sociology*. 107 (4): 905–950.
- König, René (2012) *Soziologie als Krisenwissenschaft: Durkheim und das Paradigma der französischen Gesellschaft*. Wiesbaden: VS-Verlag.
- Koselleck, Reinhart (1973) *Kritik und Krise. Eine Studie zur Pathogenese der bürgerlichen Welt*. Frankfurt a.M.: Suhrkamp.
- Koselleck, Reinhart (1979) *Vergangene Zukunft: Zur Semantik geschichtlicher Zeiten*. Frankfurt a.M.: Suhrkamp.
- Koselleck, Reinhart (1982) Krise. In: *Geschichtliche Grundbegriffe: Historisches Lexikon zur politisch-sozialen Sprache in Deutschland* Herausgegeben von: Otto Brunner, Werner Conze und Reinhart Koselleck, 617–650. Stuttgart: Klett-Cotta.
- Krasmann, Susanne (2003) *Die Kriminalität der Gesellschaft. Zur Gouvernementalität der Gegenwart*. Konstanz: UVK.
- Krasmann, Susanne (2012) Targeted killing and its law: On a mutually constitutive relationship. *Leiden Journal of International Law*. 25 (03): 665–682.
- Krause, Florentin, Hartmut Bossel und Karl-Friedrich Müller-Reißmann (1980) *Energievende – Wachstum und Wohlstand ohne Erdöl und Uran*. Frankfurt a.M.: Fischer.
- Krause, Sebastian M., Stefan Boerries und Stefan Bornholdt (2013) Econophysics of adaptive power markets: When a market does not dampen fluctuations but amplifies them. *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*. 99 (1): 1–5.
- Kreutzfeldt, Malte (2015) Viel Geld für weniger Kohle. *taz, die tageszeitung*. 4.11.2015.
- Krugler, David F (2006) *This is only a test: How Washington DC prepared for nuclear war*. Basingstoke, New York: Palgrave Macmillan.
- Kuhn, Thomas S. (1976) *Die Struktur wissenschaftlicher Revolutionen*. Frankfurt a.M.: Suhrkamp.
- Laak, Dirk van (1999) Der Begriff Infrastruktur und was er vor seiner Erfindung besagte. *Archiv für Begriffsgeschichte*. 41 (1): 280–299.
- Laak, Dirk van (2001) Infra-strukturgeschichte. *Geschichte und Gesellschaft*. 27 (3): 367–393.
- Laak, Dirk van (2012) Pionier des Politischen? Infrastruktur als europäisches Integrationsmedium. In: *Verkehrsgeschichte und Kulturwissenschaft: Analysen an der Schnittstelle von Technik, Kultur und Medien*. Herausgegeben von: Christoph Neubert und Gabriele Schabacher, 165–188. Bielefeld: transcript.
- Lakoff, Andrew (2007) Preparing for the next emergency. *Public Culture*. 19 (2): 247–271.
- Lakoff, Andrew (2008) The generic biothreat. Or, how we became unprepared. *Cultural Anthropology*. 23 (3): 399–428.

- Lakoff, Andrew und Stephen J. Collier (Hg.) (2008) *Biosecurity interventions: Global health and security in question*. New York, Chichester: Columbia University Press.
- Lampland, Martha und Susan Leigh Star (2009) Reckoning with standards. In: *Standards and their Stories. How quantifying, classifying, and formalizing practices shape everyday life*. Herausgegeben von: Martha Lampland und Susan Leigh Star, 3–24. Ithaca: Cornell University Press.
- Landecker, Hannah (2016) Antibiotic resistance and the biology of history. *Body & Society*. 22 (4): 19–52.
- Langenohl, Andreas (2013) Finanzialisierung politischer Sicherheit: Das Beispiel der »Euro-Rettung«. In: *Verunsicherte Gesellschaft – Überforderter Staat. Zum Wandel der Sicherheitskultur*. Herausgegeben von: Christopher Daase, Stefan Engert und Julian Jungk, 279–298. Frankfurt a.M.: Campus.
- Langenohl, Andreas (2015) Collateralized politics: The transformation of trust in sovereign debt in the wake of the Eurozone crisis. *Behemoth. A Journal on Civilisation*. 8 (1): 67–90.
- Langley, Paul (2013) Anticipating uncertainty, reviving risk? On the stress testing of finance in crisis. *Economy and Society*. 42 (1): 51–73.
- Langley, Paul (2014) *Liquidity lost: The governance of the global financial crisis*. Oxford: Oxford University Press.
- Larkin, Brian (2013) The politics and poetics of infrastructure. *Annual Review of Anthropology*. 42: 327–343.
- Latour, Bruno (1987) *Science in action. How to follow scientists and engineers through society*. Cambridge: Harvard University Press.
- Latour, Bruno (1990) Technology is society made durable. *The Sociological Review*. 38 (S1): 103–131.
- Latour, Bruno (2001a) *Das Parlament der Dinge. Für eine politische Ökologie*. Frankfurt a.M.: Suhrkamp.
- Latour, Bruno (2001b) Eine Soziologie ohne Objekt? *Berliner Journal für Soziologie*. 11 (2): 237–252.
- Latour, Bruno (2004) Why has critique run out of steam? From matters of fact to matters of concern. *Critical inquiry*. 30 (2): 225–248.
- Latour, Bruno (2007) *Eine neue Soziologie für eine neue Gesellschaft. Einführung in die Akteur-Netzwerk-Theorie*. Frankfurt a.M.: Suhrkamp.
- Latour, Bruno (2008) *Wir sind nie modern gewesen. Versuch einer symmetrischen Anthropologie*. Frankfurt a.M.: Suhrkamp.
- Latour, Bruno (2013) Facing Gaia: Six Lectures on the Political Theology of Nature. Gifford Lectures on natural religion. [http://macaulay.cuny.edu/eportfolios/wakefield15/files/2015/01/LATOURGIFFORD-SIX-LECTURES\\_1.pdf](http://macaulay.cuny.edu/eportfolios/wakefield15/files/2015/01/LATOURGIFFORD-SIX-LECTURES_1.pdf) (abgerufen am 23.03.2016).
- Latour, Bruno (2014) *Existenzweisen. Eine Anthropologie der Modernen*. Berlin: Suhrkamp.
- Latour, Bruno und Steve Woolgar (1979) *Laboratory life: The construction of scientific facts*. Princeton: Princeton University Press.

