Stefan Steiger

# Cybersicherheit in Innen- und Außenpolitik

## Deutsche und britische Policies im Vergleich

[transcript] Politik in der digitalen Gesellschaft

Stefan Steiger
Cybersicherheit in Innen- und Außenpolitik

**Politik in der digitalen Gesellschaft** | Band 4

Die freie Verfügbarkeit der E-Book-Ausgabe dieser Publikation wurde ermöglicht durch POLLUX – Informationsdienst Politikwissenschaft

und der Open Library Community Politik 2022 – einem Netzwerk wissenschaftlicher Bibliotheken zur Förderung von Open Access in den Sozial- und Geisteswissenschaften:

**Vollsponsoren:** Freie Universität Berlin – Universitätsbibliothek | Staatsbibliothek zu Berlin | Universitätsbibliothek der Humboldt-Universität zu Berlin | Universitätsbibliothek Bielefeld | Universitätsbibliothek der Ruhr-Universität Bochum | Universitäts- und Landesbibliothek Bonn | Staats- und Universitätsbibliothek Bremen | Universitäts- und Landesbibliothek Darmstadt | Sächsische Landesbibliothek Staats- und Universitätsbibliothek Dresden (SLUB) | Universitäts- und Landesbibliothek Düsseldorf | Universitätsbibliothek Frankfurt am Main | Justus-Liebig-Universität Gießen | Niedersächsische Staats- und Universitätsbibliothek Göttingen | Universitätsbibliothek der FernUniversität in Hagen | Staats- und Universitätsbibliothek Carl von Ossietzky, Hamburg | Gottfried Wilhelm Leibniz Bibliothek - Niedersächsische Landesbibliothek | Technische Informationsbibliothek (TIB Hannover) | Universitätsbibliothek Kassel | Universitätsbibliothek Kiel (CAU) | Universitätsbibliothek Koblenz · Landau | Universitäts- und Stadtbibliothek Köln | Universitätsbibliothek Leipzig | Universitätsbibliothek Marburg | Universitätsbibliothek der Ludwig-Maximilians-Universität München | Max Planck Digital Library (MPDL) | Universität der Bundeswehr München | Universitäts- und Landesbibliothek Münster | Universitätsbibliothek Erlangen-Nürnberg |Bibliotheks- und Informationssystem der Carl von Ossietzky Universität Oldenburg | Universitätsbibliothek Osnabrück | Universitätsbibliothek Passau | Universitätsbibliothek Vechta | Universitätsbibliothek Wuppertal | Vorarlberger Landesbibliothek | Universität Wien Bibliotheks- und Archivwesen | Zentral- und Hochschulbibliothek Luzern | Universitätsbibliothek St. Gallen | Zentralbibliothek Zürich

**Sponsoring Light**: Bundesministerium der Verteidigung | ifa (Institut für Auslandsbeziehungen), Bibliothek | Landesbibliothek Oldenburg | Ostbayerische Technische Hochschule Regensburg, Hochschulbibliothek | ZHAW Zürcher Hochschule für Angewandte Wissenschaften, Hochschulbibliothek

**Mikrosponsoring:** Stiftung Wissenschaft und Politik (SWP) - Deutsches Institut für Internationale Politik und Sicherheit | Leibniz-Institut für Europäische Geschichte

Die Reihe wird herausgegeben von Jeanette Hofmann, Norbert Kersting, Claudia Ritzi und Wolf J. Schünemann.

**Stefan Steiger**, geb. 1985, arbeitet im Bereich IT-Sicherheit am Universitätsrechenzentrum Heidelberg. Zuvor war er am Institut für Politische Wissenschaft der Universität Heidelberg sowie am Institut für Sozialwissenschaften an der Universität Hildesheim tätig. Zu seinen Forschungsinteressen zählen Cybersicherheitspolitik, Außenpolitikanalyse sowie die politische Kommunikation im digitalen Raum.

Stefan Steiger

# Cybersicherheit in Innen- und Außenpolitik

Deutsche und britische Policies im Vergleich

[transcript]

Diese Studie wurde 2020 unter dem Titel »Deutsche und britische Cybersicherheitspolitiken im Vergleich: Eine rollentheoretsiche Analyse« an der Fakultät für Wirtschafts- und Sozialwissenschaften der Ruprecht-Karls-Universität Heidelberg als Dissertation angenommen.
Gutachter: Prof. Dr. Sebastian Harnisch, Prof. Dr. Wolf J. Schünemann

**Bibliografische Information der Deutschen Nationalbibliothek**
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.




**Erschienen 2022 im transcript Verlag, Bielefeld**


Umschlaggestaltung: Maria Arndt, Bielefeld
Satz: Sebastian M. Schlerka, Bielefeld
Druck: Majuskel Medienproduktion GmbH, Wetzlar
Print-ISBN 978-3-8376-6064-7
PDF-ISBN 978-3-8394-6064-1
EPUB-ISBN 978-3-7328-6064-7
https://doi.org/10.14361/9783839460641
Buchreihen-ISSN: 2699-6626
Buchreihen-eISSN: 2703-111X

Gedruckt auf alterungsbeständigem Papier mit chlorfrei gebleichtem Zellstoff.
Besuchen Sie uns im Internet: *https://www.transcript-verlag.de*
Unsere aktuelle Vorschau finden Sie unter *www.transcript-verlag.de/vorschau-download*

# Inhaltsverzeichnis

# Vorwort

Diese Studie ist im Rahmen meiner Promotion an der Universität Heidelberg entstanden. Viele haben mich auf dem Weg zur Fertigstellung dieses Buches begleitet und zum Gelingen des Promotionsprozesses beigetragen. Bei ihnen möchte ich mich ganz herzlich für die Unterstützung auf der manchmal beschwerlichen Reise bedanken.

Großer Dank gilt selbstverständlich meinem Doktorvater Prof. Dr. Sebastian Harnisch. Er hat mich stets bestärkt, aber auch kritische Punkte offen und konstruktiv angesprochen. Sein Rat und seine Führung waren nicht nur maßgeblich für den erfolgreichen Abschluss der Promotion – ohne seine Unterstützung hätte ich den Weg vermutlich gar nicht erst angetreten. Von unschätzbarem Wert war darüber hinaus mein Zweitgutachter Prof. Dr. Wolf J. Schünemann, der es mir ermöglicht hat, in der zweiten Hälfte der Promotionsphase an die Universität Hildesheim zu wechseln. Durch sein unermüdliches Engagement zunächst in Heidelberg und dann in Hildesheim konnte ich viele spannende neue Themen auch abseits der Dissertation erschließen. Seine unerreichte Fähigkeit, mich aus meiner Komfortzone zu bewegen, hat mich nicht nur zu einem besseren Wissenschaftler gemacht.

Bei Dr. Ronja Ritthaler-Andree bedanke ich mich für die zahllosen gemeinsamen Arbeitstage in der Bibliothek und die vielen Gespräche, die so manche Tiefpunkte wesentlich erträglicher machten. Für die vielen fachlichen Impulse danke ich ferner den TeilnehmerInnen des Doktorandenkolloquiums an der Professur für Internationale Beziehungen und Außenpolitik: Melanie Bräunche, Sebastian Cujai, Jason Franz, Maximilian Jungmann, Luxin Liu, Tijana Lujic, Dr. Eva Mayer, Fanny Schardey, Dr. Caja Schleich und Martina Větrovcová.

Für intensive Debatten rund um die Rollentheorie danke ich Stefan Artmann, Dr. Gordon Friedrichs und Dr. Josie-Marie Perkuhn. Kerstin Zettl danke ich für die Zusammenarbeit im Bereich der Cyberkonfliktforschung und die zahllosen Stunden bei der Analyse verschiedener Cyberangriffe.

Für die finanzielle Unterstützung danke ich der Friedrich-Ebert-Stiftung. Den HerausgeberInnen der Reihe Politik in der digitalen Gesellschaft Prof. Dr. Jeanette Hofmann, Prof. Dr. Claudia Ritzi, Prof. Dr. Norbert Kersting und Prof. Dr. Wolf J. Schünemann danke ich für die Aufnahme in die Reihe.

Besonderer Dank gilt meiner Partnerin Ana dafür, dass sie meine Welt bereichert und mir immer neue Perspektiven eröffnet. Der letzte Dank gilt meinen Eltern Monika und Klaus – ohne ihre bedingungslose Unterstützung in allen Lagen wäre ich nie so weit gekommen. Ihnen ist dieses Buch gewidmet.

Mai 2021

# Abbildungsverzeichnis

# Tabellenverzeichnis

# Abkürzungsverzeichnis

**(D)DoS** – (Distributed)-Denial-of-Service

**ARPA** – Advanced Research Projects Agency

**BfV** – Bundesamt für Verfassungsschutz
**BKA** – Bundeskriminalamt
**BMI** – Bundesministerium des Innern
**BMVg** – Bundesministerium der Verteidigung
**BND** – Bundesnachrichtendienst
**BSI** – Bundesamt für Sicherheit in der Informationstechnik
**BverfG** – Bundesverfassungsgericht

**CCC** – Chaos Computer Club
**CDU** – Christlich Demokratische Union Deutschlands
**CIA** – Central Intelligence Agency
**CMA** – Computer Misuse Act 1990
**CNE** – Computer Network Exploitation
**CNO** – Computer Network Operation
**CSNET** – Computer Science Network
**CSP** – Communication Service Provider
**CSU** – Christlich-Soziale Union in Bayern

**DNS** – Domain Name System
**DRIPA** – Data Retention and Investigatory Powers Act 2014
**DUP** – Democratic Unionist Party

**EADS** – European Aeronautic Defence and Space
**EFF** – Electronic Frontier Foundation
**EU** – Europäische Union

**FBI** – Federal Bureau of Investigation
**FDP** – Freie Demokratische Partei
**FIfF** – Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung

**FISA** – Foreign Intelligence Surveillance Act
**FÜV** – Fernmeldeverkehr-Überwachungs-Verordnung

**GCHQ** – Government Communications Headquarters
**GG** – Grundgesetz

**HRA** – Human Rights Act 1998
**HTTP** – Hypertext Transfer Protocol

**IAB** – Internet Architecture Board
**IB** – Internationale Beziehungen
**ICANN** – Internet Corporation for Assigned Names and Numbers
**IETF** – Internet Engineering Task Force
**IOCA** – Interception of Communications Act 1985
**IoCCO** – Interception of Communications Commissioner
**IoT** – Internet of Things
**IPA** – Investigatory Powers Act 2016
**IPC** – Investigatory Powers Commissioner
**IPT** – Investigatory Powers Tribunal
**ISC** – Intelligence and Security Committee
**ISP** – Internet Service Provider
**IT** – Informationstechnik
**IuKDG** – Informations- und Telekommunikationsdienste-Gesetz

**Kdo CIR** – Kommando Cyber- und Informationsraum

**MI5** – Security Service
**MI6** – Secret Intelligence Service
**MoA** – Memorandum of Agreement
**MoD** – Ministry of Defence

**NCSC** – National Cyber Security Centre
**NHS** – National Health System
**NOCP** – National Offensive Cyber Programme
**NSA** – National Security Agency
**NSS** – National Security Strategy

**OECD** – Organisation for Economic Co-operation and Development
**OPM** – Office of Personnel Management
**OSZE** – Organisation für Sicherheit und Zusammenarbeit in Europa

**PGP** – Pretty Good Privacy
**PNR** – Passenger Name Records

**RIPA** – Regulation of Investigatory Powers Act 2000

**SCS** – Special Collection Service
**SMTP** – Simple Mail Transfer Protocol
**SNP** – Scottish National Party
**SPD** – Sozialdemokratische Partei Deutschlands
**StGB** – Strafgesetzbuch
**StPO** – Strafprozessordnung

**TCP/IP** – Transmission Control Protocol/Internet Protocol
**TKÜ** – Telekommunikationsüberwachung
**TKÜV** – Telekommunikations-Überwachungsverordnung
**TLG** – Two-Level Game
**TLS** – Transport Layer Security
**TTP** – Trusted Third Party

**UCLA** – University of California
**UN** – United Nations
**UN GGE** – United Nations Group of Governmental Experts
**URL** – Uniform Resource Locator

**VPN** – Virtual Private Network

**W3C** – World Wide Web Consortium
**WiKG** – Gesetz zur Bekämpfung der Wirtschaftskriminalität

**ZITiS** – Zentrale Stelle für Informationstechnik im Sicherheitsbereich

# 1. Einleitung

Die rasante globale Verbreitung des Internets[1] hat in den vergangenen 25 Jahren tiefgreifende wirtschaftliche sowie gesellschaftliche Veränderungen ermöglicht. Aus einem Netzwerk, das ursprünglich den militärischen sowie wissenschaftlichen Informationsaustausch sicherstellen bzw. erleichtern sollte, wurde nach der kommerziellen Öffnung zu Beginn der 1990er Jahre zunächst ein »Spielplatz« für Nerds und dann ein zentraler Wirtschaftsraum sowie ein Ort des kulturellen Austauschs. Heute gibt es in modernen Staaten kaum noch Lebensbereiche, die nicht von digitalen Technologien durchdrungen werden. BürgerInnen konsumieren und kommunizieren über globale Plattformen, die mit dem Internet neue Geschäftsmodelle erschlossen bzw. etablierte Unternehmenspraktiken auf den neuen Handlungsraum übertragen haben. Die nächste Entwicklungsstufe – das Internet of Things (IoT) – beginnt rasch Gestalt anzunehmen. Viele Gegenstände des täglichen Gebrauchs werden dann ebenso flächendeckend online sein, wie die Steuerungssysteme zentraler gesellschaftlicher Infrastrukturen. Die nächste industrielle Revolution, die durch die Vernetzung und die gezielte Nutzung erzeugter Daten effizientere Wirtschaftsprozesse ermöglicht, hat laut Ansicht einiger ExpertInnen bereits begonnen. Die Entwicklung künstlicher Intelligenz hat

1 Als Internet wird im Folgenden das mittels TCP/IP verbundene Netzwerk verschiedener (Teil-)Netze (Autonomer Systeme) bezeichnet. Dieser Zusammenschluss von Rechnern ermöglicht es theoretisch zwischen allen verbundenen Punkten Informationen in Form von Datenpaketen auszutauschen. Im Folgenden werden die Begriffe Internet, Netz und Cyberspace synonym verwendet. Es ist aber darauf hinzuweisen, dass der Begriff Cyberspace konzeptionell umfassender ist, da er auch jene digital vernetzten Geräte einschließt, die nicht mit dem Internet verbunden sind (air gap). Das Internet ist damit nur ein (großer) Teil des Cyberspace, der daneben noch zahllose weitere Netzwerke privater, wirtschaftlicher und staatlicher Akteure umfasst, die nicht mit dem Internet verbunden sind und damit auch nicht unmittelbar über das Internet erreicht und angegriffen werden können (Tabansky, 2011). Sofern nicht explizit darauf hingewiesen wird, ist im Folgenden auch mit der Bezeichnung Internet dieses weite Verständnis gemeint.

dabei das Potenzial den Arbeitsmarkt und damit die Gesellschaftsordnung der Zukunft nachhaltig zu verändern (Frey und Osborne, 2017).[2]

Das IoT droht aber auch zu einem sicherheitspolitischen Problem zu werden, da viele Geräte technisch schlecht gegen Angriffe geschützt sind. Eine Studie hat bspw. ein Szenario skizziert, in dem AngreiferInnen durch die Übernahme von besonders energieintensiven Geräten Verbrauchsschwankungen erzeugen und dadurch weitreichende Stromausfälle auslösen könnten (Soltan, Mittal und Poor, 2018). Das Mirai-Botnet[3] hat gezeigt, dass IoT-Geräte wie IP-Kameras oder Fernseher für Angriffe gekapert und missbraucht werden können. Mit einem großen DDoS-Angriff[4] legte das Botnet im Oktober 2016 einen zentralen DNS-Dienst[5] lahm und sorgte so dafür, dass große Teile des Internets für viele NutzerInnen nicht mehr erreichbar waren (Mansfield-Devine, 2016).

Das Internet ist im Zuge seiner sozialen Integration aber nicht erst mit dem Aufkommen des IoT zu einer Quelle gesellschaftlicher Unsicherheit und zum Medium des Konfliktaustrages geworden. Während in der Frühphase des Netzes Schadsoftware noch oft von individuellen AkteurInnen aus technischer Neugier oder zur Reputationssteigerung in einer relativ kleinen (Peer-)Gruppe von HackerInnen eingesetzt wurde, gehen aktuelle Schätzungen davon aus, dass (organisierte) Cyberkriminalität weltweit jährlich Schäden in Höhe von bis zu 600 Milliarden US-Dollar verursacht (McAfee und CSIS, 2018, S. 4). Die Geschäftsmodelle reichen dabei vom Handel mit illegalen Gütern wie Waffen oder Drogen im Darknet, über den massenhaften Versand von Spam- und (Spear)Phishingmails, bis zur Verbreitung von Erpressungstrojanern (Ransomware), die die Geräte der Opfer verschlüsseln und nur gegen Lösegeldzahlung wieder zugänglich machen.

---

2 Eine umfassende Vernetzung ist weder als wünschenswerter teleologischer Endpunkt der Entwicklung zu verstehen – derartige Tendenzen bleiben immer durch die AkteurInnen umkehrbar (möglicherweise unter Inkaufnahme erheblicher Opportunitätskosten) – noch als sich den AkteurInnen aufzwingender Prozess eines technischen Determinismus (s. dazu Kapitel 2.4).

3 Ein Botnet bezeichnet ein Netz von Rechnern, die von AngreiferInnen übernommen und zentral ferngesteuert werden. Meist handelt es sich hierbei um Rechner, die aufgrund veralteter Software angreifbar sind (Singer und Friedman, 2014, S. 44). Das Mirai-Botnet nutzte schlecht gesicherte IoT-Geräte, um Angriffe durchzuführen.

4 (D)DoS-Angriffe sorgen dafür, dass ein Zielsystem systematisch überlastet wird. Die Überlastung kann dabei auf verschiedene Ressourcen zielen bspw. die Rechenleistung oder die Internetanbindung. Ein Dienst ist in der Folge für NutzerInnen nicht mehr erreichbar.

5 Die Abkürzung DNS steht für Domain Name System und bezeichnet die Infrastruktur, die für die eindeutige Zuordnung zwischen maschinenlesbaren IP-Adressen und URLs benötigt wird (Singer und Friedman, 2014, S. 295). Der Ausfall eines DNS-Dienstes führt dazu, dass NutzerInnen Internetseiten nicht mehr erreichen können, da die Zuordnung zwischen URL und IP-Adresse nicht erfolgen kann.

Es sind aber nicht nur Kriminelle, die die neuen Verwundbarkeiten der digitalen Gesellschaft ausnutzen. Auch politische Konflikte finden Widerhall im Netz. Die Bandbreite angreifender AkteurInnen ist dabei ebenso zahl- und facettenreich wie die verschiedenen Angriffsmöglichkeiten. Politisch motivierte nichtstaatliche Hacktivists nutzen das Netz, um durch öffentlichkeitswirksame Aktionen, wie bspw. (D)DoS-Angriffe oder die Veröffentlichung gestohlener Dokumente (doxing), ein größeres Publikum auf ihre Anliegen aufmerksam zu machen (Karatzogianni, 2015; Sauter, 2014). Terrororganisationen greifen auf Cyberangriffe zurück, um bspw. Finanzmittel zu generieren oder propagandistische Botschaften zu verbreiten (Schweitzer, Siboni und Yogev, 2013). Regierungen erweitern und komplementieren durch Cyberangriffe ihr außen- und sicherheitspolitisches Handlungsrepertoire. Die Möglichkeiten reichen dabei von umfassenden Spionageaktivitäten gegen Staaten, Unternehmen und gesellschaftliche Akteure – wie sie bspw. durch die Snowden-Enthüllungen 2013 aufgedeckt wurden – über kinetisch folgenreiche Angriffe – etwa zur Unterminierung des iranischen Nuklearwaffenprogramms durch den Wurm Stuxnet – bis zur Verschränkung konventioneller Kriegführung mit Cyberangriffen – bspw. im Zuge des Kaukasuskrieges 2008. BeobachterInnen gehen davon aus, dass in zukünftigen Konflikten mit einer zunehmenden Verknüpfung von konventionellen Mitteln des Konfliktaustrags, Cyberangriffen und Maßnahmen zur Informationsmanipulation zu rechnen ist (Libicki, 2017). Regierungen delegieren Angriffe dabei mitunter an nichtstaatliche Akteure (sog. Proxies), um die eigene Urheberschaft systematisch abstreiten zu können (Maurer, 2018).

Diese Ausdifferenzierung auf der Akteursseite ist mit einer qualitativen Weiterentwicklung der Cyberangriffe und der quantitativen Zunahme von Vorfällen verbunden. War Malware in der Frühphase der Netzentwicklung noch häufig Analogon zum konventionellen Scherzartikel, ist Schadsoftware heute meist deutlich komplexer und potenziell folgenreicher. Möglich wird der Einsatz von Schadsoftware durch die zahlreichen Sicherheitslücken (vulnerabilities), die in Hard- als auch Software vorhanden sind und die teilweise durch AngreiferInnen gezielt ausnutzbar sind (exploits). Da die Anforderungen an Funktionalität und Interoperationalität von IT immer anspruchsvoller werden, wächst auch deren Fehleranfälligkeit (Gaycken, 2011).

Sicherheitspolitik wird zudem durch die Globalität des Internets und die technischen Charakteristiken vor neue Herausforderungen gestellt (bspw. durch das Attribtutionsproblem). Diese Situation hat aber nicht nur dazu geführt, dass Staaten neue regulatorische Maßnahmen zum Umgang mit Cybersicherheit ergriffen haben, auch wissenschaftlich erfährt die Thematik zunehmend Aufmerksamkeit:

> »In previous generations, young people who wanted to be relevant in the foreign-policy establishment studied Russian or learned about nuclear disar-

> mament. After 9/11, Arabic language skills, as well as expertise on the Middle East, offered an entrée into foreign policy. Today, students of foreign affairs should understand how the internet works on a technical level and study the varied threats that fall under the broad umbrella of so-called cyber issues.« (Burns und Cohen, 2017)

WissenschaftlerInnen haben immer wieder auf die besondere Komplexität des Untersuchungsgegenstands hingewiesen und die Bedeutung interdisziplinärer Expertise betont (Kello, 2013; Segal, 2016). Der Forschungsgegenstand Cybersicherheit hat, aufgrund der politischen Implikationen, daher in den vergangenen Jahren vermehrt Aufmerksamkeit auch jenseits der Informatik gefunden. Um den politischen Umgang mit Problemen der IT-Sicherheit geht es auch in der vorliegenden Untersuchung der deutschen und britischen Cybersicherheitspolitiken.

## 1.1 Untersuchungsgegenstand und Relevanz

Wenn im Folgenden von Cybersicherheitspolitiken gesprochen wird, dann liegt dem ein enges, an die Informatik angelehntes, Verständnis von IT-Sicherheit zugrunde. Es basiert auf einer Definition, auf die sich die beiden Untersuchungsstaaten bereits 1991 in internationalem Austausch mit den Niederlanden und Frankreich verständigt haben. Danach umfasst die IT-Sicherheit die Gewährleistung der Vertraulichkeit, Integrität sowie Verfügbarkeit von Daten bzw. datenverarbeitenden IT-Systemen (DTI, 1991, S. 1).[6] Ausgehend von dieser Definition wird im Folgenden untersucht, inwiefern die beiden Untersuchungsstaaten Cybersicherheit zu sicherheitspolitischen Zwecken (offensiv) unterminieren bzw. welche Praktiken sie als illegitim betrachten.[7]

Der Fokus auf die offensiven Cybersicherheitspolitiken ist angebracht, da diese national wie international besonders umstritten sind und wissenschaftlich bisher vergleichsweise wenig Aufmerksamkeit erfahren haben. International konnte im Rahmen einer Group of Governmental Experts der UN (UN GGE) zwar Einigkeit darüber erzielt werden, dass völkerrechtliche Regelungen und insbesondere die Charta der Vereinten Nationen prinzipiell auf den Cyberspace übertragbar sind (United Nations, 2013b), was das konkret bedeutet, ist aber nach wie vor unklar. So scheiterte im Jahr 2017 die letzte UN GGE. Zentraler Streitpunkt war dabei

6 Diese drei Schutzziele werden anhand der englischen Anfangsbuchstaben (confidentiality, integrity and availability) meist als CIA-Triad bezeichnet (Andress, 2014, S. 5-9).

7 Da es in dieser Untersuchung um die Entwicklung der Cybersicherheit in diesem engen Kernverständnis geht, ist die mitunter erhebliche extensionale Erweiterung, die der Begriff erfahren hat (bspw. im Kontext der Verbreitung von Desinformation), nicht Teil der Analyse (Schünemann und Steiger, 2019).

offenbar die Bedeutung des Selbstverteidigungsrechts im Cyberspace (Henriksen, 2019). Aber nicht nur bei der militärischen Nutzung des Internets besteht Unsicherheit. Die Snowden-Enthüllungen haben ferner gezeigt, dass Cyberangriffe zur Informationsgewinnung auch gegen befreundete Staaten eingesetzt werden (Spiegel, 2014b). Im Bereich des Strafrechts konnte zwar relativ schnell geklärt werden, was als unangemessenes Verhalten gewertet werden soll. International konnten mit der Convention on Cybercrime im Rahmen des Europarates auch strafrechtliche Regelungen harmonisiert werden. Domestisch ist aber nach wie vor umstritten, wann und in welchem Umfang staatliche Ermittlungsbehörden IT-Sicherheit unterminieren sollten (Roggan, 2018).

Das Internet als sicherheitspolitischer Handlungsraum mit globaler Architektur und universellen Protokollen, die nicht primär auf Sicherheitserwägungen fußen (s. Kapitel 2.4.1), stellt staatliche Praktiken vor besondere Herausforderungen. Denn einerseits wird die Trennung zwischen innerer und äußerer Sicherheit im globalen Netz problematisch, da Pakete stets auch über Knoten im Ausland geleitet werden können und andererseits befinden sich zentrale Infrastrukturen nicht in staatlicher Hand. Gleichzeitig ist das Netz mittlerweile für das Funktionieren nahezu aller bedeutenden gesellschaftlichen Infrastrukturen in Industriestaaten essenziell. Verkehrsleitsysteme können ebenso digital gesteuert werden wie die Wasser- oder Energieversorgung. Das Internet ist damit nicht nur selbst zu einer zentralen gesellschaftlichen Infrastruktur geworden. Es ist vielmehr zu der Infrastruktur geworden, von deren Funktionieren zahlreiche andere Infrastrukturen abhängen: »the Internet has become a backbone of backbones« (Choucri, 2012, S. 151).

Eindrückliche Vorfälle in jüngerer Vergangenheit haben offengelegt, dass diese Verwundbarkeiten auch praktisch nutzbar sind bzw. bereits genutzt werden. In der Ukraine verursachte ein Cyberangriff im Dezember 2016 einen kurzfristigen Stromausfall von dem mehr als 200.000 BürgerInnen betroffen waren (Wired, 2016). Die rasche Verbreitung des Wurms WannaCry im Mai 2017 traf unter anderem das britische Gesundheitssystem (National Health System (NHS)) und hatte zur Folge, dass Krankenhäuser ihre PatientInnen nicht mehr planmäßig versorgen konnten (National Audit Office, 2018).[8]

8 WannaCry steht auch exemplarisch für die unintendierten Konsequenzen, die mit staatlichen Cybersicherheitspolitiken verbunden sein können. Die Malware beruht auf einer Sicherheitslücke im Betriebssystem Windows, die von der NSA EternalBlue getauft wurde. Aufgrund der potenziellen Nützlichkeit für offensive Cyberoperationen wurde die Lücke geheimgehalten. Allerdings verlor die NSA die Kontrolle über dieses Wissen und die Gruppe Shadow Brokers verbreitete die Informationen im Netz. Die NSA hatte Microsoft zwar kurz nach Bemerken des Datenlecks über die Lücke informiert und Microsoft veröffentlichte im März 2017 ein entsprechendes Update, da dieses von NutzerInnen aber nur langsam instal-

Ein Angriff auf das Netz und insbesondere kritische Infrastrukturen kann für Gesellschaften dabei potenziell verheerende (kaskadierende) Folgen haben. Diese neue Verwundbarkeit hat Hollywoodfilme wie Stirb Langsam 4.0 schon früh dazu inspiriert, den digitalen Knockout vernetzter Gesellschaften auszumalen und auch in der (populär)wissenschaftlichen Auseinandersetzung mit der Thematik wird immer wieder mit Szenarien folgenschwerer Cyberangriffe argumentiert. Auch wenn es empirisch noch keine Vorfälle mit derart gravierenden Effekten gegeben hat. In Anbetracht der bisher kinetisch zumeist folgenlosen Cyberangriffe ist ein beständiges Skizzieren von Worst-Case-Szenarien kritisch hinterfragt worden (Dunn Cavelty, 2013; Schünemann und Steiger, 2019).

Aber auch wenn sich Horrorszenarien von kinetisch folgenreichen Cyberangriffen bisher nicht realisiert haben, haben Regierungen die wachsende Angriffsfläche zum Anlass genommen neue regulatorische Maßnahmen zu ergreifen, um mit den Risiken im Cyberspace umzugehen. Das Netz und die mit ihm verbundene Perzeption neuer Herausforderungen hat dementsprechend seit Ende der 1990er Jahre zentrale Bedeutung in sicherheitspolitischen Dokumenten erlangt. Sichtbarer Ausdruck sind unter anderem die Cybersicherheitsstrategien, die mittlerweile von zahlreichen Industrienationen ausgearbeitet und implementiert wurden (Bundesministerium des Innern, 2011; Cabinet Office, 2009). Auch in Deutschland und Großbritannien[9] haben die Regierungen dieses Problem adressiert und neue Kapazitäten zur offensiven Nutzung des Netzes aufgebaut.

Die Lektüre dieser Dokumente zeigt, dass sich staatliche Sicherheitspolitik in diesem Feld mit unterschiedlichen Spannungen konfrontiert sieht. Einerseits sind die Regierungen daran interessiert, das Netz als Wirtschaftsraum und IT als Mittel der Effizienzsteigerung möglichst umfassend zu nutzen. Sie sind aus dieser Warte an einem sicheren Cyberspace interessiert, der den Wirtschaftssubjekten nicht durch Unsicherheit die Bereitschaft zur Investition oder zum Handeln allgemein nimmt. Ferner fördern demokratische Regierungen die Nutzung des Internets zur freien Verbreitung von Informationen oder zur vertraulichen Kommunikation. Andererseits sehen Regierungen im Netz aber auch ein Mittel, mit dem klassische sicherheitspolitische Ziele erreicht werden können. Hierzu ist es aber mitunter nötig, IT-Sicherheit zu unterminieren, bspw. dann, wenn es darum geht, Kriminelle abzuhören, nachrichtendienstliche Aufklärung zu betreiben oder die Infrastruktur gegnerischer Staaten im Konfliktfall zu unterminieren. Durch die Geheimhaltung und Nutzung von Sicherheitslücken wird der Staat so selbst zum Akteur, der IT-Unsicherheit schafft (Nissenbaum, 2005).

---

liert wurde, konnte WannaCry im Mai trotzdem viele Rechner, darunter die des NHS, infizieren und lahmlegen (The Washington Post, 2017).

9 Mit Großbritannien ist im Folgenden stets das Vereinigte Königreich Großbritannien und Nordirland gemeint.

Die Cybersicherheitspolitiken stehen damit potenziell in Spannung mit dem Erhalt bzw. der Förderung volkswirtschaftlichen Wohlstands und der Gewährleistung demokratischer Freiheitsrechte. Beim Einsatz zumeist klandestiner Cyberoperationen stellt sich ferner die Frage, wie Exekutiven demokratisch kontrolliert werden können. Als globaler Handlungsraum stellt der Cyberspace damit nicht nur die internationalen Beziehungen vor Herausforderungen, sondern auch die domestischen Verhältnisse zwischen Regierungen, Parlamenten, Judikativen, Unternehmen, VertreterInnen der Zivilgesellschaft sowie BürgerInnen. Die Analyse von Cybersicherheitspolitiken ist somit empirisch nicht nur aufgrund der zunehmenden Vernetzung, der damit einhergehenden gesellschaftlichen Verwundbarkeit und der Zunahme qualitativ hochwertiger Angriffe relevant, sondern auch, weil sie zentrale demokratische und wirtschaftliche Abwägungen erfordern und damit soziale Relationen domestisch wie international berühren.

Die Regierungen haben ihre Cybersicherheitspolitiken dabei in unterschiedlichen Handlungsfeldern definiert. Das Untersuchungsinteresse dieser Studie bezieht sich konkret auf die Politikentwicklung in drei zentralen Bereichen. Erstens auf den Kontext der Strafverfolgung. Zur Regulation krimineller Handlungen haben die Regierungen explizite Regelungen akzeptablen Verhaltens etabliert und diese in ihre nationalen Strafrechtsordnungen integriert. Teilweise wurden diese auch auf internationaler Ebene harmonisiert. Im Kontext der polizeilichen Ermittlungspraktiken haben die Exekutiven in diesem Zusammenhang aber auch selbst Maßnahmen ergriffen, die die IT-Sicherheit unterminieren. Diese Praktiken wurden in den Strafprozessordnungen kodifiziert. Zweitens auf den Bereich der Nachrichtendienste. Die Snowden-Enthüllungen 2013 haben gezeigt, dass auch Demokratien das Netz umfassend zur Informationsgewinnung im Ausland nutzen (Signals Intelligence). Internationale (Cyber)Spionage ist rechtlich jedoch nicht reguliert. Was als akzeptables staatliches Verhalten gilt, ist folglich nicht expliziert, sondern ggf. nur aus etablierten Praktiken internationalen Rechts ableitbar (Buchan, 2016, 2019). Drittens auf die militärische Nutzung des Netzes. Regierungen haben sukzessive damit begonnen, militärische Cyberkapazitäten aufzubauen (Lewis und Neuneck, 2013). Abgesehen vom Konsens, dass internationales Recht und insbesondere die Charta der Vereinten Nationen prinzipiell auf den Cyberspace übertragbar ist (United Nations, 2013b), ist jedoch auch in diesem Kontext, das staatliche Verhalten weitgehend unreguliert.

Die drei Untersuchungsbereiche zeichnen sich damit durch unterschiedliche Akteurskonstellationen und Regelungsarrangements aus. Sie betreffen auch in unterschiedlicher Weise die internationalen Beziehungen sowie das Verhältnis zwischen domestischen AkteurInnen.

Zudem ist die Untersuchung theoretisch relevant, da mit dem Netz als sicherheitspolitischem Handlungsfeld neue theoretische Herausforderungen verbunden sind. Zentrale Analysekonzepte der Internationalen Beziehungen (IB) sind po-

tenziell schwierig auf den Cyberspace übertragbar. Die analytischen Potenziale etablierter Theorien der IB werden durch den neuen Handlungsraum infrage gestellt. Die Einschätzungen darüber, inwiefern tradierte Konzepte der IB auf den Cyberspace übertragbar sind, divergieren dabei erheblich. Während einige ForscherInnen davon ausgehen, dass erprobte Konzepte weiterhin tragfähig sind (Craig und Valeriano, 2018; Reardon und Choucri, 2012), werden die analytischen Potenziale von anderen WissenschaftlerInnen skeptisch beurteilt (Diersch und Schmetz, 2017; Mayer, 2017). Letztere Einschätzung bezieht sich oft auf das unklare Verhältnis zwischen technischen Infrastrukturen und den sozial handelnden AkteurInnen. Diese Beziehung ist erst in den letzten Jahren von Studien aufgegriffen und ein technischer Determinismus problematisiert worden (Carr, 2016; Dunn Cavelty, 2018; McCarthy, 2015).[10]

Illustrieren lässt sich die Problematik der Übertragbarkeit von IB-Theorien an einer für den Neorealismus entscheidenden Debatte über die Bedeutung von Macht im Cyberspace. Welche Staaten im Cyberspace mächtig sind, ist schwieriger zu beurteilen als in der analogen Welt. Realistisch argumentierende WissenschaftlerInnen haben darauf hingewiesen, dass konventionell überlegene Staaten durch Cyberkapazitäten nur marginale Vorteile gegenüber anderen Staaten erzielen könnten. Insbesondere wenn diese weniger abhängig von IT seien. Demgegenüber könnten unterlegene Staaten durch den Aufbau von Cyberfähigkeiten auch stärkere herausfordern und ihre Position so relativ verbessern (Lindsay, 2013). Die konventionell überlegenen und auch im Cyberspace ressourcenstärksten Staaten könnten so aufgrund ihrer IT-Abhängigkeit doch die schwächeren sein. Die realweltliche Machtverteilung wäre dann digital zumindest partiell invertiert. Das Verhältnis zwischen Macht on- bzw. offline ist aber nach wie vor ungeklärt (Craig und Valeriano, 2018, S. 90). Die Machtkonstellationen im Cyberspace und potenzielle Wechselwirkungen mit anderen Machtressourcen (bspw. einem vernetzten Militär) sind unklar. Damit sind neorealistisch auch nur bedingt systemische Verhaltenserwartungen ableitbar.

Eine wissenschaftliche Auseinandersetzung mit dem Untersuchungsgegenstand ist daher nicht nur aufgrund der praktischen gesellschaftlichen Implikationen relevant. Er ist auch wissenschaftlich bedeutsam, um theoretisch angemessen mit Cybersicherheit umgehen zu können und ein besseres Verständnis zu ermöglichen.

10 Ein theoretisches Defizit, das in Kapitel 2.4 näher beleuchtet wird.

## 1.2 Forschungsstand, Desiderate und Fragestellung

Die politikwissenschaftliche Forschung hat sich dem neuen Gegenstand Cybersicherheit aus unterschiedlichen Blickwinkeln angenähert. Eine erste prominente Studie legten John Arquilla und David Ronfeldt 1993 vor, sie wurde auch tonangebend für künftige akademische und politische Debatten. Unter dem Titel »Cyberwar is coming!« (Arquilla und Ronfeldt, 1993) diskutierten die Autoren verschiedene Auswirkungen der Informationstechnik auf zukünftige Formen der Kriegführung. Sie legten damit den Grundstein für verschiedene Studien, die sich bis heute konzeptionell mit den Folgen der Verbreitung von Informations- und Kommunikationstechnik für den Konfliktaustrag befassen.

In dieser Tradition stehen Untersuchungen, die grundlegende Fragen nach den Wirkungen des neuen sicherheitspolitischen Handlungsraumes adressieren. Konkret untersuchen Studien in diesem Kontext bspw. die Übertragbarkeit tradierter strategischer Konzepte auf den Cyberspace – häufig wird in diesem Kontext über Abschreckung debattiert (Brantly, 2018; Fischerkeller und Harknett, 2017; Harknett und Nye, 2017; Libicki, 2018; Lindsay, 2015; Nye, 2017; M. Schulze, 2019) – ferner finden sich hier Untersuchungen, die der Frage nachgehen, was Macht im Cyberspace bedeutet und wie sie genutzt werden kann (Nye, 2010; Sheldon, 2014; Siedler, 2016; Willett, 2019) oder ob es Cyberwaffen gibt, bzw. was unter dem Begriff zu verstehen ist (Goines, 2017; Rid und McBurney, 2012; Stevens, 2018). In diesem Zusammenhang stehen auch Diskussionen über das Verhältnis zwischen Offensive und Defensive in der Cybersicherheitspolitik. Oftmals wird in diesem Kontext die These debattiert, die Offensive sei der Defensive im Netz überlegen, da die Verteidigung permanent beim Schutz der eigenen Systeme, die zumeist mit kommerzieller Software betrieben werden und daher (unbekannte) Sicherheitslücken aufweisen, wachsam sein müsse, während AngreiferInnen nur einmal erfolgreich sein müssten. Ferner sei die Schwelle zur Konfliktfähigkeit im Cyberspace auch durch nichtstaatliche Akteure leichter zu überwinden (Gartzke und Lindsay, 2015; Lindsay und Gartzke, 2018).

Weiterhin finden sich in diesem Kontext Studien, die sich mit den strategischen Besonderheiten des Netzes und deren Implikationen für sicherheitspolitisches Handeln beschäftigen. Hier wurde bspw. immer wieder auf das sogenannte Attributionsproblem hingewiesen, das sowohl eine Abschreckung von, als auch eine schnelle Reaktion auf Cyberangriffe schwierig mache, da diese durch die Paketvermittlung im Internet immer über verschiedene Stationen (in unterschiedlichen Ländern) geleitet werden können. Ferner können AngreiferInnen fremde Schadsoftware verwenden, Rechner in bereits verdächtigen Drittländern kapern oder nichtstaatliche Akteure (Proxies) mit der Durchführung von Attacken beauftragen. All dies erhöhe die Unsicherheit und erschwere die Cybersicherheitspolitiken bzw. gezielte Reaktionen auf Angriffe. WissenschaftlerInnen haben sich

daher mit den technischen und später auch politischen Herausforderungen dieser Problematik beschäftigt (Berghel, 2017; Egloff und Wenger, 2019; Green, 2015; Guitton, 2017; Lindsay, 2015; Rid und Buchanan, 2014; Schulzke, 2018).