- Lau, Christoph (1989) Risikodiskurse: Gesellschaftliche Auseinandersetzungen um die Definition von Risiken. *Soziale Welt*. 40 (3): 418–436.
- Laufenberg, Mike (2014) *Sexualität und Biomacht. Vom Sicherheitsdispositiv zur Politik der Sorge*. Bielefeld: transcript.
- Law, John (2004) *After method: Mess in social science research*. London: Routledge.
- Law, John (2006) Disaster in agriculture: Or foot and mouth mobilities. *Environment and Planning A*. 38 (2): 227.
- Leanza, Matthias (2011) Die Geschichte des Kommenden. Zur Historizität der Zukunft im Anschluss an Luhmann und Foucault. *Bebemoth. A Journal on Civilisation*. 4 (2): 11–25.
- Leanza, Matthias (2015) Emotionale Immunisierung. Das Subjekt der Salutogenese. In: *Handbuch Theraputisierung und Soziale Arbeit. Verallgemeinerung theraputisierender Perspektiven und Praktiken*. Herausgegeben von: Roland Anhorn und Marcus Balzereit, 409–424. Wiesbaden: VS-Verlag.
- Lee, Benjamin und Edward LiPuma (2004) *Financial derivatives and the globalization of risk*. Durham: Duke University Press.
- Lemke, Thomas (1997) *Eine Kritik der politischen Vernunft. Foucaults Analyse der modernen Gouvernementalität*. Hamburg: Argument.
- Lemke, Thomas (2006) *Die Polizei der Gene. Formen und Felder genetischer Diskriminierung*. Frankfurt a.M., New York: Campus.
- Lemke, Thomas (2007a) *Biopolitik zur Einführung*. Hamburg: Junius.
- Lemke, Thomas (2007b) *Gouvernementalität und Biopolitik*. Wiesbaden: VS-Verlag.
- Lemke, Thomas (2011) Beyond Foucault. From biopolitics to the government of life. In: *Governmentality. Current issues and future challenges*. Herausgegeben von: Ulrich Bröckling, Susanne Krasmann und Thomas Lemke, 165–184. New York, Oxon: Routledge.
- Lenton, Timothy M., Hermann Held, Elmar Kriegler, Jim W. Hall, Wolfgang Lucht, Stefan Rahmstorf und Hans Joachim Schellnhuber (2008) Tipping elements in the Earth's climate system. *Proceedings of the National Academy of Sciences*. 105 (6): 1786–1793.
- Lentzos, Filippa und Nikolas Rose (2009) Governing insecurity: Contingency planning, protection, resilience. *Economy and Society*. 38 (2): 230–254.
- Lessenich, Stephan (2009) Mobilität und Kontrolle. Zur Dialektik der Aktivgesellschaft. In: *Soziologie, Kapitalismus, Kritik. Eine Debatte*. Herausgegeben von: Klaus Dörre, Stephan Lessenich und Hartmut Rosa, 126–179. Frankfurt a.M.: Suhrkamp.
- Lessenich, Stephan (2016) *Neben uns die Sintflut. Die Externalisierungsgesellschaft und ihr Preis*. Berlin: Hanser.
- Lindseth, Brian (2011) The pre-history of resilience in ecological research. *limn*. 1 (1): 35–37.
- Lobo-Guerrero, Luis (2012) Connectivity as the strategization of space: The case of the port of Hamburg. *Distinktion: Scandinavian Journal of Social Theory*. 13 (3): 310–321.

- Loick, Daniel (2012) *Kritik der Souveränität*. Frankfurt a.M., New York: Campus.
- Lorey, Isabell (2011) *Figuren des Immunen. Elemente einer politischen Theorie*. Zürich: diaphanes.
- Lovelock, James (2000) *Gaia: A new look at life on earth*. Oxford: Oxford Paperbacks.
- Lovelock, James (2009) *The vanishing face of Gaia: A final warning*. New York: Basic Books.
- Lovelock, James E. und Lynn Margulis (1974) Atmospheric homeostasis by and for the biosphere: the Gaia hypothesis. *Tellus*. 26 (1–2): 2–10.
- Lovins, Amory B. (1976) Energy strategy: The road not taken? *Foreign Affairs* (October): 186–218.
- Lovins, Amory B. (1977) Resilience in energy strategy. *New York Times*. 24.07.1977.
- Lovins, Amory B. (1978) *Sanfte Energie. Das Programm für die energie- und industrie-politische Umrüstung unserer Gesellschaft*. Reinbeck: Rowohlt.
- Lovins, Amory B. und L. Hunter Lovins (1982) *Brittle power. Energy strategy for national security*. Andover: Brick House Publishing Company.
- Luhmann, Niklas (1971a) Die Knappheit der Zeit und die Vordringlichkeit des Befristeten. In: *Politische Planung. Aufsätze zur Soziologie von Politik und Verwaltung*, 143–164. Wiesbaden: VS-Verlag.
- Luhmann, Niklas (1971b) Lob der Routine. In: *Politische Planung. Aufsätze zur Soziologie von Politik und Verwaltung*, 113–142. Wiesbaden: VS Verlag.
- Luhmann, Niklas (1976) The future cannot begin: Temporal structures in modern society. *Social Research*. 43 (1): 130–152.
- Luhmann, Niklas (1980) Temporalisierung von Komplexität. Zur Semantik neuzeitlicher Zeitbegriffe. In: *Gesellschaftsstruktur und Semantik. Studien zur Wissenssoziologie der modernen Gesellschaft*, 235–300. Frankfurt a.M.: Suhrkamp.
- Luhmann, Niklas (1991a) Am Ende der kritischen Soziologie. *Zeitschrift für Soziologie*. 20 (2): 147–152.
- Luhmann, Niklas (1991b) *Soziale Systeme. Grundriss einer allgemeinen Theorie*. Frankfurt a.M.: Suhrkamp.
- Luhmann, Niklas (1992a) Die Beschreibung der Zukunft. In: *Beobachtungen der Moderne*, 129–147. Wiesbaden: VS-Verlag.
- Luhmann, Niklas (1992b) Ökologie des Nichtwissens. In: *Beobachtungen der Moderne*, 129–147. Wiesbaden: VS-Verlag.
- Luhmann, Niklas (1997) Selbstorganisation und Mikrodiversität: Zur Wissenssoziologie des neuzeitlichen Individualismus. *Soziale Systeme*. 3 (1): 23–32.
- Luhmann, Niklas (1998a) *Die Gesellschaft der Gesellschaft. Erster Teilband*. Frankfurt a.M.: Suhrkamp.
- Luhmann, Niklas (1998b) *Die Gesellschaft der Gesellschaft. Zweiter Teilband*. Frankfurt a.M.: Suhrkamp.
- Luhmann, Niklas (2000) *Organisation und Entscheidung*. Opladen, Wiesbaden: Westdeutscher Verlag.
- Luhmann, Niklas (2003) *Soziologie des Risikos*. Berlin, New York: Walter de Gruyter.

- Luhmann, Niklas (2008) *Ökologische Kommunikation. Kann die moderne Gesellschaft sich auf ökologische Gefährdungen einstellen?* Wiesbaden: VS-Verlag.
- Luke, Timothy W. (2010) Power loss or blackout: The electricity network collapse of August 2003 in North America. In: *Disrupted cities: When infrastructure fails*. Herausgegeben von: Stephen Graham, 55–68. New York, London: Routledge.
- Lury, Celia, Luciana Parisi und Tiziana Terranova (2012) Introduction: The becoming topological of culture. *Theory, Culture & Society*. 29 (4–5): 3–35.
- Machiavelli, Niccolo (1978) *Der Fürst*. Stuttgart: Kröner.
- MacKenzie, Donald (2004) The big, bad wolf and the rational market: portfolio insurance, the 1987 crash and the performativity of economics. *Economy and Society*. 33 (3): 303–334.
- MacKenzie, Donald (2006) *An engine, not a camera. How financial models shape markets*. Cambridge, London: MIT Press.
- MacKenzie, Donald (2007) The material production of virtuality: innovation, cultural geography and facticity in derivatives markets. *Economy and Society*. 36 (3): 355–376.
- MacKenzie, Donald (2011) How to make money in microseconds. *London Review of Books*. 33 (10): 16–18.
- MacKenzie, Donald (2013) Mechanizing the Merc: The Chicago Mercantile Exchange and the rise of high-frequency trading. Working Paper.
- MacKenzie, Donald, Daniel Beunza, Yuval Millo und Juan Pablo Pardo-Guerra (2012) Drilling through the Allegheny Mountains: liquidity, materiality and high-frequency trading. *Journal of Cultural Economy*. 5 (3): 279–296.
- Malm, Andreas und Alf Hornborg (2014) The geology of mankind? A critique of the Anthropocene narrative. *The Anthropocene Review*. 1 (1): 62–69.
- Mandelbrot, Benoît und Richard L. Hudson (2006) *The (mis)behavior of markets: A fractal view of financial turbulence*. New York: Basic Books.
- Mandelbrot, Benoît und Nassim Taleb (2010) Mild vs. wild randomness: Focussing on those risks that matter. In: *The known, the unknown and the unknowable in financial risk management. Measurement and theory advancing practice*. Herausgegeben von: Francis X. Diebold, Neil A. Doherty und Richard J. Herring, 47–58. New Jersey: Princeton University Press.
- Mann, Michael (1984) The autonomous power of the state: Its origins, mechanisms and results. *European Journal of Sociology*. 25 (2): 185–213.
- Margulis, Lynn (1999) *Symbiotic planet: a new look at evolution*. New York: Basic Books.
- Marquardt, Nadine (2016) Counting the countless: Statistics on homelessness and the spatial ontology of political numbers. *Environment and Planning D: Society and Space*. 34 (2): 301–318.
- Marquardt, Nadine (2017) Zonen infrastruktureller Entkopplung. Urbane Prekarität und soziotechnische Verknüpfungen im öffentlichen Raum. In: *Infrastrukturen der Stadt*. Herausgegeben von: Michael Flitner, Julia Lossau und Anna-Lisa Müller, 89–104. Wiesbaden: VS-Verlag.

- Marres, Noortje (2007) The issues deserve more credit. Pragmatist contributions to the study of public involvement in controversy. *Social Studies of Science*. 37 (5): 759–780.
- Marres, Noortje (2012) *Material participation: technology, the environment and everyday publics*. Basingstoke, New York: Palgrave Macmillan.
- Marres, Noortje und Javier Lezaun (2011) Materials and devices of the public: An introduction. *Economy and Society*. 40 (4): 489–509.
- Marx, Karl (1968) *Das Kapital, Marx-Engels Werke. Band 23*. Berlin: Dietz Verlag.
- Marx, Karl (1969) Zur Judenfrage. In: *Marx-Engels Werke. Band 1*, 347–377. Berlin: Dietz-Verlag.
- Marx, Karl und Friedrich Engels (1990) Manifest der Kommunistischen Partei. In: *Marx-Engels Werke. Band 4*, 459–493. Berlin: Dietz Verlag.
- Masco, Joseph (2009) Life underground: Building the bunker society. *Anthropology Now*. 1 (2): 13–29.
- Masco, Joseph (2010) Bad weather: On planetary crisis. *Social Studies of Science*. 40 (1): 7–40.
- Masco, Joseph (2014) *The theater of operations: National security affect from the Cold War to the War on Terror*. Durham: Duke University Press.
- Massumi, Brian (2007) Potential politics and the primacy of preemption. *Theory and Event*. 10 (2).
- Massumi, Brian (2009) National enterprise emergency: Steps toward an ecology of powers. *Theory, Culture & Society*. 26 (6): 153–185.
- Massumi, Brian (2010a) The future birth of an affective fact. The political ontology of threat. In: *The Affect Theory Reader*. Herausgegeben von: Melissa Gregg und Gregory J. Seigworth, 52–70. Durham: Duke University Press.
- Massumi, Brian (2010b) *Ontomacht: Kunst, Affekt und das Ereignis des Politischen*. Berlin: Merve.
- Matzerath, Horst (1991) »Kommunale Leistungsverwaltung«: Zu Bedeutung und politischer Funktion des Begriffs im 19. und 20. Jahrhundert. In: *Kommunale Leistungsverwaltung und Stadtentwicklung vom Vormärz bis zur Weimarer Republik*. Herausgegeben von: Hans Heinrich Blotvogel, 3–24. Köln: Böhlau.
- Maurer, Bill (2012) Payment: Forms and functions of value transfer in contemporary society. *Cambridge Anthropology*. 30 (2): 15–35.
- Mayntz, Renate (2009) The changing governance of large technical infrastructure systems. In: *Über Governance. Institutionen und Prozesse politischer Regelung*, 121–150. Frankfurt a.M.: Campus.
- Mbembe, Achille (2003) Necropolitics. *Public Culture*. 15 (1): 11–40.
- McFarlane, Colin und Jonathan Rutherford (2008) Political infrastructures: governing and experiencing the fabric of the city. *International Journal of Urban and Regional Research*. 32 (2): 363–374.
- McGoey, Linsey (2012) Strategic unknowns: Towards a sociology of ignorance. *Economy and Society*. 41 (1): 1–16.