Die stärkere Hinwendung zum tatsächlichen sozialen Umgang mit dem neuen Problemfeld war der Einsicht geschuldet, dass potenziell folgenschwere Cyberangriffe zwar theoretisch möglich, bislang aber ausgeblieben sind. ForscherInnen wiesen daher spätestens ab den 2010er Jahren vermehrt auch darauf hin, dass es eines besseren Verständnisses der sozialen Praktiken bedürfe, um bspw. die bisherige Zurückhaltung zu verstehen (Betz und Stevens, 2011, S. 124). Damit wurde ein Defizit vieler theoretisch-technischer Analysen aufgeworfen, die die soziale Integration von Technik sowie deren (Um-)Deutung und praktische Nutzung oft ausgespart oder nur kursorisch betrachtet haben. Dies soll technischen Analysen nicht die Relevanz absprechen, verdeutlicht aber, die Notwendigkeit empirischer Untersuchungen (Schünemann und Steiger, 2019). Die vorliegende Arbeit kann daher einen Beitrag dazu leisten, zu verstehen, wie der Handlungsraum durch die Regierungen der Bundesrepublik und des Vereinigten Königreichs gestaltet wird und wie sie einigen dieser Unsicherheiten begegnet sind.

Ein Großteil der skizzierten Studien zeichnet sich ferner durch einen Fokus auf besonders folgenschwere Cyberangriffe aus. Damit wurde früh in der wissenschaftlichen Auseinandersetzung mit dem neuen Forschungsgegenstand ein militärischer Analysefokus gesetzt. Prominenter Ausdruck dieser Perspektive ist das Bild eines Cyberwar, das bis heute für zahlreiche auch deutsche Publikationen titelgebend wirkt (Gaycken, 2011; Kurz und Rieger, 2018).[11] Diese konzeptionelle Engführung wurde immer wieder aus unterschiedlichen Perspektiven bemängelt. Die Kritiklinien haben dabei zur weiteren Ausdifferenzierung des Feldes beigetragen.

Eine konzeptionelle Kritik wurde aus der gleichen wissenschaftlichen Community formuliert, aus der auch die ersten Analysen hervorgingen (den positivistischen *strategic studies*). KritikerInnen konstatierten aber, dass der Kriegsbegriff im Kontext des neuen Handlungsraumes unangemessen sei. Einflussreich vorgetragen wurde diese Einschätzung von Thomas Rid (2012; 2013) und Eric Gartzke (2013). Thomas Rid argumentierte 20 Jahre nach Arquilla und Ronfeldt in seiner Studie »Cyber war will not take place«, dass Cyberangriffe nicht als kriegerische Akte verstanden werden könnten. Um dies zu belegen überprüfte Rid, inwiefern digitale Angriffe der Kriegsdefinition von Carl von Clausevitz entsprechen könnten. Gemessen an drei Indikatoren, wonach sich Kriege 1. durch Gewaltsamkeit, 2. Zweckdienlichkeit und 3. eine politische Natur auszeichneten, hat sich nach Rid noch kein Cyberangriff als kriegerischer Akt qualifiziert. Aus seiner Sicht dienen Cyberangriffe letztlich der Spionage, Subversion oder Sabotage. Sie sind damit

11 Für eine Problematisierung s. Schünemann/Steiger (2019).

keine neuen sicherheitspolitischen Phänomene. Ein Cyberwar im Wortsinne sei zudem unwahrscheinlich, da ein Opponent nur mit Cyberangriffen allein kaum zur Kapitulation gezwungen werden könnte (Rid, 2012). Mit Blick auf etablierte Kriegsdefinitionen argumentiert auch Eric Gartzke, dass Cyberangriffe allein ungeeignet seien, klassische militärische Ziele zu erreichen – bspw. die Eroberung und Verteidigung von Territorien (Gartzke, 2013). Diese Einschätzungen blieben allerdings nicht unwidersprochen, WissenschaftlerInnen haben darauf hingewiesen, dass ein Cyberwar im Zeitalter vernetzter Streitkräfte durchaus möglich ist (Clarke und Knake, 2010; Stiennon, 2015; Stone, 2013) bzw. sogar bereits stattfindet (Arquilla, 2012).

Eine zweite, empirische Kritik an der Ausrichtung auf besonders folgenreiche Vorfälle und militärische Aspekte der Cybersicherheit wurde sowohl von ForscherInnen aus der Konfliktforschung sowie von sozialkonstruktivistischen WissenschaftlerInnen aus dem Bereich der kritischen Sicherheitsstudien vorgebracht (Dunn Cavelty, 2013; Valeriano und Maness, 2015). VertreterInnen der Konfliktforschung bemängelten, dass Studien immer wieder um die gleichen, besonders prominenten Fälle kreisten. So gibt es zahlreiche Studien zu auch medial vieldiskutierten Angriffen bspw. gegen Estland 2007 (Herzog, 2011; Ottis, 2008), gegen Georgien 2008 (S. P. White, 2018), zu Stuxnet 2010 (Farwell und Rohozinski, 2011; Lindsay, 2013; Zetter, 2014), zum Sony-Hack 2014 (Sharp, 2017; Shaw und Jenkins, 2017) oder zu den durch Malware verursachten Stromausfällen in der Ukraine (Shackelford u. a., 2017). Vergleichende Studien, die verschiedene Fälle analysieren und dabei nicht nur die qualitativen Spitzen des Konfliktgeschehens abbilden, sind aber noch immer rar. Eine Folge dieser Kritik sind erste Projekte und Datensätze, die sich zum Ziel gemacht haben, politische Cyberangriffe strukturiert zu vermessen und so empirisch fundierte Analysen zu ermöglichen (Council on Foreign Relations, 2020; Steiger u. a., 2018; Valeriano und Maness, 2014).

Aus Perspektive der kritischen Sicherheitsstudien wurde betont, dass der Fokus auf Extreme potenziell eine problematische Militarisierung des Netzes ermögliche (Dunn Cavelty, 2012). Diese Arbeiten haben ebenfalls maßgeblich dazu beigetragen, die Begriffswahl kritisch zu reflektieren. Auch wenn die Debatte um die Anwendbarkeit des Kriegsbegriffs mittlerweile abgeflaut ist, ist unbestritten, dass zahlreiche Regierungen damit begonnen haben, ihre Streitkräfte mit offensiven Cyberkapazitäten auszustatten (Lewis und Neuneck, 2013). Nur wenige Studien haben aber theoriegeleitet untersucht, welche Mechanismen unterschiedliche staatliche Cybersicherheitspolitiken ermöglichen. Es gibt zwar Studien, die sich empirisch mit Cybersicherheitspolitiken befassen, diese sind aber zumeist theoriearm und deskriptiv (Austin, 2018; Baumard, 2017; Schallbruch und Skierka, 2018; Tabansky und Ben-Israel, 2015). Sie liefern daher keine Antworten auf die entscheidende Frage, was unterschiedliche Cybersicherheitspolitiken ermöglicht. Außerdem befassen sich die meisten empirischen Studien mit den prominen-

testen Fällen – den USA, China oder Russland (Christou, 2017; Sliwinski, 2014). Häufig befassen sich empirische Analysen auch mit den defensiven Maßnahmen, insbesondere dem Schutz kritischer Infrastrukturen (Argomaniz, 2015; Barichella, 2018; Brem, 2015; Dunn Cavelty und Kristensen, 2008; Freiberg, 2015; T. Schulze, 2006; Voeller, 2010).

Wenn Cybersicherheitspolitiken theoriegeleitet untersucht wurden, dann erfolgte das zumeist unter Rückgriff auf die Kopenhagener Schule (Sekuritisierungstheorie). Aus dieser Sicht unterstützte der wissenschaftliche Fokus auf Extrembeispiele staatliche Sekuritisierungstendenzen. Studien zeichneten dabei nach, wie Cyberangriffe sprachlich als Gefahr für die nationale Sicherheit konstruiert wurden. Empirisch lag der Fokus dieser Studien zumeist auf den Entwicklungen in den USA (Bendrath, Eriksson und Giacomello, 2007; Dunn Cavelty, 2008; Lawson u. a., 2016). Es gibt aber auch Analysen zur Bundesrepublik oder dem Vereinigten Königreich (Barnard-Wills und Ashenden, 2012; M. Schulze, 2016). Nur wenige Untersuchungen haben aber Vergleiche unterschiedlicher Cybersicherheitspolitiken durchgeführt (Gorr und Schünemann, 2013; Guitton, 2013). Diese Studien konnten nachzeichnen, wie Regierungen unter Verweis auf unterschiedliche Gefahren wie den internationalen Terrorismus oder feindliche Staaten, den Cyberspace mehr und mehr zu einem sicherheitspolitischen Handlungsfeld machten, in dem sie folglich ihre Kompetenzen erweiterten.

Die Untersuchungen konnten so zeigen, wie die Cybersicherheit zu einem Problem der nationalen Sicherheit wurde (Nissenbaum, 2005). Die Studien weisen aber (in unterschiedlichem Maße) auch Defizite und Blindstellen auf. Auch sie waren zumeist an der Militarisierung des Internets interessiert und untersuchten, wie das Netz und die damit verbundenen Gefahren als Problem für nationale Sicherheit konstruiert wurden. Sie konstatieren zumeist eine Sekuritisierung des Cyberspace, gehen aber nur selten darauf ein, dass der sicherheitspolitische Handlungskorridor nicht homogen ist. Vielmehr zerfällt der staatliche Schutzanspruch im Cyberspace in verschiedene Handlungsfelder, die durch unterschiedliche Akteurskonstellationen geprägt sind und dadurch variante Sekuritisierungsgrade ermöglichen. Die vorliegende Studie begegnet diesem Defizit durch eine systematische Unterscheidung zwischen drei Bereichen der Cybersicherheitspolitik. Auf diesem Weg soll die Entwicklung der Sicherheitspolitik differenzierter nachvollzogen werden. Dies ist theoretisch angemessen, will man ein ganzheitlicheres Bild der Cybersichehreitspolitken entwerfen, das nicht suggeriert, die Politik habe sich zunächst der Kriminalität zugewendet, um im Anschluss durch die Verbindung mit kritischer Infrastruktur auch militärische Maßnahmen zu ermöglichen. Diese Darstellung verstellt den Blick dafür, dass es zu parallelen Entwicklungen der Cybersicherheitspolitiken gekommen ist, die es in unterschiedlichen Handlungskontexten ermöglicht hat, staatlichen Sicherheitsbehörden neue Kompetenzen zuzuweisen. Anders formuliert: als die militärische

Sekuritisierung des Internets möglich wurde, endete damit nicht die Weiterentwicklung der Cybersicherheitspolitik bzw. die Kompetenzausweitung mit Bezug zur Kriminalitätsbekämpfung. Diese Entwicklung steht bei den meisten Sekuritisierungsstudien aber nicht mehr im Fokus des Interesses, obwohl sich auch hier wichtige gesellschaftliche Implikationen und Folgen für die IT-Sicherheit ergeben. Ein umfassenderes Bild der Cybersicherheitspolitik sollte auch jene Kontexte integrieren und systematisch analysieren, in denen Regierungen unterhalb der Schwelle der nationalen Sicherheit für sich in Anspruch genommen haben, Cyberangriffe durchzuführen. Hinzu kommt, dass nicht nur Cyberangriffe selbst zur Sekuritisierung des Netzes beigetragen haben, sondern dass Regierungen auch mit Blick auf traditionelle sicherheitspolitische Herausforderungen für sich auch in Anspruch nehmen, IT-Sicherheit zu unterminieren. So zielen bspw. die offensiven Maßnahmen im Bereich der Strafverfolgung oder der Nachrichtendienste nicht primär auf Cyberkriminalität, sondern auf die Prävention und Verfolgung traditioneller Straftaten.

Neben dieser empirischen Blindstelle, können auch theoretische Prämissen der Sekuritisierungstheorie im Cyberspace problematisch sein. So ist die Beurteilung dessen, was als »außergewöhnliche« Maßnahme gelten kann – der entscheidende Gradmesser für eine erfolgreiche Sekuritisierung (Floyd, 2015) – in einem neuen Handlungsraum, in dem das Normalmaß noch nicht etabliert ist, besonders schwierig und auch Analogieschlüsse sind potenziell problematisch. Ferner ist die Sekuritisierungstheorie auf einen zugänglichen Diskurs angewiesen. Praktiken, über die nicht gesprochen wird, können so schwerer analysiert werden (Dunn Cavelty, 2008, S. 132-137). Geheimhaltung ist zwar auch für diese Untersuchung ein Problem. Der rollentheoretische Fokus auf soziale Praxis erlaubt aber zumindest einen flüchtigen Blick auf die Praktiken (wenn sie bspw. durch WhistleblowerInnen oder JournalistInnen aufgedeckt werden). Weiterhin wird die Sekuritisierung zumeist als ein Prozess zwischen der Regierung und einer zumeist ausschließlich domestischen Audienz konzeptualisiert. Dies verstellt potenziell den Blick für internationale Einflüsse bzw. deren Interaktion mit der domestischen Ebene. Ein Defizit, dem im Rahmen dieser Untersuchung durch den Entwurf eines rollentheoretischen Zwei-Ebenen-Spiels begegnet werden soll. Zudem ist die Handlungsträgerschaft der Audienz in der Sekuritisierungstheorie umstritten. Einige AutorInnen halten den Einfluss der Audienz für gering (Côté, 2016; Léonard und Kaunert, 2011). Außerdem haben die Studien nur selten untersucht, inwiefern die Cybersicherheit durch Interaktionsprozesse ggf. wieder politisiert wurde. Für derartige Prozesse sprechen Gesetzesnovellen in unterschiedlichen Ländern, die die Kontrollrechte der Judikative und Legislative ausgebaut haben (bspw. das BND-Gesetz in der Bundesrepublik oder der Investigatory Powers Act in Großbritannien).

Die vorliegende Studie kann damit einen Beitrag dazu leisten, die etablierten Sekuritisierungsbefunde einerseits mit Blick auf unterschiedliche Handlungskontexte zu qualifizieren und ein differenzierteres Bild der Cybersicherheitspolitiken und deren (parallelen) Entwicklung in drei Untersuchungsbereichen zeichnen. Sie kann weiterhin deren Fokus auf Diskurse durch die Integration von Praktiken ausweiten und mit Hilfe des Vergleichs zudem systematisch Unterschiede zwischen den Untersuchungsstaaten aufdecken. Zudem verschränkt sie innen- und außenpolitische Einflüsse systematisch durch das Zwei-Ebenen-Rollenspiel. Insbesondere dieser Punkt sorgt dafür, dass die Arbeit nicht nur die theoriegeleitete Außenpolitikforschung bereichern kann, sondern auch Anschlüsse an eine andere sozialkonstruktivistische Forschungslinie mit Blick auf das Feld der Cybersicherheit erlaubt.

Auf internationaler Ebene hat sich die sozialkonstruktivistische Forschung mit der Emergenz von Cybersicherheitsnormen beschäftigt (Erskine und Carr, 2016; Finnemore, 2016; Hathaway, 2017; Maurer, 2011). In diesem Kontext wurde bspw. die Norm einer staatlichen Sorgfaltsverantwortung (due diligence) für Cyberangriffe aus dem eigenen Territorium debattiert. Hiernach sollten es Regierungen nicht dulden bzw. unterstützen, dass »ihr« Netz zur Durchführung illegaler Cyberoperationen genutzt wird (Antonopoulos, 2015; Bendiek, 2016; Liu, 2017; Takano, 2018). Außerdem werden in diesem Forschungsstrang bisher erfolglose Bestrebungen zur Regulation von Angriffsfähigkeiten (im Sinne der Rüstungskontrolle) und zur Durchführung von Cyberoperationen analysiert (Baribieri, Danis und Polito, 2018; Eggenschwiler und Silomon, 2018; Stevens, 2018). Die Untersuchungen in diesem Kontext haben überwiegend ernüchternde Befunde zur Emergenz von Normen und deren Bindewirkung geliefert. So konstatiert Melissa Hathaway »that states are not following their own doctrines of restraint«, dies könne zu Fehlattributionen und Eskalationen führen (Hathaway, 2017, S. 1).

Durch die Analyse der deutschen und britischen Cybersicherheitspolitiken können auch deren Implikationen für die emergente Cybersicherheitsordnung eingeschätzt werden. Ferner ist dieser Forschungsstrang dafür kritisiert worden, dass er mitunter eine einheitliche Trennlinie zwischen Demokratien und autokratischen Regimen suggeriert. Diese Darstellung verdeckt aber gleich zwei Befunde, nämlich, dass auch zwischen demokratischen Staaten Differenzen bei der Gestaltung ihrer Cybersicherheitspolitiken bestehen und dass diese Politiken auch domestisch umstritten sind (Maurer, 2019). Die Unterstützung oder Ablehnung bestimmter Normen ist daher auch unter Demokratien variant. Dieser Befund wurde bislang allerdings noch kaum durch empirische Vergleiche untersucht. Die Analyse der Cybersicherheitspolitiken zweier Demokratien ist vor diesem Hintergrund fruchtbar und kann dazu beitragen, die verkürzte Darstellung zu differenzieren. In diesem Zusammenhang kann diese Untersuchung die

unterschiedlichen Perspektiven auf und Herausforderungen von Normen in zwei Demokratien beleuchten und bestehende Einschätzungen ergänzen.

Christopher Whyte hat offene Fragen sowie die Desiderate zur Integration internationaler und domestischer Einflüsse auf die Cybersicherheitspolitik wie folgt skizziert:

> »[…] scholars would do well to consider the cyberpolitics field as one amenable to study under the auspices of both the IR and comparative politics research programs. Doing so would aid in accomplishing the much-needed step of integrating the main branches of the research program on cyberspace and politics that currently exist with the assumptions and sociological explorations of those authors that have, to date, considered the digital world in a more holistic fashion. Then, the field would be better placed to begin the incorporation of research projects that answer questions on the determinants of variations in state-society cyber relationships and foreign policy outcomes.« (Whyte, 2018, S. 12)

In diesem Kontext sollten Whyte zufolge bspw. Fragen nach unterschiedlichen historischen Erfahrungen und deren Folgen für die nationalen Cybersicherheitspolitiken untersucht werden (ebd., S. 12).

Die vorliegende Studie leistet einen Beitrag hierzu. Durch den systematischen Vergleich der deutschen und britischen Cybersicherheitspolitiken sollen die unterschiedlichen Einflüsse identifiziert werden, die die unterschiedlichen Politiken ermöglichen. Konkret wendet sich diese Untersuchung folgenden Fragen zu:

1. Wie haben sich die Cybersicherheitspolitiken der deutschen und britischen Regierungen in den Bereichen Strafverfolgung, Nachrichtendienste und Militär zwischen 1997 und 2019 entwickelt?
2. Welche Einflüsse haben Veränderungen der Politiken ermöglicht?

Die vorliegende Studie adressiert damit signifikante empirische und theoretische Forschungslücken und leistet einen Beitrag zum besseren Verständnis der Cybersicherheitspolitiken in den Untersuchungsstaaten. Aus empirischer Perspektive analysiert und vergleicht die Untersuchung die Cybersicherheitspolitiken zweier Staaten, die in der Forschung bisher nur wenig Beachtung gefunden haben. Theoretisch entwirft die Studie unter Rückgriff auf die symbolisch-interaktionistische Rollentheorie ein Zwei-Ebenen-Spiel, das das internationale Rollenspiel durch ein domestisches Pendant ergänzt und so das Verhältnis von Innen- und Außenpolitik aus rollentheoretischer Perspektive neu ausleuchtet. Eine theoretische Weiterentwicklung, die besonders angesichts des Untersuchungsgegenstandes und der mit ihm verbundenen schwierigen Trennung zwischen Innen- und Außenpolitik geboten scheint.

## 1.3 Aufbau der Studie

Um die Fragestellungen zu beantworten ist die Studie im Folgenden in vier Kapitel untergliedert. Im nächsten Abschnitt wird der theoretische Rahmen der Untersuchung vorgestellt. Hier werden zuerst die wissenschaftstheoretischen Grundannahmen skizziert und die Rollentheorie mit ihren Wurzeln im Pragmatismus dargestellt. Anschließend wird die symbolisch interaktionistische Rollentheorie in ihrer Anwendung zur Außenpolitikanalyse präsentiert und damit zentrale Bezugspunkte hergestellt. Im dritten Schritt wird die Konzeption eines rollentheoretischen Zwei-Ebenen-Spiels eingeführt und die Rollentheorie so um ein zweites, domestisches Rollenspiel zur Analyse der Cybersicherheitspolitiken ergänzt. Dem folgt ein kurzer Blick auf techniksoziologische Ansätze, mit deren Hilfe die theoretischen Besonderheiten des Untersuchungsgegenstandes und die damit verbundenen Implikationen verdeutlicht werden. Ferner wird hier das Verhältnis zwischen handelnden AkteurInnen und technischer Infrastruktur erläutert. Diese Betrachtung wird durch einen kurzen empirischen Exkurs veranschaulicht, der die Internetentwicklung skizziert.

Im zweiten Kapitel wird die Methodik vorgestellt. Zunächst wird in diesem Kontext die Fall- sowie Quellenauswahl begründet und die Wahl des Untersuchungszeitraums plausibilisiert. Weiterhin wird das interpretative Vorgehen, das an die Grounded-Theory-Methodologie und das Practice Tracing angelehnt ist, beschrieben. Abschließend werden die drei unterschiedlichen Rollen (Beschützer, Wohlstandsmaximierer sowie Garant liberaler Grundrechte) vorgestellt und definiert.

Mit dem dritten Kapitel beginnt die empirische Analyse der Cybersicherheitspolitiken. Die drei empirischen Kapitel folgen dabei der gleichen Struktur. Nach einer kurzen Einführung in den jeweiligen Untersuchungsbereich wird die Entwicklung der Cybersicherheitspolitik zunächst in Deutschland und dann im Vereinigten Königreich untersucht. Ein kurzes Zwischenfazit fasst die wichtigsten Erkenntnisse zusammen.

Im vierten Kapitel werden die zentralen empirischen und theoretischen Befunde vorgestellt und kritisch diskutiert. Abgeschlossen wird die Untersuchung durch eine Reflexion der Limitationen der Studie sowie einen Ausblick auf weitere Forschung zu staatlichen Cybersicherheitspolitiken.

# 2. Theorie: Pragmatismus, Rollentheorie und Techniksoziologie

In den vergangenen Jahren griffen ForscherInnen immer häufiger auf rollentheoretische Ansätze zur Analyse von Außenpolitiken zurück. Die Ursprünge der Theorie liegen allerdings nicht in der Politikwissenschaft bzw. IB-Forschung, sondern in der Sozialpsychologie der sogenannten Chicago School und der Philosophie des US-amerikanischen Pragmatismus. Sie wurde also zunächst zum Verständnis individuellen Akteursverhaltens konzipiert und erst später auf andere Kontexte übertragen, um bspw. das Verhalten kollektiver Akteure (Staaten) zu untersuchen. Die Rollentheorie ist ein entsprechend heterogenes interdisziplinäres Projekt, das auch in der Außenpolitikanalyse mit unterschiedlichen analytischen Ansatzpunkten und methodischen Zugängen angewendet wurde. WissenschaftlerInnen, die die Rollentheorie für empirische Analysen genutzt haben, haben in ihren Studien in unterschiedlichem Maße die pragmatistischen Ursprünge aufgegriffen.

Im Folgenden werden die (meta)theoretischen Annahmen der Studie offengelegt. Das Kapitel orientiert sich dabei an vier Wegmarken: Zunächst werden die Annahmen expliziert, die die Arbeit mit den »klassischen« PragmatistInnen teilt. In diesem Kontext wird der wissenschaftstheoretische Ausgangspunkt der Untersuchung dargelegt. Denn, auch wenn nicht alle SozialwissenschaftlerInnen PhilosophInnen sein müssen, eine Sensibilität für die eigenen epistemologischen und ontologischen Grundannahmen ist für das Design einer kohärenten Studie – konkret die Wahl und Passung von Theorie und Methode – unerlässlich (Della Porta und Keating, 2008, S. 20). Ferner enthält jede wissenschaftliche Untersuchung metatheoretische Annahmen, die für deren Einschätzung maßgeblich sind. Eine transparente Reflexion des eigenen Standpunkts ist daher geboten:

> »[…] one can bracket metatheoretical inquiry, but this does not free one's work, theoretical or otherwise, of metatheoretical assumptions. All work has underlying epistemological and ontological assumptions, and these establish the intellectual parameters of our inquiries, determining what we think the social and political universe comprises and what counts as valid knowledge of that universe. Second, our metatheoretical assumptions, however subliminal

> they might be, affect the kinds of practically relevant knowledge we can produce.« (Reus-Smit, 2013, S. 590)

In einem zweiten Schritt wird die Rollentheorie in ihrer Anwendung zur Außenpolitikanalyse vorgestellt. Wesentlicher analytischer Bezugspunkt der Untersuchung ist dabei die symbolisch interaktionistische Spielart der Rollentheorie, die maßgeblich von George Herbert Mead entwickelt wurde. Durch sie werden die pragmatistischen Grundlagen weiter expliziert und auf den Untersuchungsgegenstand bezogen. In diesem Kontext geht es sodann um die Integration innenpolitischer Einflüsse in die Rollentheorie. Indem die Studie das Rollenspiel auf internationaler Ebene durch ein domestisches Pendant ergänzt, entwickelt sie, in Anlehnung an bestehende Konzepte wie *role contestation* (Cantir und Kaarbo, 2012, 2016a) und das *Two-Level Game* (Putnam, 1988), einen systematischen, rollentheoretischen Zugang zur Analyse des Verhältnisses von Innen- und Außenpolitik. Im vierten Schritt werden abschließend die theoretischen Implikationen des Untersuchungsgegenstandes reflektiert. Hier wird dargelegt, inwiefern Technik (das Internet) Politik beeinflusst und wie das Verhältnis zwischen den handelnden AkteurInnen und technischen Infrastrukturen beschaffen ist. Konkret gilt es die Frage zu klären, ob es in der Cybersicherheitspolitik Handlungspraktiken (Rollen) gibt, die bereits durch die technischen Bedingungen vorgegeben sind (technischer Determinismus) oder ob AkteurInnen Technik frei formen (sozialer Determinismus)?

## 2.1 Wissenschaftstheoretische Grundannahmen: Pragmatismus und Rollentheorie

Die Wurzeln der Rollentheorie liegen im philosophischen Pragmatismus wie er wesentlich von William James, John Dewey und Charles Sanders Peirce geprägt wurde.[1] Mit ihnen teilt die Arbeit wesentliche wissenschaftstheoretische Grundannahmen. Zunächst ist aber darauf hinzuweisen, dass der Pragmatismus kein kohärentes Theoriegebäude ist, vielmehr gibt es auch hier unterschiedliche Positionen. Daher gibt es auch Debatten darüber, was unter dem Begriff Pragmatismus subsumiert werden sollte (Baert, 2009; Gould und Onuf, 2009; Margolis, 2006). Dennoch gibt es Kernannahmen, die die pragmatistischen Positionen verbinden. Wesentlicher Referenzpunkt der Denkschule ist – wie der Name bereits vermuten lässt[2] – die Praxis menschlichen Handelns. So konstatiert Gunther

1 Überblicke über den Pragmatismus sowie einzelne VertreterInnen bietet bspw. der Sammelband von John Shook und Joseph Margolis (2006).

2 Pragmatik von griechisch pragmatiké (téchnē), der Kunst, richtig zu handeln; s. dazu auch William James (1922, S. 42).

Hellmann: »Ausgangspunkt allen pragmatistischen Denkens ist der Primat der Praxis, die Verankerung allen menschlichen Handelns in konkreten Situationen« (Hellmann, 2010, S. 150). Es ist daher nicht verwunderlich, dass die Rollentheorie mit einem aufkommenden »practice turn« in den IB wachsende Aufmerksamkeit erfahren hat (Bueger und Gadinger, 2015, S. 449).

Prinzipiell kann die Rollentheorie als eine sozialkonstruktivistische Theorie verstanden werden. Gould und Onuf konstatieren sogar »[…] some constructivists are beginning to realize they have been pragmatists all along« (Gould und Onuf, 2009, S. 27). Es bestehen aber auch Unterschiede zu etablierten sozialkonstruktivistischen Ansätzen, etwa mit Blick auf die Entstehung von Wissen und Realität:

> »Practice theories argue against individualistic-interest and norm-based actor models. They situate knowledge in practice rather than ›mental frames‹ or ›discourse‹. Practice approaches focus on how groups perform their practical activities in world politics to renew and reproduce social order. They therefore overcome familiar dualisms — agents and structures, subjects and objects, and ideational and material — that plague IR theory.« (Bueger und Gadinger, 2015, S. 449)

Der Pragmatismus entwirft eine eigene Perspektive auf epistemologische und ontologische Grundfragen, die auch für die vorliegende Studie bedeutsam sind. Um die Ansprüche (und Bewertungsmaßstäbe) der eigenen Arbeit zu klären, werden im Folgenden zunächst die zentralen Begriffe Wissen und Wahrheit näher betrachtet.

Die besondere Bedeutung der Praxis wird bereits bei der pragmatistischen Annäherung an den, für die Wissenschaft zentralen, Begriff der Wahrheit deutlich. Hervorzuheben ist zunächst die Ablehnung einer Korrespondenztheorie der Wahrheit, wie sie bspw. im philosophischen Realismus vertreten wird. Eine entscheidende Frage ist dabei: »Gibt es wirklich propositional strukturierte Dinge in der Welt, die unabhängig von unserem Denken und Sprechen sind? Oder ist Propositionalität nicht vielmehr ein spezifisches Merkmal unseres Denkens und Sprechens?« (P. Baumann, 2006, S. 159). PragmatistInnen stehen der Annahme, dass eine beobachterunabhängige Welt objektiv erschließbar ist, kritisch gegenüber, da diese stets unbeweisbar bleiben muss:

> »For at the heart of the realist position is the thought that a belief could be the best it could be by way of accounting for the evidence and fulfilling our other aims in inquiry and yet it could still be false. It could still fail to get right the believer-independent world. So what is the nature of this link between empirical adequacy and the literal truth? What reason do we have for assum-

> ing that beliefs that are empirically adequate are beliefs that are likely to get right the believer-independent world?« (Misak, 2006, S. 404)

Der Pragmatismus behauptet nicht, dass es keine beobachter-unabhängige Welt gibt, aber sie kann nicht objektiv erschlossen werden bzw. der Nachweis, dass die Erschließung erfolgreich war, lässt sich unmöglich führen (Rorty, 2000, S. 185). Es ist daher auch nicht zielführend weiter über diese Option zu reflektieren. Zweifel an der Außenwelt (bzw. deren Erschließbarkeit) mündeten in der Philosophiegeschichte meist entweder in skeptizistischen oder idealistischen Positionen. Der Pragmatismus umschifft die metaphysischen Untiefen dieser Positionen, indem er auf soziale Praxis rekurriert. Auch PragmatistInnen beginnen mit einem Zweifel. Allerdings nicht mit dem alles hinterfragenden Zweifel der SkeptikerInnen, sondern mit den Zweifeln, die Handelnden in konkreten Situationen begegnen. Peirce legt dar, warum aus pragmatistischer Sicht der radikale Zweifel der SkeptikerInnen weder angemessen noch zielführend ist:

> »We cannot begin with complete doubt. We must begin with all the prejudices which we actually have when we enter upon the study of philosophy. These prejudices are not to be dispelled by a maxim, for they are things which it does not occur to us can be questioned. Hence this initial skepticism will be a mere self-deception, and not real doubt; and no one who follows the Cartesian method will ever be satisfied until he has formally recovered all those beliefs which in form he has given up. It is, therefore, as useless a preliminary as going to the North Pole would be in order to get to Constantinople by coming down regularly upon a meridian. A person may, it is true, in the course of his studies, find reason to doubt what he began by believing; but in that case he doubts because he has a positive reason for it, and not on account of the Cartesian maxim.« (Peirce, 1868, S. 140f.)

In Ermangelung unhintergehbarer Maßstäbe zur Ergründung der realen Welt, richten PragmatistInnen den Blick auf die soziale Praxis und die Erfahrungshorizonte handelnder AkteurInnen. Sie stellen dabei die cartesianische Formel »cogito ergo sum« auf den Kopf und argumentieren, dass Menschen in konkreten Situationen denken müssen um handlungsfähig zu sein (Hellmann, 2010, S. 150). Der pragmatistische Zugang verschmilzt dabei die Unterscheidung zwischen Erkenntnis- und Handlungstheorie (ebd., S. 152). Als Gegenentwurf rekurrieren sie auf den direkten empirischen Bezug in konkreten Handlungssituationen und die Erfahrungen der AkteurInnen.

> »Dewey's postulate of immediate empiricism holds that things are what they are experienced as, and if things are experienced differently, then no one account is real and the others unreal. What matters is 'what sort of experience is

> denoted or indicated: a concrete and determinate experience, varying, when it varies, in specific real elements, and agreeing, when it agrees, in specific real elements, so that we have a contrast, not between a Reality, and various approximations to, or phenomenal representations of Reality, but between different realms of experience'.« (Cochran, 2002, S. 532)

Das bedeutet, dass Menschen nicht über Wahrheit im Sinne des Realismus verfügen, sondern dass sie für durch Erfahrungen bestätigte Überzeugungen temporär den Status des Für-Wahr-Haltens vergeben.[3] Auch hierbei bleibt der Pragmatismus an sozialer Praxis orientiert. Peirce argumentiert, dass Menschen ausgehend von einem Zweifel in einer konkreten Situation nach einer Überzeugung (*belief*) suchen, die diesen Zweifel ausräumt und dann Handeln ermöglicht.

Den Prozess zu einer gefestigten Überzeugung zu gelangen nennt Peirce *Inquiry*, was zumeist mit Forschungsprozess übersetzt wird, da PragmatistInnen diesen Prozess auch als idealtypisch für ein wissenschaftliches Vorgehen verstehen (Hellmann, 2010, S. 150). Die gewonnene Überzeugung wird solange handlungsleitend, wie sie sich in der Praxis als nützlich erweist. Daraus folgt die pragmatistische Maxime »belief is a rule for action« (Peirce, 1878, S. 291). Die Überzeugung ist aber kein dauerhaft fester Untergrund. Peirce greift zur Illustration auf das Bild eines Moores zurück, das an einigen Stellen tragfähig erscheint und das weitere Fortschreiten ermöglicht, an anderen Stellen ist es jedoch nicht belastbar und auch einstmals sicher geglaubte Pfade können wieder unbegehbar werden. Überzeugungen bleiben daher immer durch neue Erfahrungen reversibel. Herbert Blumer hat diesen Umstand mit Hinweis auf die praktische Widerständigkeit der Welt verdeutlicht. Er spricht davon, dass die empirische Welt Menschen gleichsam auf ihre Handlungen antwortet (»talk back«) (Blumer, 1986 [1969], S. 22). Wann immer hierbei bestehende Überzeugungen in konkreten Handlungssituationen substanziell herausgefordert werden, passen Menschen ihre Überzeugungen an. Aus pragmatistischer Perspektive gelten folglich die Überzeugungen als wahr, die sich langfristig im praktischen Gebrauch bewähren (Misak, 2006, S. 404).

Moderne PragmatistInnen (insbesondere Richard Rorty (1992) und Donald Davidson (2001; 2004)) haben vor diesem Hintergrund auf die Sprachabhängigkeit von Beobachtungen bzw. die Relativität von Weltbild und Überzeugungen hingewiesen. [4] Damit hängt es vom Weltbild der/des Beobachtenden ab, welche Beobachtungen zur Widerlegung oder Rechtfertigung bestimmter Annahmen und Aus-

3 Gould und Onuf attestieren vor diesem Hintergrund »pragmatism gives constructivists all the philosophical support they need to proceed« (2009, S. 32).

4 In der wissenschaftstheoretischen Debatte wird das Problem der Relativität von Weltbild und Überzeugungen zumeist unter dem Begriff der *Theoriebeladenheit* wissenschaftlicher Beobachtungen diskutiert. Aktuelle philosophische Auseinandersetzungen mit der Theoriebeladenheit wissenschaftlicher Beobachtungen greift bspw. das von Ioannis Votsis, Michela Ta-

sagen akzeptiert werden. Veränderungen in den Weltbildern sind zwar möglich, kommen dann aber einer »Bekehrung« im Wittgensteinschen Sinne gleich (Hellmann, 2010, S. 155f.).[5] PragmatistInnen gehen davon aus, dass Beobachtungen nicht nur theoriebeladen, sondern auch sprachabhängig sind. Das bedeutet, »dass Wissen (Wahrheit) nicht *ge*funden, sondern *er*funden wird« (ebd., S. 154, Hervorhebung im Original, Anm. d. Verf.). PragmatistInnen stehen auch deshalb der im Wissenschaftlichen Realismus (bspw. von Alexander Wendt (1999)) vertretenen Grundannahme, dass auch immaterielle Entitäten real seien und zudem verlässlich von WissenschaftlerInnen erschlossen werden könnten, kritisch gegenüber. Der Pragmatismus kritisiert hierbei sowohl die Annahme, dass diese Phänomene im strengen Sinne real sind (ontologische Annahme) als auch die Position, dass diese von ForscherInnen sicher identifiziert werden könnten (epistemologische Annahme). Der Pragmatismus vertritt damit Zweifel am Wendtschen Konstruktivismus, die auch von anderen konstruktivistischen ForscherInnen formuliert wurden und die den Mittelweg zwischen positivistischen und post-positivistischen Perspektiven für problematisch halten. Ein wesentliches Spannungsverhältnis in Wendts Position erwächst aus der epistemologischen Annahme erhöhter wissenschaftlicher Rationalität (zur verlässlichen Erschließung der Welt) einerseits und sozialer Konstruktion bei den untersuchten AkteurInnen (Ontologie) andererseits. Dies sorgt zwar dafür, dass die Position an positivistische Wissenschaftsverständnisse anschlussfähig bleibt, in letzter Instanz ist sie aber nicht konsequent. Aus dieser Perspektive bleibt der von Wendt vertretene »Mittelweg« auf der Mitte des Weges stehen (Ulbert, 2014, S. 260f.).

In dem Moment, in dem der Pragmatismus die Suche nach Übereinstimmung mit der Realität aufgibt, verschiebt sich die Fragestellung bei der Suche nach Wahrheit maßgeblich: »We can say that the interesting question is not

---

cca und Gerhard Schurz (2015) herausgegebene Sonderheft des Journal for General Philosophy of Science auf.

5 Diese Bekehrung ist vergleichbar mit Thomas Kuhns Paradigmenwechsel. Kuhn argumentiert, dass wissenschaftliche Paradigmen ontologisch inkommensurabel sind (1996, S. 103). In einer starken Interpretation kann es aus dieser Perspektive, in Ermangelung einer theorieneutralen Sprache, keine objektiven Maßstäbe zur Wahl einer Theorie geben, da sich mit dem Paradigmenwechsel gleichsam die Welt selbst verändert: »In so far as their only recourse to that world is through what they see and do, we may want to say that after a revolution scientists are responding to a different world« (Kuhn, 1996, S. 111) (Für eine Einführung in die wissenschaftstheoretische Position Thomas Kuhns s. bspw. Bailer-Jones und Friebe, 2009; Bird, 2000; Hoyningen-Huene, 1989). Dies ist ein auch dem Pragmatismus nahe stehender Gedanke (solange er nicht durch eine holistische Interpretation überspitzt wird (Davidson, 2004, S. 14)), denn er führt letztlich zu der Erkenntnis, dass, was als wissenschaftliches Vorgehen anerkannt ist, mit einem Paradigmenwechsel verändert wird und damit sozialer Deutung unterliegt: »[…] what is regarded as rational activity is itself as much a social as an intellectual matter« (Hollis, 1994, S. 87).