- Meadows, Donella H., Dennis L. Meadows, Jorgen Randers und Williams W. Behrens (1972) *The limits to growth*. New York: Universe Books.
- Meyer, Katrin (2009) Kritik der Sicherheit. Vom gouvernementalen Sicherheitsdenken zur Politik der geteilten Sorge. *traverse*. 1: 25–39.
- Mezzadra, Sandro und Brett Neilson (2013) Extraction, logistics, finance: Global crisis and the politics of operations. *Radical Philosophy*. 178 (März, April): 8–18.
- Miller, Rich (2011) NYSE's data fortress powering the financial cloud. <http://www.datacenterknowledge.com/archives/2011/06/30/nyses-data-fortress-powering-the-financial-cloud/> (abgerufen 23.03.2016).
- Minten, Dominique (2015) Kratzer am Klima-Vorbild Deutschland. *Frankfurter Allgemeine Zeitung*. 02.11.2015.
- Mirowski, Philip (1989) *More heat than light. Economics as social physics, physics as nature's economics*. Cambridge, New York, Melbourne: Cambridge University Press.
- Mirowski, Philip (2009) Postface. Defining neoliberalism. In: *The road from Mont Perlin. The making of the neoliberal thought collective*. Herausgegeben von: Philip Mirowski und Dieter Plehwe, 417–455. Cambridge, London: Harvard University Press.
- Mitchell, Timothy (2002) *Rule of experts: Egypt, techno-politics, modernity*. Berkeley, Los Angeles: University of California Press.
- Mitchell, Timothy (2009) Carbon democracy. *Economy and Society*. 38 (3): 399–432.
- Mitchell, Timothy (2011) *Carbon democracy: Political power in the age of oil*. London, New York: Verso.
- Mol, Annemarie (2002) *The body multiple: Ontology in medical practice*. Durham: Duke University Press.
- Mukerji, Chandra (2007) Stewardship politics and the control of wild weather: Levees, seawalls, and state building in 17th-century France. *Social Studies of Science*. 37 (1): 127–133.
- Mukerji, Chandra (2010) The territorial state as a figured world of power: Strategies, logistics, and impersonal rule. *Sociological Theory*. 28 (4): 402–424.
- Mumford, Lewis (1964) Authoritarian and democratic technics. *Technology and Culture*. 5 (1): 1–8.
- Muniesa, Fabian, Yuval Millo und Michel Callon (2007) An introduction to market devices. *The Sociological Review*. 55 (2): 1–12.
- Munster, Rens van (2005) Logics of security: The Copenhagen School, risk management and the war on terror. In *Political Science Publications 10/2005*. Syddansk: Syddansk Universitet.
- Nassehi, Armin (2009) *Der soziologische Diskurs der Moderne*. Frankfurt a.M.: Suhrkamp.
- NATO (2001) 50 years of Infrastructure. NATO Security Investment Programme is the sharing of roles, risks, responsibilities, costs and benefits. Brüssel: NATO's Infrastructure Committee.
- NBB (2007) Financial stability review. Brüssel: National Bank of Belgium.



- Nelson, Sara Holiday (2014) Resilience and the neoliberal counter-revolution: From ecologies of control to production of the common. *Resilience*. 2 (1): 1–17.
- Neocleous, Mark (2008) *Critique of security*. Edinburgh: Edinburgh University Press.
- Neu, Claudia (2009a) Daseinsvorsorge und territoriale Ungleichheit. In: *Daseinsvorsorge. Eine gesellschaftswissenschaftliche Annäherung*. Herausgegeben von: Claudia Neu, 80–96. Wiesbaden: VS-Verlag.
- Neu, Claudia (2009b) Daseinsvorsorge. Eine Einleitung. In: *Daseinsvorsorge. Eine gesellschaftswissenschaftliche Annäherung*. Herausgegeben von: Claudia Neu, 9–21. Wiesbaden: VS-Verlag.
- Neu, Claudia (Hg.) (2009c) *Daseinsvorsorge. Eine gesellschaftswissenschaftliche Annäherung*. Wiesbaden: VS-Verlag.
- Neumann, Franz (1984) *Behemoth. Struktur und Praxis des Nationalsozialismus 1933–1944*. Frankfurt a.M.: Fischer.
- NHWSP (2014) Nationales Hochwasserschutzprogramm. Kriterien und Bewertungsmaßstäbe für die Identifikation und Priorisierung von wirksamen Maßnahmen sowie ein Vorschlag für die Liste der prioritären Maßnahmen zur Verbesserung des präventiven Hochwasserschutzes. Kiel: Bund/Länderarbeitsgemeinschaft Wasser (LAWA).
- Nienhaus, Lisa (2014) Die neue Burg der EZB. *Frankfurter Allgemeine Zeitung*. 20.10.2014.
- O'Malley, Pat (2003) Governable catastrophes: A comment on Bougen. *Economy and Society*. 32 (2): 275–279.
- O'Malley, Pat (2010) Resilient subjects: Uncertainty, warfare and liberalism. *Economy and Society*. 39 (4): 488–509.
- O'Malley, Pat (2012) *Risk, uncertainty and government*. London: Routledge.
- Ong, Aihwa (2006) *Neoliberalism as exception: Mutations in citizenship and sovereignty*. Durham: Duke University Press.
- Ong, Aihwa (2007) Neoliberalism as a mobile technology. *Transactions of the Institute of British Geographers*. 32 (1): 3–8.
- Ong, Aihwa und Stephen J. Collier (Hg.) (2005a) *Global assemblages: Technology, politics, and ethics as anthropological problems*. Malden, Oxford: Blackwell.
- Ong, Aihwa und Stephen J. Collier (2005b) Global assemblages. Anthropological problems. In: *Global assemblages. Technology, politics and ethics as anthropological problems*. Herausgegeben von: Aihwa Ong und Stephen J. Collier, 3–21. Malden, Oxford: Blackwell.
- Opitz, Sven (2008) Zwischen Sicherheitsdispositiv und Securitization: Zur Analytik illiberaler Gouvernementalität In: *Gouvernementalität und Sicherheit. Zeitdiagnostische Beiträge im Anschluss an Foucault*. Herausgegeben von: Patricia Purtschert, Katrin Mayer und Yves Winter, 201–228. Bielefeld: transcript.
- Opitz, Sven (2011) Widerstreitende Temporalitäten. Recht in Zeiten des Risikos. *Behemoth. A Journal on Civilisation*. 4 (2): 58–82.
- Opitz, Sven (2012) *An den Grenzen des Rechts. Inklusion/Exklusion im Zeichen der Sicherheit*. Weilerswist: Velbrück.