›Knowledge or opinion? Objective or subjective?‹ but rather ›Useful vocabulary or relatively useless vocabulary?‹« (Rorty, 2000, S. 186). Dies führt zu wichtigen Implikationen mit Blick auf den Status von Theorien bzw. deren Bewertungsmaßstäbe und auf die wissenschaftliche Praxis im Allgemeinen. Aus einer Ablehnung der Korrespondenztheorie der Wahrheit folgt unmittelbar, dass Theorien bzw. die hieraus abgeleiteten Hypothesen nicht – wie vor einer Kontrastfolie – an der Realität geprüft und am Grad ihrer Entsprechung bemessen werden können. Aus pragmatistischer Perspektive bilden wissenschaftliche Theorien nicht Realität ab, sondern entfalten Nutzen im Umgang mit empirischen Phänomenen (Misak, 2006). Auf den ersten Blick könnten KritikerInnen nun zu dem Schluss gelangen, diese Position führe in einen Anything-Goes-Relativismus á la Paul Feyerabend.[6] PragmatistInnen haben sich mit diesem Problem eingehend auseinandergesetzt und argumentiert, dass aufgrund der Sozialität und der Anforderung praktischer Nützlichkeit eben gerade nicht »alles geht«, aber gleichsam alles als fallibel gelten muss.[7] Wenn es keine unhinterfragbaren Maßstäbe zur Bewertung wissenschaftlicher Erkenntnis gibt, kann das Ziel nur darin bestehen, die wissenschaftliche Gemeinschaft von der Nützlichkeit bzw. empirischen Angemessenheit der erzielten Ergebnisse zu überzeugen: »[…] there is no test for whether a belief accurately represents reality except justification of the belief in the terms provided by the relevant community« (Rorty, 2000, S. 185). Für die vorliegende Studie bedeutet das konkret, die WissenschaftlerInnen zu überzeugen, die in den IB häufig als »Interpretivist«[8] bezeichnet werden. Da auch Wissenschaft ein soziales Unterfangen ist, ist die intersubjektive Einschätzung durch die wissenschaftliche Referenzgruppe entscheidender Gradmesser.[9] Anerkennung durch die wissenschaftliche Peergruppe wird eine Untersuchung aber nur erhalten, wenn sie den in der Referenzgruppe geteilten Bewertungsmaßstäben entspricht. Das bedeutet, sie muss in diesem Fall mit einem logischen, transparenten und kohärenten Forschungsdesign zu plausiblen Erkenntnissen über die empirische Entwicklung der Cybersicherheitspolitiken beider Untersuchungsstaaten gelangen. Die prag-

6 Es ist anzumerken, dass auch Feyerabend selbst die Formulierung anything goes nie als wissenschaftliches Prinzip verstanden hat (Hellmann, 2010, S. 171).

7 Der Vorwurf ignoriert nämlich unter anderem die Tatsache, dass AkteurInnen immer in soziale Kontexte eingebunden sind und dass Intersubjektivität für Staaten wie für ForscherInnen stets die Grenze kollektiver wie individueller Imaginationsfreiheit bildet, solange Handeln in einem sozialen Kontext anschlussfähig oder auch nur verständlich bleiben soll.

8 Überblicke über verschiedener IB-Forschungspositionen anhand epistemologischer und ontologischer Grundannahmen geben bspw. (Carlsnaes, 2013; Della Porta und Keating, 2008; Jackson, 2011; King, Keohane und Verba, 1994; Lake, 2013).

9 Für eine Einschätzung der »Objektivität der Wissenschaften als soziales Phänomen« s. bspw. auch Torsten Wilholt (2009).

matistisch geprägte symbolisch interaktionistische Rollentheorie bildet dazu den analytischen Rahmen.

## 2.2 Analytische Bezugspunkte: Die symbolisch interaktionistische Rollentheorie in der Außenpolitikforschung

In seinem Aufsatz *National Role Conceptions in the Study of Foreign Policy* nutzte Kalevi Holsti (1970) erstmals Rollen zur Analyse von Außenpolitik. Unter Rückgriff auf Regierungsdokumente von 71 Staaten, identifizierte er 17 verschiedene nationale Rollenkonzeptionen, die die Außenpolitiken erklären. In dieser Studie griff Holsti explizit Gedanken bereits erwähnter Pragmatisten (bspw. Dewey und Mead) auf und machte das Konzept der Rolle für die Analyse staatlichen Verhaltens nutzbar. In der Folge haben WissenschaftlerInnen immer wieder auf Rollen als analytische Konzepte zur Untersuchung staatlichen Verhaltens zurückgegriffen. Ohne einem methodologischen Individualismus das Wort zu reden, sei an dieser Stelle explizit darauf hingewiesen, dass der Pragmatismus zum Verständnis individuellen menschlichen Verhaltens angetreten ist. Die vorliegende Studie teilt die Überzeugung, dass letztlich nur Menschen Handlungsträgerschaft (Akteurschaft) zukommt. Wenn Individuen im Verbund agieren, wenn also von kollektiven Akteuren gesprochen wird, bezeichnet das aus pragmatistischer Perspektive eine Struktur kollektiven Handelns (Roos, 2010, S. 59). Daher ist es auch angemessen von Staaten bzw. sozial organisierten Gruppen als Rollenträgern zu sprechen (McCourt, 2014, S. 34-37). Damit wird auch der Kritik an der Rollentheorie begegnet, sie operiere mit einem unangemessenen menschlichen Analogieschluss (Harnisch, 2012a, S. 51).

Frühe Studien operierten dabei häufig mit einem analytischen Schwerpunkt auf den Ego-Teilen der Rollen und beleuchteten weniger die Interaktion und damit die Bedeutung signifikanter Anderer. Die Analyse von Regierungsdokumenten und die Verknüpfung mit dem außenpolitischen Verhalten bei Holsti steht exemplarisch für dieses Vorgehen. Aspekte symbolischer Interaktion rückten erst später in Rückbesinnung auf die theoretischen Ursprünge stärker in den wissenschaftlichen Fokus (Harnisch, 2012b, S. 7).

Nicht alle Studien, die zur Untersuchung von Außenpolitik auf die Rollentheorie zurückgegriffen haben, teilen die zuvor skizzierten wissenschaftstheoretischen Prämissen oder die Annahmen des Symbolischen Interaktionismus. Das Feld rollentheoretischer Untersuchungen umfasst verschiedene methodische Zugänge. Das Spektrum reicht dabei von interpretativen Studien bis zu quan-

tifizierenden, spieltheoretischen Analysen.[10] Dementsprechend unterschiedlich sind auch die Einschätzungen kausaler oder konstitutiver Wirkungen materieller Faktoren auf Rollen. Während, wie häufig in den IB, die eher positivistischen US-amerikanischen WissenschaftlerInnen oft auf die materiellen Grundlagen von Rollen und deren kausale Wirkung verweisen, argumentieren europäische ForscherInnen dagegen häufiger im pragmatistischen Sinne für eine Interpretation von Rollen als Ausdruck handlungsleitender Überzeugungen und damit Gründen für Akteursverhalten (ebd.).[11] Auch wenn in frühen Studien die Alter-Teile von Rollen zugunsten der Ego-Parts (empirisch) vernachlässigt wurden, kann doch als verbindende Annahme aller RollentheoretikerInnen die Prämisse gelten, dass Rollen nicht ohne Bezug zu anderen (Gegen-)Rollen und damit zu Sozialstruktur gedacht werden können (ebd., S. 7).

Entsprechend der explizierten wissenschaftstheoretischen Grundlagen, orientiert sich die vorliegende Studie an der interpretativen Linie der Rollentheorie, die wesentliche Bezüge zum Symbolischen Interaktionismus von George Herbert Mead (1979) aufweist. Wie den bereits vorgestellten Pragmatisten, ging es auch Mead um das Verständnis menschlichen Handelns. Er verteidigte dabei die menschliche Freiheit gegen zwei aufkommende Denkschulen: Den Behaviorismus einerseits, der den Menschen letztlich als ein auf Reize nur reagierendes, von seiner Umwelt getriebenes Individuum sah und gegen die Psychoanalyse andererseits, die davon ausging, dass Verhaltensmuster bereits durch unbewusste frühkindliche Ereignisse festgelegt werden, die später nur noch leichte Abweichungen von einem dann perpetuierten Verhaltensrepertoire zulassen (Abels, 2010, S. 15f.). Auch Mead rekurriert unmittelbar auf die soziale Praxis und konzipiert den Menschen als praktisch handelndes und vernunftbegabtes Wesen. Da Mead selbst kein umfassendes Werk zu seiner Arbeit publiziert hat, wurden Teile der theoretischen Annahmen durch Herbert Blumer, einen Schüler Meads, später unter dem Rubrum *Symbolischer Interaktionismus* veröffentlicht (Blumer, 1986 [1969]). Wie der Name bereits offenbart, ist die symbolvermittelte Interaktion zentraler analytischer Bezugspunkt.

Aus dieser Perspektive erschließen AkteurInnen die Welt durch Interaktion und vermitteln Bedeutungen über (signifikante) Symbole (Mead, 1979). Herbert

10 Überblicke über unterschiedliche Strömungen der Rollentheorie in der Außenpolitikforschung bieten bspw. Harnisch (2018), Breuning (2017), Walker (2017) oder Thies (2010).

11 Stellvertretend für eine materiellere Orientierung kann auch Alexander Wendt interpretiert werden, wenn er konstatiert, dass nicht alle Akteure in gleichem Maße signifikant sind und dass deren Bedeutung etwa von Machtressourcen abhängig ist (Wendt, 1999, S. 327). Es ist unbestritten, dass Ressourcen durchaus die Übernahme bestimmter Rollen erleichtern, allerdings sind die materiellen Grundlagen nicht entscheidend. Aus symbolisch interaktionistischer Sicht ist die soziale Praxis also die entsprechende Bezugnahme in konkreten Handlungssituationen der entscheidende Gradmesser.

Blumer hat wesentliche Kerngedanken des Symbolischen Interaktionismus folgendermaßen formuliert:

> »The first premise is that human beings act toward things on the basis of the meanings that the things have for them. […] The second premise is that the meaning of such things is derived from, or arises out of, the social interaction that one has with one's fellows. […]« (Blumer, 1986 [1969], S. 2)

Die konkrete Frage, die sich hieraus für diese Studie ergibt, ist: Welche Rollenkonstellationen prägen diesen Interaktionsprozess in der deutschen und britischen Cybersicherheitspolitik?

Durch Sprache und (signifikante) Symbole ist es Menschen möglich, sich selbst zu objektivieren und aus der Rolle des Anderen auf sich zurückzublicken (»taking the role of the other« (Mead, 1979, S. 254)). Die Möglichkeit, die Ego-Perspektive zumindest temporär zu verlassen und aus gesellschaftlicher Perspektive auf sich selbst Bezug zu nehmen, ist konstitutiv für die menschliche Sozialität. Erst mit der Einbindung in eine Gesellschaft und durch den Blick aus deren Perspektive, wird der Mensch zum Akteur, da er sich seiner selbst erst aus Perspektive des Anderen wirklich gewahr werden kann (ebd., S. 56). Rollen werden in dieser Untersuchung als soziale Positionen verstanden, die mit einer temporären Funktionsübernahme für eine soziale Gruppe verbunden sind. Rollen sind dabei bidirektional aufeinander bezogene relationale Konstrukte, die sich aus Eigen- (Ego) und Fremderwartungen (Alter) zusammensetzen (Harnisch, 2012b, S. 8). Die Annahme relationaler sozialer Konstitution ist dabei keine neue symbolisch-interaktionistische, sie findet sich mit Bezug zur Identitätsbildung bspw. bereits in Hegels Phänomenologie des Geistes (1989 [1807]).[12] Hegel beschreibt das dialektische Verhältnis von Herr- und Knechtschaft und konstatiert: »Das Selbstbewußtsein ist *an* und *für sich*, indem und dadurch, daß es für ein Anderes an und für sich ist; d. h. es ist nur als ein Anerkanntes [Hervorhebung im

12 Mitunter wurden die beiden Begriffe Identität und Rolle synonym verwendet. Die systematische Differenzierung zwischen beiden Konzepten hat in der Außenpolitikanalyse erst seit kurzem vermehrt akademische Aufmerksamkeit erfahren (Harnisch, 2018). Während Rollen auf Handeln in Gruppen ausgerichtet sind, bieten Identitäten AkteurInnen ein kohärentes Selbst, das auch zur Abgrenzung von Anderen dient (McCourt, 2012, 2014). Prinzipiell lässt sich festhalten, dass eine Rolle theoretisch ersatzlos aufgegeben werden kann, ohne dass die/der AkteurIn aufhört zu existieren. Eine Identität kann dagegen nur mit dem Auslöschen des Akteurs/der Akteurin verschwinden. Ferner kann ein/e AkteurIn problemlos mehrere Rollen in unterschiedlichen Handlungskontexten wahrnehmen. Ein/e AkteurIn verfügt dagegen nur über eine (wandelbare und ggf. vielschichtige) Identität, die ihm/ihr (selbst) seine Einzigartigkeit in Abgrenzung zu anderen garantiert.

Original; Anm. d. Verf.]« (Hegel, 1989 [1807], S. 145). Diese Annahme wird grundsätzlich auch von der Rollentheorie geteilt. Allerdings wahrt sie dem Individuum Gestaltungsfreiheit, sodass Gesellschaft das Individuum nicht determiniert.

Erst Rolle und komplementäre Gegenrolle führen zu einer stabilen sozialen Beziehung. Stabil ist in diesem Fall nicht als harmonisch oder friedvoll fehlzuinterpretieren, denn auch zwischen Feinden kann eine stabile (konfliktive) Beziehung bestehen, solange sich beide als Feinde betrachten und entsprechend handeln.[13] Um den interaktiven Charakter besser zu illustrieren, soll das Verhältnis kurz am Beispiel des Beschützers (Rolle) und Beschützten (Gegenrolle) erläutert werden. Übernimmt ein/e AkteurIn in einer sozialen Gruppe die Rolle eines Beschützers, so ist sie/er darauf angewiesen, dass diese von den Beschützten durch die Einnahme der komplementären Gegenrolle(n) stabilisiert wird. Da die Beschützer-Rolle mit besonderen Funktionen und damit einhergehend Kompetenzen verbunden ist (bspw. dem Monopol auf legitime Gewaltanwendung zur Gefahrenabwehr), müssen diese ebenfalls in der Interaktion bestätigt werden. Warum die Gegenrolle akzeptiert wird, ist dabei zunächst unerheblich (bspw. aus Furcht vor Repression, wirtschaftlichem Interesse, Tradition oder Anerkennung der Legitimität), denn die Übernahme der Gegenrolle der Beschützten konstituiert soziale Wirklichkeit. Soziale Interaktion mit ihren konstitutiven Wirkungen bildet damit den Nukleus symbolisch interaktionistischer Rollentheorie. Durch diesen analytischen Fokus ist es der Rollentheorie möglich, auf tradierte Handlungslogiken zu verzichten. Die Gründe für eine Rollenübernahme können mannigfaltig sein. Im Gegensatz zu rationalistisch argumentierenden Theorien ist aber bspw. keine Interessenkonvergenz nötig, um stabile Rollenbeziehungen und damit Sozialstruktur zur Folge zu haben. An Stelle etablierter Handlungslogiken wie Angemessenheit, Argumentation oder Rationalität, die alle auf einen vor der Praxis liegenden Referenzpunkt rekurrieren, rückt die Logik der Interaktion als zentrales Moment. »Denn egal ob strategisch oder verständigungsorientiert gehandelt wird, nach außen ist beides Handeln nur Rollenhandeln […]. Auch strategisches Verhalten hat soziale Folgen, und zwar für beide Interaktionspartner« (M.-O. Baumann, 2014, S. 55). Im Unterschied zu anderen rollentheoretischen Studien, analysieren pragmatistisch orientierte Untersuchungen daher die konstitutiven Effekte sozialer Interaktion und bspw. nicht »nur« ego-zentrierte Rollenkonzeptionen der Regierungen (McCourt, 2014, S. 13f.).

Aufgrund des Bezugs von Ego und Alter sowie der damit einhergehenden Rückbindung an resultierende Sozialstruktur, wurde von rollentheoretisch arbeitenden WissenschaftlerInnen immer wieder auf die besondere Position von Rollen zwischen AkteurInnen und Struktur hingewiesen. Ein analytischer Vorteil

13 Auch konfliktive Rollenkonstellationen können Erwartungssicherheit und damit ontologische Sicherheit bieten (s. Mitzen, 2006).

von Rollen, die damit theoretisch eine Scharnierposition zwischen AkteurInnen und Struktur einnehmen, liegt aus dieser Perspektive in der Überwindung eines Akteur-Struktur-Dualismus und damit in einer möglichen Verknüpfung der verschiedenen Forschungsperspektiven in Foreign Policy Analysis und IB (Cantir und Kaarbo, 2016b; Harnisch, 2018; C. G. Thies und Breuning, 2012; Walker, 2011). Dieser Aspekt soll an dieser Stelle kurz weiterverfolgt werden, da er auch bei der Diskussion der theoretischen Implikationen des Internets (einer globalen technischen (Infra-)Struktur) nochmals bedeutsam wird.

Wird in den IB das Verhältnis von Akteur und Struktur verhandelt – konkret: deren ko-konstitutive Beziehung – wird häufig auf die Strukturationstheorie von Anthony Giddens (1984) zurückgegriffen; nicht zuletzt aufgrund des prominenten Bezugs bei Alexander Wendt (1999, S. 139-189). Ulrich Roos weist aber zurecht darauf hin, dass die Strukturation prinzipiell nur langsame, inkrementelle Veränderungen zur Erklärung strukturellen Wandels anbietet und damit unmittelbar in Spannung zu pragmatistischen Annahmen steht, die das kreative Potenzial zur Problemlösung betonen, das menschlichen AkteurInnen eigen ist. Wenngleich Giddens Veränderungen von Überzeugungen für möglich hält, unterstellt er doch eine starke Tendenz zur Perpetuierung strukturerhaltender Verhaltensweisen (Roos, 2010, S. 54). Das für den Pragmatismus entscheidende Momentum kreativen Problemlösens, insbesondere in Situationen, die durch ein hohes Maß an Erwartungsunsicherheit geprägt sind, findet im engen Korsett der Strukturation keinen substanziellen Entfaltungsraum. Das ist aus zwei Gründen problematisch: Erstens stellt sich die Frage nach der Freiheit, Handlungsträgerschaft und – damit verbunden – der (politischen) Verantwortung der AkteurInnen. Wenn Struktur eine Tendenz zur Selbsterhaltung aufweist, ist der Einfluss der Handelnden stark begrenzt und es bestehen kaum echte Alternativoptionen. Zweitens klammert die Strukturation damit einen interaktionistischen Mechanismus für strukturellen Wandel aus, der nicht nur langsame und inkrementelle Veränderungen zulässt (s. hierzu M.-O. Baumann, 2014). Beide Probleme werden im Folgenden kurz diskutiert.

Theoretisch entscheidend ist in diesem Kontext der menschliche Umgang mit Unsicherheit. Menschen stehen in unbekannten Handlungssituationen vor der Herausforderung kreativ zu agieren und Unsicherheit durch Praxis zu überwinden. Dieser Überwindungsprozess ist zentrales Motiv des Pragmatismus. Er findet sich in Deweys Differenzierung zwischen »determinate« und »indeterminate situations« (Dewey, 1938, S. 104-105) ebenso wie in Peirces' Prozess der »Inquiry« (Peirce, 1877). Um den Umgang mit einer durch Handlungsunsicherheit geprägten Situation darzustellen, etabliert Mead die Unterscheidung zwischen I und Me. Hierdurch veranschaulicht er die besondere Bedeutung menschlicher Kreativität im praktischen Handeln detaillierter als die beiden anderen Pragmatisten. Mead zerlegt das Selbst in zwei Teile oder Phasen, um diesen Prozess genauer darzu-

stellen. Dabei fungiert das I als kreativer und weitgehend eigenständiger Part, während das Me dagegen das bereits sozial verortete Selbst darstellt (Mead, 1979, S. 173-178 sowie 192-200). Situationen in denen das Meadsche I den Handelnden selbst überrascht und in diesem Zuge Handlungsunsicherheit überwindet, sind mit den Annahmen von Giddens kaum vereinbar. Es sind aber diese Situationen bzw. der Umgang mit ihnen, die den AkteurInnen sowohl ein substanzielles Maß an Freiheit als auch strukturelle Gestaltungsmöglichkeiten eröffnen.

Sozialkonstruktivistischen Ansätzen in den IB wurde in diesem Kontext vorgeworfen, sie sprächen den AkteurInnen prinzipiell die Möglichkeit zu, sich Situationen voluntaristisch so zu denken, wie es ihnen beliebt und implizierten damit ein unangemessenes Maß von Freiheit. In Erwiderung wurde von SozialkonstruktivistInnen zurecht auf die Bedeutung der Intersubjektivität hingewiesen (Guzzini, 2000, S. 155). Da AkteurInnen stets in sozialen Kontexten handeln, sind sie darauf angewiesen, dass ihr Verhalten verstehbar oder anschlussfähig ist. Geht es um die Bedeutung einer geteilten Lebenswelt, kann mit Mead in diesem Kontext einerseits auf die Bedeutung intersubjektiv geteilter signifikanter Symbole verwiesen werden (Mead, 1979, S. 56, 89). Andererseits kann, setzt man keine geteilte Lebenswelt voraus, die Relationalität von Rolle und Gegenrolle bzw. die sozialstrukturelle Anschlussfähigkeit in diesem Kontext sogar als doppelte Intersubjektivitätsbedingung interpretiert werden. Mead erhält Freiheit der AkteurInnen daher maßgeblich durch die Unterscheidung zwischen I und Me. »It is because of the ›I‹ that we say that we are never fully aware of what we are, that we surprise ourselves by our own action« (ebd., S. 174). Menschen sind dazu in der Lage sich selbst zu überraschen, das I ist dabei für den Handelnden nie vollständig vorhersehbar. Auch wenn Situationen häufig geprobt wurden, besteht doch immer die Möglichkeit, aus bestehenden Mustern auszubrechen (ebd., S. 177 f.). Dieses unkalkulierbare Potenzial, in Verbindung mit der reflexiven Intelligenz, die es ermöglicht unterschiedliche Handlungsmöglichkeiten auszuleuchten, erlaubt es Menschen zwischen Handlungsoptionen abzuwägen und sich dabei selbst zu überraschen (ebd., S. 243). Die Rollentheorie in symbolisch interaktionistischer Lesart bietet AkteurInnen dadurch nicht nur die Möglichkeit passiv strukturell vorgegebene Rollen zu übernehmen (role taking), sondern kreativ neue Rollen zu entwerfen (role making) und so, wenn diese neuen Rollen durch komplementäre Gegenrollen bestätigt werden, konstitutiv neue soziale Ordnung zu schaffen (Harnisch, 2012a). Die pragmatistische Rollentheorie von Mead steht daher auch einer substantialistischen (bzw. strukturell-funktionalistischen) von Talcott Parsons vertretenen Interpretation von Rollen entgegen, wonach diese strukturbedingt bereits vor den AkteurInnen bestehen und quasi nur noch übernommen werden müssen (McCourt, 2014, S. 21f.).

Damit bietet die Rollentheorie den AkteurInnen eine substanzielle Freiheit unter der auch ein gehaltvolles Verständnis von (politischer) Verantwortlichkeit

möglich wird und zwar ohne Strukturbedingungen Relevanz abzusprechen.[14] Im Gegenteil: Erst durch die Einbindung in eine Sozialstruktur kann der Mensch überhaupt zur/zum AkteurIn werden. Sozialer Bezug ermöglicht Individuen erst sich selbst als AkteurInnen zu begreifen, da sie sich in die Rolle der Anderen versetzen und so auf sich zurückblicken können. Durch Handlungen in der Gesellschaft und insbesondere durch das kreativ schaffende Potenzial des I können AkteurInnen aber auch Sozialstruktur verändern: »The ›I‹ is the response of the individual to the attitude of the community as this appears in his own experience. His response to that organized attitude in turn changes it« (Mead, 1979, S. 196).

Auch wenn AkteurInnen mit Strukturbedingungen konfrontiert sind, die sie nicht selbst geschaffen haben, lässt sich durch eine Rückbindung der Sozialstruktur an menschliches Handeln doch verdeutlichen, dass Struktur selbst keine aktive Handlungsträgerschaft besitzt, sondern wie eine Reflexion zurückliegendes menschliches Handeln widerspiegelt und so auf aktuell wie zukünftig Handelnde wirkt. Durch die Möglichkeiten des I wird struktureller Wandel nicht nur langfristig und in inkrementellen Schritten möglich, sondern kann theoretisch auch rascher erfolgen. Schnellere strukturelle Veränderungen sind aber abhängig von komplementärer Gegenrollenübernahme durch signifikante Andere. Konkret bedeutet das, schneller struktureller Wandel ist davon abhängig, dass er von anderen AkteurInnen in der Interaktion affirmiert wird (M.-O. Baumann, 2014). Damit

14 An dieser Stelle soll nicht in die Untiefen philosophischer Debatten zu Willensfreiheit und Determinismus hinabgestiegen werden. Es ist allerdings erkennbar, dass Mead die AkteurInnen nicht durch strukturelle Einflüsse determiniert sieht (Baldwin, 1988). Diese Annahme findet sich, zumeist zwar nur implizit, bei europäischen VertreterInnen der Rollentheorie, die Rollen als »reasons for action« verstehen (Harnisch, 2012b, S. 7). Die philosophische Frage, inwiefern zwischen Gründen frei entschieden werden kann, ob ein freier Wille im Wortsinn überhaupt wünschenswert sein kann bzw. ob es nicht ausreichend für einen substanziellen Freiheitsbegriff ist, von einem Prinzip alternativer Handlungsmöglichkeiten auszugehen, soll an dieser Stelle nicht weiter verfolgt werden (eine Einführung in diese Fragen bietet bspw. Schälike (2010)). Nach wie vor wird über das Spannungsfeld zwischen wissenschaftlichen Zielen im Sinne der Naturwissenschaften und der Analyse menschlichen Verhaltens debattiert: »For example, the debate over whether or not we can develop a science of human conduct and society can be linked to issues of free will, since science's goals of prediction and control are not appropriate if people have free will« (Baldwin, 1988, S. 153f.). Ob dieses Spannungsverhältnis besteht, hängt aber auch maßgeblich von der Definition von Erklärung ab. Während einige WissenschaftlerInnen die substanzielle Unterscheidung zwischen Erklären und Verstehen aufrecht erhalten und argumentieren, dass menschliches Verhalten nur von innen verstanden und nicht von außen (kausal) erklärt werden kann (Hollis und Smith, 1990), haben PragmatistInnen für ein »weiches« Verständnis von Erklärung plädiert, das keine abstrakten, naturgesetzähnlichen Regelmäßigkeiten postuliert und keine Ursachen angibt, die die Handelnden selbst nicht verstehen würden (McCourt, 2014, S. 49f.).

ist bereits deutlich, dass Struktur bzw. Strukturveränderungen Resultat menschlichen Handelns sind. Zwar handeln AkteurInnen unter Strukturbedingungen, die sie nicht frei gewählt haben und die sie mit unterschiedlich widerständigen Handlungskorridoren konfrontieren. Dennoch sind Struktur und deren Veränderungen aus dieser Perspektive Resultat menschlicher Interaktion und nicht unabhängig wirkende Ursachen für menschliches Verhalten. »Wäre dem nicht so, würde den Ideen der Handlungsfreiheit und der Verantwortung für das eigene Tun die Grundlage entzogen werden. Dann wäre alles Handeln ein von der Mode gelenktes bloßes Verhalten« (Roos, 2010, S. 74). Durch die Rückbindung von Rollen bzw. menschlichem Handeln an Struktur, wird deutlich, dass Strukturen keine aktive verursachende Wirkung zukommt. Strukturen sind Ergebnis menschlicher Handlungen – dies inkludiert sowohl deren intendierte als auch unintendierte Folgen – als solche beeinflussen sie in reflektierender Wechselwirkung wiederum AkteurInnen. Das ko-konstitutive Verhältnis wird dadurch nicht aufgelöst. Aktiv wirkt aber immer menschliche Handlung: »It is the social process in group life that creates and upholds the rules, not the rules that create and uphold group life« (Blumer, 1986 [1969], S. 19).

Mit Blick auf den kreativen Umgang mit Handlungsunsicherheit, ist ein emergentes Politikfeld wie die Cybersicherheitspolitik ein rollentheoretisch interessanter Untersuchungsgegenstand. Dies gilt insbesondere auch mit Blick auf andere sozialkonstruktvistische Theorien, die eine Logik der Angemessenheit vertreten, da in diesem neuen Feld noch keine Überzeugung besteht, welche Normen gelten und was angemessenes Verhalten darstellt. Es fehlt also die Bemessungsgrundlage, die Orientierung bieten könnte. Die Akteure können zwar auf tradierte Handlungsrepertoires zurückgreifen oder etablierte Akteure adressieren, inwiefern diese Referenzen von signifikanten Anderen akzeptiert werden, ist aber zunächst schwer antizipierbar. In der Cybersicherheitspolitik etablieren die Akteure durch Interaktion eine (für diesen Kontext) »neue« Sozialstruktur, die erst dann verlässlichere Handlungsorientierung im Sinne einer Routinesituation bieten kann, sobald sie eine gewisse »Dichte« erreicht hat. Staatliche Bestrebungen, bspw. Standards angemessenen Verhaltens (Normen) aus anderen Politikfeldern in Analogie auf das neue Handlungsfeld zu übertragen, sind Ausdruck des Bemühens, bestehende Handlungsunsicherheiten zu überwinden. Da der Cyberspace die Staaten aber zumindest teilweise vor neue Probleme stellt, ist die Anwendbarkeit vieler Analogien zwischen den Akteuren umstritten. Es dauerte fast 20 Jahre bis sich Staaten einig waren, dass die grundlegendste aller internationalen Handlungsregeln (die Charta der Vereinten Nationen) auf den Cyberspace übertragbar ist (UN, 2013, S. 8). Wobei es sogar bei der weiteren Explikation dieser basalen Regeln zu erheblichem Dissens bspw. mit Blick auf das Selbstverteidigungsrecht kam, sodass der Prozess zur Normbildung auf Ebene der Vereinten Nationen

zumindest vorerst erheblich ins Stocken geraten, wenn nicht gar gescheitert ist (Schmitt und Vihul, 2017; Segal, 2017; Soesanto und D'Incau, 2017).

Mit den Worten Wendts kann diese Situation als »first encounter« – ein erstes Aufeinandertreffen der Akteure in einem spezifischen Handlungskontext – bezeichnet werden (1999, S. 108). Auch wenn in einer, bereits vor der globalen Öffnung des Internets, weitgehend globalisierten Welt sicher nicht mehr von einem buchstäblichen ersten Aufeinandertreffen verschiedener Akteure gesprochen werden kann, so scheint das Bestandsrepertoire kontext-erprobter Handlungsroutinen doch so »dünn«, dass im pragmatistischen Sinn von einer »indeterminate situation« (Dewey, 1938, S. 105) auszugehen ist. Sicherheitspolitische Erwägungen und entsprechende Praktiken der Staaten mit Bezug zum Internet begannen erst Mitte bzw. Ende der 1990er Jahre. In dieser Zeit trafen die Akteure (sowohl Staaten als auch nichtstaatliche Akteure) erstmals in diesem Handlungskontext aufeinander.

Zwei Einflüsse können aus rollentheoretischer Perspektive dabei die Praktiken der Staaten prägen: Das historische Selbst (welche tradierten Handlungsmuster können und sollen auf den Cyberspace übertragen werden) sowie die Interaktion mit unterschiedlichen signifikanten Anderen (wer sind die Interaktionspartner).

Das historische Selbst bietet AkteurInnen einen Orientierungspunkt zur Gestaltung des eigenen Handelns unter Rückgriff auf die eigenen Erfahrungen, da es die Erfahrungen zurückliegender Interaktionen abbildet. Um zu entscheiden, wie eine Rolle konkret gestaltet werden soll, können AkteurInnen Bezug auf ihre positiven oder negativen historischen Erfahrungen nehmen, wobei diese unterschiedlich weit in der Vergangenheit liegen können. Mead diskutiert diese Möglichkeit der Selbstobjektivierung über den Erfahrungshorizont unter anderem mit dem Hinweis darauf, dass die Erfahrungsbestände nicht für alle Zeit fixiert sind, sondern dass es vielmehr möglich ist (insbesondere negative) Erfahrungen zurückzulassen. Die historischen Selbstbilder sind somit kein unverrückbarer Referenzpunkt, der sich AkteurInnen in ähnlichen Handlungssituationen stets aufzwingt, sondern wandelbare und überwindbare Orientierungsmarken, die angewendet werden können, aber nicht müssen. Die Referenz muss daher für jeden Handlungskontext und in jeder praktischen Situation erneut aktualisiert werden (Mead, 1979, S. 143, 171). Aus Perspektive der Außenpolitikforschung wurde in diesem Kontext bspw. argumentiert, dass die Rolle der Volksrepublik China wesentlich vom historischen Bezugspunkt (bspw. Opfer kolonialer Aggression) abhänge (Harnisch, 2016). Die Cybersicherheitspolitiken der beiden Untersuchungsstaaten sind daher möglicherweise beeinflusst von unterschiedlichen sicherheitspolitischen Vorerfahrungen bzw. Selbstbildern, die sowohl domestische als auch internationale Erfahrungen widerspiegeln. Der deutschen Außenpolitik wurde etwa attestiert dem Idealtypus der Zivilmacht besonders nahe zu kommen. Sie zeichnet sich demnach, aufgrund der expliziten Abgrenzung zum negativen

historischen Selbst – der NS-Diktatur – durch eine Präferenz für multilaterales Handeln, eine Bereitschaft zum Souveränitätstransfer und eine Akzeptanz umfassender Normen auch bei kurzfristig entgegenstehenden nationalen Interessen aus (Frenkler u. a., 1997; Harnisch und H. Maull, 2001; H. W. Maull, 2007, 1990/91). Die britische Außenpolitik ist dagegen durch einen weitreichenden Gestaltungsanspruch geprägt, der sich nicht zuletzt aus dem historischen Erbe des Commonwealth und der englischen Sprachfamilie ableitet. Besondere Bekanntheit erlangte die Vorstellung der britischen Einflusssphäre, die Winston Churchill in einer Rede 1948 vorstellte. In dieser identifizierte der Premierminister drei wesentliche Bezugspunkte für die britische Außenpolitik: das Commonwealth, die englischsprachige Welt sowie ein vereintes Europa.[15] Die britische Außenpolitik ist damit durch einen umfassenderen Gestaltungsanspruch geprägt. Obwohl auch Großbritannien in der jüngeren Vergangenheit außenpolitisch negative Erfahrungen gemacht hat (bspw. die Suezkrise 1956), gibt es kein starkes negatives Selbst, sondern eine besondere Betonung der besonderen Beziehungen zu den USA. Nicht zuletzt hierdurch sind auch die Mittel zur Zielerreichung robuster (Cornish, 2013; Gaskarth, 2014, 2016; Gilmore, 2015). Wenn in diesem Kontext im Folgenden von positiven oder negativen historischen Selbstbildern die Rede ist, bezieht sich diese wertende Einschätzung stets auf die Beurteilung durch die Exekutiven. Sie lassen keine feste Zuschreibung von Wirkrichtungen zu. So können negative historische Selbstbilder sowohl beschränkend als auch katalytisch auf die Beschützer-Rollen wirken. Ein Beispiel hierfür sind die negativen Selbstbilder des NS-Regimes in Deutschland oder als Terroropfer im Vereinigten Königreich. Beide werden von den Regierungen negativ beurteilt, es wird also versucht, eine ähnliche Erfahrung in der Zukunft zu vermeiden und die Politiken entsprechend zu gestalten. Im Falle Deutschlands wirkt dieses negative historische Selbst beschränkend auf die Beschützer-Rolle, da die Kompetenzen der Sicherheitsbehörden kritisch gesehen werden. In Großbritannien wirkt das negative Selbst katalytisch auf die Beschützer-Rolle, da erneute Terroranschläge vermieden werden sollen und die Sicherheitsbehörden weniger als Gefahr gesehen werden.

Es ist daher zu untersuchen, inwiefern historische Selbstbezüge in der Cybersicherheitspolitik auftauchen und ob sie akzeptiert oder verworfen werden. Da mit dem Cyberspace ein neuer Handlungsraum entstanden ist, ist es durchaus möglich, dass tradierte Handlungsweisen infrage gestellt und historische Verweise abgelehnt oder erst gar nicht aufgeworfen werden.

Referenzen zu unterschiedlichen signifikanten Anderen können ferner die Cybersicherheitspolitiken der Untersuchungsstaaten beeinflussen. Wie bereits expliziert sind signifikante Andere der zentrale Bezugspunkt von Rollen. Durch die Übernahme komplementärer Gegenrollen entscheiden sie über die resultierende

15 Zitiert nach Avi Shlaim (1975).

Sozialstruktur. Mead unterscheidet zwischen signifikanten Anderen, also besonders relevanten EinzelakteurInnen, organisierten Anderen (bspw. internationale Organisationen) und einem generalisierten Anderen (bspw. die internationale Staatengemeinschaft) (Mead, 1979, S. 152-163, 265). Da Rollen sowohl von Eigen- als auch Fremderwartungen geprägt sind, können sie auf unterschiedliche signifikante Andere referenzieren und aufgrund divergierender sozialer Anschlussfähigkeit auch zu unterschiedlichen Praktiken führen. Eine besonders umfassende Interpretation der Beschützer-Rolle kann bspw. in einer sozialen Gruppe A akzeptiert werden, während die gleiche Rolle für eine andere Gruppe B nicht akzeptabel wäre. RollentheoretikerInnen haben in diesem Kontext unterschiedliche kausale und konstitutive Mechanismen identifiziert, wie AkteurInnen in Interaktion Rollen verändern: bspw. Lernen, Imitation, Emulation, Sozialisation, Altercasting oder Rollenkonflikte (Harnisch, 2012a,b; Jönsson, 1984; Malici, 2006; Turner, 1990).

Ein weiterer Mechanismus der Rollenwandel ermöglicht und erst in den letzten Jahren in den Fokus der wissenschaftlichen Betrachtung gerückt ist, sind domestische Prozesse der Rollenkontestation (*role contestation*) (Cantir und Kaarbo, 2012, 2016a).[16] RollentheoretikerInnen haben in diesem Kontext die lange Zeit

16 Dieser neue Ansatz führt aber auch dazu, dass etablierte Konzepte, wie Rollenkonflikte problematischer werden. Der theoretische Umgang mit Rollenkonflikten variiert in verschiedenen Studien deutlich. Das hat zur Folge, dass die Grenzlinien zwischen verschiedenen Konzepten mitunter verschwimmen (Harnisch, 2018). Ferner wurde mit der Rollenkontestation ein Analysekonzept eingeführt, das explizit auf die domestischen Prozesse in Staaten ausgerichtet ist und teilweise sehr nahe an Rollenkonflikte heranreicht. In beiden Fällen werden Rollen problematisch, da sie mit Widerständen konfrontiert werden. TheoretikerInnen, die sich mit Rollenkonflikten befasst haben, argumentieren dabei zumeist unter der Annahme unitarischer Akteure, die sich entweder mit gegenläufigen Fremderwartungen konfrontiert sehen oder die versuchen verschiedene Rollen (oder Rollenelemente – intra-role conflict) zu übernehmen, die zumindest in Teilen inkompatibel sind. Das Konzept der Rollenkontestation gibt die Annahme unitarischer staatlicher Akteure auf und geht davon aus, dass Rollen innerstaatlich in verschiedenen Konstellationen umstritten sein können (Cantir und Kaarbo, 2016b, S. 5f.). Vergleicht man die beiden Konzepte aus dieser Perspektive, so scheint es einen konzeptionellen Unterschied zwischen Rollenkonflikt und Rollenkontestation zu geben. Sie ergibt sich daraus, dass die Rollen durch externe Andere oder durch domestische Akteure herausgefordert werden. Da Rollen keine Handlungsträgerschaft zukommt, ist stets ein Akteur erforderlich, der einen solchen Konflikt sozial aktualisiert. In dem Zuge, in dem man die Annahme unitarischer staatlicher AkteurInnen aufgibt und die domestische Ebene erschließt, ist auch immer ein Handelnder benennbar (das gilt auch für intra-Rollenkonflikte). Damit fällt auch die Annahme, dass es einheitlichen Akteuren gewahr wird, dass ein Rollenkonflikt vorliegt. Mit anderen Worten die Wurzeln der Rollentheorie und die Anthropomorphisierung des Staates öffnet hier eine Lücke. Dies wird spätestens dann klar, wenn man versucht, im gedanklichen Umkehrschluss, das für Staaten entwickelte Konzept der Rollenkontestation auf ein menschliches Individuum zu übertragen. Ohne eine dissoziative Persönlichkeitsstörung zu unterstellen, scheint das undenkbar. Diese konzeptionelle Nähe führt un-

als Black-Box behandelte domestische Sphäre geöffnet und die Annahme aufgegeben, Staaten seien unitarische Akteure, in denen Rollen unwidersprochen geteilt würden. Die vorliegende Studie greift die bisherigen Ansätze zur domestischen Herausforderung von Rollen auf und entwickelt diese weiter, um auf diesem Weg eine rollentheoretische Möglichkeit zur Analyse der Interaktion zwischen Innen- und Außenpolitik zu entwerfen, die ferner auch nichtstaatliche Akteure integriert.

Dies ist nicht nur im Sinne einer Theorieentwicklung wünschenswert, sondern darüber hinaus im Bereich der Cybersicherheitspolitik auch empirisch geboten. Denn erstens hat kaum ein Phänomen die Trennung zwischen Innen- und Außenpolitik derart herausgefordert wie das Internet, das durch seine globale Infrastruktur neue Kommunikations- und Handlungsräume schafft. Aus sicherheitspolitischer Warte ermöglicht das Netz Angriffe über Staatengrenzen hinweg, wodurch geografische Entfernungen ihre Relevanz verlieren (Cairncross, 2001). Die physische Erreichbarkeit eines Zieles ist damit nicht mehr ausschlaggebend. Stattdessen geht es um die potenzielle Verwundbarkeit aufgrund verwendeter Systeme. Ferner ist die Verfolgung der AngreiferInnen im Internet besonders schwierig, da eine zweifelsfreie Attribution durch technische Beweise aufgrund der globalen Architektur und deren gezielten (Aus)Nutzung durch AngreiferInnen erschwert wird. AngreiferInnen können so auch aus dem Innern agieren, für ihre Angriffe aber externe Infrastrukturen nutzen und so den Eindruck eines Angriffes von außen erwecken. Zweitens stellt das Internet die Handlungsfähigkeit der Nationalstaaten grundlegend infrage. Da zentrale Infrastrukturen des Netzes nicht in staatlicher Hand sind, fordert der neue Handlungsraum die Akteure nicht nur entlang der Trennlinie innen-außen heraus, sondern erfordert zudem die Beachtung nichtstaatlicher Akteure, die gesellschaftlich besonders relevante – IT-Versorgung ermöglichende oder IT-abhängige – Infrastrukturen betreiben (bspw. Internetknoten oder die Energieversorgung). Gefahren aus dem Cyberspace stellen Unternehmen dabei vor besondere Herausforderungen. Denn einerseits fehlen häufig wirtschaftliche Anreize, ein hohes Maß an Sicherheit zu gewährleisten. Andererseits ist die Gefahrenlage im Cyberspace teilweise brisanter. Solange es primär um die Gewährleistung physischer Integrität industrieller Anlagen ging, konnten Unternehmen durch eigene – oder teilweise auch durch staatlich vorgeschriebene – Maßnahmen (Werksschutz, etc.) die Risiken soweit reduzieren, dass dies auch aus staatlicher Perspektive akzeptabel war. Im Cyberspace hingegen kann es vorkommen, dass Betreiber kritischer Infrastrukturen mit Angriffen staatlicher Akteure konfrontiert werden, die potenziell einen ungleich größeren Aufwand für Angriffe auf sich nehmen können. In Analogie illustriert bedeutet

---

ter anderem dazu, dass die Trennlinie zwischen Rollenkonflikt und -kontestation in Studien leicht verwischt (Cantir und Kaarbo, 2012; Pelletier und Massie, 2017).

das konkret: Wenn staatliche AngreiferInnen physisch vor den Toren eines Atomkraftwerkes stehen, hat der Staat bereits bei der Wahrung territorialer Integrität versagt. Aufgrund der Globalität des Internets ist diese direkte Konfrontation auch ohne das Aushebeln einer vorgelagerten staatlichen Schutzinstanz (der territorialen Grenze) möglich. Ob und wie dieser neue entgrenzte Handlungsraum genutzt wird, hängt dabei von der interaktiven Bedeutungszuweisung, also den Rollen, ab. Durch sie kann auch die territoriale Ordnung im Cyberspace reifiziert werden, das kann der Fall sein, wenn bspw. tradierte Vorstellungen nationaler Souveränität auf das Netz übertragen werden.

## 2.3 Rollentheorie zwischen Innen- und Außenpolitik: Ein rollentheoretisches Zwei-Ebenen-Spiel

Die Trennung zwischen Innen- und Außenpolitik ist nicht erst durch die aufkommende Verbreitung digitaler Massenkommunikation herausgefordert worden. Auch Phänomene wie der Klimawandel oder die grenzübergreifende Verbreitung von Krankheiten haben die analytische Trennung problematischer werden lassen. Die vergleichende Außenpolitikforschung ist daher immer stärker dazu übergegangen, interne und externe Faktoren mehr und mehr zusammenzudenken (s. bspw. Beasley, 2013). Das Verhältnis von Innen- und Außenpolitik wurde aber auch schon zuvor aus verschiedenen theoretischen Perspektiven analysiert (Schultz, 2013).

Aus neorealistischer Perspektive wurde die Bedeutung der Innenpolitik zumeist entweder negiert, marginalisiert oder, sofern anerkannt, deren Einfluss negativ bewertet. Ein Argument, das von RealistInnen in diesem Kontext angeführt wird, beruht auf der Annahme, dass die Exekutive mit dem nationalen (Sicherheits)Interesse ein Gut verfolgt, das die Interessen aller domestischen Akteure transzendiert und über das die Regierung, aufgrund ihres privilegierten Informationszugangs, relativ exklusiv verfügt. Die Erfordernisse einer potenziell stets feindseligen anarchischen Umwelt offenbaren sich aus dieser Perspektive unmittelbar nur der Regierung. Nach einer Phase der Ausklammerung innenpolitischer Einflüsse, hat die realistische Denkschule mit aufkommendem neoklassischen Realismus domestische Faktoren zwar als intervenierende Variablen aufgenommen, die die langfristigen Wirkungen des internationalen Systems, zumindest kurzfristig, beeinflussen können (Rose, 1998; Taliaferro, Lobell und Ripsman, 2009):[17]

17 Diese konzeptionelle Öffnung ist es auch, die Valerie Hudson (2014, S. 206) zur Feststellung kommen lässt: »neoclassical realists are doing foreign policy analysis.«

> »When states do not respond ideally to their structural situations, neorealism tells us we should find evidence of domestic politics and ideas distorting the decision-making process.« (Rathbun, 2008, S. 296)

Der Sprachgebrauch (distort) weist aber bereits darauf hin, dass innenpolitische Einflüsse, die die Exekutive bei der Umsetzung der Außenpolitik »behindern«, aus dieser Perspektive letztlich negativ bewertet werden. Im (realistischen) Idealfall wirkt der internationale Anarchiedruck nach innen so integrierend, dass die Exekutive bei der Verfolgung der außenpolitischen Agenda nicht nur nicht gestört, sondern in ihrem Kurs durch die domestischen Akteure zusätzlich gestärkt wird. Ist dies nicht der Fall und kommt es zu einer Situation in der innerstaatliche Faktoren die Außenpolitik stören, so ist es wahrscheinlich, dass der Staat auch im Außenverhältnis geschwächt wird, da ihm bspw. die Möglichkeiten fehlen, notwendige Ressourcen zur Realisierung der notwendigen Außenpolitik zu extrahieren. Folglich ist der Staat nicht in der Lage, auf systemische Anforderungen adäquat zu reagieren. Die von allen Staaten verfolgten Ziele »power and wealth« können dann nicht mehr optimal erreicht werden (Mastanduno, Lake und Ikenberry, 1989, S. 462). Da domestische Einflüsse der »richtigen« Politik entgegenstehen können und da nur die Exekutiven im Stande sind diese »richtige« Politik zu erkennen, können die Regierungen die öffentliche Meinung entweder ignorieren oder versuchen, sie durch gezielte Manipulation für eigene Zwecke nutzbar zu machen. Dementsprechend wird die domestische Sphäre von neorealistisch argumentierenden WissenschaftlerInnen auch als nahezu wehrloser Spielball der Exekutiven gesehen: »Public opinion on national security issues is notoriously fickle and responsive to elite manipulation and world events« (Mearsheimer, 1990, S. 41).

Aus realistischer Perspektive sind damit die innerstaatlichen Institutionen ebenso wie gesellschaftliche Gruppen keine Rollenträger auf Augenhöhe. Die wirklich bedeutsame Referenz der Regierung liegt außerhalb des Staates. Kurz gesagt führen die Erfordernisse des internationalen Systems, mit denen die Exekutive exklusiv vertraut ist, aus realistischer Perspektive dazu, dass Regierungen das außenpolitische Rollenspiel im Innern unilateral dominieren (Harnisch, 2014, S. 5f.). Schafft die Exekutive es nicht, die domestische Sphäre zu kontrollieren, bleibt der Staat hinter seiner eigentlichen außenpolitischen Leistungsfähigkeit zurück bzw. zeigt nicht das Verhalten, das der Realismus erwarten würde (Schultz, 2013, S. 480).

Aus Sicht des Liberalismus verläuft das Verhältnis von Innen- und Außenpolitik analytisch in genau entgegengesetzter Richtung. Das bedeutet, der Bezugspunkt, an dem sich Außenpoltik ausrichtet, liegt hier im Innern, nicht im anarchischen internationalen System (Harnisch, 2014, S. 7). Aus liberaler Perspektive ist Außenpolitik im Gegensatz zum Realismus ein Prozess der »bottom-up« ver-

läuft und der durch einen institutionell-prozessualen »transmission-belt« dafür sorgt, dass die Regierung gesellschaftliche Interessen auch nach außen vertritt (Moravcsik, 1997, S. 517f.). Liberale Argumente betonen dementsprechend, dass unterschiedliche innerstaatliche Akteure verschiedene Interessen vertreten und dass sich diese dann auf die Außenpolitik übertragen. Die Exekutive ist in dieser Perspektive nicht losgelöst von der Gesellschaft und privilegiert, sondern mit der Gesellschaft verschränkt. Die in einer Gesellschaft vorhandenen Präferenzen werden auf die Regierung übertragen, die diesen dann auch in der Außenpolitik Ausdruck verleiht. Für den Prozess der Präferenzübertragung bietet Andrew Moravcsik drei verschiedene Modi an: einen kommerziellen, einen ideellen sowie einen republikanischen Liberalismus (ebd.). Abgesehen von der Aussage, dass diese drei Mechanismen im Zusammenspiel besser funktionieren als separiert, bleibt aber offen, wie sie miteinander in Beziehung stehen oder wann welcher besonders einflussreich ist. Durch die gesellschaftliche Rückbindung der Exekutive wird die Regierung zu einem Akteur unter mehreren und verliert die Vormachtstellung gegenüber anderen domestischen Akteuren. Dies resultiert aber nicht, wie von RealistInnen befürchtet, in einer »schlechten« Außenpolitik. Im Gegensatz zum Realismus besteht in dieser Denkschule eine tiefe Skepsis gegenüber der realistischen Annahme, dass Regierungen unbeeinflusst und ohne Beschränkungen die beste Außenpolitik für das Gemeinwesen verfolgen würden. »Gute« Außenpolitik wird aus dieser Perspektive erst wahrscheinlich, wenn die innerstaatlichen Interessen aufgenommen und Regierungshandeln Kontrolle unterworfen wird. Dieser Gedanke findet sich bereits in Kants Schrift Zum ewigen Frieden; in der er mit Blick auf die Erklärung von Kriegen für eine republikanische Verfassung plädiert:

> »Wenn [...] die Beistimmung der Staatsbürger dazu erfordert wird, um zu beschließen, ›ob Krieg sein solle, oder nicht‹, so ist nichts natürlicher, als daß, da sie alle Drangsale des Krieges über sich selbst beschließen müßten [...], sie sich sehr bedenken werden, ein so schlimmes Spiel anzufangen: Da hingegen in einer Verfassung, wo der Untertan nicht Staatsbürger, die also nicht republikanisch ist, es die unbedenklichste Sache von der Welt ist, weil das Oberhaupt nicht Staatsgenosse, sondern Staatseigentümer ist, [...] diesen also wie eine Art von Lustpartie aus unbedeutenden Ursachen beschließen [...] kann.« (Kant, 1965 [1795], S. 113)

In der liberalen Theoriefamilie ist in diesem Kontext bspw. empirisch nachgewiesen worden, dass Demokratien signifikant häufiger gewaltsame Konflikte für sich entscheiden können als Autokratien. Dieser Befund wurde unter anderem mit Verweis auf die gesellschaftliche Kontrolle der Exekutive erklärt, die diese davon abhalte eigene Ziele zu verfolgen und mit Kriegen Rentengewinne für sich zu erzielen (Bueno de Mesquita u. a., 1999; Lake, 1992). Wenden sich liberale TheoretikerInnen explizit dem Zusammenspiel von Innen- und Außenpolitik zu,

so stehen dabei die Kompatibilität bzw. Komplementarität der auf die Regierung übertragenen Interessen im Mittelpunkt des Forschungsinteresses (bspw. in Moravcsiks liberalem Intergouvernementalismus (1993)). Zur Analyse der Verschränkung von domestischer und internationaler Ebene, ist aus liberaler Perspektive ferner das Two-Level Game (TLG) von Robert Putnam besonders einflussreich geworden (Putnam, 1988). Putnam nimmt an, dass Regierungen an zwei Verhandlungstischen sitzen – einem domestischen und einem internationalen – und dort ihre Interessen vertreten. In beiden Verhandlungskontexten bestehen dabei unterschiedliche Präferenzen und damit Winsets. In dieser Konstellation ist es den Exekutiven prinzipiell möglich die beiden Tische strategisch gegeneinander auszuspielen, um die präferierten Resultate zu erzielen. Regierungen können bspw. an einem Verhandlungstisch behaupten, eine vorgeschlagene Lösung sei am anderen nicht durchsetzbar, um so weitere Konzessionen zu erreichen (ebd., S. 434, 453).

Während der Realismus die Dominanz der Exekutive beim Verfolgen der Außenpolitik hervorhebt, rekurrieren liberal argumentierende WissenschaftlerInnen also auf die domestische Rückbindung der Regierung und die Übertragung innerstaatlicher Interessen auf Regierungshandeln. Dieser umgekehrte Fokus führt aber dazu, dass liberale Studien (Rück)Wirkungen der internationalen Ebene auf die innerstaatlichen Institutionen und Prozesse aus dem Blick verlieren und damit Phänomene, die meist als »second image reversed« (Gourevitch, 1978) bezeichnet werden, nicht abbilden (Harnisch, 2014, S. 9).

SozialkonstruktivistInnen haben dagegen zum Verständnis ähnlichen staatlichen Verhaltens auf geteilte ideelle Faktoren (bspw. Kulturen) verwiesen (Finnemore, 1996). Wie im Realismus, lag auch hier der Fokus zunächst oft auf der internationalen Ebene. Positivistisch formuliert, wurden internationale Normen zunächst als unabhängige Variablen verstanden, die staatliches Verhalten (im Idealfall normkonformes Verhalten / Compliance) erklären, bzw. es wurde untersucht, welche Einflüsse Staaten zu normkonformem Verhalten veranlassen können. Empirische Untersuchungen konnten hier bspw. zeigen, wie die Verbreitung internationaler Menschenrechtsnormen innerstaatliche Anpassungen in unterschiedlichen Ländern zur Folge hatten (Finnemore, 1993; Risse, Ropp und Sikkink, 1999). Aus dieser Perspektive werden die nationalstaatlichen Exekutiven zur Einhaltung einer Norm erzogen: »This process by which international norms are internalized and implemented domestically can be understood as a process of *socialization* [Hervorhebung im Original; Anm. d. Verf.]« (Risse, 1999, S. 5). Regierungen bleibt dabei »nur« die Rolle eines Sozialisanden, der in unterschiedlichen Phasen durch internationale Organisationen, andere Staaten und transnationale NGOs zu normkonformem Verhalten angeleitet wird. Wobei auch ein Scheitern des Prozesses theoretisch möglich bleibt, jedoch zumeist ein Fokus auf erfolgreiche Verläufe vorherrschte. Die Tendenz, nicht länger von relativ stabilen ideellen

Strukturen auszugehen und daraus staatliches Verhalten abzuleiten, ist erst seit kurzem Teil der sozialkonstruktivistischen Forschungsagenda. Zu diesem neuen Feld, das explizit auch die domestischen Ursachen abweichenden Verhaltens analysiert, gehören bspw. Untersuchungen zur Kontestation von Normen (Bloomfield, 2016; McKune und Shazeda, 2018; Wiener, 2008).

Wie bereits erwähnt, wurde zur Analyse von Cybersicherheitspolitiken aus sozialkonstruktivistischer Perspektive zumeist auf die Sekuritisierungstheorie der Kopenhagener Schule zurückgegriffen. Auch sie geht nicht von stabilen Strukturen aus, sondern zeichnet nach, wie ein Problem durch einen Sprechakt, der von einem Referenzpublikum affirmiert wird, zu einem Sicherheitsproblem gemacht wird. Neben den bereits im Einleitungskapitel skizzierten Defiziten, ist auch der Umgang mit dem Verhältnis von Innen- und Außenpolitik bzw. die Annahme zum Referenzpublikum problematisch. Der Einsatz von »extraordinary measures« wird erst möglich, wenn das Publikum die soziale Konstruktion bestätigt (Buzan, Waever und Wilde, 1998, S. 25). Ob das Publikum aber über substanzielle Handlungsträgerschaft verfügt oder ob es auch durch den Sekuritisierenden manipuliert werden kann, ist nicht klar definiert. Eine gehaltvolle intersubjektive Bestätigung bleibt daher aus. Auch wenn empirische Studien versucht haben, dieses Problem zu mildern und die Handlungsträgerschaft des Publikums zu erhalten (Côté, 2016; Floyd, 2015; Léonard und Kaunert, 2011), bleibt doch der Verdacht, dass das Publikum, ähnlich wie im Realismus, durch die Regierung manipuliert oder kooptiert werden kann (Harnisch, 2014, S. 10). Ferner kann die Sekuritisierungstheorie nur nachzeichnen, wie ein Problem zum Sicherheitsproblem wurde. Warum der entsprechende Prozess so verlaufen ist, kann sie nicht darlegen. Sozialkonstruktivistischen Ansätzen allgemein ist daher von PragmatistInnen vorgehalten worden, dass sie nicht über einen Mechanismus verfügen, der Wandel politischer Kulturen bzw. die Entstehung geteilter Lebenswelten erfassen könne und dass der Pragmatismus bzw. die symbolisch interaktionistische Rollentheorie diese Blindstelle durch die bereits skizzierte Logik der Interaktion und die daraus folgende Emergenz sozialer Realität schließen kann (M.-O. Baumann, 2014; Harnisch, 2014; McCourt, 2014).

RollentheoretikerInnen haben in den letzten Jahren damit begonnen, auch innenpolitische Prozesse zu erfassen und damit domestische Einflüsse rollentheoretisch nachvollziehbar zu machen (Brummer und C. G. Thies, 2015; Cantir und Kaarbo, 2016a; Harnisch, 2020; Jones, 2017; Kaarbo, 2015; Keane und Wood, 2016; Oppermann, 2012; Wehner und C. G. Thies, 2014). Besonders einflussreich wurde dabei das von Cantir und Kaarbo entwickelte Konzept der Rollenkontestation (*role contestation*) (Cantir und Kaarbo, 2012, 2016b). Konzeptioneller Ausgangspunkt ist die Annahme, dass Rollen nicht, wie zuvor angenommen, unumstritten und homogen sind, sondern, dass diese von innenpolitischen Akteuren herausgefordert und letztlich auch verändert werden können. Cantir und Kaarbo gehen davon

aus, dass diese Prozesse der Rollenanfechtung sowohl innerhalb politischer Eliten (horizontal) oder auch zwischen Eliten und Öffentlichkeit(en) (vertikal) verlaufen können (Cantir und Kaarbo, 2012, S. 11-12). Diese Bestrebungen innenpolitische Prozesse für rollentheoretische Analysen zugänglich zu machen, werden in dieser Untersuchung weitergeführt.

Um die Rollengenese auch innenpolitisch zu analysieren, geht die Untersuchung davon aus, dass es nicht nur ein Rollenspiel auf internationaler Ebene gibt, sondern dass gleichsam ein innenpolitisches Pendant besteht, in dem die domestischen signifikanten Anderen die sozialen Funktionsübernahmen der Regierung durch komplementäre Rollenübernahme akzeptieren müssen. Die Studie folgt damit zumindest der Putnamschen Metaphorik eines Zwei-Ebenen-Spiels. Während Putnam aber auf rationale Zielerreichung und die präferierten Ergebnisse in einem Winset (bzw. zwei Winsets) aufbaut, geht es bei einer rollentheoretischen Analyse um in Interaktion bestätigte soziale Anschlussfähigkeit – also die komplementäre Gegenrollenübernahme durch signifikante Andere im Inneren wie Äußeren. Entscheidend ist die soziale Realisation in der Interaktion. Ferner ist Putnams TLG auf Situationen der Vertragsratifikation zugeschnitten, in der zwei klare Winsets zwischen unterschiedlichen Akteuren identifiziert werden können und der Vertragstext als quasi finales Moment die Fixiernadel zwischen die beiden Punkte setzt. Ein rollentheoretisches TLG kann für ein sehr viel weiteres, weniger formal gebundenes und fluideres Spektrum unterschiedlicher sowohl kooperativer als auch konfliktiver Interaktionen angewendet werden. Außerdem beschränkt es die Perspektive nicht auf relativ isoliert betrachtete Aushandlungsprozesse, sondern ermöglicht die dichte (sowohl kontextuelle als auch historische) Beschreibung von Interaktionspraxis in beiden Interaktionssphären.

Diese Untersuchung greift die Überlegungen zu domestischen Einflüssen auf das Verhalten von Staaten auf und argumentiert, dass, denkt man die Implikationen innenpolitischer Auseinandersetzungen um Rollen konsequent zu Ende, auch auf domestischer Ebene ein ergänzendes Rollenspiel ähnlich dem internationalen stattfindet. So wird die Rollentheorie systematisch für Rückwirkungseffekte (second image reversed (Gourevitch, 1978)) internationaler Sozialstruktur auf binnenstaatliche Sozialstruktur geöffnet und das Verhältnis von Innen- und Außenpolitik besser verständlich. Damit kann das internationale Rollenspiel bspw. auch das Kontestationsverhalten im Innern beeinflussen. Das bedeutet aber nicht, dass einem der beiden Rollenspiele ex ante ontologische Priorität eingeräumt wird. Theoretisch sind Wirkungen in beide Richtungen möglich. Die beiden Rollenspiele beeinflussen sich wechselseitig:

> »The model suggests that the two role-taking processes are interactive: international role taking and making feeds back into domestic role taking (second

*Abbildung 1: Das rollentheoretische Zwei-Ebenen-Spiel, Quelle: Eigene Darstellung*

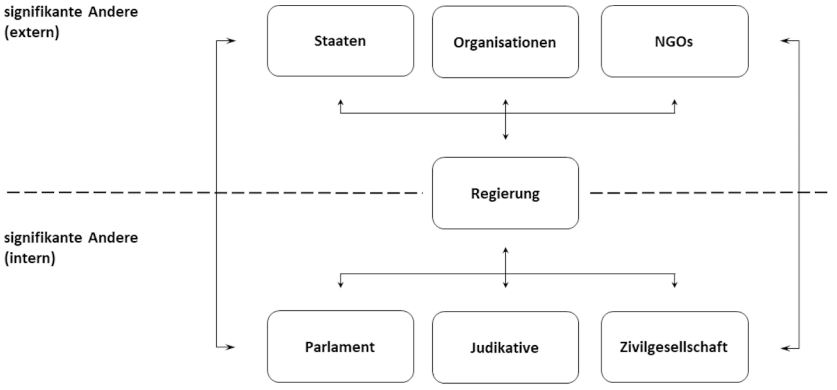



image reversed) and domestic role taking enables and/or restrains external role taking.« (Harnisch, 2014, S. 2)

Das rollentheoretische Zwei-Ebenen-Spiel ist in Abbildung 1 schematisch dargestellt.

Regierungen übernehmen für das Gemeinwesen bestimmte Funktionen und um diese Rollen auszufüllen, bedarf es der komplementären Einnahme der Gegenrollen durch die domestischen signifikanten Anderen.[18] Beim Menschen sieht Mead den notwendigerweise im Verborgenen ablaufenden Austauschprozess zwischen I und Me. Für staatliche Akteure lässt sich dieser Prozess mit einem innenpolitischen rollentheoretischen TLG abbilden. Es wird aber darauf verzichtet, die für den virtuellen Kreislauf verwendete Begrifflichkeit von I und Me auf die innerstaatliche Sphäre zu übertragen. Denn dieser Analogieschluss wirft einige substanzielle Fragen auf: Warum sollte bspw. die Regierung als kreatives I bezeichnet werden, wenn doch auch hier, gerade in den angeschlossenen Ministerien beständig die Positionen anderer Akteure mitgedacht werden oder warum sollte das Parlament das sozialverortete Me widerspiegeln, wo doch hier Regierungspläne kurzfristig durch wenige Parlamentsmitglieder zum Stillstand gebracht werden können. Welchen Part sollten organisierte Gesellschaftliche Akteure spielen? Im Sinne Meads müssten vielmehr alle Akteure über ein I und Me verfügen, so-

18 Da die kollektiven Rollenträger als Strukturen kollektiven Handelns verstanden werden, bleiben »horizontale« Kontestationsprozesse (also Binnendynamiken) im Sinne Cantirs und Kaarbos (2012) natürlich abbildbar.

dass der Analogieschluss letztlich die genuinen Besonderheiten individueller und kollektiver Ebene verwischen würde.[19]

Eine Frage, die es dennoch zu erläutern gilt, ist, ob sich die domestische und die internationale Ebene unterscheiden? Bei einer ersten Betrachtung des Gegenstandes liegt es nahe, davon auszugehen, dass Erwartungssicherheit und klarere Sozialstrukturen im Innern aus rollentheoretischer Perspektive ein zentrales Unterscheidungsmerkmal beider Sphären sein könnten. Prinzipiell wäre das eine Anknüpfung an das klassische Distinktionsmerkmal zwischen innen- und außenpolitischer Sphäre: das Vorhandensein einer zentralen Sanktionsgewalt oder mit anderen Worten die Unterscheidung zwischen Hierarchie im Domestischen und Anarchie im Internationalen (Axelrod und Keohane, 1985). Diese Unterscheidung (bzw. eine Differenzierung anhand verschiedener Grade von Erwartungssicherheit) scheint auch Holsti nahezulegen, wenn er schreibt:

> »Generally, the expectations of other governments, legal norms expressed through custom, general usage, or treaties, and available sanctions to enforce these, are ill-defined, flexible, or weak compared to those that exist in an integrated society and particularly within formal organizations.« (Holsti, 1970, S. 243)

Dies kann aber nicht ex ante bestimmt werden, da sich die innerstaatlichen Zustände deutlich unterscheiden können. Die Differenzierung ist damit notwendigerweise eine empirische. In etablierten Demokratien (wie den beiden Untersuchungsstaaten) scheint dies eine plausible Annahme zu sein. Betrachtet man aber »failed states«, wird schnell deutlich, dass im internationalen System mehr Erwartungssicherheit bestehen kann als innerhalb einiger Staaten. »Failed states« sind ja gerade deshalb international keine Akteure im substanziellen Sinn, weil sie bspw. keine Ressourcen extrahieren und für eine Politik Gefolgschaft organisieren können, d.h. weil es keine stabilen domestischen Rollen und/oder RollenträgerInnen gibt (vgl. bspw. Bochmann, 2018; Ghani und Lockhart, 2008; T. Howard, 2016). Ferner sind auch in den internationalen Beziehungen die Strukturen nicht nur durch Anarchie geprägt. Unterschiedlich dichte Sozialstrukturen ergeben sich für die Akteure bspw. durch Einbindung in verschiedene internationale Organisationen oder Regime. Wendt geht bspw. von der NATO als einem Verbund aus, der sich durch freundschaftliche Beziehungen und damit ein erhöhtes Maß von Erwartungssicherheit auszeichnet und der damit mit innerstaatlichen Strukturen vergleichbar sei (Wendt, 1999, S. 205). Die sozialen Positionen im Innern können zwar durch längere Erfahrungshorizonte unmittelbarer Interaktion sowie ggf. formell kodifizierte Arrangements (bspw. durch eine

19 Letztlich endete eine weitere, konsequente I und Me Fortführung in letzter Instanz notwendigerweise wieder bei den Individuen.

Verfassung) geprägt sein, eine Alleinstellung gegenüber der internationalen Ebene lässt sich aber nicht konstatieren. Außerdem kann in jungen Staaten eine derartige Routine in der Interaktionspraxis nicht bereits theoretisch unterstellt werden. In den beiden untersuchten Demokratien ist es zwar plausibel, davon auszugehen, dass die zentralen Institutionen, also das Parlament, die Judikative und organisierte nichtstaatliche Interessen (bspw. Unternehmen), signifikante Andere sind, deren komplementäre Gegenrollenübernahme für eine stabile Politik bedeutsam ist. Das ist aber keine ex ante bestimmbare Konstante. Bereits in defekten Demokratien oder in Autokratien sind die signifikanten Anderen höchstwahrscheinlich andere Akteure, bspw. Parteiorgane, Herrscherdynastien oder das Militär. Aus diesen Gründen kann auch nicht ohne empirische Analyse bestimmt werden, unter welchen Umständen Regierungen bspw. signifikante Andere im Innern ignorieren können. In den beiden Untersuchungsstaaten ist es den Regierungen aufgrund der sozialen Ordnung nicht möglich, das Parlament oder die Gerichtsbarkeit mittel- oder langfristig unbeachtet zu lassen. Bei kurzfristigen Entscheidungen ist dies dagegen ggf. möglich. Wie die Dynamik zwischen den domestischen Rollenträgern gestaltet ist, ist damit genauso Teil der empirischen Untersuchung der Cybersicherheitspolitiken.

Es stellt sich ferner die Frage, welche zentralen Funktionen die Regierung bei der Regulierung und Gewährleistung von Cybersicherheit übernimmt. Auch diese Frage ist letztlich eine empirische. Die Rollen wurden, im Sinne eines durch die Grounded Theory (Strauss und Corbin, 1996) angeleiteten Vorgehens, in den staatlichen Dokumenten identifiziert (s. Kapitel 3.2). Die domestischen Rollen: Beschützer, Wohlstandsmaximierer und Garant liberaler Grundrechte legen daher, auch wenn sie an moderne Staatskonzepte erinnern (Kink und Ziegler, 2013; Leibfried und Zürn, 2006; Thiele, 2012), keine teleologische oder strukturalistische Lesart der Rollentheorie nahe, sondern sind empirische Phänomene in den beiden Untersuchungsstaaten. Eine strukturalistische Perspektive, wie sie prominent von Talcott Parsons vertreten wird, geht im Unterschied dazu davon aus, dass es bestimmte Rollen gibt, die systemisch bedingt ausgefüllt werden müssen, die daher auf Systemerhalt ausgerichtet sind und die schon vor den handelnden AkteurInnen existieren (substantialistische Position) (Parsons, 1991). Die drei generischen Rollen entsprechen dieser strukturalistischen Konzeption nicht. Sie sind nicht bereits da und müssen nur noch übernommen werden, sondern auch sie müssen kreativ entworfen und in sozialer Interaktion bestätigt werden. Sie müssen auch nicht zwangsläufig auf den Erhalt bestehender Ordnung ausgerichtet sein. Regierungen können durchaus die Schutzfunktion und damit die Beschützer-Rolle aufgeben (bswp. auch selektiv für bestimmte Bevölkerungsteile) und so nicht mehr systemerhaltend agieren. Eine Entwicklung hin zu einem »failed state« bleibt so theoretisch immer möglich. In einem neuen Politikfeld wie der Cybersicherheitspolitik sind zunächst auch domestisch die Rollen noch

nicht verteilt, sodass die Wechselwirkung der beiden Handlungsräume besonders aufschlussreich sein kann.

Auch wenn im Rahmen dieser Analyse die Beschützer-Rolle im Mittelpunkt des Interesses steht, können die beiden anderen Rollen nicht ignoriert werden, da es in wechselnden Interaktionszusammenhängen zu unterschiedlichen Wechselwirkungen zwischen ihnen kommt. Abhängig vom Kontext kann es zu Situationen kommen, in denen die verschiedenen Rollen einmal katalytisch oder beschränkend aufeinander wirken. Die Beschützerrolle kann bspw. mit Verweis auf die Rolle des Wohlstandsmaximierers angefochten werden, wenn es etwa um die Schwächung von Verschlüsselung geht, da diese maßgebliche Geschäftsgrundlage im Cyberspace ist. Die Rollen können sich jedoch auch ergänzen. In dieser Situation kann die Beschützer-Rolle weiter ausgebaut werden – bspw. wenn es um die Bekämpfung von Kriminalität oder die Erreichung von nationaler Autonomie im Bereich der Cybersicherheit geht. Die Rolle als Garant liberaler Grundrechte kann einem Aufwuchs der Beschützer-Rolle entgegenwirken, wenn bspw. als unangemessen empfundene Kompetenzen zur Gewährleistung von Sicherheit erlassen werden. Sie kann aber auch zu einer Erweiterung der Rolle beitragen, wenn bspw. verbriefte Rechte (die freie und faire Wahl) gefährdet scheinen und besonderen Schutz erfordern.

Aus der Perspektive des hier skizzierten rollentheoretischen TLGs ergibt sich die Außenpolitik damit aus der Interaktion von internationalem und nationalem Rollenspiel, das durch jeweils unterschiedliche signifikante Andere geprägt ist und in dem durch Akteure auch unterschiedliche historische Selbstbilder angeführt werden. Die Stabilisierung der beiden Rollenspiele, d.h. die sozialstrukturelle Anschlussfähigkeit nach innen wie nach außen ist dabei der entscheidende Gradmesser. Sie hängt, wie bereits dargelegt, nicht von Logiken der Angemessenheit, Konsequenzialität oder Argumentation ab, sondern ergibt sich aus der praktischen Interaktion.

## 2.4 Der Cyberspace als (sicherheits-)politisches Handlungsfeld: Theoretische Implikationen

Befasst man sich mit der gesellschaftlichen Regulation des Internets, lohnt es sich, einen Schritt zurückzutreten und zu Fragen, inwiefern dieser Umgang bereits durch die technischen Besonderheiten des Untersuchungsgegenstands determiniert wird. Mit anderen Worten geht es im Folgenden darum zu klären, ob und wenn ja inwiefern das Internet den Akteuren bereits Rollen vorschreibt oder (weniger stark), ob es die Übernahme mancher Rollen erschwert bzw. begünstigt. Nachdem im vorigen Kapitel für ein Verständnis der Rollentheorie argumentiert wurde, das den Akteuren eine substanzielle Handlungsträgerschaft zuschreibt,

wird im Folgenden überprüft, ob der Regulationsgegenstand (das Internet) diese Ansicht konterkariert.

Die differenzierte Betrachtung technischer Einflüsse auf soziale Zusammenhänge ist in den IB selten. Dieses Defizit wurde in den letzten Jahren erstmals eingehender thematisiert und die damit verbundenen Probleme diskutiert (Carr, 2016, S. 2). Mit Blick auf den Theoriebestand der Disziplin konstatiert bspw. Maximilian Mayer:

> »Most international relations (IR) theories are surprisingly indifferent to the emergence and consequences of new technologies.« […] »Theoretical schools and paradigmatic debates have either eschewed technologies as a subject matter or simply taken an instrumentalist stance, defining technologies as mute sources of state power.« (Mayer, 2017, S. 12 bzw. 29)

Zu einer ähnlichen Schlussfolgerung gelangt Daniel McCarthy, der feststellt, dass die Forschung, die sich unter anderem mit technischen Belangen befasst, diese entweder als bloße Instrumente staatlicher Akteure auffasst oder aber einen technischen Determinismus vertritt. Laut McCarthy ist dabei die Auffassung eines technischen Determinismus besonders weit verbreitet (McCarthy, 2015, S. 15 bzw. 28f.). Die grundlegende Skepsis teilt auch Myriam Dunn Cavelty. Sie stellt fest, dass Techniksoziologie bzw. -philosophie und IB-Theorien bisher kaum voneinander Notiz genommen haben und dass dieses akademische Desinteresse eine Blindstelle in der empirischen Cybersicherheitsforschung zur Folge hat. Während eine positivistische Theorieschule den Cyberspace als teilweise objektiv »defekt« und damit reparaturbedürftig sieht, konzipiert eine post-positivistische Perspektive das Internet nicht als objektives Problem, sondern als unterschiedlich wahrgenommenes und als unterschiedlich bedrohlich eingeschätztes Phänomen. Diese unterschiedlichen Standpunkte führen dazu, dass die erste Position verschiedene politische Lösungen für die Probleme sucht und analysiert. Die zweite untersucht (kritisch) die aus der Wahrnehmung resultierenden Politiken. Eine dritte Perspektive, die Technik bspw. konsequent als Teil der Sozialstruktur begreift, kann helfen, die Defizite der bisherigen theoretischen Betrachtungen zu überwinden und das Verhältnis zwischen Technik und Gesellschaft besser zu verstehen (Dunn Cavelty, 2018).

Dieses Kapitel entwirft diese Perspektive aus pragmatistisch-rollentheoretischer Perspektive. Hierzu werden zunächst Dokumente aus der netzpolitischen Gemeinschaft aufgegriffen, um die hier vertretenen Sichtweisen vorzustellen. Anschließend wird der theoretische Umgang mit Technik in der Techniksoziologie diskutiert und die wesentlichen Perspektiven auf das Verhältnis von Gesellschaft und Technik vorgestellt: der technische und der soziale Determinismus. Abschließend entwirft das Kapitel in Anlehnung an Werner Rammert (2016) eine rollentheoretische Sicht auf das Verhältnis von Technik und Gesellschaft. Das ist

notwendig, da mit der Einschätzung dieses Verhältnisses substanzielle Folgen verbunden sind. Teilt man bspw. die Auffassung eines starken technischen Determinismus, bedeutet das, dass sich Technik in einem beständigen Fortschrittsprozess selbst hervorbringt. Menschliche Interventionen stehen dieser Entwicklung dann weitgehend ohnmächtig gegenüber und Rollen würden direkt aus der technischen Struktur folgen. Wissenschaftliche Unterfangen, wie die Technikfolgenabschätzung, können dann zum fatalistischen Blick in eine kaum abwendbare Zukunft werden.

Die implizite Annahme, dass die Informationstechnik unmittelbar sozialstrukturierende Wirkungen entfaltet, findet sich prominent bei VertreterInnen der Netzgemeinschaft. Bereits Ende der 1970er Jahre verfolgten AktivistInnen Visionen eines technisch katalysierten Libertarismus. Wesentlich beeinflusst wurden diese Bestrebungen durch neue Möglichkeiten in der Krypographie. 1977 entwickelten Ron Rivest, Adi Shamir und Leonard Adleman (1978) die erste praktische Umsetzung eines asymmetrischen Verschlüsselungsverfahrens.[20] Unter Rückgriff auf Überlegungen von Whitfield Diffie und Martin Hellman (1976) ermöglichte das Verfahren den AnwenderInnen erstmals verschlüsselt zu kommunizieren, ohne offen einen gemeinsamen Schlüssel über einen potenziell kompromittierten Kommunikationskanal austauschen zu müssen. Dieses neue Verfahren ermöglichte die Entstehung einer Bewegung, die häufig als Krypto-Anarchismus bezeichnet wird. Thomas Rid konstatierte in diesem Kontext: »It is probably the only mathematical algorithm that spurned its own political philosophy« (2016, S. 248). Da das Problem des vertrauensvollen Schlüsselaustausches gelöst war, wurde Kryptographie theoretisch für alle nutzbar. Es stand in der Folge frei, vertraulich zu kommunizieren – die technischen Fähigkeiten vorausgesetzt. VerfechterInnen der neuen Verschlüsselung erkannten darin die Möglichkeit, sich staatlichen Zugriffen gänzlich zu entziehen und so das Gewaltmonopol des Staates nachhaltig aushöhlen zu können. Besonders einflussreich formulierte diese Ansicht Timothy May 1988 in seinem *Crypto Anarchist Manifesto*, hierin heißt es:

> »Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. [...] Interactions over networks will be untraceable, via extensive re- routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. [...] These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.

20 Bekannt wurde das Verfahren unter dem Akronym RSA, basierend auf den Nachnamen der Entwickler. Für eine technische Erläuterung des Verfahrens s. bspw. Paar und Pelzl, 2016.

> The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy.« (May, 1988)

May legte damit nahe, dass soziale Kräfte die Ausbreitung von Verschlüsselung nicht würden aufhalten können. Auch die sozialstrukturellen Effekte sind aus dieser Perspektive unvermeidliche Folge der technischen Entwicklung. Mit Blick auf einige aktuelle Ereignisse scheinen Teile des geschilderten Szenarien eingetreten zu sein. Debatten über die verbreitete Nutzung von Kryptographie durch Kriminelle oder Terrororganisationen und die schwierige Kontrolle der Technologie zeigen, dass Verschlüsselung ein willkommenes Werkzeug für verdeckt agierende Gruppen ist, die sich staatlichem Zugriff zu entziehen versuchen.[21] Der Verweis auf Schattenökonomien in verschlüsselten Bereichen des Netzes scheint wie eine Vorwegnahme der öffentlichen Diskussion, die sich erst viel später um eine dunkle Seite des Internets entsponnen hat. Insbesondere sogenannte Darknets[22] und deren kriminelle Nutzung wurden in jüngerer Vergangenheit intensiv debattiert (Chertoff, 2017). Häufig wurde hierbei auch eine begrenzte staatliche Handlungsfähigkeit attestiert; dennoch gelingt die Strafverfolgung auch in verschlüsselten Bereichen des Internets (Olsen, Schneier und Zittrain, 2016; Zajácz, 2017). Eine intensive staatliche Auseinandersetzung mit Verschlüsselung begann in den 1990er Jahren und hält, in verschiedenen Konjunkturen, bis heute an (Kehl, Wilson und Bankston, 2015; Madsen u. a., 1998; Traylor, 2016). Neben der staatlichen Widerständigkeit zeigt sich aber auch eine soziale, die deutlich weitreichender und einflussreicher ist, als May zu antizipieren scheint. Auch heute, mehr als 40 Jahre nach Entwicklung, ist die asymmetrische Verschlüsselung nicht flächendeckend bei den EndnutzerInnen angekommen.