- Opitz, Sven (2013) Was ist Kritik? Was ist Aufklärung? Zum Spiel der Möglichkeiten bei Niklas Luhmann und Michel Foucault. In: *Kritische Systemtheorie. Zur Evolution einer normativen Theorie*. Herausgegeben von: Marc Amstutz und Andreas Fischer-Lescano, 39–62. Bielefeld: transcript.
- Opitz, Sven (2015) Regulating epidemic space: the nomos of global circulation. *Journal of International Relations and Development*. Online vor Druck. doi: 10.1057/jird.2014.30.
- Opitz, Sven (2016) Neue globale Kollektivität: Das Kosmopolitische bei Ulrich Beck und Bruno Latour. *Soziale Welt*. 67 (3): 249–266.
- Opitz, Sven und Ute Tellmann (2012) Global territories: Zones of economic and legal dis/connectivity. *Distinktion: Scandinavian Journal of Social Theory*. 13 (3): 261–282.
- Opitz, Sven und Ute Tellmann (2015a) Europe as infrastructure: Networking the operative community. *South Atlantic Quarterly*. 114 (1): 171–190.
- Opitz, Sven und Ute Tellmann (2015b) Future emergencies: Temporal politics in law and economy. *Theory, Culture & Society*. 32 (2): 107–129.
- Ortmann, Günther (2003) *Regel und Ausnahme. Paradoxien sozialer Ordnung*. Frankfurt a.M.: Suhrkamp.
- Osborne, Thomas (1996) Security and vitality: Drains, liberalism and power in the nineteenth century. In: *Foucault and political reason: Liberalism, neo-liberalism and the rationalities of government*. Herausgegeben von: Andrew Barry, Thomas Osborne und Nikolas Rose, 99–121. Oxon: Routledge.
- Ouma, Stefan (2010) Global standards, local realities: Private agrifood governance and the restructuring of the Kenyan horticulture industry. *Economic Geography*. 86 (2): 197–222.
- Palmer, Donald und Michael Maher (2010) A normal accident analysis of the mortgage meltdown. In: *Markets on trial: The economic sociology of the U.S. financial crisis*. Herausgegeben von: Michael Lounsbury und Paul M. Hirsch, 219–256. Bingley: Emerald Group Publishing.
- Pardo-Guerra, Juan Pablo (2010) Creating flows of interpersonal bits: The automation of the London Stock Exchange. 1955–90. *Economy and Society*. 39 (1): 84–109.
- PCCP (1997) Critical Foundations. Protecting America's Infrastructure. Washington: President's Commission on Critical Infrastructure Protection.
- Pelzer, Peter (2007) Basel II, oder: Die Einsicht in die unzureichende Verlässlichkeit reiner Quantifizierung. In: *Zahlenwerk*. Herausgegeben von: Andrea Mennicken und Hendrik Vollmer, 105–121. Wiesbaden: VS-Verlag.
- Perrow, Charles (1987) *Normale Katastrophen. Die unvermeidbaren Risiken der Großtechnik*. Frankfurt a.M.: Campus.
- Perrow, Charles (2010) The meltdown was not an accident. In: *Markets on trial: The economic sociology of the U.S. financial crisis*. Herausgegeben von: Michael Lounsbury und Paul M. Hirsch, 309–330. Bingley: Emerald Group Publishing.

- Perrow, Charles (2011) *The next catastrophe: Reducing our vulnerabilities to natural, industrial, and terrorist disasters*. New Jersey: Princeton University Press.
- Peter, Christoph J. (2008) Deutschlands geheimer Superbunker. *Der Spiegel*. 18.03.2008.
- Petryna, Adriana (2002) *Life exposed: biological citizens after Chernobyl*. Princeton: Princeton University Press.
- Pfadenhauer, Michaela (2009) Auf gleicher Augenhöhe. Das Experteninterview – ein Gespräch zwischen Experte und Quasi-Experte. In: *Experteninterviews. Theorien, Methoden, Anwendungsfelder*. Herausgegeben von: Alexander Bogner, Beate Littig und Wolfgang Menz, 99–116. Wiesbaden: VS-Verlag.
- Pias, Claus (2009) Abschreckung Denken. Herman Kahns Szenarien. In: *Abwehr. Modelle – Strategien – Medien*. Herausgegeben von: Claus Pias, 169–187. Bielefeld: transcript.
- Pickering, Andrew (2004) The science of the unknowable: Stafford Beer's cybernetic informatics. *Kybernetes*. 33 (3/4): 499–521.
- PIK (2016) Kippelemente. Achillesfesen im Erdsystem. Potsdam Institut für Klimafolgenforschung. <http://www.pik-potsdam.de/services/infothek/kipp-elemente> (abgerufen am 23.03.2016).
- Pinch, Trevor und Richard Swedberg (2008) *Living in a material world: Economic sociology meets science and technology studies*. Cambridge: MIT Press.
- Polanyi, Karl (1957) *The great transformation. The political and economic origins of our time*. Boston: Beacon.
- Porter, Theodore M. (1996) *Trust in numbers: The pursuit of objectivity in science and public life*. Princeton: Princeton University Press.
- Power, Michael (1999) *The audit society: Rituals of verification*. New York, Oxford: Oxford University Press.
- Power, Michael (2005) The Invention of Operational Risk. *Review of International Political Economy*. 12 (4): 577–599.
- Power, Michael (2007) *Organized uncertainty: Organizing a world of risk management*. Oxford: Oxford University Press.
- Power, Michael (2009) The risk management of nothing. *Accounting, Organizations and Society*. 34 (6): 849–855.
- Purtschert, Patricia, Katrin Mayer und Yves Winter (Hg.) (2008) *Gouvernementalität und Sicherheit. Zeitdiagnostische Beiträge im Anschluss an Foucault*. Bielefeld: transcript.
- Rabinow, Paul (1995) *French Modern. Norms and forms of the social environment*. Chicago: University of Chicago Press.
- Rabinow, Paul (2003) *Anthropos today: Reflections on modern equipment*. Princeton: Princeton University Press.
- Rabinow, Paul (2008) *Marking time: On the anthropology of the contemporary*. Princeton: Princeton University Press.
- Radkau, Joachim (2011) *Die Ära der Ökologie: Eine Weltgeschichte*. München: C.H. Beck.