---

21 Bis zum Jahr 2000 war in den USA der Export starker Verschlüsselung verboten. Dies führte bspw. zu dem Kuriosum, dass eine Software zur Verschlüsselung – PGP (Pretty Good Privacy) – durch einen analogen Ausdruck des Codes außer Landes gebracht und in Schweden wieder digitalisiert wurde, da die Restriktion nicht für Druckerzeugnisse galt (Brunst, 2012, S. 335).

22 Häufig wird der Begriff nicht definiert und Synonym zu Deep Web verwendet. Das Deep Web ist der Teil des Internets, der nicht durch Suchmaschinen indexiert wird und daher nicht ohne weiteres zugänglich ist. Das Darknet wird ebenfalls nicht indexiert, kann darüber hinaus aber zudem nicht ohne entsprechende kryptographische Verfahren betreten werden (Ehney und Shorter, 2016). Die bekanntesten und meistgenutzten Darknets sind TOR, I2P und Freenet (D. Moore und Rid, 2016, S. 15).

In einem anderen Bereich hat sich die libertäre Utopie früher Netizens ebenfalls nicht bewahrheitet. Oft wird in Beiträgen, die sich mit dem Verhältnis zwischen Staat und Internet befassen, auf die *Declaration of the Independence of Cyberspace* von John Perry Barlow (1996) verwiesen. Zumeist wird hierbei die bekannte Eröffnungsformel zitiert. Fragt man aber weiter, wie der vielzitierte staatenlose Zustand erreicht wird und verfolgt die Argumentation des Textes, zeigen sich auch hier Anleihen eines technischen Determinismus. Barlow erkennt zwar, ähnlich wie May, dass es staatlichen Widerstand gegen diese Emanzipation geben wird. Allerdings argumentiert auch er mit Rückgriff auf die Zwangsläufigkeit der technischen Entwicklung. An einigen Stellen suggeriert der Text daher, dass staatliches Eingreifen zwar temporär möglich, aufgrund der technischen Gegebenheiten letztlich aber wirkungslos sei.

> »In China, Germany, France, Russia, Singapore, Italy and the United States, you are trying to ward off the virus of liberty by erecting guard posts at the frontiers of Cyberspace. These may keep out the contagion for a small time, but they will not work in a world that will soon be blanketed in bit-bearing media.« (Barlow, 1996)

Beide Perspektiven aus der Netzgemeinde teilen die Auffassung, dass die Verbreitung des Internets zwangsläufig zu einer Abnahme staatlicher Regulationsfähigkeit führt und dass damit die Rolle des Staates notwendigerweise schwindet. Die Beschützer-Rolle kann bspw. aufgrund der Verschlüsselung nicht mehr (umfassend) wahrgenommen werden. Staatliche Interventionen in die Infrastruktur spielen in den Überlegungen der NetzaktivistInnen keine substanzielle Rolle bzw. sind zum Scheitern verurteilt. Es kann aber, auch 25 Jahre nach Öffnung des World Wide Web, konstatiert werden, dass der Traum eines staatsfreien Internets bisher nicht realisiert wurde – auch wenn sich die Vision einer zunehmend vernetzten Welt verwirklicht hat. Vielmehr besteht zunehmend zwischenstaatlicher Dissens, wie weitreichend die staatliche Kontrolle über das Internet sein soll.[23]

---

23 Deutlich wurde der Konflikt bspw. während der World Conference on International Telecommunication 2012 in Dubai. Zwar wurde der Modus der Multistakeholder Governance immer wieder herausgefordert (DeNardis, 2013; M. L. Mueller, 2010), die Auseinandersetzung in Dubai war aber zweifellos ein Kulminationspunkt der Debatte. Während ein freies und offenes Internet insbesondere durch liberale Demokratien geschützt wird, bevorzugen zahlreiche Autokratien ein stärker staatlich reguliertes System. Diese unterschiedlichen Ordnungsvorstellungen finden Ausdruck in verschiedenen Vorschlägen zur Regulierung des Internets. Die demokratischen Staaten unterstützen dabei ein Modell der weitgehenden Selbstorganisation, wie es seit 1998 mit der Internet Corporation for Assigned Names and Numbers (ICANN) besteht. Viele Autokratien, die durch ein freies Internet ihre Regimestabilität gefährdet sehen, präferieren eine Verwaltung des Internets unter der Aufsicht der International Telecom-

Blickt man auf theoretische Diskussionen in den IB, so stehen bspw. Debatten zwischen offensiven und defensiven Realisten, die den rüstungstechnologischen Entwicklungsstand als einen maßgeblichen Faktor für staatliches Konfliktverhalten anführen, in der Tradition deterministisch geprägter Auffassungen (Glaser und Kaufmann, 1998). In der wissenschaftlichen Auseinandersetzung mit dem Internet sind Perspektiven, die argumentieren, dass Technik wesentlicher Treiber sozialer Entwicklung ist, seltener zu finden als bei netzpolitischen AktivistInnen. Auch wenn bspw. Larry Diamond vom Internet als »liberation technology« (2010, S. 70) schreibt, relativiert er doch, dass die Technik allein keine zwingende soziale Wirkrichtung hat. Ob das Internet eher demokratische Ertüchtigung oder autokratische Kontrolle begünstigt, ist in der Forschung umstritten. Insbesondere frühe Untersuchungen zu neuen Partizipationsformen gehen teilweise von einer direkten demokratiefördernden Wirkung des Internets aus. Diese Perspektive, mitunter als »netzoptimistisch« (Kneuer, 2015, S. 47) bezeichnet, betont besonders die Egalisierung der Machtverhältnisse (Stier, 2017, S. 15). Beispiele für diese positiven Einschätzungen sind Shirky (2009; 2011) und Benkler (2008). KritikerInnen dieser Einschätzung betonen, dass ihre Machtressourcen Staaten dazu in die Lage versetzen, auch umfassende soziale Kontrolle über das Internet auszuüben. Entsprechend pessimistisch beurteilen sie die demokratisierende Wirkung des Internets. Diese Position wird bspw. von Evgeny Morozov (2011), Kalathil und Boas (2003) oder Ronald Deibert (2013; 2012; 2010; 2012) vertreten.

Technikdeterministisch inspirierte Perspektiven, die eine durch die Verbreitung des Internets katalysierte Überwindung autokratischer Herrschaft prognostizieren, erfuhren insbesondere mit den Aufstandsbewegungen des sogenannten Arabischen Frühlings (Jünemann und Zorob, 2012; Schneiders, 2013) wachsenden Zulauf. Howard und Hussain (2011) gehen bspw. nicht nur davon aus, dass die sozialen Medien für die Entstehung der Proteste von entscheidender Bedeutung waren, sie fragen ferner, ob die neuen Technologien möglicherweise umfassenderen Einfluss auf das Konfliktverhalten hatten. Sie konstatieren, dass die Aufstände, von einigen Ausnahmen abgesehen, verhältnismäßig unblutig verlaufen seien und fragen, inwiefern dieser Umstand mit der Verbreitung von Handys mit Kamerafunktion in Verbindung steht (P. N. Howard und Hussain, 2011, S. 47-48). Eine gewaltsame Eskalation blieb möglicherweise aus, da entsprechende Videos diese potenziell weltweit sichtbar gemacht hätten. Ein ähnliches Argument vertritt Mridul Chowdhurry mit Blick auf Demokratisierungsbewegungen in Myanmar.

---

munication Union und damit verbunden das Prinzip *one state one vote* (Valeriano und Maness, 2015).

> »It is possible that the Internet saved the lives of many protestors, because the Junta feared even greater criticism from images of troops killing monks and civilians. The presence of the Internet in a dictatorial regime may save lives.« (Chowdhurry, 2008, S. 14)

Beide Einschätzungen gehen davon aus, dass Technik die Aufstände nicht nur mit ermöglicht hat, sondern, dass auch der Verlauf entscheidend durch die technischen Gegebenheiten beeinflusst war. Ähnliche Argumente finden sich auch in der neueren Konfliktforschung. Der Einfluss moderner IT auf das konventionelle Konfliktgeschehen wird entsprechend kontrovers diskutiert.[24]

Der von Howard und Hussain oder Chowdhurry vermutete befriedende Einfluss der Technik wird aber mit Verweis auf den gleichen Wirkmechanismus (die rasche Verbreitung von Informationen weltweit) auch auf den Kopf gestellt. Das Verhalten von Terrorgruppen zeigt bspw., dass die technischen Gegebenheiten auch zu einem anderen Verhalten führen können. Die bewusste Produktion von Bildern extremer Gewaltsamkeit, um etwa die eigene Entschlossenheit und religiöse Überzeugung vor einem möglichst großen Publikum zu dokumentieren, deuten in diese Richtung (Friss, 2015). Entsprechend vertreten KonfliktforscherInnen auch die gegenläufige These, Barbara Walter argumentiert:

> »Finally, the Internet could potentially eliminate the restraints that limit the abuse of local citizens by rebel and government leaders. [...] By freeing combatants from the need to solicit local support, the Internet may also be freeing them to engage in more civilian abuse.« (Walter, 2017, S. 481)

Da Konfliktparteien mit dem Internet Öffentlichkeiten und AnhängerInnen auf der ganzen Welt erreichen können, sind sie weniger auf die Unterstützung örtlicher AkteurInnen angewiesen – so das Argument. Diese widersprüchlichen Thesen zeigen bei genauer Betrachtung eindrücklich, dass Technik allein nicht soziales Verhalten determiniert, sondern dass die Verwendung von Technik maßgeblich von der sozialen Konstruktion der Handelnden abhängig ist. Aus rollentheoretischer Perspektive ist in den skizzierten Fällen nicht die Technik entscheidend für das Verhalten der Akteure. Vielmehr scheint der adressierte signifikante Andere ausschlaggebend zu sein. Während die staatlichen Akteure in Myanmar oder der arabischen Welt mit ihrem Verhalten möglicherweise dem generalisierten Anderen – der Staatengemeinschaft – gerecht werden wollten, auch um bspw. eine Intervention Dritter zu verhindern, steht für den IS die Rekrutierung bzw. Radikalisierung potenzieller Sympathisanten im Mittelpunkt. Ausschlaggebend für

24 Einen ersten Überblick bietet bspw. das von Nils Weidmann (2015) herausgegebene Sonderheft *Communication, Technology, and Political Conflict* im Journal of Peace Research oder der Aufsatz *Studying the Internet and Violent Conflict* von Anita Gohdes (2018).

das Verhalten ist dann die antizipierte Position des Anderen mit dem Rollenkomplementarität angestrebt wird. Hierbei sind natürlich Fehleinschätzungen der Akteure nicht ausgeschlossen. Ist Technik also letztlich doch neutrales Instrument politisch Handelnder?

Systematische Analysen des Verhältnisses von Technik und Gesellschaft finden sich in der Techniksoziologie bzw. -philosophie.[25] In zahlreichen Betrachtungen verschiedener Disziplinen galt lange die technikdeterministische Annahme, dass Technik gesellschaftliche Prozesse überformt und eigenen Logiken folgt, die durch soziale Einflussnahme nur sehr begrenzt regulierbar seien. Sozialstruktur wird in dieser Perspektive zum Ergebnis technischer Entwicklung. Ein Vertreter des starken, auch als genetisch bezeichneten (Ropohl, 1999), Technikdeterminismus ist bspw. Jacques Ellul (1964). Wie die bereits zitierten Netzaktivisten geht der starke Technikdeterminismus von einer technischen Eigendynamik aus, gegen die die Gesellschaft machtlos ist. Dieser Ansicht liegt die Prämisse zugrunde, dass Technisierung in sich determiniert ist (Häußling, 2014, S. 120). Diese Position nimmt nicht nur an, dass technische Gegebenheiten soziale Effekte zur Folge haben, sie unterstellt ferner, dass sich Technik auch selbst hervorbringt und in diesem Prozess nicht beeinflussbar ist. Die Gesellschaft wird hier zum Spielball technischer Entwicklung und kann sich nur darauf beschränken Risiken und ggf. Schäden zu minimieren. Eine aktiv gestaltende Einflussmöglichkeit bleibt nicht. Folglich sind aus dieser Perspektive die Rollen der staatlichen Akteure maximal Anpassungsreaktionen auf technische Entwicklungen.

Eine etwas schwächere Form des technischen Determinismus, auch als konsequenziell bezeichnet (Ropohl, 1999), stellt den Verwendungszusammenhang von Technik in den Mittelpunkt der Betrachtung und konstatiert eine determinierende Wirkung bestehender Technik auf soziale Zusammenhänge. Als Vertreter dieser Ansicht wird häufig der »Gründungsvater der Technikfolgenabschätzung« (Häußling, 2014, S. 120) William F. Ogburn angeführt. Besondere Bekanntheit erlangte seine These des »cultural lag«. Ogburn geht davon aus, dass wissenschaftlich-technische Entwicklung aufgrund ihres schnellen Voranschreitens die gesellschaftliche Ordnung maßgeblich prägt bzw. vor sich hertreibt.

> »Mittlerweile entwickelt sich die Technik, wird auf die Gesellschaft losgelassen und reißt alles mit sich fort. […] Wie eine riesige Woge rollt die Technik weiter, während die Regierungsstruktur wie der Fels der Zeiten in einer Welt der Unordnung steht — eine unwiderstehliche Gewalt trifft auf ein unbewegliches Objekt.« (Ogburn, 1969, S. 199)

25 Einführungen in die Techniksoziologie bieten bspw. Häußling (2014), Mai (2011) oder Weyer (2008).

In seiner Analyse rückte er besonders den Verwendungskontext von Technik ins Zentrum. Wie Technik entsteht und ob dieser Prozess sozial steuerbar ist, bleibt weitgehend unberücksichtigt. Vergleicht man beide Perspektiven, den starken und den schwachen (bzw. genetischen und konsequenziellen) technischen Determinismus, zeigt sich der zentrale Unterschied beider Ansätze in der Differenzierung von Entwicklungs- und Verwendungskontext von Technik. Während der genetische Technikdeterminismus davon ausgeht, dass technische Entwicklung sich selbst determiniert und damit auch den Entwicklungskontext integriert, spart die konsequenzielle Perspektive den Entwicklungskontext weitgehend aus und fokussiert bspw. auf Sachzwänge (Schelsky, 1965), die aus bestehender Technik und deren Verwendung folgen (Häußling, 2014, S. 137).[26] Aus technikdeterministischer Perspektive wird bspw. immer wieder die Entwicklung des Steigbügels und die damit verbundenen gesellschaftlichen Folgen debattiert. Lynn White konstatierte in seiner Studie *Medieval Technology and Social Change* »Few inventions have been so simple as the stirrup, but few have had so catalytic an influence on history« (1962, S. 38). Vor der Erfindung des Steigbügels war es berittenen Truppen, aufgrund des fehlenden Halts, kaum bzw. nur unter großem Risiko möglich, direkt in den Kampf einzugreifen. Der Steigbügel versetzte die Kavallerie dagegen in die Lage auch schwere Waffen zum Einsatz zu bringen und trotzdem sicher im Sattel zu bleiben. Die Franken nutzten diese neuen Streitkräfte besonders effektiv und erlangten so militärstrategische Vorteile, die auch in einer Expansion ihres Herrschaftsgebiets resultierten. Ferner folgten aus den neuen Strategien wiederum neue technische Anpassungen der Kriegsführung. Die gestiegene Bedeutung berittener Krieger schlug sich aber nicht nur militärisch, sondern auch in der Gesellschaftsordnung der Karolinger nieder. Aus der kämpfenden Elite wurde rasch auch eine politisch besonders einflussreiche Größe (L. White, 1962, S. 30-37). Der Steigbügel hat damit nicht nur die mittelalterliche Kriegsführung nachhaltig verändert, er hat zudem zu weitreichenden sozialstrukturellen Veränderungen geführt. Die expansive Politik des Frankenreichs und der politische Aufstieg der militärischen Elite ist aus dieser Perspektive Resultat technischen Fortschritts.

---

26 Die Unterscheidung zwischen Entwicklungs- und Verwendungskontext ist nicht unproblematisch, da sie eine logische Trennung postuliert, die empirisch nicht immer eingelöst werden kann. Betrachtet man bspw. eine Technik wie das Internet, so offenbaren sich Unwägbarkeiten. Auch wenn die grundlegende Funktionsweise des Internets (die TCP/IP-Protokollfamilie) seit der Entwicklung des Internets stabil geblieben ist, zeigt sich doch, dass sich das Netz, insbesondere auf Applikationsebene deutlich verändert hat. Die Entwicklung von HTTP und damit die Entstehung des World Wide Web, wie es heute genutzt wird, ist nur ein Beispiel hierfür. Es wird deutlich, dass das Internet eher evolutionär weiterentwickelt wird. Entwicklungs- und Verwendungskontext können folglich ineinander kollabieren. Trotzdem ist die Unterscheidung zur Differenzierung der Ansätze hilfreich.

Aber auch White argumentiert nicht ausschließlich technikdeterministisch, wie ihm mitunter unterstellt wird. Vielmehr schließt er auch die Möglichkeit einer sozialen Steuerbarkeit der technischen Entwicklung nicht aus. Insbesondere vor der Implementierung einer technischen Innovation sieht er soziale Faktoren als ebenfalls einflussreich.

> »As our understanding of the history of technology increases, it becomes clear that a new device merely opens a door; it does not compel one to enter. The acceptance or rejection of an invention, or the extent to which its implications are realized if it is accepted, depends quite as much upon the condition of a society, and upon the imagination of its leaders, as upon the nature of the technological item itself.« (L. White, 1962, S. 28)

Die wachsende Berücksichtigung sozialer Einflüsse auf die Gestaltung und Verwendung von Technik ist Teil einer Debatte, die durch verschiedene Disziplinen verlaufen ist und immer mehr dazu geführt hat, dass technikdeterministische Ansätze vermehrt durch sozialdeterministische Perspektiven herausgefordert wurden (Mai, 2011, S. 41 f.).[27]

Ansätze, die die entscheidende Bedeutung sozialer Konstruktion von Technik betonen, sind ebenso variantenreich wie ihre technikdeterministischen Pendants. Unter der Bezeichnung Social Shaping of Technology wurde einer der ersten Versuche unternommen, Perspektiven, die den Technikdeterminismus herausforderten und stattdessen auf soziale Einflüsse rekurrieren, systematisiert zu bündeln (D. A. MacKenzie und Wajcman, 1999). Im Mittelpunkt stand hierbei das Bestreben, einer genetisch-deterministischen Logik zu begegnen. Damit rückte zunächst der Entwicklungskontext von Technik in den Fokus der Aufmerksamkeit. Auf diese Weise konnte die Gesellschaft nicht mehr als von Technik bzw. deren Entwicklung getrieben begriffen werden. Ein argumentativer Ansatzpunkt für Donald MacKenzie und Judy Wajcman (1999) ist die Annahme, dass bei der Technikentwicklung versucht werde, Ziele zu erreichen, die in sozialen Kontexten formuliert wurden. In ihrer Argumentation stützen sie sich dabei maßgeblich auf sozialkonstruktivistische Ansätze der Wissenschaftstheorie. Dem Argument, dass technische Entwicklung durch ökonomische Rationalität geleitet werde, begegnen MacKenzie und Wajcman mit dem Hinweis, dass auch diese sozial konstruiert sei und dass bspw. in Fällen sozialer Abhängigkeiten eine Effektivitätssteigerung durch technischen Fortschritt bewusst verhindert werden kann, um soziale Strukturen zu erhalten. Ob und inwiefern ökonomische Erwägungen technische Entwicklung beeinflussen, hängt damit ebenfalls von sozialer Konstruktion ab (ebd.).

27 Das bedeutet nicht, dass soziale Einflüsse zuvor unberücksichtigt geblieben sind, die Diskussion war jedoch lange durch technikdeterministische Perspektiven geprägt.

Den Einfluss sozialer Konstruktion auf die Entwicklung von Technik illustriert Roger Häußling (2014, S. 240-242), in Anlehnung an Wiebe Bijker (1995), am Beispiel des Fahrrades. Bei der Entwicklung des Fahrrades waren unterschiedliche Faktoren einflussreich und eine dem heutigen Fahrrad ähnliche Lösung konnte sich zunächst nicht durchsetzen. Stattdessen fand vorerst das Hochrad die meisten Befürworter. Dieser Umstand lag in erster Linie am Einfluss junger Männer, die im Fahrrad nicht primär ein Transportmittel sahen, sondern ein Sportgerät. Während das Hochrad so für diese Gruppe zum gut funktionierenden Mittel sportlicher Betätigung wurde, war es für andere ein schlecht funktionierendes Fortbewegungsmittel. Für Frauen war es aufgrund geltender Kleidungskonventionen überhaupt nicht nutzbar (Bijker, 1995, S. 75-77). Diese Situation änderte sich erst, als auch die besonders einflussreiche Gruppe junger Männer die Vorteile des heutigen Fahrraddesigns zu schätzen lernte. Zunächst wurden Fahrräder mit zwei gleichgroßen, luftgefüllten Reifen mit dem Hinweis auf deren bessere Fahreigenschaften und damit erhöhte Sicherheit beworben. Das fand jedoch kaum Resonanz, da dies nur die erforderlichen sportlichen Fähigkeiten reduzierte. Erst als deutlich wurde, dass die neue Konstruktion bei Rennen deutlich schneller war als die Vorgänger, wurde der Sicherheitsgewinn auch als Fortschritt sportlichen Wettbewerbs gesehen und die neue Bauweise fand weitere Verbreitung. Bei genauerer Betrachtung zeigt sich aber, dass auch sozialkonstruktivistische Ansätze bei der Auseinandersetzung mit Technik an Grenzen stoßen. Roger Häußling argumentiert mit Blick auf eine möglicherweise unintendierte Konsequenz des neuen Fahrraddesigns bspw. dass die neue Bauform auch emanzipatorische Folgen hatte, da das neue Fahrrad eher mit Kleidungskonventionen für Frauen vereinbar war (Häußling, 2014, S. 242). Es liegt daher der Schluss nahe, dass Techniken nach deren Etablierung wiederum »als objektivierte Formen von Gesellschaft auf die Gesellschaft zurück [-wirken; Anm. d. Verf.]« (ebd., S. 239). So entfalten sie dann (ggf. auch unintendierte) soziale Wirkungen. Das Verhältnis von Technik und Gesellschaft ist daher nicht unidirektional beschreibbar.

Ansätze, die ausschließlich über eine soziale Formung von Technik argumentieren, geraten hierdurch ebenfalls an Grenzen. Im Folgenden soll daher kurz skizziert werden, wie eine rollentheoretische Position aussehen kann. Werner Rammerts (2016) pragmatistische Technik- und Sozialtheorie bietet hierfür einen guten Anknüpfungspunkt. Orientiert an Theoretikern wie John Dewey, Andrew Pickering, George Herbert Mead, Hans Joas und Anthony Giddens, entwickelt Rammert eine Perspektive aus der »*Technik* zugleich als integraler Bestandteil und besonderer Aspekt der Gesellschaft betrachtet [wird; Anm. d. Verf.]. Sie ist selbstverständlicher Teil der *Sozialstruktur* [Hervorhebungen im Original; Anm. d. Verf.]« (Rammert, 2016, S. 4). Ähnlich wie MacKenzie und Wacjman (1999) geht auch Rammert davon aus, dass Technik immer Resultat »sozialen Handelns« ist (ebd., S. 4). Sie ist damit Ausdrucksform gesellschaftlicher Desiderate und nicht

durch einen genetischen Technikdeterminismus getrieben. Aus den diskutierten Ansätzen der Technikforschung zieht Rammert den Schluss, »dass die gesellschaftliche Konstruktion der Technik nicht durch das Wirken einer einzigen Strukturlogik erklärt werden kann« (Rammert, 2016, S. 27). Ferner löst Rammert die kategoriale Trennung zwischen Entstehungs- und Verwendungskontext auf und geht stattdessen davon aus, dass Technik, sobald sie verwendet wird, einer sozialen Re-Interpretation durch Interaktion offen steht. Der sozialstrukturelle Status von Technik ist damit abhängig von »interaktiver Aneignung und manchmal auch innovativer Umgestaltung« (ebd., S. 4). Technische Entwicklung verläuft aus dieser Perspektive als »soziotechnische Evolution« (ebd., S. 17). In einer ersten Entwicklungsphase (Variation) werden verschiedene Möglichkeiten zur technischen Bearbeitung eines Problems erprobt. Dies erfolgt ggf. noch in geschlossenen (wissenschaftlichen) Gruppen. In der zweiten Phase (Selektion) wird durch die Beteiligten eine der Varianten ausgewählt. Die dritte Phase (Stabilisierung) bettet die neue Technik als Teil der Sozialstruktur ein (ebd., S. 17f.).

Neben der Auflösung von Entstehungs- und Verwendungskontext, wendet sich Rammert dezidiert gegen Ansätze, die im Umgang mit Technik ausschließlich instrumentelles Handeln sehen. Deutlich wird dies etwa mit Blick auf Konsumverhalten. Geht es bspw. um den Kauf eines Autos, so sind mehr Aspekte entscheidend, als nur von A nach B zu gelangen. Ob ein Auto als Sportgerät, Investitionsgegenstand, Transportmittel, Umweltprojekt oder Statussymbol gesehen wird, entscheidet maßgeblich über dessen Akzeptanz und Verwendung. Techniken sind dabei zweifach an Gesellschaft rückgebunden: »Einerseits sind sie selbst vergegenständlichte Kultur […], andererseits werden sie in ihrer Gestalt und Genese durch besondere kulturelle *Stile* und *Orientierungen* geprägt [Hervorhebungen im Original; Anm. d. Verf.]« (ebd., S. 4).

Um sich aus der dualistischen Perspektive (Gesellschaft-Technik) zu lösen, plädiert Rammert für eine Konzeption von »Techniksoziologie als Sozialtheorie« (2016, S. 54). Auf dieser Basis besteht kein »Grund, die Technik aus der Konstitution der alltäglichen Lebenswelt herauszuhalten und sie nur für gesonderte Wirklichkeiten vorzubehalten« (ebd., S. 48). Dies ist mit Blick auf die ausgreifende Digitalisierung besonders einleuchtend. Technik wird damit gleichsam als Teil der Sozialstruktur verstanden. Rammert nähert sich mit dieser Auffassung aus pragmatistischer Sicht dem Foucaultschen Dispositiv. Für DiskursforscherInnen sind Dispositive perpetuierte Ausdrucksformen diskursiver Auseinandersetzungen. Sie können in materieller oder immaterieller Form vorliegen und entfalten dauerhafte Wirkung auf Gesellschaften (Keller, 2013). Pragmatistisch orientiert sich Rammert hier an der Position von John Dewey. Die vom Technikdeterminismus bzw. Sozialkonstruktivismus postulierten ontologischen Unterschiede zwischen Gesellschaft und Technik werden aus dieser Position abgelehnt. Alle Versuche durch Dekonstruktion eine kategoriale Unterscheidung zwischen Gesellschaft

und Technik zu etablieren bleiben letztlich ohne Substanz. Die gesellschaftlichen Praktiken führen zu neuen technischen Innovationen oder in fortlaufender Interaktion zur Neudeutung bestehender Technik. Diese Prozesse vollziehen sich aber nicht in technikfreier Isolation, sondern sind stets in eine technische Umwelt eingebettet. Auch wenn hier eine Art verteilter Akteurschaft postuliert wird, bleiben menschliche AkteurInnen aus dieser Perspektive doch die einzigen, die dieses Verhältnis distanziert reflektieren, bewerten und kreativ steuern können (Rammert, 2016, S. 58-68). Gibt man den dualistischen Standpunkt auf, rückt die Funktion, die Technik »in Erfahrung und Handlung praktisch zugewiesen wird«, in den Mittelpunkt der Aufmerksamkeit (ebd., S. 64). Aus dieser Perspektive wird auch nicht mehr nach objektiven Gründen gesucht, warum eine Technik einer anderen bevorzugt wird. Das bereits diskutierte neue Fahrraddesign erfüllte die Funktionsanforderungen verschiedener Akteursgruppen gleichermaßen. Dadurch erfuhr es auch umfassende Unterstützung und damit gesellschaftliche Verbreitung. Die Anschlussfähigkeit an das Rollenkonzept zeigt sich hier besonders deutlich. Die Gründe, aus denen AkteurInnen die neue Bauweise unterstützten, waren möglicherweise sehr unterschiedlich und trotzdem ging daraus eine technische Lösung hervor. Damit ist auch aus rollentheoretischer Perspektive ein Verständnis von Technik als Teil der Sozialstruktur naheliegend. Das Internet ist in diesem Verständnis sowohl rollengeprägt als auch rollenprägend. Um diesen Umstand zu illustrieren, wird an dieser Stelle in einem kurzen empirischen Exkurs die Entstehung des Internets skizziert.

### 2.4.1 Empirischer Exkurs: Die Entwicklung des Internets

An dieser Stelle soll kurz auf die Frage eingegangen werden, was es bedeutet, das Internet als Teil der Sozialstruktur zu verstehen. Inwiefern ist das Netz gesellschaftlich gestaltet und nach wie vor gestaltbar bzw. wo liegen besonders verankerte Widerständigkeiten? Rammert unterscheidet drei idealtypische Reifegrade einer Technik anhand der Tiefe ihrer sozialen Integration (ebd., S. 29). In diesen Stadien ist Technik unterschiedlich leicht bzw. schwer veränderbar. In der ersten Entstehungsphase werden technische Lösungen für ein Problem unter den beteiligten AkteurInnen ausgehandelt. Diese erste Phase durchlief die dem Internet zugrundeliegende Technik als Paul Baran und andere Wissenschaftler mit der Forschung an paketvermittelter Kommunikation begannen und erste Nutzungskontexte (militärische wie wissenschaftliche) erschlossen wurden. Diese Periode dauerte etwa von 1956 bis zum Beginn der 1980er Jahre (Braun, 2010; Naughton, 2016) und es war nicht der technologische Fortschritt, im Sinne eines genetischen-Determinismus, der die Entwicklung einleitete. Nicht die bloße technische Möglichkeit paketvermittelter Kommunikation sorgte für die Entwicklung des Netzes. Auch ökonomische Überlegungen waren nicht ausschlaggebend. Im Gegenteil, so-

gar als die Arbeiten an der Technik bereits begonnen hatten und Paul Baran 1965 erste Ideen zur Paketvermittlung dem amerikanischen Telekommunikationsunternehmen AT&T präsentierte, lehnten die UnternehmensvertreterInnen die neue Technologie ab. Der entscheidende Innovationsimpuls ging dagegen von einem politischen Schockmoment aus. Als die Sowjetunion am 4. Oktober 1957 den ersten Satelliten in die Erdumlaufbahn brachte, löste das in den USA eine Welle der Forschungsförderung aus. Dass dieser historische Erfolg nicht den USA gelang, stellte das Selbstverständnis sowie die Technologieführerschaft der Vereinigten Staaten grundlegend in Frage und führte zu einem massiven Ausbau der zivilen und militärischen Forschungsförderung (Hafner und Lyon, 1996). Erste Ansätze zu paketvermittelter Kommunikation hatten Paul Baran bei RAND und Donald Davies im britischen National Physical Laboratory zwar bereits 1956 verfolgt, diese wurden aber erst durch die 1958 in den USA gegründete Advanced Research Projects Agency (ARPA) entscheidend vorangetrieben. Die ARPA förderte unter anderem den Erwerb mehrerer Hochleistungsrechner, die an verschiedenen Standorten zum Einsatz gebracht wurden. Um diese Investition optimal nutzen zu können, sollten die Ressourcen kooperativ von möglichst vielen WissenschaftlerInnen genutzt werden können. Aus diesem Grund wurden die Bemühungen intensiviert, eine verlässliche Kommunikationsmethode zwischen diesen Rechnern zu etablieren. In diesem Zuge wurde auch die Forschung an den Techniken intensiviert, die dem Internet zugrunde liegen (Braun, 2010; Cohen-Almagor, 2011; Naughton, 2016).

Nach grundlegenden, theoretischen Überlegungen zu paketvermittelter Kommunikation wurde auf dem ACM-Symposium 1967 sowohl von VertreterInnen der ARPA als auch den beteiligten zivilen WissenschaftlerInnen, das Potenzial der paketvermittelten Kommunikation betont und eine erste technische Implementierung geplant. Zentrales Anliegen war es, ein Netzwerk zu etablieren, das offen erweiterbar und funktional nicht festgelegt war. Einzige Bedingung war die verlässliche Weitergabe von Paketen ohne feste Routen. Die hiermit transportierten Informationen konnten unterschiedlicher Natur sein. Um dieses Ziel zu erreichen, war es nötig, eine gemeinsame Sprache für die vernetzten Rechner zu definieren, die aufgrund ihrer unterschiedlichen Hardware nicht direkt miteinander kommunizieren konnten. Diese Voraussetzung wurde in einem ersten Schritt über externe Hardware, sogenannte Interface Message Processors, erfüllt. Am 29. Oktober 1969 wurden die ersten Informationen zwischen Rechnern an der University of California (UCLA) und dem Stanford Research Institute ausgetauscht. Ende des Jahres waren bereits die ersten vier Rechner des ARPANET verbunden. Die Computer kommunizierten dabei nach einem einheitlichen Standard (NCP später TCP bzw. TCP/IP) (Kleinrock, 2010). Mit der Festlegung auf verbindliche Protokolle sowie erste Institutionen, die diese entwickeln und pflegen sollten, wurde die Technik zunächst nur begrenzt und informell sozial

rückgebunden. Die nahezu ausschließlich US-amerikanische, wissenschaftliche NutzerInnengemeinschaft prägte maßgeblich die nach wie vor in Teilen der internetnahen Institutionen verbreitete konsensorientierte Entscheidungsfindung und Funktionsweise des Internets. Die Verwaltung des Domain Name Systems [28] wurde bspw. von Jon Postel an der UCLA übernommen. Bei der technischen Entwicklung griffen die WissenschaftlerInnen immer wieder auf bestehende Strukturen bzw. Erfahrungen zurück. So wurde das Netz in Konkurrenz und Abgrenzung zur leitungsvermittelten (Telefon)Kommunikation entwickelt. Zur Implementierung nutzte man jedoch die bestehende Telefoninfrastruktur und baute die neue Technik auf der bestehenden physischen Grundlage auf. Auch die Entwicklung der neuen Protokolle erfolgte nicht ohne Rückgriff auf Erfahrungen bspw. auf das für Funknetze entwickelte Aloha-Verfahren. 1972 war der Vorgänger des Internets, das ARPANET, weitgehend funktionsfähig. 15 Standorte waren über das Netz verbunden und bereits bei der frühen praktischen Nutzung stellte sich heraus, dass die NutzerInnen rasch eine Neuinterpretation des Mediums vornahmen. Zwar wurden, wie geplant, die Rechnerkapazitäten geteilt, aber der erste Vorläufer des Internets wurde darüber hinaus schnell zum beliebten Kommunikationskanal zwischen WissenschaftlerInnen (Braun, 2010; Naughton, 2016).

Das Netz hatte einen ersten unintendierten sozialstrukturierenden Effekt, »[…] the community of users came up with a new conception of what 'networking' meant – not so much the sharing of *machines* as the linking of *people*« (Naughton, 2016, S. 9, Hervorhebungen im Original, Anm. d. Verf.). Das neue Medium veränderte das kollaborative Arbeiten der beteiligten WissenschaftlerInnen, die wiederum das neue Medium kreativ neu-interpretierten und es entsprechend technisch weiterentwickelten. In einer kleinen und homogenen NutzerInnengruppe waren diese technischen Anpassungen noch vergleichsweise leicht umsetzbar. Das Netz wurde vom Instrument effizienter Ressourcennutzung immer mehr zum sozialen Austauschmedium. Diese Bedeutungszuschreibung führte dazu, dass neue Protokolle etabliert wurden. Erste Mailfunktionen wurden bereits 1971 etabliert. Die erste Version des Simple Mail Transfer Protocol (SMTP) stammt aus dem Jahr 1982. Bei der Entwicklung und Implementierung der Mailfunktion waren Sicherheitsbedenken von geringer Bedeutung, da die NutzerInnen ohnehin vertrauenswürdig waren. Entsprechend wurde bspw. auf eine sichere Authentifizierung der AbsenderInnen verzichtet, dies ermöglichte die Fälschung (spoofing) von Mailadressen. Dieser Umstand wurde erst in der späteren Entwicklung des

28 Das DNS ist eine der wenigen Instanzen im Internet, die hierarchisch geregelt werden müssen. An der privilegierten Stellung der USA in der Verwaltung des DNS haben sich daher häufig Konflikte entzündet (Bradshaw und DeNardis, 2016; Bradshaw, DeNardis u. a., 2016; DeNardis, 2013; Hammond, 2013; Hill, 2016; Housen-Couriel, 2013; M. Mueller und Badiei, 2017; Raustiala, 2017; Stifel, 2017).

Internets problematisch, da nach der kommerziellen Öffnung mehr und mehr Akteure das Internet nutzten. Mit den neuen NutzerInnen fand auch die Kriminalität ihren Weg in das Netz und die technischen Spezifikationen ermöglichten verschiedene Formen krimineller Aktivitäten (bspw. die Verbreitung von Spam) (Braun, 2010; Naughton, 2016). In dieser frühen Phase der Netzentwicklung wird deutlich, dass die Technologie noch leicht durch die beteiligten AkteurInnen steuerbar war, Anpassungen an die sich wandelnden Anforderungen konnten relativ schnell implementiert werden. Der Geist der US-amerikanischen Wissenschaftsgemeinschaft wurde in dieser Zeit tief in die technischen Grundstrukturen des Internets eingeschrieben.

In den frühen 1980er Jahren begann die Stabilisierungsphase des Internets. Ein wesentlicher Schritt bestand in der Trennung des militärischen (MILNET) und wissenschaftlichen (ARPANET) Teils im Jahr 1983. Mit dieser Teilung wurden die ursprünglichen Entwicklungsmotivationen getrennt und ein wesentlicher Grundstein für die Entstehung eines zivilen Internets gelegt. Die Trennung in zwei verschiedene Netze dokumentiert darüber hinaus, dass auch zu diesem Zeitpunkt die technische Entwicklung noch leicht durch wenige politische Akteure in den USA steuerbar war. Exemplarisch für die Formbarkeit steht die Entscheidung des Pentagon, die 1983 die TCP/IP-Protokollfamilie zur bis heute allgemeingültigen Verkehrssprache des Internets erklärte. Alle Geräte, die über TCP/IP kommunizieren, waren und sind damit potenziell in der Lage, Teil des Internets zu werden. Als deutlich wurde, dass sich TCP/IP als Standard durchsetzen würde, entstanden auch in anderen Staaten TCP/IP-basierte Netzwerke (bspw. das EUnet), die später, aufgrund des offenen Standards, zum Netz der Netze verbunden werden konnten (Braun, 2010). In dieser Phase wurde auch innerhalb der USA ein weiteres TCP/IP-Netzwerk unter der Aufsicht der NSF aufgebaut – das Computer Science Network (CSNET). Hierdurch erweiterte sich die Nutzergemeinde um WissenschaftlerInnen, die nicht unmittelbar durch die ARPA gefördert wurden (Naughton, 2016, S. 11).