- Rasch, Philip J., Paul J. Crutzen und Danielle B. Coleman (2008) Exploring the geoengineering of climate using stratospheric sulfate aerosols: The role of particle size. *Geophysical Research Letters*. 35 (2).
- Redfield, Peter (2008) Sacrifice, triage and global humanitarianism. In: *Humanitarianism in question: Politics, power, ethics*. Herausgegeben von: Michael Barnett und Thomas G. Weiss, 196–214. Ithaca: Cornell University Press.
- Redfield, Peter (2013) *Life in crisis: The ethical journey of doctors without borders*. Berkley, Los Angeles, London: University of California Press.
- Reemtsma, Jan Philipp (2010) Gewalt und Vertrauen. *Psychotherapeut*. 55 (2): 89–97.
- Reid, Julian (2006) *The biopolitics of the war on terror. Life struggles, liberal modernity, and the defence of logistical societies*. Manchester: Manchester University Press.
- Renn, Ortwin und Florian Keil (2008) Systemische Risiken: Versuch einer Charakterisierung. *GALA – Ecological Perspectives for Science and Society*. 17 (4): 349–354.
- Rheinberger, Hans-Jörg (2002) *Experimentalsysteme und epistemische Dinge: eine Geschichte der Proteinsynthese im Reagenzglas*. Göttingen: Wallstein.
- Rifkin, Jeremy (2011) *Die dritte industrielle Revolution: Die Zukunft der Wirtschaft nach dem Atomzeitalter*. Frankfurt a.M.: Campus.
- Riles, Annelise (2006) Introduction: In Response. In: *Documents: artifacts of modern knowledge*. Herausgegeben von: Annelise Riles, 1–38. Minneapolis: University of Michigan Press.
- Riles, Annelise (2011) *Collateral knowledge: Legal reasoning in the global financial markets*. Chicago: University of Chicago Press.
- Rochlin, Gene I., Todd R. La Porte und Karlene H. Roberts (1998) The self-designing high-reliability organization: Aircraft carrier flight operations at sea. *Naval War College Review*. 51 (3): 97–113.
- Rockström, Johan, Will Steffen, Kevin Noone, Åsa Persson, F. Stuart Chapin, Eric F. Lambin, Timothy M. Lenton, Marten Scheffer, Carl Folke und Hans-Joachim Schellnhuber (2009) A safe operating space for humanity. *Nature*. 461 (7263): 472–475.
- Rödel, Malaika (2014) *Geschlecht im Zeitalter der Reproduktionstechnologien: Natur, Technologie und Körper im Diskurs der Präimplantationsdiagnostik*. Bielefeld: transcript.
- Roitman, Janet (2013) *Anti-crisis*. Durham: Duke University Press.
- Ronellenfisch, Michael (2004) Daseinsvorsorge als Rechtsbegriff. Aktuelle Entwicklungen im nationalen und europäischen Recht. In: *Ernst Forstboff. Kolloquium aus Anlass des 100. Geburtstags von Prof. Dr. Dr. h.c. Ernst Forstboff*. Herausgegeben von: Willi Blümel, 53–114. Berlin: Duncker & Humblot.
- Rosa, Hartmut (2003) Social acceleration: Ethical and political consequences of a desynchronized high-speed society. *Constellations*. 10 (1): 3–33.
- Rose, Nikolas (1992) Governing the enterprising self. In: *The values of the enterprise culture*. Herausgegeben von: Paul Heelas und Paul Morris, 141–164. London: Roudledge.

- Rose, Nikolas (1993) Government, authority and expertise in advanced liberalism. *Economy and Society*. 22 (3): 283–299.
- Rose, Nikolas (1996a) The death of the social? Re-figuring the territory of government. *Economy and Society*. 25 (3): 327–356.
- Rose, Nikolas (1996b) Governing advanced liberal democracies. In: *Foucault and political reason*. Herausgegeben von: Andrew Barry, Thomas Osborne und Nikolas Rose, 37–64. Chicago: University of Chicago Press.
- Rose, Nikolas (2007) *The politics of life itself: Biomedicine, power, and subjectivity in the twenty-first century*. Princeton: Princeton University Press.
- Rose, Nikolas und Peter Miller (1992) Political power beyond the state. Problematics of government. *The British Journal of Sociology*. 43 (2): 173–205.
- Rothschild, Emma (1995a) Social security and laissez faire in eighteenth-century political economy. *Population and Development Review*. 21 (4): 711–744.
- Rothschild, Emma (1995b) What is security? *Daedalus*. 124 (3): 53–98.
- Rothschild, Emma (2001) *Economic sentiments. Adam Smith, Condorcet, and the enlightenment*. Cambridge, London: Harvard University Press.
- RSK (2011) Anlagenspezifische Sicherheitsüberprüfung (RSK-SÜ) deutscher Kernkraftwerke unter besonderer Berücksichtigung der Ereignisse in Fukushima-I (Japan). Salzgitter: Reaktorschutzkommission und Bundesamt für Strahlenschutz.
- Saar, Martin (2003) Nachwort. In: *Die Wahrheit der juristischen Formen*, 157–187. Frankfurt a.M.: Suhrkamp.
- Sahlins, Marshall (2010) Infrastructuralism. *Critical Inquiry*. 36 (3): 371–385.
- Sanden, Joachim (2006) Das Vorsorgeprinzip im europäischen und deutschen Umweltrecht. Weiterentwicklung und Impulse für das internationale Recht. *Osaka University Law Review* (53): 243–270.
- Sassen, Saskia (1996) *Metropolen des Weltmarkts: Die neue Rolle der Global Cities*. Frankfurt a.M.: Campus.
- Sassen, Saskia (2008) Neither global nor national: novel assemblages of territory, authority and rights. *Ethics & Global Politics*. 1 (1–2): 61–79.
- Sauer, Matt und Michael Versace (2012) Sandy surfaces the Importance of the »Human Machine« on Wall Street. Herausgegeben von IDC-Community. New York.
- Schellnhuber, Hans-Joachim (1999) »Earth system« analysis and the second Copernican revolution. *Nature*. 402 (6761): 19–23.
- Scheuerman, William E. (1999) The economic state of emergency. *Cardozo Law Review*. 21: 1869–1894.
- Schmitt, Carl (2004) *Politische Theologie: Vier Kapitel zur Lehre von der Souveränität*. Berlin: Duncker & Humblot.
- Schmitt, Carl (2011) *Der Nomos der Erde im Völkerrecht des Jus Publicum Europaeum*. Berlin: Duncker & Humblot.