Die Phase der Stabilisierung endet mit der Kommerzialisierung und globalen Verbreitung des Internets Mitte der 1990er Jahre. In dieser Phase wurde das Internet schnell zu einem internationalen Verbund verschiedener Netze und damit auch für die USA schwerer kontrollierbar. So scheiterte bspw. ein Versuch die etablierte Protokollfamilie nochmals zu ändern, da sich TCP/IP zum weitverbreiteten Standard in UNIX-Systemen entwickelt hatte (Braun, 2010, S. 204). Das Verhalten der USA allein beeinflusst die Entwicklung des Internets nicht mehr so maßgeblich wie in den Anfangsjahren seiner Entwicklung (Rovner und T. Moore, 2017). Die Entscheidungen über das Design des Netzes werden jetzt in verschiedenen (technischen) Gremien (IETF, ICANN, etc.) zwischen unterschiedlichen Akteuren verhandelt. Damit sind auch die beiden Untersuchungsstaaten an der Weiterent-

wicklung des Internets beteiligt. Sie wurden aber auch durch das globale Netz verändert.[29]

Das Internet hat, als Teil einer zunehmend globalen Sozialstruktur, Praktiken ermöglicht, die vorher undenkbar waren. Dabei unterlag es beständiger sozialer Umdeutung und interaktiver Rekonfiguration. Ausgehend von der kollaborativen Nutzung wissenschaftlicher Infrastrukturen über große geografische Distanzen (einer der intendierten Zwecke), hat das Internet nicht nur wissenschaftliches Arbeiten nachhaltig verändert. Die in der Frühphase des Internets gelegten Strukturen erschweren bzw. erleichtern heute verschiedene Politiken im Internet und entfalten somit nach wie vor sozialstrukturelle Wirkungen. Mit Blick auf Cybersicherheit wird häufig über tief im Netz verankerte Probleme, wie das der Attribution debattiert. Dass Cyberangriffe technisch kaum eindeutig attribuierbar sind, liegt in den Kernprotokollen des Internets begründet, die nie darauf ausgelegt waren, Sicherheit gegenüber Angriffen zu gewährleisten, da der Kreis der NutzerInnen zunächst vertrauenswürdig war. Diese technischen Grundsatzentscheidungen sind allerdings nicht unumkehrbar. Ein Beispiel hierfür sind die Bestrebungen territoriale, politische Souveränität auf das Internet zu übertragen bzw. die in diesem Kontext diskutierten technischen Maßnahmen (Maurer u. a., 2014). Autokratische Tendenzen zur besseren Kontrolle des Internets können bspw. als Abwehrreaktion auf den, dem Internet inhärenten, Wert der diskriminierungsfreien Informationsweitergabe interpretiert werden. Trotz der hohen Kosten sind die Staaten in der Lage, sich auch gänzlich aus dem globalen Netz zurückzuziehen bzw. sich diese Option technisch zu wahren. Bestrebungen in Russland ein abgetrenntes und selbstverwaltetes Netzsegment zu etablieren,

29 Die normative Frage, ob das Internet seinen Siegeszug um die Welt ohne gesellschaftliche Zustimmung angetreten hat und damit Tatsachen geschaffen wurden, über die nie verhandelt worden ist bzw. werden konnte, ist nicht einfach zu beantworten. Jürgen Habermas spricht bspw. von einer »Kolonialisierung« (1982, S. 10) bestehender sozialer Verhältnisse, wenn Phänomene praktisch ohne Beteiligung der Betroffenen sozialstrukturelle Wirksamkeit entfalten. Roger Häußling (2014, S. 215) veranschaulicht diesen Befund an Prozessen der Globalisierung. Er argumentiert, dass die Technik und Wirtschaft nahezu im Alleingang Realitäten geschaffen haben, mit denen sich die Gesellschaften zu arrangieren haben. Aus pragmatistischer Sicht sind die BürgerInnen allerdings an Prozessen der Globalisierung ebenfalls beteiligt, genau wie an der Ausbreitung des Internets. Als KonsumentInnen bestimmen sie bspw. darüber mit, welche Produktionsverhältnisse akzeptabel sind, als InternetnutzerInnen akzeptieren oder verweigern sie die Bedingungen der Interaktion im Netz. Der Hinweis, dass es über die detaillierte Ausgestaltung der globalisierten Welt keinen gleichberechtigten Diskurs gegeben hat und damit nicht der Logik eines »zwanglosen Zwangs des besseren Arguments« (Habermas, 1982, S. 52) gefolgt wurde, ist sicher nicht verfehlt, bedeutet aus pragmatistischer Sicht aber nicht, dass die AkteurInnen durch ihr Verhalten die sozialstrukturellen Gegebenheiten nicht stützen.

haben das Potenzial die technische Struktur des Internets dauerhaft zu verändern (Nikkarila und Ristolainen, 2017). Die eigene Isolation ist hierbei noch eine relativ einfache Maßnahme, da sie unilateral verfolgt werden kann. Sollen dagegen grundlegende Funktionsweisen des Internets verändert werden, erfordert das umfassende Eingriffe in die technischen Protokolle des Internets. Die technische (Weiter)Entwicklung wird aber in weitgehend apolitischen Gremien wie der Internet Engineering Task Force (IETF), dem Internet Architecture Board (IAB) oder dem World Wide Web Consortium (W3C) beschlossen (Nye, 2016). Der Einfluss einzelner Staaten auf die Entscheidungsfindung für das gesamte Netz ist daher begrenzt. Dennoch sind auch tiefgreifende Veränderungen in der technischen Infrastruktur möglich, auch wenn heute kein Staat mehr unilateral das gesamte Internet nach seinen Vorstellungen verändern kann.

Das Netz ist damit Artefakt der US-Politik während des kalten Krieges (gesteuerte Innovationsförderung) unter den gegebenen technischen Möglichkeiten. Die derzeitige Form des Internets ist folglich nicht nur abhängig von physikalisch-technischen Machbarkeiten, sondern auch Ausdruck der US-amerikanischen Rolle als »Ideenstrukturgeber bzw. Basic Service Provider« für das Internet (Schünemann, Harnisch und Artmann, 2018, S. 268). Rollentheoretisch gesprochen waren die USA in dieser Entstehungsphase der einzige signifikante Andere des Internets. Dementsprechend konnten sie die Technik in dieser Phase unilateral formen. Mit dem Internet wurde in der Folge ein ursprünglich rein US-amerikanischer Teil Sozialstruktur sukzessive um die Welt exportiert. Hierdurch hat sich die Zahl der signifikanten Anderen deutlich erhöht (sowohl um staatliche als auch nichtstaatliche Akteure). Zudem wurde das Netz nicht nur für mehr und mehr Akteure relevant, es wurde auch für eine wachsende Zahl von Rollen bedeutsam. Stand zunächst noch die Wirtschaftsförderung im Mittelpunkt folgten dann weitere Nutzungsbereiche, sodass die Akteure in unterschiedlichen Rollen begonnen haben, das Netz zu nutzen. Die Widerständigkeit gegen technische Veränderungen resultiert damit aus einer tieferen sozialen Integration der Technik.[30]

Soll das Internet als kohärentes Ganzes erhalten bleiben ist dazu folglich eine Koalition vieler – staatlicher als auch nichtstaatlicher – Akteure nötig, die Wandel in ihren unterschiedlichen Rollen mittragen. Die Hürden, Rollenkomplementarität zwischen allen Beteiligten herzustellen, sind entsprechend groß, aber nicht unüberwindbar. Das Internet weist so zwar eine gewisse technische Widerständigkeit auf, bleibt aber als Teil globaler Sozialstruktur gestaltbar. Den Staaten steht so theoretisch auch die Möglichkeit offen, grundlegende Funktionsweisen

30 Dass Technik selbst zum Akteur wird, ist theoretisch möglich (Stichwort künstliche Intelligenz), bspw. dann wenn Algorithmen an den internationalen Finanzmärkten auf die Aktionen anderer Algorithmen reagieren und damit etwa zu reellen Kursverlusten führen.

der technischen Infrastruktur zu verändern, um ihre neu definierten Rollen auszufüllen. Zwischen den Extrempositionen unilateraler (ggf. auch multilateraler) Isolation und koordinationsaufwendiger grundlegender technischer Umstrukturierung spannt sich ein weites Handlungsfeld zur politischen Gestaltung des Internets. In der Forschung zur Internet Governance werden Tendenzen zur (partiellen) staatlichen Isolation und damit Prozesse der Fragmentierung des Internets besonders häufig thematisiert (Demchak und Dombrowski, 2011; Lazanski, 2013; M. Mueller, 2017). Aber auch Debatten über die zentralen Funktionsweisen (Protokolle) des Internets lassen sich aus dieser Perspektive als Auseinandersetzung mit den technischen Widerständigkeiten des Netzes bzw. deren Veränderung verstehen. Sie sind Ausdruck des Bemühens, Entscheidungen, die hauptsächlich die Forschergemeinde in den USA in der Frühphase des Internets der Struktur noch unilateral einschreiben konnten, zu modifizieren und so das Netz der eigenen (domestischen) Sozialstruktur kompatibler zu machen. Veränderungen der grundlegenden Internetinfrastruktur wirken dabei häufig sowohl auf die domestische als auch internationale Sozialstruktur. Maßnahmen wie die Regulierung von VPN-Tunneln in China zielen zwar auf die domestische Sphäre, beeinflussen daneben aber auch internationale Belange (in diesem Fall die Kommunikation global operierender Konzerne). Auch die Debatten um neue Verschlüsselungsprotokolle lassen sich so als Auseinandersetzung und kreative Umdeutung des Mediums zur Erfüllung der staatlichen Beschützer-Rolle sehen (bspw. wenn es darum geht »Hintertüren« in TLS 1.3 einzuführen (heise.de, 2018b)).

Der Exkurs in die Techniksoziologie hat verdeutlicht, dass das Verhältnis von Politik und Technik durch die Theorien der IB bisher nicht angemessen beleuchtet worden ist und dass ein Verständnis von Technik als Teil der Sozialstruktur dabei helfen kann, die empirischen Phänomene besser zu verstehen. Diese Studie sieht im Internet daher ein Teil der (globalen) Sozialstruktur, die in Interaktion zwischen verschiedenen Akteuren aufgelöst, umgestaltet oder fortgeführt werden kann. Die Cybersicherheitspolitik ist für diese Auseinandersetzung eine der entscheidenden Arenen.

# 3. Methodik und Konzeption

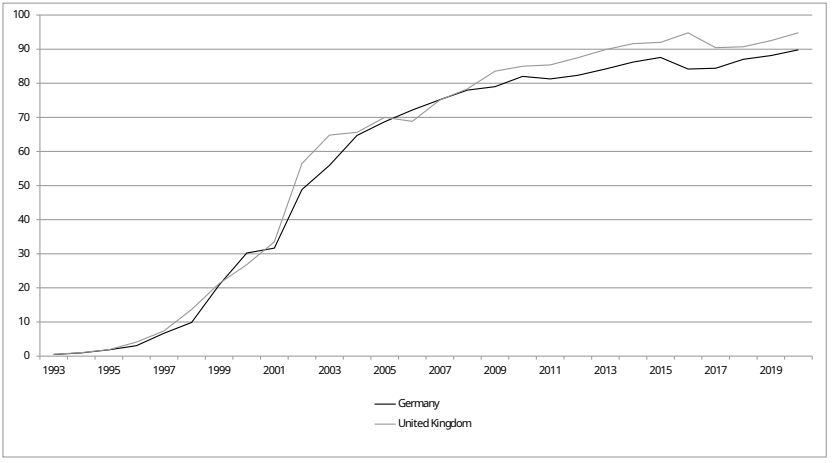
Bei der vorliegenden Studie handelt es sich um eine diachronisch-ländervergleichende Analyse, die die Entwicklung der Cybersicherheitspolitiken in zwei Untersuchungsstaaten nachzeichnen und verstehen will. Im Folgenden wird das entsprechende methodische Vorgehen vorgestellt und die grundlegenden Konzepte erläutert. Das Kapitel adressiert dazu vier Themenkomplexe. Zunächst werden die Argumente erörtert, die zur Auswahl der beiden Untersuchungsstaaten, der analysierten Dokumente und zur Festlegung des Untersuchungszeitraums geführt haben. Der zweite Abschnitt befasst sich mit dem eigentlichen Analyseprozess des empirischen Materials und orientiert sich an der Grounded-Theory-Methodologie in Verbindung mit Practice Tracing. Anschließend werden die drei Rollen Beschützer, Wohlstandsmaximierer und Garant liberaler Grundrechte sowie die drei Analysebereiche kurz eingeführt. Abschließend werden die forschungsleitenden Annahmen expliziert, die sich aus den theoretisch-methodischen Überlegungen ergeben.

## 3.1 Auswahlentscheidungen: Fälle, Quellen und Untersuchungszeitraum

Deutschland und das Vereinigte Königreich wurden als Vergleichsfälle gewählt, da sie sich durch viele Gemeinsamkeiten auszeichnen, vermutlich aber dennoch unterschiedliche Cybersicherheitspolitiken verfolgen. Bei den Untersuchungsstaaten handelt es sich um zwei westeuropäische parlamentarische Demokratien, die sich weiterhin durch (überschneidende) Mitgliedschaften in zahlreichen internationalen Organisationen auszeichnen (bspw. in der OSZE, der EU[1], der NATO und dem Europarat). Neben diesen institutionellen Gemeinsamkeiten, bestehen

1 Auch wenn der britische Austritt aus der EU mit dem Referendum vom 23. Juni 2016 beschlossen wurde, war Großbritannien doch bis zum Ende des Untersuchungszeitraums Mitglied der EU.

*Abbildung 2: Entwicklung der Internetnutzerzahlen in Deutschland und Großbritannien 1993-2017 (in Prozent der Bevölkerung), Quelle: World Bank (2019)*




auch mit Blick auf die (ökonomische) Nutzung und die gesellschaftliche Einbettung des Internets kaum Unterschiede. 2017 verfügten 93% aller Haushalte in Deutschland über einen Internetanschluss, im Vereinigten Königreich waren es 94%. Mehr als dreiviertel aller BürgerInnen in beiden Staaten nutzen das Netz täglich (Eurostat, 2018a). Die zunehmende gesellschaftliche Integration des Netzes ist dabei in beiden Staaten über den gesamten Untersuchungszeitraum parallel verlaufen (s. Abbildung 2). Auch die wirtschaftliche Nutzung ist nahezu identisch: 2017 nutzten 95% aller Unternehmen im Vereinigten Königreich das Internet, in Deutschland waren es 97% (Eurostat, 2018b). Weiterhin gibt es in beiden Staaten wichtige Internetknoten (LINX in London sowie DE-CIX in Frankfurt am Main), die gemessen am Datendurchsatz zu den größten weltweit zählen. Auch in einschlägigen Indizes liegen die beiden Untersuchungsstaaten oft nahe beisammen. So sind Deutschland und Großbritannien bspw. im 2011 erstellten Cyber Power Index mit den Rängen 4 und 1 Teil der internationalen Spitzengruppe (Booz Allen Hamilton, 2011, S. 4). Damit sind beide Staaten auch bei der Ausgestaltung der internationalen Cybersicherheitsordnung von Bedeutung.

Zum Verständnis von variantem Verhalten in der Cybersicherheitspolitik, kann folglich aber nicht auf materielle Differenzen (bspw. in der Abhängigkeiten von IT) rekurriert werden. Positivistisch gesprochen folgt die Fallauswahl damit der Logik der »similar systems with different outcomes« bei der Fälle mit möglichst ähnlich ausgeprägten unabhängigen Variablen betrachtet werden, die

sich aber durch unterschiedlich ausgeprägte abhängige Variablen voneinander unterscheiden (Jahn, 2015, S. 64f.).[2]

Wie bereits im vorangegangen Kapitel dargelegt, ist die These, dass sich die Cybersicherheitspolitiken der beiden Untersuchungsstaaten trotz der zahlreichen Gemeinsamkeiten unterscheiden, eine plausible Ausgangsannahme. Empirische Analysen zu den Außen- und Sicherheitspolitiken beider Staaten haben signifikante Unterschiede offengelegt (Cornish, 2013; Harnisch, 2013; Junk und Daase, 2013; B. White, 2013). Die vorliegende Studie untersucht daher, ob bzw. inwiefern sich Differenzen auch in einem neuen sicherheitspolitischen Handlungsfeld finden und durch welche innen- und außenpolitischen Interaktionen die Politiken ermöglicht werden.

Die Wahl des Untersuchungszeitraums richtet sich daher nach dem Entstehen bzw. dem gesellschaftlichen Relevantwerden dieses neuen Interaktionsfeldes. Er beginnt 1995 und endet mit dem Jahr 2019. 1995 wurde als Ausgangspunkt der Analyse gewählt, da in diesem Jahr in beiden Staaten die gesellschaftliche Internetnutzung erstmals die 1%-Schwelle überschritten hat und in den Folgejahren rasant zugenommen hat. Damit wurde das Netz Mitte der 1990er Jahre auch für Privatpersonen nutzbar und Sicherheitsprobleme, die mit dem Netz verbunden waren, konnten zunehmend zu gesellschaftlichen Problem werden, die auch politisch reguliert werden mussten.[3] Die Interaktionsdichte ist in den Folgejahren ebenfalls gestiegen.

Um die Cybersicherheitspolitiken der beiden Untersuchungsstaaten zu analysieren, wurden zunächst die für dieses Politikfeld zentralen Akteure in beiden Untersuchungsstaaten identifiziert. Da die Rollen der Regierungen im Mittelpunkt des Forschungsinteresses stehen, bildeten die ersten Cybersicherheitsstrategien der beiden Untersuchungsstaaten den Startpunkt zur Erschließung der Akteure (Bundesministerium des Innern, 2011; Cabinet Office, 2009). Diese Dokumente sind besonders geeignet, die komplexe Konstellation aus Sicht der Exekutiven zu erschließen, da in diesen Strategien das Thema erstmals ganzheitlich betrachtet wurde und die unterschiedlichen, zuvor ergriffenen, Maßnahmen zusammenführend skizziert wurden. Die Dokumente legen damit nicht nur die relevanten Akteure aufseiten der Regierungen (Ministerien und Behörden) offen, sondern

2 Die Analyse folgt dieser Logik aber freilich ohne den Anspruch aus der Analyse allgemeingültige Gesetzmäßigkeiten im Sinne eines nomologischen Wissenschaftsverständnisses offenzulegen, sondern mit dem Ziel die Politiken und damit auch die vermuteten Unterschiede zu verstehen (s. Kapitel 2 und 3.2).

3 Es gab zwar in beiden Staaten bereits vor diesem Zeitpunkt Regelungen zum Umgang mit Computerkriminalität, diese richteten sich aber auf Wirtschaftskriminalität und waren noch nicht auf weiträumig vernetzte Systeme zugeschnitten.

nehmen auch Bezug auf parlamentarische Einflüsse (bspw. Kontrollbefugnisse) und legen Schnittstellen zu nichtstaatlichen Akteure offen.

Sie geben ferner erste Aufschlüsse darüber, welche Funktionen die Exekutive in der Cybersicherheitspolitik übernimmt. Ausgehend von diesen Dokumenten wurde dann der weitere Untersuchungszeitraum, sowohl vor als auch nach deren Veröffentlichung, durch die Sichtung weiterer Dokumente schrittweise erschlossen. Auf diesem Weg konnte identifiziert werden, welche signifikanten Anderen die Cybersicherheitspolitik beider Staaten beeinflussen bzw. dies versuchen. Weiterhin wurden auf diesem Weg zusätzliche Dokumente anderer Akteure integriert, die wiederum neue Akteure offenlegten. Das Resultat dieser ersten Erschließung der Akteure ist in Tabelle 1 abgebildet und folgte der interpretativ-offenen Vorgehensweise der Grounded-Theory-Methodologie (s. Abschnitt 3.2).[4]

*Tabelle 1: Institutionen und Akteure, Quelle: Eigene Darstellung*

| | **Deutschland** | **United Kingdom** |
|---|---|---|
| **Exekutive** | Bundesregierung | HM Government |
| Ministerien | Bundeskanzleramt, Bundesministerium des Innern, Bundesministerium der Verteidigung, Auswärtiges Amt, Bundesministerium der Justiz, Bundesministerium für Verkehr und digitale Infrastruktur, Bundesministerium für Wirtschaft | Cabinet Office, Home Office, Ministry of Defence, Foreign Commonwealtch Office, Department for Business, Energy and Industrial Strategy |
| Behörden | Bundesamt für Sicherheit in der Informationstechnik, Bundesbeauftragter für den Datenschutz, Nationales Cyber-Abwehrzentrum | Office of Cyber Security and Information Assurance, Investigatory Powers Commissioner, National Cyber Security Centre |
| Polizeien | Bundeskriminalamt | National Crime Agency |
| Nachrichtendienste | Bundesnachrichtendienst | Government Communications Headquarters (GCHQ) |
| Streitkräfte | Bundeswehr | British Armed Forces |

4 Auch wenn einige Unterschiede bestehen (bspw. die Mitgliedschaft im Nachrichtendienstverbund 5-Eyes), ergeben sich mit Blick auf die internationalen signifikanten Anderen zahlreiche Überschneidungen. Daher wird an dieser Stelle auf eine tabellarische Darstellung verzichtet. Weiterhin wurden Institutionen im Verlauf des Untersuchungszeitraumes umbenannt, restrukturiert oder neugegründet. Die Darstellung zeigt Denominationen Stand Ende 2019.

| | | |
|---|---|---|
| **Legislative**<br>Ausschüsse und Gremien | Bundestag, Bundesrat<br>Auswärtiger Ausschuss, Innenausschuss, Verteidigungsausschuss, Wirtschaftsausschuss, Enquete-Kommission Internet und digitale Gesellschaft, Parlamentarisches Kontrollgremium, G 10 Kommission, Ausschuss Digitale Agenda, NSA-Untersuchungsausschuss | House of Commons, House of Lords<br>Foreign Affairs Committee, Home Affairs Committee, Defence Committee, Business Innovation and Skills Committee, Science and Technology Committee, Intelligence and Security Committee, National Security Strategy Committee |
| **Judikative** | Bundesverfassungsgericht, Bundesgerichtshof | High Court of Justice of England and Wales, The Supreme Court, Investigatory Powers Tribunal |
| **Nichtstaatliche Akteure** | | |
| Zivilgesellschaft | Chaos Computer Club, Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V., Gesellschaft für Informatik e.V., Gesellschaft für Freiheitsrechte e.V., Humanistische Union e.V., Reporter ohne Grenzen e.V. | Amnesty International, Article 19, Privacy International, Open Rights Group, Big Brother Watch, English PEN, Liberty, Electronic Frontier Foundation, Access Now, JUSTICE, Rights Watch UK, Human Rights Watch |
| Unternehmen und Branchenverbände | BITKOM, eco, DE-CIX, Deutsche Telekom, SAP | GreenNet, British Telecommunications, techUK |

Diesem Schritt folgte die Erhebung der relevanten Dokumente direkt bei den identifizierten Akteuren. Dazu wurde auf die entsprechenden Internetseiten zurückgegriffen und dort systematisch nach den Begriffen IT-Sicherheit bzw. Cybersicherheit gesucht und die resultierenden Dokumente dem Untersuchungskorpus hinzugefügt.[5] Diese Datengrundlage wurde dann um weitere Quellen ergänzt, die im Analyseprozess gefunden wurden und für die Interaktionen der Akteure bedeutsam waren. Diese Datengrundlage enthält folglich Reden, Strategiedokumente, Gesetzesvorhaben, Stellungnahmen, Berichte, Parlamentsdebatten, Gutachten, Pressemitteilungen und Gerichtsurteile. Sie ermöglicht damit die Rekonstruktion der wesentlichen Interaktionen zwischen Exekutive, Legislative, Judikative und nichtstaatlichen Akteuren.

Diese, von den Akteuren selbst generierten, Quellen dienen dazu, die Interaktionen zu rekonstruieren und so einerseits die emergente Sozialstruktur zu erfassen und zusätzlich, der zweiten Prämisse Blumers folgend, die Bedeutungszuschreibung zu analysieren. Allerdings lässt sich Praxis nicht nur aus den

5 Im Englischen wurden die Begriffe IT-security und cybersecurity verwendet. Um unterschiedliche Schreibweisen zu integrieren, wurden auch die folgenden Terme gesucht: D - Cyber Sicherheit, Cyber-Sicherheit; UK - cybersecurity, cyber security, IT security. Dokumente, die ausschließlich technische Bezüge bspw. Anleitungen zur Implementierung bestimmter Standards enthalten, wurden verworfen.

Dokumenten der Akteure herausdestillieren. Daher haben pragmatistisch arbeitende WissenschaftlerInnen ihre Untersuchungskorpora oft durch weitere Quellen (meist Medienbeiträge und wissenschaftliche Literatur) ergänzt (M.-O. Baumann, 2014, S. 89), denn nicht jeder Interaktion korrespondiert ein (zugänglicher) textförmiger Beleg der Akteure. Diese ergänzenden Daten können zwar nur mittelbar zur Interpretation der Bedeutungszuschreibung durch die handelnden Akteure beitragen, sie legen aber dennoch Interaktionen offen und dienen so als komplementäres Element zu anderen Quellen. Nicht zuletzt hierin liegt ein Vorteil praxisorientierter Ansätze, die auch durch Berichte Dritter Erkenntnis über die Interaktionspraktiken gewinnen können. Im Kontext dieser Analyse ist diese flankierende Ergänzung durch Medienbeiträge besonders bedeutend, da die Studie in mindestens zwei Teilen der Untersuchung (den Bereichen der Nachrichtendienste und der Militärs) mit der Problematik staatlicher Geheimhaltung umgehen muss. Die Veröffentlichungen investigativ arbeitender JournalistInnen haben, nicht nur im Zuge der Snowden-Enthüllungen, die Erkenntnisse über die staatlichen Cybersicherheitspolitiken signifikant erweitert. Auf ihrer Grundlage wurden zuvor geheime Politiken publik und die intensive (öffentliche) Interaktion zwischen den beteiligten Akteuren ermöglicht. Die jeweiligen Interaktionskontexte werden daher durch Berichte entsprechender Medien vervollständigt.[6] Auf diesem Weg wurden aus den politischen Systemen (Regierung, Judikative, Parlament) für Deutschland 110 und für Großbritannien 131 Dokumente erhoben. Diese wurden durch Quellen von nichtstaatlichen Akteuren, internationalen Organisationen sowie Medien ergänzt. Insgesamt umfasst der Korpus mehr als 350 Dokumente.

Um Untersuchungszeiträume möglichst repräsentativ abzudecken, wird meist eine zeitliche Gleichverteilung der Quellen angestrebt (Roos, 2010, S. 57 bzw. 80f.). Für diese Untersuchung konnte dieses Ziel jedoch nicht erreicht werden, da das

6 Dabei wurde auf Beiträge in folgenden Medien zurückgegriffen: Der Spiegel, Süddeutsche Zeitung, Die Zeit, Die Welt, The Guardian, The Telegraph, The Independent und The Times. Ebenfalls berücksichtigt wurden Berichte von speziell mit IT-Sicherheit befassten Medien wie heise.de oder wired.com. Daten von Enthüllungsplattformen wie Wikileaks wurden nur dann beachtet, wenn sie durch relevante Akteure aufgegriffen wurden oder in den genannten landesweiten Medien thematisiert wurden. Dies liegt einerseits in der praxisorientierten Forschungsperspektive begründet. Solange die Handelnden diese Informationen nicht aufgreifen (das bedeutet nicht zwingend einen expliziten Bezug, sondern kann auch durch die Problematisierung einer, in geleakten Dokumenten, erwähnten Praxis erfolgen) und weiterhin interagieren als gäbe es diese Dokumente nicht, solange haben sie auch keinen Einfluss auf die (sichtbare) Interaktion. Andererseits ist der Umgang mit geleakten Informationen problembehaftet, da deren Authentizität nur schwer verlässlich verifizierbar ist. Die Snowden-Dokumente wurden ebenfalls nicht als Primärquellen hinzugezogen, da diese quellenkritisch besonders problematisch sind (s. Stellungnahme Thomas Rid (Deutscher Bundestag, 2016a, S. 36)).

neue Politikfeld zu Beginn des Untersuchungszeitraumes noch relativ wenig Beachtung gefunden hat. Erst im Zeitverlauf und mit zunehmender Bedeutung des Netzes ist auch die Interaktionsdichte gestiegen. Sichtbarer Ausdruck der gewachsenen Bedeutung sind die Cybersicherheitsstrategien, die beide Regierungen Ende der 2000er bzw. zu Beginn der 2010er Jahre formuliert haben. Dementsprechend entfällt die Mehrheit der analysierten Dokumente auf den Zeitraum nach 2010, in dem auch die Entwicklung der Cybersicherheitspolitik erheblich an Dynamik gewonnen hat.

## 3.2 Die interpretative Analyse: Grounded-Theory-Methodologie und Practice Tracing

Wie andere pragmatistisch inspirierte Studien, ist auch die vorliegende Untersuchung durch ein rekonstruktives, erschließend-interpretatives Vorgehen geprägt (Franke, 2013; Franke und Roos, 2017; Herborth, 2017). Um aus dem Datenmaterial Erkenntnisse zu gewinnen, wurde ein zweistufiges Analyseverfahren gewählt, das in der ersten Phase an der Grounded-Theory-Methodologie (Strauss und Corbin, 1996) orientiert ist und in der zweiten Phase auf Practice Tracing (Pouliot, 2017) zurückgreift. Beiden Ansätzen ist gemeinsam, dass es nicht darum geht, kausale Gesetzmäßigkeiten zu finden, sondern durch eine in der Empirie verankerte, interpretative Analyse die Interaktionspraxis in den jeweiligen Kontexten offenzulegen und damit das Verständnis der Politiken zu ermöglichen. Die Grounded-Theory-Methodologie wurde angewendet, um die generischen Rollen beider Regierungen sowie die zentralen Interaktionsfelder zu identifizieren. Die Vorgehensweise wurde also dazu genutzt, zentrale Konzepte aus der Empirie zu rekonstruieren und damit die Grundlagen zu etablieren, die dann die weitere Analyse ermöglichten. Practice Tracing diente als konstitutiv-logische Variante des Process Tracing und erlaubt es, die Entwicklung der Cybersicherheitspolitiken systematisch nachzuvollziehen und die Rollen zueinander in Beziehung zu setzen. Beide Ansätze sind dabei wesentlich durch den US-amerikanischen Pragmatismus geprägt.

Eine rekonstruktionslogische Vorgehensweise, die sich an der Methodologie der Grounded-Theory orientiert, zeichnet sich dadurch aus, dass »die Forschenden ihren Gegenständen mit einer offenen Grundhaltung [begegnen; Anm. d. Verf.] und […] eine hohe Bereitschaft [zeigen; Anm. d. Verf.], sich von den Ergebnissen ihrer Rekonstruktionen überraschen zu lassen« (Franke und Roos, 2017, S. 620). Für diese Studie bedeutet das konkret, dass nicht mit vordefinierten Rollen in die Analyse gestartet wurde, sondern, dass diese in einem ersten empirischen Interpretationsschritt aus den Daten gewonnen wurden. Im ersten Zugang wurden daher die Rollen identifiziert, die die Regierungen in der Cybersicher-

heitspolitik regelmäßig übernehmen bzw. die Rollen, die die Politiken regelmäßig beeinflussen. Ferner ging es darum, die wichtigen Handlungskontexte zu finden, in denen sich Cybersicherheitspolitik entfaltet. Dabei mussten die Konzepte so abstrakt sein, dass sie zur Analyse beider Untersuchungsstaaten nützlich waren und folglich den Vergleich ermöglichten. Dieser Schritt folgte den Prinzipien der Grounded-Thoery-Methodologie, die besonderen Wert auf die offene, gegenstandsbezogene Erschließung der empirischen Daten legt: »In this method, data collection, analysis, and eventual theory stand in close relationship to one another« (Strauss und Corbin, 1998, S. 12). Konkret nutzte die Analyse hierzu das offene Kodieren:

> »Das offene Kodieren zielt darauf ab, den Sinn der einzelnen Handlungs- bzw. Textsequenzen zu rekonstruieren und die sich darin ausdrückenden Handlungsregeln mit einem Code zu versehen. Hierbei werden die verschiedenen Handlungsregeln gewissermaßen flexibel inventarisiert und der Forscher erhält im Laufe des offenen Kodierens einen immer kompletteren Überblick über die im Material sich ausdrückenden Handlungsregeln.« (Franke und Roos, 2017, S. 634)

In diesem Prozess, der stets den gegenwärtigen Erkenntnisstand kritisch reflektiert und versucht die Analyse gezielt fortzuentwickeln, wurden die Quellen nach den Rollen und Interaktionsräumen (s. Abschnitt 3.3) durchsucht. Die Quellenwahl wurde dabei so gestaltet, dass zunächst möglichst viele verschiedene Akteure und Handlungskontexte berücksichtigt wurden. Dann wurden systematisch weitere Quellen einbezogen, die zielgerichtet die weitere Schärfung der Konzepte erlaubten. Diese Analyse wurde beendet, als die zusätzliche Aufnahme von Quellen keine weiteren Erkenntnisse mehr lieferte und damit der Punkt der Sättigung erreicht war: »A category is considered saturated when no new information seems to emerge during coding, that is, when no new properties, dimensions, conditions, actions/interactions, or consequences are seen in the data« (Strauss und Corbin, 1998, S. 136).

Durch diese erste interpretative Sichtung des empirischen Materials konnten drei generische Rollen identifiziert werden, die die Regierungen beider Untersuchungsstaaten in der Cybersicherheitspolitik regelmäßig übernehmen bzw. die die Cybersicherheitspolitiken beeinflussen. Es sind dies: Beschützer, Wohlstandsmaximierer und Garant liberaler Grundrechte. Ferner wurden in diesem Analyseschritt drei Handlungskontexte offengelegt, die für die Cybersicherheitspolitiken zentral sind. Sowohl die Rollen als auch die Handlungskontexte werden im folgenden Abschnitt 3.3 kurz eingeführt.

Nachdem das offene Kodieren verwendet wurde, um das »konzeptionelle Inventar« der Untersuchung zu generieren, wurde im Anschluss daran auf Practice

Tracing zurückgegriffen, um die wesentlichen Interaktionen zwischen den Akteuren nachzuvollziehen. Da der Analysefokus auf sozialer Praxis liegt, ist die Methode gut für eine rollentheoretische Untersuchung geeignet. Vincent Pouliot konzipiert Practice Tracing dabei als eine interpretative Variante des Process Tracing (Bennett und Checkel, 2017; Collier, 2011), die auch mit nicht-positivistischen ontologischen und epistemologischen Annahmen vereinbar ist und auch damit gut zur rollentheoretischen Ausrichtung dieser Untersuchung passt (Pouliot, 2017, S. 239).

Der Ansatz zielt einerseits darauf, durch eine dichte Beschreibung der empirischen Ereignisse, die Prozesse zu rekonstruieren, die Politiken ermöglichen, um dann hieran anknüpfend »Mechanismen« zu identifizieren, die abstrakt genug sind, auch auf andere Fälle anwendbar zu sein. Mechanismen sind dabei abstrakte Konzepte die erst im Forschungsprozess generiert werden und dabei helfen Vergleichbarkeit herzustellen (ebd., S. 238f.).

> »[…] social mechanisms are abstracted away from context: their whole point is to depart from reality, not to match it. As such, the mechanisms coined by researchers do not have empirical referents that would make them true or false. Instead of testing theoretical constructs, then, one should show their heuristic usefeulness […] Mechanisms refer to analytical classes of ways of doing things that the analyst deems worthwhile to group together in view of cross-case analysis.« (Ebd., S. 252f.)

Die mittels Grounded-Theory-Methodologie identifizierten drei Rollen lassen sich folglich schon als Mechanismen im Sinne des Practice Tracing verstehen, also als Konzepte, die auch von den Fällen abstrahiert werden können und beim Verständnis anderer Cybersicherheitspolitiken potenziell nützlich sein können.[7] Practice Tracing wurde, hierauf aufbauend, dazu verwendet, die Interaktionen in ihren Verläufen schrittweise nachzuvollziehen und ein Verständnis der Entwicklung der Cybersicherheitspolitiken zu ermöglichen.

Bei der Untersuchung der konkreten Interaktionsprozesse wechselt die/der Forschende beim Practice Tracing, wie auch in der Grounded-Theory-Methodologie, beständig zwischen Induktion, Interpretation und Abstraktion, um die Einflüsse offenzulegen, die die Politiken ermöglichen: »Practice tracing is thus an

7 Das bedeutet nicht, dass sie immer in gleicher Weise wirken. Vielmehr entsteht die jeweilige Wirkung immer erst in der konkreten Interaktion. Die Annahme, dass Regierungen Schutzfunktionen ausfüllen und versuchen das ökonomische Wohlergehen zu gewährleisten, ist aber auch für andere Fälle plausibel. Für Demokratien ist es ferner plausibel anzunehmen, dass sie die Freiheitsrechte schützen (Wobei bei einer Entwicklung hin zu einer Autokratie diese Funktionsübernahme aufgegeben werden kann. Daher scheint dieser Teil nur für etablierte Demokratien plausibel vgl. Kapitel 2).

abductive methodology, based on the joining together of emipirics and analytics« (Pouliot, 2017, S. 252). Ganz im Sinne der pragmatistischen Perspektive wird die erreichte Erkenntnis dabei stets als fallibel und offen für Herausforderungen verstanden »[…] because configurations of practices are so complex and shifting […] one can never claim to have found the one causal practice« (ebd., S. 259). Mittels Practice Tracing wurde für jeden der Untersuchungsbereiche ein möglichst plausibler Interaktionsverlauf rekonstruiert (s. Kapitel 4). Ferner soll durch diese Methode untersucht werden, ob es in diesen Interaktionsverläufen weitere Gemeinsamkeiten oder Unterschiede zwischen den Fällen gibt, die den konkreten Umgang mit dem neuen Problemfeld in beiden Staaten prägen.

## 3.3 Rollen und Handlungskontexte

Da die Arbeit einen Beitrag zur sicherheitspolitischen Forschung liefern soll, steht die Rolle als Beschützer im Zentrum des Analyseinteresses. Die Materialauswahl hat bereits verdeutlicht, dass das empirische Material so gewählt wurde, dass sicherheitspolitische exekutive Funktionsübernahmen sowie deren Herausforderung strukturiert nachvollzogen werden können. Andere Rollen, die die Regierungen ebenfalls übernommen haben, bspw. um das Netz zur Steigerung des nationalen Wohlstands zu nutzen, scheinen nur an den Stellen auf, an denen Berührungspunkte zur Beschützer-Rolle bestehen. Dies bedeutet nicht, dass diese anderen Rollen empirisch weniger bedeutend sind. Der Forschungszuschnitt und die analytische Engführung ergibt sich vielmehr aus dem sicherheitspolitischen Erkenntnisinteresse. Wenn im Folgenden die drei Rollen beschrieben werden, die für die britische und deutsche Cybersicherheitspolitik besonders relevant sind, ist damit folglich nicht impliziert, dass die Arbeit alle drei empirisch in gleichrangiger Weise eingehend analysiert. Vielmehr geht es darum zu untersuchen, wie die Beschützer-Rolle ausgestaltet wurde. Dies erfolgte aber teilweise unter Verweis auf andere Rollenübernahmen. Diese sind daher für die Analyse nicht gänzlich ausblendbar und für das Verständnis der Politikentwicklung hilfreich.

Die Regierungen haben bereits mit der Öffnung des Internets begonnen, den Schutzanspruch für ihre Bevölkerungen auch online gegen neue Gefahren durchzusetzen. Die Beschützer-Rolle zeichnet sich in der Cybersicherheitspolitik durch eine doppelte Funktionsübernahme aus: Erstens fallen hierunter Maßnahmen zur Gewährleistung von Sicherheit, die durch Verletzung der Cybersicherheit »erkauft« werden. Konkret geht es also um Situationen, in denen der Staat IT-Sicherheit bricht, um sicherheitspolitisch handlungsfähig zu bleiben oder zu werden. Dies kann im Rahmen der Strafverfolgung bspw. zum digitalen Abhören von Kriminellen notwendig sein. Zweitens umfasst die Beschützer-Rolle Definitionen und Sanktionen für unangemessene Unterminierungen von IT-Sicherheit

im Cyberspace. Hier wird festgelegt, was als akzeptables Verhalten im Netz angesehen wird. In der Beschützer-Rolle tritt eines der einleitend skizzierten Dilemmata der Cybersicherheitspolitik offen zutage (s. Kapitel 1): Regierungen unterminieren und fördern Cybersicherheit in unterschiedlichen sicherheitspolitischen Handlungskontexten (Nissenbaum, 2005).

Wann immer die Regierungen Funktionen mit Bezug zu einer dieser beiden Ebenen übernehmen oder delegieren, wird das folglich als Beschützer-Rolle bezeichnet. Wenn die Regierungen die Referenz der Rolle, den Regelungsbereich, die Befugnisse zur Erreichung der Schutzziele oder ein Delegationsverhältnis verändern, wird das als Wandel der Rolle verstanden. Genau genommen hat die Beschützer-Rolle zwei Referenzen: Eine nimmt Bezug auf das zu schützenswerte Gut (Schutz für wen/was?), die zweite weist auf den abzuwehrenden Anderen (Schutz vor wem?). Diese beiden Referenzen sind theoretisch veränderbar.

Oft kommt es bei Veränderungen der Beschützer-Rolle zu Wechselwirkungen mit den beiden weiteren Rollen, die daher auch in der empirischen Analyse erscheinen. Eine Wechselwirkung ergibt sich dabei im Kontext der ökonomischen Nutzung des Netzes. Die globale Vernetzung und die Möglichkeit praktisch verzögerungsfrei Informationen auszutauschen, hat das Internet rasch zu einem bedeutenden Wirtschaftsfaktor gemacht, der entscheidenden Einfluss auf gesellschaftlichen Wohlstand haben kann. Die Rolle Wohlstandsmaximierer zielt auf den Erhalt, den Ausbau bzw. die Wiederherstellung der ökonomischen Leistungsfähigkeit der Gesellschaft. Sicherheitspolitische Regulationen können diesen neuen Wirtschaftsraum beeinflussen. Die zweite Funktion, die häufig Verbindungen mit der Beschützer-Rolle aufweist, bezieht sich auf die Wahrung von Grundrechten bzw. der demokratischen Ordnung (bspw. der Gewaltenteilung). Maßnahmen der Cybersicherheitspolitik werfen hier bspw. die Frage nach dem Schutz der Privatsphäre im digitalen Raum auf oder beziehen sich auf die Kontrolle der Exekutive. Bereits mit dem Aufkommen der neuen Technologie waren Hoffnungen auf eine erweiterte demokratische Teilhabe und eine Schwächung von autoritären Regimen verbunden (s. Kapitel 2). Demokratische Regierungen sehen sich daher in der Pflicht die demokratischen Freiheiten auch online zu schützen oder gar zu verbreiten. Die Rolle als Garant liberaler Grundrechte umfasst folglich Funktionsübernahmen, die darauf zielen liberale Freiheits-, Abwehr- und Partizipationsrechte zu garantieren bzw. diese auszuweiten oder wiederherzustellen sowie die Gewährleistung der demokratischen Ordnung.