- Schnitzler, Antina von (2013) Traveling technologies: infrastructure, ethical regimes, and the materiality of politics in South Africa. *Cultural Anthropology*. 28 (4): 670–693.
- Schnitzler, Antina von (2008) Citizenship prepaid: Water, calculability, and technopolitics in South Africa. *Journal of Southern African Studies*. 34 (4): 899–917.
- Schumacher, Ernst Friedrich (2011) *Small is beautiful: A study of economics as if people mattered*. New York City: Random House.
- Schutzkommission (1996) Mögliche Gefahren für die Bevölkerung bei Großkatastrophen und im Verteidigungsfall. Bonn: Schutzkommission beim Bundesministerium des Innern.
- Schutzkommission (2001) Zweiter Gefahrenbericht der Schutzkommission beim Bundesminister des Innern: Bericht über mögliche Gefahren für die Bevölkerung bei Großkatastrophen und im Verteidigungsfall. Bonn: Schutzkommission beim Bundesministerium des Innern.
- Schutzkommission (2006) Dritter Gefahrenbericht der Schutzkommission beim Bundesminister des Innern. Bonn: Schutzkommission beim Bundesministerium des Innern.
- Schutzkommission (2011) Vierter Gefahrenbericht der Schutzkommission beim Bundesminister des Innern. Bonn: Schutzkommission beim Bundesministerium des Innern.
- Schwartz, Peter und Doug Randall (2003) An abrupt climate change scenario and its implications for United States national security. [http://www.edf.org/documents/3566\\_AbruptClimateChange.pdf](http://www.edf.org/documents/3566_AbruptClimateChange.pdf) (abgerufen 23.03.2016).
- Scott, James C. (1998) *Seeing like a state: How certain schemes to improve the human condition have failed*. New Haven: Yale University Press.
- Sennelart, Michel (2006) Situierung der Vorlesungen. In: *Die Geburt der Biopolitik (Geschichte der Gouvernementalität II). Vorlesungen am Collège de France, 1978–1979*, 445–489. Frankfurt a.M.: Suhrkamp.
- Serres, Michel (1981) *Der Parasit*. Frankfurt a.M.: Suhrkamp.
- Serres, Michel (1994) *Der Naturvertrag*. Frankfurt a.M.: Suhrkamp.
- Serres, Michel (2008a) *Aufklärungen: Fünf Gespräche mit Bruno Latour*. Berlin: Merve.
- Serres, Michel (2008b) *The five senses: A philosophy of mingled bodies*. New York, London: Continuum Publishing.
- Silver, Beverly J. (2005) *Forces of labor: Arbeiterbewegungen und Globalisierung seit 1870*. Berlin: Assoziation A.
- Simmel, Georg (1992) *Soziologie. Untersuchung über die Formen der Vergesellschaftung. Gesamtausgabe Band II*. Frankfurt a.M.: Suhrkamp.
- Simondon, Gilbert (1992) The Genesis of the Individual. In: *Incorporations*. Herausgegeben von: Jonathan Crary und Sanford Kwinter, 296–319. New York: Zone Books.
- Simondon, Gilbert (2012) *Die Existenzweise technischer Objekte*. Zürich: diaphanes.
- Sloterdijk, Peter (2004) *Schäume. Sphären III: Plurale Sphärologie*. Frankfurt a.M.: Suhrkamp.

- Speer, Albert (1969) *Erinnerungen*. Berlin: Propyläen.
- Stäheli, Urs (1998) Die Nachträglichkeit der Semantik. Zum Verhältnis von Sozialstruktur und Semantik. *Soziale Systeme*. 4 (2): 315–339.
- Stäheli, Urs (2000) *Sinnzusammenbrüche. Eine dekonstruktive Lektüre von Niklas Luhmanns Systemtheorie*. Göttingen: Velbrück.
- Stäheli, Urs (2007) *Spektakuläre Spekulation. Das Populäre der Ökonomie*. Frankfurt a.M.: Suhrkamp.
- Stäheli, Urs (2013) Entnetzt Euch! Praktiken und Ästhetiken der Anschlusslosigkeit. *Mittelweg* 36. 2013 (4): 3–28.
- Star, Susan Leigh (1999) The ethnography of infrastructure. *American Behavioral Scientist*. 43 (3): 377–391.
- Star, Susan Leigh und James R. Griesemer (1989) Institutional ecology, »translations« and boundary objects: Amateurs and professionals in Berkeley's Museum of Vertebrate Zoology, 1907–39. *Social Studies of Science*. 19 (3): 387–420.
- Stengers, Isabelle (2008) *Spekulativer Konstruktivismus*. Berlin: Merve.
- Stenmanns, Julian (2014) Contingent Territory. Sovereignty, Territoriality and the European Central Bank (unveröffentlichte Hausarbeit). Frankfurt a.M.
- Stoler, Ann Laura (2014) Fieldwork in Philosophy. Refiguring Social Inquiry's Conceptual Ground. Sechs Vorlesungen. <https://http://www.youtube.com/watch?v=boQAsz7axWc> (abgerufen 23.03.2016).
- Stone, Deborah (2002) Beyond moral hazard. Insurance as moral opportunity. In: *Embracing risk. The changing culture of risk and responsibility*. Herausgegeben von: Tom Baker und Jonathan Simon, 52–79. Chicago, London: University of Chicago Press.
- Strathern, Marilyn (2003) *Commons and borderlands: Working papers on interdisciplinarity, accountability and the flow of knowledge*. Herefordshire: Sean Kingston Publishing.
- Sunstein, Cass (2007) *Gesetze der Angst. Jenseits des Vorsorgeprinzips*. Frankfurt a.M.: Suhrkamp.
- Swyngedouw, Erik (2006) Circulations and metabolisms: (hybrid) natures and (cyborg) cities. *Science as Culture*. 15 (2): 105–121.
- TAB (2011) Was bei einem Blackout geschieht. Folgen eines langandauernden und großräumigen Stromausfalls. Berlin: Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag.
- Taleb, Nassim Nicholas (2007) *The Black Swan. The impact of the highly improbable*. New York: Penguin.
- Taylor, Charles (2004) *Modern social imaginaries*. Durham, London: Duke University Press.
- Tellmann, Ute (2011) The economic beyond governmentality. The limits of conduct. In: *Governmentality. Current issues and future challenges*. Herausgegeben von: Ulrich Bröckling, Susanne Krasmann und Thomas Lemke, 285–303. London: Routledge.
- Tellmann, Ute (2013) Catastrophic populations and the fear of the future: Malthus and the genealogy of liberal economy. *Theory, Culture & Society*. 30 (2): 135–155.