Mit diesen Rollen sind damit beständig an die Regierungen herangetragene Erwartungen verbunden, die diese zum Ausgleich bringen muss, um stabile domestische wie internationale Beziehungen zwischen den Handelnden zu etablieren bzw. aufrechtzuerhalten.

*Tabelle 2: Definition der drei Rollen, Quelle: Eigene Darstellung*

| Rolle | Kurzbeschreibung |
|---|---|
| Beschützer | Funktionsübernahmen, die auf den Ausbau, Erhalt oder ggf. die Wiederherstellung von Sicherheit zielen und IT-Sicherheit unterminieren sowie Funktionsübernahmen, die auf den Ausbau, Erhalt oder ggf. die Wiederherstellung von Cybersicherheit zielen. |
| Wohlstandsmaximierer | Funktionsübernahmen, die auf den Ausbau, Erhalt oder ggf. die Wiederherstellung ökonomischer Leistungsfähigkeit zielen. |
| Garant liberaler Grundrechte | Funktionsübernahmen, die auf den Ausbau, Erhalt oder ggf. die Wiederherstellung von Partizipations-, Abwehr- und Freiheitsrechten zielen. |

Zwischen diesen generischen Rollen kann es zu unterschiedlichen Wechselwirkungen kommen.[8] Wie im Theoriekapitel bereits angeklungen ist, differenziert die Analyse drei verschiedene Wirkungen, die in der empirischen Analyse bedeutend sein können. Erstens können die unterschiedlichen Funktionsübernahmen dazu führen dass die Beschützer-Rolle erweitert wird – katalytische Wirkung. Sie liegt vor, wenn der Regelungsbereich oder die Regelungstiefe der Beschützer-Rolle durch Bezug zu anderen Rollen ausgebaut wird. Dies kann bspw. dann der Fall sein, wenn durch zunehmende Cyberangriffe Firmen wachsende Verluste erleiden zu deren Vermeidung dann sicherheitspolitische Maßnahmen ergriffen werden. Zweitens kann die Beschützer-Rolle durch Prozesse der Rollenkontestation eingeschränkt werden – beschränkende Wirkung. Sie liegt vor, wenn der Regelungsbereich oder die Regelungstiefe der Beschützer-Rolle verringert wird. Das kann bspw. der Fall sein, wenn weitreichende staatliche Eingriffe in die Verschlüsselung Geschäftsgrundlagen unterminieren und daher eine restriktive, sicherheitspolitisch gewünschte, Regulierung unterbleibt. Die dritte theoretische Möglichkeit ist folglich, dass es entweder keine Beeinflussung gibt, bzw. dass diese indifferent oder ambivalent ist. Zusätzlich kann auch das historische Selbst katalytisch oder beschränkend wirken. Wie die Interaktion verläuft und welche Dynamiken letztlich auftreten, kann nur in der konkreten Handlungssituation interpretiert werden.

Die Entscheidung darüber, welche Arenen für die Cybersicherheitspolitik zentral sind, wurde ebenfalls nicht ex ante getroffen, sondern ist Ergebnis der ersten Analyse. Die Unterscheidung von drei Handlungsräumen dient dem Ziel, den systematischen Vergleich beider Fälle zu strukturieren. Sie folgt gleichzeitig einer rollentheoretischen Logik, da die Interaktionen in den Analysebereichen aufgrund

8 Das bedeutet nicht, dass die Rollen selbst diese Wechselwirkungen entfalten, sondern, sie entstehen durch die Interaktion der Handelnden (s. Kapitel 2).

der verschiedenen Handelnden unterschiedlich verlaufen können. Die Differenzierung fußt dabei auf der institutionellen Ausgestaltung des Interaktionsrahmens. Bei der Analyse wurde deutlich, dass die Regierungen Cybersicherheitspolitik weitgehend entlang tradierter sicherheitspolitischer Institutionen gestaltet haben.

Im ersten Interaktionskontext stehen daher die Kompetenzen der Strafermittlungsbehörden im Mittelpunkt des Interesses, im zweiten geht es um die Nutzung des Internets durch die Geheimdienste und im dritten um die militärische Dimension des neuen Handlungsraumes. In diesen Bereichen haben die Regierungen ihre Beschützer-Rollen im Verlauf des Untersuchungszeitraums entwickelt. Die Interaktionskontexte zeichnen sich sowohl innen- als auch außenpolitisch durch unterschiedliche Akteurskonstellationen aus. Innenpolitisch stehen in der ersten Sphäre die Polizeibehörden im Fokus des Untersuchungsinteresses. In beiden Staaten geht es hierbei um die übergeordneten Polizeien, das Bundeskriminalamt bzw. die Serious Crime Agency.[9] Im zweiten Untersuchungsbereich liegt der Analysefokus auf den Kompetenzen der Auslandsgeheimdienste.[10] Im Zentrum der Untersuchung stehen daher der Bundesnachrichtendienst sowie das GCHQ. Der dritte Komplex befasst sich mit der militärischen Nutzung des Netzes und analysiert daher, welche Aufgaben der Bundeswehr bzw. den British Armed Forces übertragen wurden. Auch internationale Interaktionen folgen dieser Differenzierung und bestätigen damit die Relevanz der Unterscheidung auf internationaler Ebene. Während in der Kriminalitätsbekämpfung der Europarat und die EU wesentliche Institutionen darstellen, verlaufen Debatten um die militärische Nutzung des Internets zumeist im Kreis der Vereinten Nationen (UN GGE) oder bilateral. Zur Spionage gibt es fast ausschließlich bilaterale Vereinbarungen und Verhandlungen, eine Ausnahme stellt der Geheimdienstverbund der angelsächsischen Staaten dar (5-Eyes).

Damit unterscheiden sich von staatlicher Seite die Institutionen, die mit den Funktionsübernahmen betraut werden. Zudem variieren die Rollenträger der Gegenrollen sowie die historischen Selbstbilder in den Untersuchungsbereichen. Daraus können unterschiedliche Interaktionsprozesse folgen. Maßnahmen, die

9 In beiden Staaten ist die Polizeigesetzgebung nicht den Bundesebenen überlassen. In Deutschland, wie in Großbritannien regeln dies die Bundesländer bzw. vier Landesteile. In beiden Staaten wurden aber substanzielle Kompetenzen den übergeordneten Polizeien übertragen. Außerdem wurden Gesetze zur Regelung der Straftatbestände sowie zur Etablierung neuer Ermittlungsbefugnisse durch die (Bundes-)Regierungen erlassen. Diese Entwicklungen stehen im Zentrum des Untersuchungsinteresses. Regelungen, die in den Landesteilen oder Bundesländern erlassen wurden, werden nur dann berücksichtigt, wenn diese Einfluss auf die Rollen der Regierungen hatten.

10 Im Fall Großbritannien auf dem mit der Signals Intelligence betrauten Dienst GCHQ.

im Bereich der Geheimdienste akzeptiert werden, werden für die Strafverfolgungsbehörden möglicherweise nicht anerkannt oder umgekehrt.

Die Differenzierung in drei Handlungskontexte ist daher eine hilfreiche Heuristik zum Verständnis der unterschiedlichen Interaktionen. Sie wird aber teilweise durch die politische Praxis unterlaufen, bspw. dann wenn für die Cybersicherheit genuin neue Institutionen geschaffen werden, die unterschiedliche Bereiche integrieren. Diese neuen Institutionen werden in der folgenden Analyse in den Kontexten betrachtet, in denen ihnen konkrete Funktionen übertragen werden. Letztlich kann aber auch durch unterschiedliche Praktiken bei der Trennung bzw. Konvergenz der Arenen das Verständnis für die Cybersicherheitspolitiken der Untersuchungsstaaten geschärft werden, schließlich werden auch sie durch unterschiedliche Interaktionsprozesse ermöglicht.

## 3.4 Forschungsleitende Annahmen

Aus den bisherigen theoretischen und methodisch-konzeptionellen Überlegungen ergeben sich verschiedene Annahmen über die Cybersicherheitspolitiken in Deutschland und Großbritannien. Sie folgen aus den theoretischen Argumenten zum rollentheoretischen Zwei-Ebenen-Spiel, aus der konzeptionellen Differenzierung der drei Rollen sowie aus den drei Handlungskontexten der Cybersicherheitspolitik. Die Annahmen lauten:

1. Die Regierungen beider Untersuchungsstaaten haben im Laufe des Untersuchungszeitraums ihre Beschützer-Rollen in der Cybersicherheitspolitik erweitert.
2. Die Beschützer-Rollen unterscheiden sich in den drei Untersuchungsbereichen aufgrund der Interaktion mit unterschiedlichen signifikanten Anderen (domestisch wie international) und aufgrund unterschiedlicher historischer Selbstbezüge. Die Regierungen müssen ihre Positionen in einem rollentheoretischen Zwei-Ebenen-Spiel einnehmen und sind dabei auf komplementäre Rollenübernahmen durch signifikante Andere angewiesen. Beide Rollenspiele stehen dabei in interaktivem Austausch und können sich gegenseitig beeinflussen.
3. Da die Untersuchungsbereiche aufgrund ihrer Akteurskonstellationen und historischen Bezüge durch unterschiedliche Interaktionsprozesse geprägt sind, kommt es zu unterschiedlichen Konvergenzen von Interaktionsarenen.
4. Es bestehen unterschiedliche Wechselwirkungen zwischen den Rollen Beschützer, Wohlstandsmaximierer und Garant liberaler Grundrechte.

Ob bzw. inwiefern sich diese Annahmen zum Verständnis der Entwicklung der Politiken als nützlich erweisen, wird in der folgenden Analyse des empirischen Materials untersucht und im Fazit erörtert.

# 4. Strafverfolgung im globalen Netz

Die rasche Verbreitung von Informations- und Kommunikationstechnik hat einerseits neue Formen der Kriminalität ermöglicht, andererseits wurden aber auch bekannte Tatbestände mittels IT durchgeführt oder vorbereitet. Das Internet ermöglicht es Kriminellen ferner, relativ problemlos über Ländergrenzen hinweg zu operieren. Aus deutscher Perspektive wurde schnell deutlich, dass »der grenzüberschreitende Charakter des Internets [...] die Sicherheits- und Strafverfolgungsbehörden vor neue Anforderungen« stellt (Deutscher Bundestag, 2001, S. 2). Eine Einschätzung die auch in Großbritannien geteilt wurde. Die Entwicklung der Politiken mit Blick auf die Bekämpfung von (Computer)Kriminalität hat sich im Wesentlichen in zwei Bereichen vollzogen: in der Formulierung des neuen IT-Strafrechts sowie in Veränderungen der Strafprozessordnung bzw. der Etablierung neuer Ermittlungsmethoden und -befugnisse, um den Polizeibehörden die Strafverfolgung in diesem neuen Handlungsraum zu ermöglichen. Diese beiden Entwicklungen werden im Folgenden für beide Untersuchungsstaaten analysiert.

Im ersten Abschnitt steht die Entwicklung des neuen IT-Strafrechts im Fokus. Hier wird zunächst dargestellt, welche neuen Straftatbestände bereits vor dem Aufkommen des Internets etabliert wurden, um auf die Missbrauchsmöglichkeiten von IT-Systemen zu reagieren. Im Anschluss wird die internationale Entwicklung mit Blick auf die Regulation von Kryptographie sowie auf die Harmonisierung des Strafrechts untersucht. Abschließend wird analysiert, welche Kompetenzen die Regierungen den Ermittlungsbehörden zugesprochen haben, um auch im Netz handlungsfähig zu sein und welche domestischen Kontestationsprozesse damit einhergingen.

## 4.1 Deutschland

### 4.1.1 Das deutsche IT-Strafrecht: Domestische Etablierung eines neuen Rechtsrahmens

Bereits geraume Zeit vor der kommerziellen Öffnung und globalen Verbreitung des Internets in den 1990er Jahren, führte die zunehmende Nutzung von Computern zu Debatten darüber, ob bzw. inwiefern durch die neue Technik strafrechtliche Lücken entstanden seien. Die ersten Diskussionen in diesem Kontext begannen in den 1970er Jahren und waren auf die missbräuchliche Nutzung von IT-Systemen in der Wirtschaft fokussiert, da Computer zu diesem Zeitpunkt noch nicht bei den EndnutzerInnen angekommen waren. 1972 setzte das Bundesjustizministerium eine Sachverständigenkommission ein, die Vorschläge zur Reform des Wirtschaftsstrafrechts erarbeiten sollte. Aber noch im Jahr 1974 sah die Bundesregierung keinen akuten Handlungsbedarf.

> »Die bisherigen praktischen Erfahrungen mit der Anwendung des geltenden Strafrechts auf diese neue Form der Kriminalität rechtfertigen die Feststellung, daß im wesentlichen keine Lücken bestehen, die allein aufgrund der spezifischen Möglichkeiten der EDV-Technik sichtbar werden könnten. […] Im Übrigen beobachtet die Bundesregierung die weitere Entwicklung mit besonderer Aufmerksamkeit, da nicht auszuschließen ist, daß größere Lücken des geltenden Strafrechts bisher nur wegen der geringen Verbreitung dieser Kriminalität verborgen geblieben sind.« (Deutscher Bundestag, 1974, S. 6)

1978 legte die Sachverständigenkommission konkrete Entwürfe zur Regulierung der Computerkriminalität vor. Diese enthielten unter anderem auch Vorschläge zur Schaffung neuer Straftatbestände. Sie mündeten in das 1. und 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität (WiKG). Während das erste Gesetz noch keine Regelungen zur Computerkriminalität enthielt, wurde mit dem am 1. August 1986 in Kraft getretenen 2. WiKG die Grundlage für die Strafbarkeit von Computerdelikten gelegt. Seit dem Einsetzen der Sachverständigenkommission hatte die Nutzung von Computern deutlich zugenommen und die Regierung sah nun die Notwendigkeit, bestehende Lücken im Strafrecht zu schließen. Das Gesetz war damit Ausdruck der Beobachtung,

> »[…] daß der zunehmende Einsatz von Datenverarbeitungsanlagen in der Wirtschaft und in der Verwaltung die Möglichkeit von strafwürdigen Mißbräuchen eröffnet, denen mit Mitteln des Strafrechts nicht hinreichend begegnet werden kann.« (Deutscher Bundestag, 1986a, S. 11)

Durch die Zuordnung zum Bereich der Wirtschaftskriminalität wird deutlich, dass der Missbrauch von Computern noch nicht als umfassendes Problem für

alle BürgerInnen gesehen wurde. Mit der Verknüpfung von Computer- und Wirtschaftskriminalität folgte die deutsche Regierung einem internationalen Trend. Explizit bezog sich die Regierung in der Gesetzesbegründung auf Empfehlungen des Europarates (ebd., S. 11). Dieser hatte bereits 1981 in einer Stellungnahme Mitgliedsstaaten zur verstärkten Bekämpfung der Wirtschaftskriminalität aufgerufen und Computerkriminalität diesem Deliktsbereich zugerechnet (Council of Europe, 1981, S. 4).

Zur Rechtfertigung des neuen Gesetzes verwies Justizminister Engelhard auf Erfahrungen mit steigenden Angriffszahlen in den USA aber auch in Deutschland, die zu einer Gefahr für die wirtschaftliche Leistungsfähigkeit geworden seien (Deutscher Bundestag, 1983b, S. 1668). Die Bundesregierung vertrat damit die auch international verbreitete Auffassung, Computer seien primär für die wirtschaftliche Prosperität und das Funktionieren der Verwaltung von Bedeutung. In der Beschlussempfehlung des Justizausschusses zum 2. WiKG heißt es daher:

> »Neue Entwicklungen im Wirtschaftsleben, wie z. B. der verstärkte Einsatz der Datenverarbeitung, haben neue Kriminalitätsformen hervorgebracht, denen mit dem bisherigen Strafrecht nicht ausreichend begegnet werden kann.« (Deutscher Bundestag, 1986b, S. 1)

Regelmäßig wurde von VertreterInnen der Regierung und des Parlaments auf den »hohen wirtschaftlichen Wert« von Daten sowie auf die wachsende IT-Abhängigkeit von Unternehmen aber auch der öffentlichen Verwaltung hingewiesen (ebd., S. 34f.). Die Notwendigkeit, neue Straftatbestände zu schaffen, wurde dabei von allen Fraktionen im Bundestag geteilt, da durch diese Delikte ein erheblicher volkswirtschaftlicher Schaden entstünde (ebd., S. 24).

Der Gesetzentwurf, der am 29. September 1983 erstmals im Bundestag debattiert wurde, war noch in Teilen von der SPD-geführten Vorgängerregierung ausgearbeitet, dann von der neuen Koalition aus CDU und FDP aufgenommen und dem Bundestag vorgelegt worden (Deutscher Bundestag, 1983b, S. 1665). Das neue Gesetz war maßgeblich durch das Bestreben geprägt, den nationalen Wohlstand durch die Vermeidung wirtschaftlicher Verluste zu erhalten bzw. auszubauen. Dabei wurde bereits auf die besonderen neuen technischen Möglichkeiten verwiesen, die Computerdelikte potenziell besonders gefährlich machten. In diesem Kontext wurde die Skalierbarkeit von Angriffen sowie die schwierige und potenziell zeitverzögerte Aufklärung der Delikte diskutiert (Deutscher Bundestag, 1983a, S. 16).

Insgesamt fügte das 2. WiKG dem Strafgesetzbuch (StGB) fünf neue Straftatbestände für Computerkriminalität hinzu: § 202a Ausspähen von Daten, § 263a Computerbetrug, § 269 Fälschung beweiserheblicher Daten, § 303a Datenveränderung und § 303b Computersabotage (Bundesgesetzblatt, 1986). Die neu-

en Paragraphen spiegelten dabei (auch in unterschiedlichen Kombinationen) die technischen Schutzziele der IT-Sicherheit wider: Vertraulichkeit, Integrität und Verfügbarkeit.

Sie sind damit der erste praktische Ausdruck der exekutiven Beschützer-Rolle im Bereich der IT. Hervorzuheben ist dabei, dass Teile der neuen Straftatbestände erst durch Vorschläge des Justizausschusses des Bundestages in das Gesetz aufgenommen wurden. Die §§ 202a sowie 303a,b wurden erst nach Beratungen im Ausschuss bzw. Anhörung von Sachverständigen in den Gesetzentwurf integriert.

Der Aufbau strafrechtlicher Regelungen wurde auch maßgeblich durch eine überparteiliche Mehrheit im Parlament vorangetrieben und unterstützt. Bemerkenswert ist, dass die neuen Tatbestände (mit Ausnahme von § 303b) dann aber doch nicht explizit mit dem Referenzobjekt Wirtschaft bzw. der öffentlichen Verwaltung verknüpft wurden. Deren Anwendbarkeit war daher auch später gegeben, als sich das Internet zunehmend zu einem Massenphänomen entwickelte. Bereits in den Debatten über das Gesetz wurde problematisiert, dass die im Zuge der Reform des Wirtschaftsstrafrechts ergangenen Regelungen nicht nur für Wirtschaftskriminelle relevant seien:

> »Weder die Vermögensdelikte wie Computerbetrug, Computersabotage und Computerspionage noch die Delikte gegen Persönlichkeitsrechte wie das Ausspähen von Daten noch die verschiedenen Verstöße gegen staatliche Sicherheitsinteressen sind typische Verhaltensweisen, die auf die sogenannten Täter mit weißem Kragen beschränkt wären. Solche Unrechtshandlungen sind vielmehr ebenso wie Diebstahl, Betrug oder Urkundenfälschung im klassischen Sinn zum Jedermann Delikt geworden, bei dem das Stimulans nicht etwa in der Eigenart des ausgeübten Berufes, sondern eher im technischen Sachverstand liegt. Man sollte deswegen im Zusammenhang mit diesem Gesetz nicht pauschal von Wirtschaftskriminalität sprechen […].« (Deutscher Bundestag, 1986c, S. 15434)

Die Erwägungen, die maßgeblich zur Erarbeitung des Gesetzentwurfes beigetragen haben, wurden also bereits bei der Verabschiedung als unzureichend betrachtet.

Dennoch waren es im Wesentlichen Erwägungen zur Sicherung unternehmerischer Freiheit, die zur Begrenzung der neuen Regeln beitrugen. Die Regierung betonte in der Gesetzesbegründung entsprechend, dass die Maßnahmen stets verhältnismäßig sein müssten und die »freiheitliche Wirtschaftsverfassung« nicht über Gebühr einschränken dürften (Deutscher Bundestag, 1983a, S. 11). Diese Bedenken schlugen sich auch konkret in der Ausgestaltung des Gesetzes nieder.

Die Regierung ging zwar davon aus, dass zur Bekämpfung des Computerbetrugs (§ 263a) technische Sicherungsmaßnahmen effektiv seien, sah aber dennoch von einer verbindlichen Regelung in diesem Bereich ab, da die Vorgaben

einerseits »wegen der fortschreitenden technischen Entwicklung nicht nur unvollkommen und wenig praktikabel« wären, sondern andererseits auch im »Widerspruch zu der persönlichen Freiheit des Betriebsinhabers« stünden (ebd., S. 16). Die Rolle als Beschützer wurde folglich durch Verweis auf die Wohlstandsmaximierung begrenzt. Auf verbindliche Maßnahmen zum unternehmerischen Selbstschutz wurde verzichtet, da derartige Vorschriften als Beschränkung wirtschaftlicher Entscheidungsfreiheit gesehen und auch von UnternehmensvertreterInnen weitgehend abgelehnt wurden. Kritischer formuliert wurde diese Zurückhaltung auch als staatlich gedeckte Chance zur unternehmerischen Sorglosigkeit gedeutet. Diese Einschätzung wurde aber lediglich von einer Minderheit (bspw. von Abgeordneten der Grünen) geteilt, die verbindlichere Regeln und ggf. auch eine Haftung von Unternehmen forderte (Deutscher Bundestag, 1986c, S. 15443).

Neben diesen Abwägungen zwischen wirtschaftlicher Freiheit und staatlichem Schutzanspruch, wurden die Regelungen ferner durch das vorherrschende AngreiferInnenbild geprägt. Debatten im Justizausschuss führten dazu, dass eine, durch die Regierung geforderte, umfassendere Strafbarkeit des § 202a verhindert wurde. Die Regierung hatte vorgeschlagen bereits das Sich-Zugriff-Verschaffen auf gesicherte Daten strafbar zu machen. Diese Bestrebungen wurden aber durch das Parlament zurückgewiesen, da die Abgeordneten in diesem Ansinnen die Gefahr einer »Überkriminalisierung« sahen (Deutscher Bundestag, 1986b, S. 28). Der Ausschuss argumentierte, dass Hacker, »die sich mit dem bloßen Eindringen z. B. in ein Computersystem begnügen, also sich keine Daten unbefugt verschaffen, von Strafe verschont bleiben [sollten; Anm. d. Verf.]« (ebd., S. 28). Die zu sanktionierenden Anderen waren Kriminelle mit kommerzieller Gewinnabsicht, nicht technikbegeisterte Jugendliche, die aus Neugier Schwachstellen suchten. Die Absicht der Regierung hatte auch in der Gesellschaft und in der sich entwickelnden IT-Community für erheblichen Widerspruch gesorgt. Im Parlament konnte in der Folge fraktionsübergreifend Einigkeit darüber hergestellt werden, dass »nur eine Regelung in Betracht kommen könne, die nicht gleich jeden jugendlichen Computer-Freak bei der Ausübung seines Hobbys zum Kriminellen stempelt« (Deutscher Bundestag, 1986c, S. 15437). Einschränkungen der Beschützer-Rolle folgten daher auch aus Kontestationen, die auf der Antizipation potenziell wenig gefährlicher Angreifer beruhten und so die Etablierung eines Gefährdungsdelikts verhinderten. Da eine weitreichende Vernetzung noch nicht vorhanden war, waren die sensibelsten Angriffe ohnehin nur durch InnentäterInnen realisierbar.

Auch wenn das 2. WiKG überwiegend durch die Interaktion zwischen domestischen Akteuren geprägt wurde, gab es doch Bezüge zu internationalen PartnerInnen, die in der gleichen Zeitspanne ähnliche gesetzliche Regelungen erlassen hatten. Neben den Empfehlungen des Europarates, orientierte sich die Bundesregierung bei der Ausgestaltung bspw. an Erfahrungen in den USA und Kanada

(§§ 303a, 303b) bzw. Österreich, Dänemark und der Schweiz (§ 263a) (Deutscher Bundestag, 1986b, S. 29f. sowie 34).

Bereits in dieser Frühphase der Rechtsentwicklung zeigte sich das dynamisch interaktive Verhältnis zwischen den zentralen exekutiven Funktionsübernahmen: Schutz und Wohlstandsmaximierung. Entsprechend der Bedeutungszuschreibung den Computer primär als essenzielles Wirtschaftsgut zu sehen, war die Rolle des Wohlstandsmaximierers katalytisch für die erste Etablierung des staatlichen Schutzanspruches in der digitalen Welt. Gleichzeitig wurden die neuen Regelungen aber auch durch diese Rolle beschränkt, da auf einen unverhältnismäßigen Eingriff in die wirtschaftliche Freiheit verzichtet werden sollte. Das 2. WiKG wurde zwar deutlich vor der Verbreitung des Internets verabschiedet, dennoch blieb es lange (bis auf Details) unverändert. Mit der Verbreitung des Internets wurden aber schnell neue Probleme deutlich und der internationale Koordinierungsbedarf wuchs rasch.

Die erste Übernahme der Beschützer-Rolle war im Wesentlichen durch die Rolle als Wohlstandsmaximierer katalysiert und begrenzt. Die Referenz der Rolle (Schutz für wen?) lag folglich auf dem Erhalt bzw. Ausbau wirtschaftlicher Prosperität. Die Beschützer-Rolle wurde daher aber auch durch ökonomische Bedenken beschränkt. Mit Blick auf Fragen der Haftung oder konkreten Vorgaben über Schutzniveaus, die potenziell in die unternehmerische Freiheit Eingreifen könnten, agierte die Bundesregierung zurückhaltend. Dies wurde auch durch die Gefahreneinschätzung ermöglicht. In dieser frühen Entwicklungsphase wurde in Deutschland noch oft über jugendliche FreizeithackerInnen debattiert, ihr Verhalten sollte durch eine zu expansive Beschützer-Rolle nicht in unangemessener Weise sanktioniert werden.

### 4.1.2 Kryptopolitik

Dass die neuen Kommunikationsmöglichkeiten, die mit dem Internet einhergingen, für die staatliche Schutzfunktion auch problematisch sein konnten, wurde bereits mit der Öffnung des Netzes debattiert. Die Auseinandersetzung um den Einsatz von Kryptographie zum Schutz von Kommunikation ist einer der ersten zentralen Kristallisationspunkte der Cybersicherheitspolitik. Die Möglichkeit durch Verschlüsselung, Kommunikation praktisch jedwedem Zugriff zu entziehen und damit staatliche Kontrolle schwierig oder gar unmöglich zu machen, sorgte auch in Deutschland früh für Besorgnis. In einer Rede betonte Innenminister Manfred Kanther 1994: »die Kryptierungsmöglichkeiten im Fernmeldeverkehr dürfen keine für die Verbrechensaufklärung unüberwindbare Hürde bilden« (Bundesregierung, 1994). In der Folge entwickelte sich sowohl domestisch als auch international eine rege Debatte über die Nutzung und Regulation von Kryptographie, die das Spannungsfeld zwischen exekutiver Schutzfunktion, Wohlstandsma-

ximierung und der Gewährleistung liberaler Freiheitsrechte im digitalen Raum offen zu Tage treten ließ. Die Auseinandersetzung löste dabei das Thema Verschlüsselung aus dem zuvor prägenden militärischen und geheimdienstlichen Kontext, da Kryptographie mit dem Internet potenziell allen interessierten NutzerInnen zur Verfügung stand und auch für die Wirtschaft zu einem wesentlichen Bestandteil der Internetaktivitäten wurde (Beucher und Schmoll, 1999, S. 529).

Unter Verweis auf die erschwerte Strafverfolgung im Internet forderte Innenminister Kanther immer wieder weitgehende Maßnahmen zur Regulation von kryptographischen Verfahren. Eine von ihm und den Sicherheitsbehörden bevorzugte Key-Recovery Variante sah vor, die zur Dekryptierung benötigten Schlüssel zu duplizieren und für den Staat erreichbar zu hinterlegen (Deutscher Bundestag, 1998a, S. 65). Eine Praxis die auch von der Regierung der USA vorangetrieben wurde, aber dort innenpolitisch auf beträchtlichen Widerstand stieß. In Deutschland entzündete sich an den Plänen des Innenministers heftige Kritik von unterschiedlichen Akteuren. So gab es aus der Zivilgesellschaft massiven Widerstand gegen die Vorschläge zur Schwächung von Verschlüsselung bzw. zur Hinterlegung von Schlüsseln. Der Chaos Computer Club (CCC) verband seine Kritik mit dem Vorwurf, der Innenminister verfolge mit der Schlüsselhinterlegung das Ziel, »den amerikanischen Geheimdiensten weltweit den problemlosen Zugriff auf jedwede elektronische Kommunikation zu sichern« (heise.de, 1997).

Dieser Vorwurf erschließt sich nur durch einen Blick auf die internationale Entwicklung zu diesem Zeitpunkt. Nachdem die US-Regierung in innenpolitischen Auseinandersetzungen um ein nationales System zur Schlüsselhinterlegung eine Niederlage erlitten hatte, wurden in der Folge die Exportrichtlinien für Kryptographie-Produkte gelockert.[1] Gleichsam als Ersatz sollten, geprägt durch die marktbeherrschende Stellung der US-Unternehmen, in der Folge umfassende internationale Lösungen zur Key-Recovery etabliert werden. Ziel der US-Regierung war es, einen internationalen Konsens herzustellen, der nur den Export von Produkten mit Key-Recovery-Funktionalität erlaubt hätte. Damit wäre ein System etabliert worden, in dem vermutlich ein wesentlicher Teil aller Zweitschlüssel bei US-Unternehmen hinterlegt worden wären. Dieses Szenario wurde auch durch die Enquete-Kommission des deutschen Bundestags äußerst kritisch gesehen:

1 Diese Systeme der Schlüsselhinterlegung werden oft auch als Key-Escrow bezeichnet und standen in der innenpolitischen amerikanischen Debatte um die Kontrolle von Kryptographie im Zentrum der Kritik. Die Regierung hatte mit dem Clipper-Chip 1993 einen Ansatz verfolgt, der einen staatlichen Zugriff auch auf verschlüsselte Daten ermöglicht hätte, da eine Schlüsseldublette bei der Regierung gespeichert worden wäre. Dies wurde domestisch heftig kritisiert und nachdem ein Informatiker 1994 einen Fehler im Design gefunden hatte, wurden die Pläne schließlich verworfen (Kehl, Wilson und Bankston, 2015).

> »Mit diesem Exportregime geht es der US-Regierung im Ergebnis vor allem darum, einen weltweiten Standard für Kryptoverfahren zu etablieren, der – unabhängig von der technischen Ausgestaltung im einzelnen – den unbemerkten Zugriff von US-Regierungsstellen auf den Klartext verschlüsselter Informationen auch ausländischer Nutzer von US-Produkten erlaubt.« (Deutscher Bundestag, 1998a, S. 67)

Entsprechend der Globalität des Internets, wäre damit auch eine umfassende internationale Einflussmöglichkeit für die USA entstanden. Die USA hätten dann mit dem Internet auch ihre eigene Beschützer-Rolle global verbreitet. Die Bestrebungen wurden so als Versuch interpretiert, die innenpolitisch geschwächte Beschützer-Rolle zu internationalisieren und dadurch zu kompensieren. Die Bundesregierung vertrat daher auch international die Position, dass der »Versuch, US-Politik in das Ausland zu exportieren, nicht akzeptabel sei« (ebd., S. 67).

Diese Einwände wurden mit dem Verweis auf die potenziellen Einschränkungen bzw. nachteiligen Effekte für die eigene Strafverfolgung begründet, da das amerikanische Modell »Spielräume anderer Regierungen zur Gestaltung einer eigenen Kryptopolitik« beschränke (ebd., S. 68). Außerdem äußerte die Enquete-Kommission Bedenken darüber, »daß die vertrauliche Datenkommunikation deutscher Nutzer dem Zugriff ausländischer Instanzen außerhalb des Geltungsbereichs deutscher Gesetze und unkontrolliert durch deutsche Gerichte ausgesetzt« werde (ebd., S. 67). Der globale Handlungsraum sollte also nicht neuen Regeln folgen, sondern wieder territorial rückgebunden werden. Deutsche Gerichte sollten über deutsche BürgerInnen urteilen.

Die restriktiven Exportregeln der USA hatten ferner auch direkte Auswirkungen auf die Beschützer-Rolle der Bundesregierung selbst. Auch wenn das 1991 gegründete Bundesamt für Sicherheit in der Informationstechnik (BSI) Verschlüsselungsprodukte aus den USA skeptisch beurteilte (Deutscher Bundestag, 1996, S. 4), nutzte die Verwaltung der Bundeswehr doch seit 1994 Lotus Notes, das durch die Exportkontrollgesetze der USA nur mit einer schwachen Verschlüsselung ausgestattet war. Um der NSA den Zugriff auf die Kommunikation zu erleichtern, wurden von einem Schlüssel mit einer Länge von 64 Bit die ersten 24 Bit mit dem öffentlichen Schlüssel der NSA verschlüsselt, »so daß die NSA letztendlich nur 40 Bit entschlüsseln« musste (Deutscher Bundestag, 1999, S. 3). Auch dieser Umstand hat möglicherweise zum deutschen Widerstand gegen die Pläne der USA beigetragen. Eindeutig ist, dass die Politik der US-Regierung als problematisch für die deutsche Wirtschaft gesehen wurde.

> »Als besondere Bedrohungsform kommt hinzu, daß Key Recovery für Wirtschaftsspionage durch Geheimdienste genutzt werden kann. Außerdem kann eine zentrale Hinterlegungsstelle selbst Ziel von Angriffen werden. Dieses Risiko wäre dann besonders evident, wenn es jemals zu dem von den USA vorge-

schlagenen weltweiten Key-Recovery-System käme.« (Deutscher Bundestag, 1998a, S. 33)

Mit diesem Argument warf die Enquete-Kommission auch ein zentrales Dilemma bei der Kontrolle von Kryptographie auf. Wenn Hintertüren oder Zweitschlüssel für Verschlüsselung geschaffen werden, besteht immer die Möglichkeit, dass ein/eine Dritte/r diese Schwachstellen findet und ausnutzt. In diesem Fall würde nicht nur riskiert, dass die USA selbst ihre Position ausnutzen könnten, sondern auch Kriminelle, Terrororganisationen oder andere Akteure könnten potenziell unbemerkt von einer solchen Lösung profitieren.

Als die US-Regierung versuchte im Rahmen des Wassenaar-Abkommens durchzusetzen, dass nur noch Produkte mit Key-Recovery-Funktion exportiert werden sollten, wurde das unter anderem durch den Widerstand der deutschen Regierung verhindert. Die Bundesregierung trug damit auch zur Liberalisierung des internationalen Krypto-Marktes bei. Sie setzte sich in der Folge auch dafür ein, die EG-Dual-Use-Verordnung für Verschlüsselungsprodukte zu lockern (Brunst, 2012, S. 335). Dies folgte einem internationalen Trend, der sich auch in den am 27. März 1997 verabschiedeten »Guidelines for Cryptography Policy« der OECD widerspiegelt, die ebenfalls einen liberalen Umgang mit Verschlüsselungsprodukten empfahlen (OECD, 1997).

Das synergetische Zusammenwirken der Rollen Wohlstandsmaximierer, Garant liberaler Grundrechte und Beschützer führten dazu, dass die Bundesregierung auf internationaler Ebene die Bestrebungen der USA ablehnten. Die Regierung erkannte zwar ebenfalls die sicherheitspolitischen Probleme, die mit einer Verbreitung von Verschlüsselung einhergingen, wollte aber eine global ausgedehnte Beschützer-Rolle der USA nicht akzeptieren. Die Kontestation der amerikanischen Bemühungen ergab sich sowohl aus wirtschaftlichen als auch bürgerrechtlichen Erwägungen. Aus Sicht des Wohlstandsmaximierers war das Risiko, amerikanischen Behörden durch die Hinterlegung von Zweitschlüsseln potenziell Zugriff auf deutsche Wirtschaftsgeheimnisse einzuräumen, nicht hinnehmbar. Auch mit Blick auf die privaten Kommunikationsinhalte deutscher BürgerInnen wurde dies kritisch gesehen. Zu diesen Bedenken kam noch eine partielle Abhängigkeit der eigenen Beschützer-Rolle hinzu. Da das deutsche Militär amerikanische Software verwendete, wurde die Fähigkeit zum Schutz eigener, sensibler Kommunikation unterminiert. Auf internationaler Ebene wirkten so alle drei Rollen synergetisch auf eine Kontestation der amerikanischen Bemühungen hin und ermöglichten eine liberale Verschlüsselungspolitik.

Die deutsche Skepsis gegenüber einer Regulierung von Verschlüsselung war aber nicht nur durch Vorbehalte gegen einen wachsenden Einfluss der USA geprägt. Kritik wurde auch gegen eine deutsche Aushöhlung kryptographischer Verfahren vorgebracht. Diese Position wurde sowohl innerhalb der Regierungskoali-

tion als auch von Akteuren der Zivilgesellschaft vertreten. Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) konstatierte bspw. eine Regulation von Kryptographie stelle »bisherige Grundrechtsprinzipien auf den Kopf«, da auch beim Verfassen von Briefen Chiffren zulässig seien und die Aufgabe der Dekryptierung allein bei den Behörden liege (FIfF, 1997). Die Forderung des Innenministers, die Schlüssel verfügbar zu hinterlegen käme, so der Vorwurf, der Aufforderung gleich, nur noch leicht lesbare Standardbriefe zu verfassen: derartiges habe »in Deutschland noch keine Diktatur gefordert« (ebd.).

Auch innerhalb der Koalition und zwischen den Ressorts waren die Vorschläge des Innenministers nicht unumstritten. Sowohl der Koalitionspartner FDP als auch der Bundeswirtschaftsminister lehnten die Regulation von Verschlüsselung ab. Daher wurden 1997 auch keine Maßnahmen zur Restriktion von Verschlüsselung in das neue Informations- und Telekommunikationsdienste-Gesetz (IuKDG) integriert. Der FDP-Justizminister Schmidt-Jorzig brachte bei der ersten Lesung des neuen IuKDG gegen eine umfassende Kryptoregulation nicht nur wirtschaftliche Argumente vor, sondern betonte ferner die Bedeutung der Verschlüsselung für die Wahrung der Bürgerrechte denn »[…] sie schafft die technische Voraussetzung dafür, daß die Idee des Postgeheimnisses in die Zukunft übertragen werden kann.« (Deutscher Bundestag, 1997b, S. 15395). Ferner verband er die Verschlüsselungsthematik mit dem freien Informationsaustausch im Internet. In diesem Zusammenhang verwies er auf die historischen Erfahrungen der Bundesrepublik:

> »Die Informationsfreiheit war schon immer eine Schutzimpfung gegen die Diktatur. Nicht umsonst – ich will es so drastisch sagen, damit wir die Wichtigkeit dieser Dimension voll im Blick haben – hatte schon Goebbels das Hören von Feindsendern unter Strafe gestellt. Wieviel machtloser sind Diktaturen, wenn man und seit man per Mausklick alle Nachrichten, alle Informationen weltweit empfangen kann?« (Ebd., S. 15395)

Auch die 1996 unter Führung des Innenministeriums (BMI) gegründete Task Force Kryptopolitik, gelangte zu der Einschätzung, dass Verschlüsselungsprodukte frei verfügbar sein sollten (Deutscher Bundestag, 1997a, S. 10). Die innenpolitische Krypto-Debattte wurde schließlich im Jahr 1999 beigelegt, als das Wirtschafts- und Innenministerium die »Eckpunkte der deutschen Kryptopolitik« vorlegten und damit die Position der Regierung definierten. Mit diesem Dokument legte die Regierung fest, dass sie nicht beabsichtige, »die freie Verfügbarkeit von Verschlüsselungsprodukten in Deutschland einzuschränken« (Bundesregierung, 2001, S. 11). Begründet wurde dies mit der Bedeutung von Verschlüsselung für den »Datenschutz der Bürger, für die Entwicklung des elektronischen Geschäftsverkehrs sowie für den Schutz von Unternehmensgeheimnissen« (ebd., S. 11). Diese Entscheidung wurde sowohl von der Wirtschaft als auch von BürgerrechtsaktivistInnen positiv aufgenommen. Im Rahmen der 58. Datenschutzkonferenz

begrüßten bspw. die Datenschutzbeauftragten des Bundes und der Länder ausdrücklich die Entscheidung der Bundesregierung und betonten dass der Einsatz von Kryptographie ein wesentlicher Bestandteil zum Schutz personenbezogener Daten sei (Der Bundesbeauftragte für den Datenschutz und die Informationssicherheit, 1999).