- Tellmann, Ute (2015) Historical ontologies of uncertainty and money: Rethinking the current critique of finance. *Journal of Cultural Economy*. 9 (1): 63–86.
- Tellmann, Ute, Sven Opitz und Urs Staeheli (2012) Operations of the global: explorations of connectivity. *Distinktion: Scandinavian Journal of Social Theory*. 13 (3): 209–214.
- Thiemann, Matthias und Mohamed Aldegwy (2015) Can economics develop reliable banking regulation? The shift to macroprudential regulation and the dangers of pseudo-optimization. *Papers in Evolutionary Political Economy*. Working Paper Series: 1–39.
- Thrift, Nigel (2007) Overcome by space. Reworking Foucault. In: *Space, knowledge and power. Foucault in geography*. Herausgegeben von: Stuart Elden und Jeremy W. Crampton, 53–58. Aldershot: Ashgate.
- Toscano, Alberto (2011) Logistics and opposition. <http://www.metamute.org/editorial/articles/logistics-and-opposition> (abgerufen am 23.03.2016).
- Toscano, Alberto (2013) Gaming the plumbing: High-frequency trading and the spaces of capital. <http://www.metamute.org/editorial/articles/gaming-plumbing-high-frequency-trading-and-spaces-capital> (abgerufen am 23.03.2016).
- Tsing, Anna (2009) Supply chains and the human condition. *Rethinking Marxism*. 21 (2): 148–176.
- UBA (2001) Späte Lehren aus frühen Warnungen. Das Vorsorgeprinzip 1896–2000. Berlin: Umweltbundesamt.
- UBA (2008) Deutschland im Klimawandel. Anpassung ist notwendig. Dessau-Roßlau: Umweltbundesamt.
- UBA (2011a) Themenblatt Anpassung an den Klimawandel – Energiewirtschaft. Dessau-Roßlau: Umweltbundesamt.
- UBA (2011b) Themenblatt Anpassung an den Klimawandel – Verkehr. Dessau-Roßlau: Umweltbundesamt.
- Urry, John (2011) *Climate change and society*. Cambridge: Polity Press.
- Urry, John und David Tyfield (2014) Special issue: Energy and society. *Theory, Culture & Society*. 31 (5).
- Valverde, Mariana (2011) Questions of security: A framework for research. *Theoretical Criminology*. 15 (1): 3–22.
- VDN (2007) Transmission Code 2007. Netz und Systemregeln der deutschen Übertragungsnetzbetreiber. Herausgegeben von Verband Deutscher Netzbetreiber. Berlin.
- Virilio, Paul (1980) *Geschwindigkeit und Politik. Ein Essay zur Dromologie*. Berlin: Merve.
- Virilio, Paul (2002) *Rasender Stillstand*. Frankfurt a.M.: Fischer.
- Virilio, Paul (2009) *Der eigentliche Unfall*. Wien: Passagen.
- Virilio, Paul (2011) *Bunkerarchäologie*. Wien: Passagen.
- Vogl, Joseph (2015) *Der Souveränitätseffekt*. Zürich, Berlin: diaphanes.
- Vollmer, Hendrik (2013) *The sociology of disruption, disaster and social change: Punctuated cooperation*. Cambridge: Cambridge University Press.



- Voss, Martin (2006) *Symbolische Formen: Grundlagen und Elemente einer Soziologie der Katastrophe*. Bielefeld: transcript.
- Walters, William (2012) *Governmentality: Critical encounters*. Oxon, New York: Routledge.
- WBGU (2007) *Welt im Wandel. Sicherheitsrisiko Klimawandel. Bericht des Wissenschaftlichen Beirats der Bundesregierung Globale Umweltveränderungen (WBGU)*. Berlin, Heidelberg, New York: Springer.
- Weber, Max (1988a) Die »Objektivität« sozialwissenschaftlicher und sozialpolitischer Erkenntnis. In: *Gesammelte Aufsätze zur Wissenschaftslehre*, 146–214. Tübingen: UTB.
- Weber, Max (1988b) Die protestantische Ethik und der Geist des Kapitalismus. In: *Gesammelte Aufsätze zur Religionssoziologie I*, 17–206. Tübingen: UTB.
- Weber, Max (2005) *Wirtschaft und Gesellschaft. Grundrisse der verstehenden Soziologie*. Frankfurt a.M.: Zweitausendeins.
- Weber, Max (2006) Politik als Beruf. In: *Politik und Gesellschaft*, 565–610. Frankfurt a.M.: Zweitausendeins.
- Wehling, Peter (2006) *Im Schatten des Wissens? Perspektiven der Soziologie des Nichtwissens*. Konstanz: UVK.
- Wehling, Peter (2013) Vom Schiedsrichter zum Mitspieler? Konturen proaktiver Bioethik am Beispiel der Debatte um Neuro-Enhancement. In: *Ethisierung der Technik - Technisierung der Ethik. Der Ethik Boom im Lichte der Wissenschafts- und Technikforschung*. Herausgegeben von: Alexander Bogner, 147–172. Baden-Baden: Nomos.
- Weick, Karl E. (1985) *Der Prozeß des Organisierens*. Frankfurt a.M.: Suhrkamp.
- Weick, Karl E. und Kathleen M. Sutcliffe (2011) *Managing the unexpected: Resilient performance in an age of uncertainty*. San Francisco: John Wiley & Sons.
- Weick, Karl E., Kathleen M. Sutcliffe und David Obstfeld (2008) Organizing for high reliability: Processes of collective mindfulness. *Crisis Management*. 3 (1): 81–123.
- Welzer, Harald (2010) *Klimakriege: Wofür im 21. Jahrhundert getötet wird*. Frankfurt a.M.: Fischer Verlag.
- Whatmore, Sarah (2006) Materialist returns: Practising cultural geography in and for a more-than-human world. *Cultural Geographies*. 13 (4): 600–609.
- WHO (2014) Antimicrobial resistance. Global report on surveillance. Genf: World Health Organization.
- Wildavsky, Aaron B. (1988) *Searching for safety*. New Brunswick, London: Transaction publishers.
- Willke, Helmut, Eva Becker und Carla Rostásy (2013) *Systemic risk: The myth of rational finance and the crisis of democracy*. Frankfurt a.M.: Campus.
- Winner, Langdon (1980) Do artifacts have politics? *Daedalus*. 109 (1): 121–136.
- Wittfogel, Karl A. (1957) Chinese society: An historical survey. *The Journal of Asian Studies*. 16 (3): 343–364.
- Wittgenstein, Ludwig (1985) *Über Gewißheit*. Frankfurt a.M.: Suhrkamp.

- Woolgar, Steve und Geoff Cooper (1999) Do artefacts have ambivalence? Moses' bridges, Winner's bridges and other urban legends in S&TS. *Social Studies of Science*. 29 (3): 433–449.
- Young, Oran R. und Will Steffen (2009) The earth system: sustaining planetary life-support systems. In: *Principles of ecosystem stewardship. Resilience based natural resource management in a changing world*. Herausgegeben von: Carl Folke, Gary P. Kofinas und Stuart F. Chapin, 295–315. New York: Springer.
- Yusoff, Kathryn (2013) The geoengine: Geoengineering and the geopolitics of planetary modification. *Environment and Planning A*. 45 (12): 2799–2808.
- Zoche, Peter, Stefan Kaufmann und Rita Haverkamp (Hg.) (2011) *Zivile Sicherheit: Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken*. Bielefeld: transcript.
- ZöS (2008) Risiken und Herausforderungen für die öffentliche Sicherheit in Deutschland. Grünbuch des Zukunftsforums öffentliche Sicherheit. Berlin: Zukunftsforum öffentliche Sicherheit.
- ZSKG (2009) Gesetz über den Zivilschutz und die Katastrophenhilfe des Bundes (Zivilschutz- und Katastrophenhilfegesetz).