Die Bundesregierung vereinbarte aber, die Situation zwei Jahre später erneut zu debattieren und zu evaluieren, ob die Strafermittlung durch Verschlüsselung maßgeblich eingeschränkt werde. Hierzu wurde der Arbeitskreis Innere Sicherheit und Verschlüsselung gegründet. Beteiligt waren das BMI, das Bundeskriminalamt (BKA), das Bundesamt für Verfassungsschutz (BfV), der Generalbundesanwalt, das Zollkriminalamt sowie das BSI (Bundesregierung, 2001, S. 3). Der Arbeitskreis kam 2001 zu dem Ergebnis, dass die Arbeit der Ermittlungs- und Sicherheitsbehörden durch den Einsatz von Verschlüsselung »noch nicht (nachhaltig) beeinträchtigt« sei (ebd., S. 7). Die Eckpunkte der deutschen Kryptopolitik blieben daher unangetastet. In der Folge wurde zwar immer wieder über die Beschränkung von Kryptographie bzw. über die Zugriffsmöglichkeiten staatlicher Stellen debattiert (insbesondere nach Terroranschlägen), die Regierung erklärte aber zuletzt 2015, dass die Eckpunkte nach wie vor gültig seien (Deutscher Bundestag, 2015c, S. 4).

Innenpolitisch wurde die Bundesregierung immer wieder mit Verweis auf ihre Rolle als Garant liberaler Grundrechte herausgefordert. Stimmen, die auf die besondere Funktion von Verschlüsselung in einer demokratischen Gesellschaft hinwiesen, kamen gleichermaßen aus Zivilgesellschaft, Parlament und Teilen der Regierung. Diese Bestrebungen wirkten besonders beschränkend auf die Beschützer-Rolle bzw. eine Unterminierung von Verschlüsselung, da sie mit den negativen historischen Selbstbildern der Bundesrepublik verknüpft wurden. Durch diese domestischen Kontestationsprozesse wurde folglich ebenfalls eine liberale Verschlüsselungspolitik ermöglicht.

### 4.1.3 Internationalisierung: Strafrechtliche Harmonisierung

Das Internet ermöglichte es Kriminellen aber nicht nur verschlüsselt zu kommunizieren, sondern es brachte auch die Möglichkeit, problemlos über Landesgrenzen hinweg zu operieren. Hierdurch entstanden für die Strafverfolgung nicht nur technische Probleme der Attribution von Angriffen, sondern auch Fragen der internationalen Kooperation. Hinzu kam, dass die Referenz zum jugendlichen Hacker in der Mitte der 1990er Jahre zunehmend kritisch gesehen wurde. Der deutsche Innenminister Kanther betonte, dass zu diesem Zeitpunkt die meisten Cyberangriffe kommerziell motiviert waren:

> »Immer noch geistert durch die Diskussion das Bild vom jungen oder gar jugendlichen Computerfreak, der – im Grunde spielerisch veranlagt – einfach Spaß am Tüfteln hat: Codeknacken als moderne Version von Superhirn. Doch das Idyll vom jugendlichen Übermut im IT-Zeitalter ist nüchtern betrachtet eine Illusion. Längst stehen wirtschaftliche Motive beim kriminellen IT-Einsatz im Vordergrund.« (Bundesregierung, 1996, S. 4)

Mit diesem veränderten AngreiferInnentyp nahm auch die Notwendigkeit der internationalen Kooperation zu, da die Schäden durch Cyberangriffe wuchsen. Die internationale Kooperation zur Bekämpfung von Cyberkriminalität wurde in verschiedenen institutionellen Kontexten seit Beginn der 1990er Jahre debattiert bspw. innerhalb der UN (1990). Im Rahmen des Europarates wurde mit der Convention on Cybercrime das erste und bislang einzige verbindliche internationale Regelwerk zur Bekämpfung von Cyberkriminalität etabliert. Das im November 2001 verabschiedete Übereinkommen sieht eine Harmonisierung des Strafrechts, internationale Kooperation (etwa bei der Rechtshilfe) sowie eine Angleichung der Ermittlungsbefugnisse aller Vertragsparteien vor (Council of Europe, 2001a). Die deutsche Regierung hat die Konvention unmittelbar nach der Öffnung gezeichnet, ratifiziert wurde sie im März 2009 (Council of Europe, 2019). Der zusammen mit dem Übereinkommen veröffentlichte Explanatory Report skizziert die problematisch gewordene Situation so:

> »Criminals are increasingly located in places other than where their acts produce their effects. However, domestic laws are generally confined to a specific territory. Thus solutions to the problems posed must be addressed by international law, necessitating the adoption of adequate international legal instruments.« (Council of Europe, 2001b, S. 2)

Vor diesem Hintergrund wurde seit 1996 an einem Übereinkommen gearbeitet. Mit der Einsicht, dass es eines internationalen Abkommens zur wirksamen Bekämpfung der Internetkriminalität bedürfe, ist auch die Einschätzung verbunden, dass es letztlich doch die Nationalstaaten sind, die diesen neuen Raum entsprechend ihrer Territorialität ordnen sollen.

Die Bundesregierung hat die Bestrebungen zur internationalen Harmonisierung der gesetzlichen Regelungen sowohl im Rahmen des Europarates als auch innerhalb der Europäischen Union stets nachdrücklich unterstützt. Sie vertrat damit die auch international verbreitete Auffassung, dass durch den globalen Handlungsraum Bedarf bestand, die nationalen Beschützer-Rollen anzugleichen, um zu gewährleisten, dass Straftaten überhaupt als solche erkannt und verfolgt werden konnten. Konkret sah die Regierung in neuen Regelungen zur internationalen Bekämpfung von Computerkriminalität die Möglichkeit, dem Trend entgegenzuwirken, »im Internet die unterschiedlichen nationalen Rechtsnormen aus-

zunutzen, um sich der Strafermittlung und/oder -verfolgung zu entziehen bzw. diese zu behindern« (Deutscher Bundestag, 2001, S. 3). Dass ein bestimmtes Verhalten in einem Staat legal, in einem anderen aber illegal war, stellte in einem entgrenzten Raum ein neues Problem dar.

Um dem zu begegnen, definierte die Convention on Cybercrime in den Artikeln 2 bis 13 verschiedene zu harmonisierende Straftatbestände. Mit dem Rahmenbeschluss 2005/222/JI folgte die EU weitgehend der Konvention des Europarates und etablierte die Straftatbestände innerhalb der Union. In dem Dokument nimmt der Rat der Europäischen Union direkt Bezug auf »die von internationalen Organisationen und insbesondere vom Europarat geleisteten Arbeiten zur Angleichung des Strafrechts« (EU, 2005, S. 67). Im Gegensatz zur Convention on Cybercrime enthielt der Rahmenbeschluss aber keine Vorgaben für die Befugnisse der Ermittlungsbehörden (ebd.).[2] Mit diesen Regelungen wurde festgelegt, welche neuen Verhaltensweisen durch die Exekutiven sanktioniert werden sollten.

Viele der in diesen Dokumenten beschriebenen Delikte waren in Deutschland bereits durch das 2. WiKG strafbar geworden. Daher folgte aus diesen Bestimmungen in Deutschland nur begrenzter Änderungsbedarf. Die strafrechtlichen Anpassungen wurden 2003 bzw. 2007 mit dem 35. und dem 41. Strafrechtsänderungsgesetz umgesetzt (Bundesgesetzblatt, 2003, 2007). Innenpolitisch wurde der neu geschaffene § 202c besonders kritisch diskutiert. Der als Hackerparagraph bekanntgewordene Abschnitt stellt auch die Erstellung sowie die Verbreitung von Hackertools unter Strafe. Aus Sicht der Wirtschaft kriminalisierte die Regierung damit auch die Tätigkeiten von SicherheitsforscherInnen, die zwangsläufig mit Software zur Identifikation von Schwachstellen arbeiten müssten. Die Kritik wurde dabei bspw. vom Branchenverband BITKOM und SAP vorgebracht (Deutscher Bundestag, 2007b, S. 10290f.). Der Chaos Computer Club (CCC) sah durch den verschärften Straftatbestand gar »den IT-Standort Deutschland« gefährdet (CCC, 2008). Der Rechtsausschuss des Bundestages teilte diese Einschätzungen allerdings nicht (Deutscher Bundestag, 2007a). Eine Klage vor dem Bundesverfassungsgericht (BverfG) blieb ebenfalls erfolglos (Bundesverfassungsgericht, 2009).

Außerdem wurde durch die Änderungen der direkte wirtschaftliche Bezug in § 303b gestrichen. Diese Neuregelung zeigt, dass durch die neuen potenziellen Angreifer in Verbindung mit der fortschreitenden Vernetzung (insbesondere kritischer Infrastrukturen) eine neue Gefahrensituation entstanden war. Daher wurde für § 303b (Computersabotage) eine Höchststrafe von zehn Jahren Freiheitsstrafe vorgesehen, »falls durch einen Angriff die Versorgung der Bevölkerung mit

2 Der Rahmenbeschluss wurde 2013 durch die Richtlinie 2013/40/EU ersetzt. Auch hier wird direkt auf die Convention on Cybercrime rekurriert und das Ziel verfolgt, dass alle EU-Mitgliedsstaaten das Abkommen ratifizieren (EU, 2013, S. 9).

lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt« würde. Hier zeigt sich deutlich die national wie international gestiegene Gefahreneinschätzung, die eine Erweiterung der Sanktionsmittel der Beschützer ermöglichte. Im Zuge der Harmonisierung wurde ferner der neue Tatbestand Abfangen von Daten geschaffen (§ 202b). Im Zuge der Anpassungen fiel weiterhin das sogenannte Hacker-Privileg aus § 202a StGB, das das bloße Eindringen in Computersysteme noch nicht unter Strafe stellte. Auch dies wurde durch die neuen Charakteristiken der AngreiferInnen ermöglicht.

Neben Vorgaben zur Gestaltung des Strafrechts und zur internationalen Kooperation enthält die Convention on Cybercrime auch Regelungen zu Ermittlungsbefugnissen der Sicherheitsbehörden. In den Artikeln 14 bis 21 beschreibt das Übereinkommen die Kompetenzen, über die Staaten bzw. die Ermittlungsbehörden der Staaten verfügen sollten, um Computerkriminalität effektiv verfolgen zu können. Von besonderer Bedeutung für die deutsche Politik sind hier die Artikel 19 und 21. Artikel 19(1) schreibt den Vertragsparteien vor, die Ermittlungsbehörden in die Lage zu versetzen:

> »a) ein Computersystem oder einen Teil davon sowie die darin gespeicherten Computerdaten und b) einen Computerdatenträger, auf dem Computerdaten gespeichert sein können, in ihrem Hoheitsgebiet zu durchsuchen oder in ähnlicher Weise darauf Zugriff zunehmen.« (Bundesgesetzblatt, 2008a, S. 1256)[3]

Artikel 21 bezieht sich auf den direkten Mitschnitt gegenwärtiger Kommunikation, die Staaten müssen Sicherheitsbehörden die rechtlichen Möglichkeiten einräumen,

> »inhaltsbezogene Daten bestimmter Kommunikationen in ihrem Hoheitsgebiet, die mittels eines Computersystems übermittelt wurden, durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen und b) einen Diensteanbieter im Rahmen seiner bestehenden technischen Möglichkeiten zu verpflichten, i) solche inhaltsbezogenen Daten durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen oder ii) bei der Erhebung oder Aufzeichnung solcher inhaltsbezogener Daten in Echtzeit mit den zuständigen Behörden zusammenzuarbeiten und diese zu unterstützen.« (Ebd., S. 1258)

3 Im Folgenden wird auf die deutsche Übersetzung des Textes zurückgegriffen, die am 10. November 2008 im Bundesgesetzblatt veröffentlicht wurde.

Mit diesen Vorschriften verständigten sich die Exekutiven auf Maßnahmen, die sie zur Erfüllung ihrer Schutzfunktionen für notwendig und angemessen hielten.[4] Es war aber in Deutschland bereits abzusehen, dass es gegen einige Bestimmungen substanziell Widerstand geben würde (heise.de, 2001a,b). Auch juristische Analysen bezweifelten, dass bspw. Maßnahmen nach Artikel 19 der Konvention durch § 102 der deutschen Strafprozessordnung (StPO) gedeckt waren (Spannbrucker, 2004, S. 188f.).

In dieser Phase wurde die Beschützer-Rolle und damit verbunden die Sanktionspotenziale deutlich ausgebaut. Diese Expansion der Kompetenzen wurde maßgeblich durch eine doppelte Veränderung der Rollenreferenz ermöglicht. Einerseits verschob sich der Fokus des Schutzgutes weiter von der Wirtschaft, ein Trend, der bereits in der Frühphase begonnen hatte und sich hier fortsetzte. Da IT zunehmend zu einer zentralen Infrastruktur wurde, löste sich die Beschützer-Rolle etwas vom wirtschaftlichen Schutzgut und fokussierte sich auf die kritischen Infrastrukturen. Mit dieser Verschiebung der Referenz (Schutz für wen?) ging eine neue Gefahreneinschätzung einher, da es nun auch darum ging, die Gesellschaft vor potenziellen physischen Folgen von Cyberangriffen zu schützen. Dies wurde auch durch die zweite Verschiebung der Referenz (Schutz vor wem?) noch deutlicher. Mit Blick auf die AngreiferInnen ging es nun nicht mehr um FreizeithackerInnen, sondern um zunehmend professionalisierte Kriminelle. Das Zusammenspiel aus verändertem Schutzgut (kritische Infrastrukturen) und neuen AngreiferInnen ermöglichte so einen Ausbau der Beschützer-Rolle. Es kam zwar zu Kontestationen mit Verweis auf wirtschaftliche Implikationen, bspw. für die IT-Sicherheitsforschung. Diese blieben vor dem Hintergrund der neuen Lageeinschätzung allerdings folgenlos.

Auf internationaler Ebene war die ausgedehnte Beschützer-Rolle anschlussfähig, da auch andere Staaten ähnliche Politiken verfolgten. Eine Harmonisierung strafrechtlicher Regulationen wurde damit durch kompatible Beschützer-Rollen ermöglicht. Eine weitgehende Kooperation erwuchs hieraus allerdings nicht. Dies lag unter anderem an folgenden domestischen Kontestationsprozessen in der Bundesrepublik, die es der Regierung bislang schwer gemacht haben, die eigene Beschützer-Rolle stabil zu etablieren sowie an der Rolle als Garant liberaler Grundrechte, die eine Delegation oder Teilung der Beschützer-Rolle schwierig macht.

4 Im Text der Konvention wird wiederholt darauf hingewiesen, dass das »Gleichgewicht gewahrt werden muss zwischen den Interessen der Strafverfolgung und der Achtung der grundlegenden Menschenrechte« (Bundesgesetzblatt, 2008a, S. 1244).

### 4.1.4 Neue Ermittlungswerkzeuge: Die Etablierung der offensiven domestischen Beschützerrolle

Besonders intensiv wurde die domestische Auseinandersetzung in der Bundesrepublik als die Regierung damit begann, die Beschützer-Rolle mit offensiven Fähigkeiten zum (physischen) Schutz vor Gefahren aus der »analogen Welt« auszustatten. Dieses Vorgehen führte zu massiven Kontestationsprozessen, da dies von der parlamentarischen Opposition und VertreterInnen der Zivilgesellschaft als unangemessener Ausbau der Rolle gesehen wurde.

Auch wenn Hintertüren in Verschlüsselung international wie domestisch durch die Regierung abgelehnt wurden, etablierte sie innenpolitisch dennoch für Strafverfolgungsbehörden die Möglichkeit, Internetkommunikation abzuhören. Damit hat sie ihre Beschützer-Rolle deutlich erweitert. Sie folgte damit später auch dem internationalen Konsens der Convention on Cybercrime. Die Regierung hat dazu eine Reihe von Maßnahmen ergriffen, die innenpolitisch besonders durch die Wirtschaft und Bürgerrechtsbewegungen herausgefordert wurden. Im Mai 1995 verabschiedete das Bundeskabinett bspw. die Fernmeldeverkehr-Überwachungs-Verordnung (FÜV) (Bundesgesetzblatt, 1995).

Da der Staat selbst die sicherheitsrelevanten Kommunikationsmittel nicht mehr betrieb, sollten die Anbieter von Kommunikationsdienstleistungen bereits vor Markteintritt dazu verpflichtet werden, technische Möglichkeiten zu schaffen, gesetzlichen Verpflichtungen zur Überwachung nachzukommen, sodass keine Lücken entstünden (Bundesregierung, 1996, S. 5). Denn »die Belange von Polizei und Justiz, und das heißt unsere eigenen Sicherheitsinteressen [dürften; Anm. d. Verf.], nicht außer acht bleiben« (ebd., S. 6f.). Die neuen Zugriffsmöglichkeiten wurden von Innenminister Kanther mit der raschen technischen Entwicklung und der Privatisierung des Marktes begründet. Die FÜV wurde 2002 durch die Telekommunikations-Überwachungsverordnung (TKÜV) ersetzt, die auch konkrete Bestimmungen zum Umgang mit verschlüsselter Kommunikation enthielt. In §8(3) der TKÜV legte die Regierung fest, dass Anbieter, sofern sie die Kommunikation selbst durch Verschlüsselung schützten, diese vor dem Erstellen der Überwachwungskopie entfernen mussten (Bundesgesetzblatt, 2002). Auf Grundlage des G-10-Gesetzes, der §§ 100a, 100b der StPO und §§ 39 bis 43 des Außenwirtschaftsgesetzes regelte die TKÜV die technische Überwachung im Fernmeldeverkehr (ebd.). Sie erlaubte damit dem Verfassungsschutz, den Bundes- sowie Landespolizeien, dem Zoll und dem BND Maßnahmen zur Telekommunikationsüberwachung (TKÜ). Die Verordnungen wurden zwar von verschiedenen Seiten kritisiert, blieben letztlich aber in Kraft. Begründet wurde diese Reform der FÜV durch den Verweis auf die Gefahr terroristischer Angriffe, die im Netz vorbereitet werden könnten.

> »Viele der schädlichen Programme und gezielten Angriffe gehen zunehmend auf das Konto organisierter Kriminalität und terroristischer Angreifer. Das Hauptmotiv ist nicht mehr wie bei den so genannten Script-Kiddies der Wunsch, an Bekanntheit zu gewinnen, sondern es geht darum, aus den Angriffen finanziellen Nutzen zu ziehen oder volkswirtschaftlichen Schaden anzurichten.« (Bundesministerium des Innern, 2005, S. 4)

Das Ausmaß der innenpolitischen Kontestation erreichte 2006 einen Höhepunkt, als sich eine intensive Debatte um die konkrete Nutzung von digitalen Ermittlungsmethoden entfaltete. Um mit der technischen Entwicklung schrittzuhalten, hatte die Bundesregierung den Strafverfolgungsbehörden zwei (Software-)Instrumente zur Verfügung gestellt: die Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung. Beide Maßnahmen sollten dazu beitragen, dass Ermittlungen nicht durch technische Hürden, wie Verschlüsselung, unmöglich gemacht werden. Die Maßnahmen unterscheiden sich in ihrer Eingriffstiefe in die Grundrechte deutlich. Die Quellen-TKÜ zielt darauf ab, Kommunikation vor der Verschlüsselung abzufangen und diese ohne eine Schwächung von Verschlüsselung abhörbar zu machen. Sie ist damit, die auf dem Endgerät der Betroffenen softwaregestützte Fortsetzung der TKÜ. Die Online-Durchsuchung ermöglicht den Behörden dagegen ein Gerät komplett zu durchsuchen (Brodowski und Freiling, 2011, S. 143-152). Beides sind Kompetenzen, die in der Convention on Cybercrime angelegt sind (Artikel 19 bzw. 21). Auch wenn den Exekutiven viel Spielraum bei deren Implementierung bleibt. Die Bundesregierung rechtfertigte diese Maßnahmen im »Programm zur Stärkung der Inneren Sicherheit« und konstatierte, dass es für Ermittlungsbehörden in Zeiten der Digitalisierung notwendig sei, Endgeräte auch ohne direkten physischen Zugriff überwachen zu können (Deutscher Bundestag, 2006).

Unter Verweis auf die Bürgerrechte wurde die exekutive Beschützer-Rolle in der Folge substanziell herausgefordert. Im Februar 2006 ordnete ein Ermittlungsrichter beim Bundesgerichtshof an, dass eine Software zur Informationsgewinnung eingesetzt werden dürfe. Konkret ging es um ein Verfahren des Generalbundesanwaltes, das im Rahmen des Verdachts auf die Gründung einer terroristischen Vereinigung geführt wurde. Der Ermittlungsrichter erlaubte den Behörden unter Verweis auf § 102 der StPO den Einsatz eines digitalen Ermittlungswerkzeugs.

> »Zur verdeckten Ausführung dieser Maßnahme wird den Ermittlungsbehörden gestattet, ein hierfür konzipiertes Computerprogramm von außen auf dem Computer des Beschuldigten zu installieren, um die auf den Speichermedien des Computers abgelegten Daten zu kopieren und zum Zwecke der Durchsicht an die Ermittlungsbehörden zu übertragen.« (Bundesgerichtshof, 2006b)

Diese Einschätzung wurde allerdings durch einen anderen Ermittlungsrichter infrage gestellt. Dieser entschied im Dezember des gleichen Jahres, dass die Online-Durchsuchung nicht durch die Regelungen der StPO gedeckt seien. § 102 StPO biete nicht den ausreichenden Rahmen, diese Maßnahme zu rechtfertigen. Auch einen weiten Analogieschluss, um analoge Ermittlungsmethoden auf die digitale Sphäre anwenden zu können, lehnte der Ermittlungsrichter ab. Er sei zu weitreichend als, dass dies ohne eigene gesetzliche Regelung möglich wäre (Bundesgerichtshof, 2006a).

Der Generalbundesanwalt legte gegen diesen Beschluss Einspruch ein. Im Januar 2007 entschied der BGH aber: »Die ›verdeckte Online-Durchsuchung‹ ist mangels einer Ermächtigungsgrundlage unzulässig. Sie kann insbesondere nicht auf § 102 StPO gestützt werden« (Bundesgerichtshof, 2007). Diese Einschätzung barg einige Risiken für die Bundesregierung, denn angeblich hatte der Bundesinnenminister dem Bundesamt für Verfassungsschutz schon 2005 per Dienstanweisung erlaubt, verdeckt Computer nach Informationen zu durchsuchen. Dem Urteil des BGH folgte noch im gleichen Jahr ein Gutachten des Wissenschaftlichen Dienstes des Bundestags, das die Rechtmäßigkeit der Online-Durchsuchung ebenfalls kritisch beurteilte (Wissenschaftlicher Dienst des Bundestages, 2007). Trotz dieses Urteils und der Einschätzung zahlreicher ExpertInnen, versuchte die nordrhein-westfälische Landesregierung dem Landesverfassungsschutz, die Online-Durchsuchung durch ein neues Gesetz zu ermöglichen. Dies führte zu einer Klage vor dem Bundesverfassungsgericht. In einem wegweisenden Urteil am 27. Februar 2008 definierte das BverfG das »Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme« (Bundesverfassungsgericht, 2008). In diesem Urteilt entschied das Gericht:

> »Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen.[5] […] Die heimliche Infiltration eines informationstechnischen Systems ist grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen.« (Ebd.)

5 »Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen.«

Die entsprechenden Regelungen des nordrhein-westfälischen Verfassungsschutzgesetzes waren damit ungültig und auch der Praxis der Bundesregierung war die Rechtmäßigkeit abgesprochen worden. Diese Entscheidung wurde sowohl von Bürgerrechtsbewegungen als auch der Internetwirtschaft begrüßt. Während Wirtschaftsvertreter die Bedeutung des Urteils für das Vertrauen der NutzerInnen in Onlinedienstleistungen hervorhoben, betonten die Bürgerrechtsbewegungen die Wirkung der Entscheidung auf die Wahrung der Grundrechte im digitalen Zeitalter (Spiegel, 2008).

Die Regierung verabschiedete noch im gleichen Jahr des BverfG-Urteils ein neues Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt, das dem BKA mit § 20k die Online-Durchsuchung unter Richtervorbehalt ermöglichte (Bundesgesetzblatt, 2008b). Das Gesetz war zuvor nicht nur von der Opposition und Bürgerrechtsbewegungen, sondern auch von der SPD abgelehnt worden. Die SPD hatte im Gesetzgebungsprozess aber noch einige Anpassungen am Entwurf erreicht, die ihre mehrheitliche Zustimmung letztlich sicherte. Die Kritik aus der Zivilgesellschaft war aber ungebrochen. Die Regierung rechtfertigte die neuen Befugnisse bspw. mit den Erfahrungen der sogenannten Sauerland-Gruppe, die Anschläge in Deutschland geplant hatte und dabei auch Verschlüsselung zur Sicherung von Informationen nutzte. Die Online-Durchsuchung sei daher »bei der Terrorbekämpfung unverzichtbar« (Deutscher Bundestag, 2008, S. 19833).

Außerdem wurde wiederholt darauf verwiesen, dass das Gesetz dem Urteil des BVerfG Rechnung trage. Das neue Gesetz entspreche »Punkt für Punkt den Vorgaben, die uns Karlsruhe gemacht hat« (ebd., S. 19834). Die Opposition kritisierte das Gesetz zum einen mit Blick auf die Kompetenzausweitung im Bereich der Gefahrenabwehr. Das BKA erhalte Kompetenzen, die bisher in den Landeskriminalämtern angesiedelt waren, so entstehe »ein deutsches FBI« (ebd., S. 19835). Das Gesetz schwäche das Trennungsgebot zwischen Polizeien und Geheimdiensten und ebne den Weg in den Überwachungsstaat (ebd., S. 19838). Auch Bürgerrechtsbewegungen kritisierten das Gesetz mit ähnlichen Argumenten scharf. Weiterhin kritisierten sie, dass das neue Gesetz den Schutz besonders sensibler BerufsträgerInnen nicht ausreichend berücksichtige. Dies führte dazu, dass unter anderem von zwei FDP-Politikern, zwei Journalisten, dem Präsidenten der Bundesärztekammer und einem Psychologen beim BVerfG Verfassungsbeschwerde eingereicht wurde (Zeit, 2009).

Im April 2016 entschied das BVerfG, dass Teile des BKA-Gesetzes verfassungswidrig seien. Prinzipiell stellte das Gericht zwar fest:

> »Die Ermächtigung des Bundeskriminalamts zum Einsatz von heimlichen Überwachungsmaßnahmen ([…] Online-Durchsuchungen, Telekommunikationsüberwachungen, […]) ist zur Abwehr von Gefahren des internationalen

> Terrorismus im Grundsatz mit den Grundrechten des Grundgesetzes vereinbar.« (Bundesverfassungsgericht, 2016b)

Allerdings waren die Befugnisse nicht spezifisch genug gestaltet und die juristische Kontrolle nicht ausreichend gewährleistet, so dass das Gericht die betreffenden Regelungen (darunter § 20k zur Online-Durchsuchung) für grundgesetzwidrig erklärte, aber der Regierung bis zum 30. Juni 2018 Zeit ließ, eine neue Regelung zu finden. Im Juni 2017 trat bereits das Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes in Kraft (Bundesgesetzblatt, 2017b). Auch diese Neufassung wurde unter anderem aufgrund der Regelungen zur Online-Durchsuchung kritisiert. Der Deutsche Anwaltsverein konstatierte sogar (bereits vor der Verabschiedung des Entwurfs), der neue § 49, der die Online-Durchsuchung regelte, falle hinter den alten § 20k zurück, da nun eine Durchsuchung schon möglich wurde, wenn »bestimmte Tatsachen die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Schädigung der in Satz 1 genannten Rechtsgüter eintritt« (Deutscher Anwaltverein, 2017a, S. 5).

Für eine weitere Welle der Kontestation sorgte die Verabschiedung des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens im Sommer 2017. Mit diesem Gesetz hatte die Regierung den Einsatz von Quellen-TKÜ und Onlinedurchsuchung nochmals ausgeweitet (Bundesgesetzblatt, 2017a). Mit § 100b etablierte die Regierung die Online-Durchsuchung in der StPO. Damit rückte die Maßnahme aus dem Bereich der Gefahrenabwehr (BKA-Gesetz) in die Strafverfolgung (Roggan, 2018). Die Regierung argumentierte, dass diese neuen Fähigkeiten zur Gewährleistung der Schutzfunktion essenziell seien. Besonders mit Blick auf Ende-zu-Ende verschlüsselte Messenger entstünden vermehrt Hürden bei der Strafverfolgung:

> »Traf man sich vor 20 Jahren noch in einer Wohnung, um kriminelle oder terroristische Aktivitäten zu planen, kann man sich heutzutage in einem Chatroom treffen. Der Gesetzgeber muss hierauf eine Antwort finden. Strafverfolger dürfen Kriminellen nicht hinterherhinken. […] Besonders schwierig wird es für die Ermittler, wenn es um Datenmaterial geht, das durch sogenannte Messengerdienste ausgetauscht wurde. Wenn Behörden keinen Zugriff auf diese Daten haben, entstehen in der Folge Räume, in denen Strafverfolgung unmöglich ist.« (Deutscher Bundestag, 2017d, S. 24586)[6]

6 Immer wieder wurde in diesem Kontext auf die Nutzung von (Ende-zu-Ende-verschlüsselten) Messengerdiensten (bspw. WhatsApp oder Signal) verwiesen, die keine Telekommunikationsdienstleister im Sinne des Telekommunikationsgesetzes sind, sondern Telemedien. Diese Telemedien unterliegen daher auch nicht den entsprechenden Anforderungen und sind somit nicht verpflichtet TKÜ-Maßnahmen der TKÜV umzusetzen. Sie wären bei einer Ende-

Die neuen Regeln waren aus Sicht der Regierung nur eine Anpassung an die neuen Kommunikationsmöglichkeiten (ebd., S. 24588, ebenso 24592). Es könne »nicht sein, dass nur die eine Seite, dass nur Terroristen und Kriminelle vom technischen Fortschritt profitieren« (ebd., S. 24591). Außerdem folge die Regierung mit dem Gesetz den rechtsstaatlichen Grundsätzen (ebd., S. 24591).

Für heftigen Widerspruch gegen die neuen Regeln sorgte einerseits, dass diese erst im Ausschuss und damit weitgehend ohne öffentliche Diskussion in die Gesetzesvorlage aufgenommen wurden, die dadurch einen völlig neuen Schwerpunkt erhalten habe. Diese Kritik wurde auch von Teilen der Regierung eingeräumt (ebd., S. 24585). Andererseits wiesen KritikerInnen auf den aus ihrer Sicht extensiven Strafenkatalog hin, der mit den Maßnahmen verfolgt werden sollte. Auch für die besonders intrusive Online-Durchsuchung waren aus ihrer Sicht zu viele Straftaten vorgesehen (Deutscher Anwaltverein, 2017b; heise.de, 2017b). Die Bundesbeauftragte für den Datenschutz sah in den Plänen der Regierung einen »klaren Verfassungsverstoß« und wies ebenfalls darauf hin, dass der 74 Paragraphen umfassende Katalog, der durch die Online-Durchsuchung verfolgt werden solle, deutlich zu groß sei (Bundesbeauftragte für den Datenschutz, 2017). Netzpolitik.org sah in dem Gesetz das »krasseste Überwachungsgesetz der Legislaturperiode« (Netzpolitik.org, 2017). Der Geschäftsführer des Branchenverbands BITKOM warnte davor, durch übermäßige Eingriffe in die IT-Sicherheit, das Vertrauen der NutzerInnen in die Dienste zu untergraben (heise.de, 2017a). Der CCC sah in den Vorschlägen eine Gefahr für die Innere Sicherheit, da sowohl für die Quellen-TKÜ als auch für die Online-Durchsuchung Sicherheitslücken ausgenutzt werden müssten, die ggf. auch von Dritten gefunden werden könnten (CCC, 2017).

Auch im Bundestag stießen die Pläne der Regierung auf deutliche Kritik. Die Opposition sah in den neuen Befugnissen, wie auch der CCC, eine Gefahr für die IT-Sicherheit. Das Geheimhalten von Sicherheitslücken berge immer das Risiko, dass Dritte diese nutzten. Außerdem seien die Maßnahmen »noch weitgehender als der große Lauschangriff aus den 90ern« und ein unverhältnismäßiger Eingriff in die Grundrechte (Deutscher Bundestag, 2017d, S. 24586f.). Der Umfang des Strafenkatalogs wurde ebenfalls von verschiedenen Fraktionen als zu umfassend kritisiert (ebd., S. 24587, ebenso 24589).

All diese Einwände führten erneut zu Beschwerden vor dem BVerfG. AktivistInnen von Digitalcourage e.V., die FDP, die Gesellschaft für Freiheitsrechte und die Humanistische Union reichten 2018 ihre Klagen ein. Sie argumentierten, das Gesetz greife unverhältnismäßig und zu unbestimmt in die intimsten Lebensbereiche der BürgerInnen ein und untergrabe die Bürgerrechte (Gesellschaft für Freiheitsrechte, 2018; ZDF, 2018).

---

zu-Ende-Verschlüsselung aber ohnehin unbrauchbar. Der Einsatz staatlicher Spähsoftware wurde daher als angemessene Reaktion vorgeschlagen.

Mit den Bestrebungen, die Beschützer-Rolle entsprechend der neuen Gefahreneinschätzung aus professionalisierten AngreiferInnen und besonders sensiblen Schutzgütern offensiv auszubauen, löste die Bundesregierung eine anhaltende Welle domestischer Kontestationsprozesse aus. Diese stützten sich maßgeblich auf die Rolle als Garant liberaler Grundrechte, auf die die Bundesregierung wiederholt hingewiesen wurde. Maßnahmen wie die Online-Durchsuchung oder die Quellen-TKÜ wurden sowohl von der Zivilgesellschaft als auch der parlamentarischen Opposition scharf kritisiert. Durch Klagen vor dem Bundesverfassungsgericht wurde die Regierung gezwungen, beim Einsatz dieser Maßnahmen zurückhaltender zu sein und sie besser zu kontrollieren. Das Zusammenspiel der unterschiedlichen GegenrollenträgerInnen ermöglichte es, dass die Regierung noch immer keine endgültig stabile Beschützer-Rolle etablieren konnte. Die Kontestation war so folgenreich, da sie sich auf Urteile des Verfassungsgerichts stützen konnten und die Regierung damit autoritativ zur Ausbalancierung der Beschützer-Rolle und der Rolle als Garant liberaler Grundrechte veranlassen konnte. Die Kontestationen gegen eine Erweiterung der Beschützer-Rolle waren am Ende des Untersuchungszeitraumes noch im Gange. Eine stabile Rollenbeziehung, die die Schutzfunktion und die Wahrung der Grundrechte ins Gleichgewicht bringt, war noch nicht gefunden.

Neben diesen Kontestationen mit Bezug zur Grundrechtskonformität der Online-Durchsuchung und der Quellen-TKÜ wurde in diesem Zeitraum parallel auch deutlich, dass die Bundesregierung technisch kaum in der Lage war, ihre Beschützer-Rolle alleine wahrzunehmen. Ausgangspunkt dieser Entwicklung war die öffentliche Diskussion um die Software zur Quellen-TKÜ. Der Chaos Computer Club deckte in einer technischen Analyse der Software auf, dass diese die gesetzlichen Maßgaben nicht erfüllte. Die Funktionalität der Software, die vermutlich von bayerischen ErmittlerInnen verwendet wurde, war nicht nur auf das Abfangen von Kommunikation vor der Verschlüsselung beschränkt, sondern ermöglichte die umfassendere Überwachung des infizierten Gerätes (CCC, 2011). Die Bundesregierung musste in diesem Kontext eingestehen, dass sie den Quellcode, der auf Bundesebene verwendeten Software, nicht einsehen konnte, da dieser als Geschäftsgeheimnis bewertet wurde. Die vorgeschriebene Funktionalität konnte daher nur durch Anwendungstests überprüft werden (Deutscher Bundestag, 2011b, S. 5). Die Software wurde durch die Behörden bei der Firma DigiTask erworben und sorgte in der Folge für massive Kritik an der Bundesregierung (Deutscher Bundestag, 2012, S. 4). Die technische Überprüfung durch den CCC hatte nämlich auch ergeben, dass die Software Sicherheitslücken aufwies, die potenziell von Dritten ausnutzbar waren. Damit konnte der Einsatz zumindest theoretisch auch Kriminellen oder anderen den Zugriff auf die infizierten Rechner erlauben. Der Beschützer hätte also auch das Tor für Unbefugte geöffnet. Zudem zeigte die Analyse, dass die Kommunikation

mit dem Programm über Server in den USA verlief. Die Opposition sah daher die Möglichkeit, dass auch amerikanische Behörden evtl. mitlesen konnten. In der Folge wurde diese Software nicht mehr genutzt (ebd., S. 1f.). In Abstimmung zwischen den Behörden wurde 2012 eine »Standardisierende Leistungsbeschreibung« für die Software erarbeitet, die die Funktionen der Software definierte (Deutscher Bundestag, 2016d, S. 6).

Die Bundesregierung setzte dann auf die Entwicklung eigener Software, dies wurde aber wieder durch privatwirtschaftliche Akteure unterstützt (Bundesministerium des Innern, 2014b). Die Arbeit an diesen Werkzeugen wurde 2015 abgeschlossen. Allerdings wurde auf dem freien Markt zusätzlich eine Ersatzoption eingekauft (Süddeutsche Zeitung, 2014b). Öffentlich wurde darüber spekuliert, dass diese Anschaffung notwendig war, da die selbst entwickelte Software zur Quellen-TKÜ nicht über die notwendige technische Funktionalität verfügte, um in allen Anwendungsumfeldern verwendbar zu sein (Welt, 2016). Diese negative Erfahrung hat die Behörden dazu veranlasst, die nächste Softwaregeneration wieder auf dem freien Markt zu beziehen (Welt, 2018). Dieser Einkauf bei kommerziellen Anbietern hat der Regierung viel Kritik beschert, da diese Software bspw. auch an die Türkei verkauft und dort gegen Oppositionelle eingesetzt wurde. KritikerInnen argumentieren daher, die Bundesregierung befeuere die Nachfrage auf einem Markt, der potenziell bedenklich sei und die IT-Unsicherheit fördere, da er von Softwareschwachstellen lebe. Weiterhin könnten Autokratien, mit Verweis auf den demokratischen Kundenkreis, ihr eigenes Verhalten rechtfertigen (Süddeutsche Zeitung, 2018). Sie wiesen damit darauf hin, dass die Regierung durch den Einkauf von Überwachungssoftware international der Reputation als Garant liberaler Grundrechte schade.

Diese Erfahrung führte dazu, dass die Regierung begann, die eigenen technischen Fähigkeiten auszubauen. Trotz prinzipieller Kritik am staatlichen Hacking, das immer auch auf Schwachstellen in Software angewiesen ist und diese daher geheim hält, hat die Bundesregierung 2016 erste Pläne entwickelt, eine Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) einzurichten. Damit trennte die Bundesregierung den Bereich der offensiven Nutzung von Cyberfähigkeiten institutionell vom defensiv ausgerichteten BSI (Süddeutsche Zeitung, 2017).

Die Regierung plante, die Ermittlungsbehörden durch diese neue Institution in die Lage zu versetzen, ihre Aufgaben besser erfüllen zu können. Konkret »geht es um eine Anpassung der technischen Fähigkeiten an die aktuellen Herausforderungen der Kommunikationswelt« (Deutscher Bundestag, 2016d, S. 2). Mit dem Erlass vom 6. April 2017 wurde die neue Institution mit 400 Planstellen offiziell als Bundesanstalt im Geschäftsbereich des BSI etabliert. ZITiS selbst erhielt keine Eingriffsbefugnisse, sondern bietet dem BKA, dem BfV und der Bundespolizei technische Unterstützung mit Blick auf deren operative »IT-Fähigkeiten«

(Deutscher Bundestag, 2018d, S. 2). Eine Kernaufgabe ist dabei die Kryptoanalyse (ebd., S. 10).

Damit baute die Bundesregierung die Kapazitäten aus, die zur Umgehung von Verschlüsselung notwendig sind. Eine Entwicklung, die parallel auch auf europäischer Ebene bei Europol stattfand und dort ebenfalls durch die Bundesregierung unterstützt wurde (Deutscher Bundestag, 2018b). Der Präsident der Zentralen Stelle für Informationstechnik im Sicherheitsbereich Wilfried Karl betonte in diesem Kontext aber, dass dies die Kryptopolitik der Bundesregierung nicht verändere:

> »Es gibt heute Verschlüsselungsmethoden, die mathematisch nicht zu brechen sind. Wir maßen uns nicht an, hierfür eine Lösung zu finden. Aber es gibt durchaus Möglichkeiten, mit entsprechender Hardware und schlauen Algorithmen sowie den entsprechenden Experten zu Ergebnissen zu kommen. Etwa, wenn eine Verschlüsselung nicht ordentlich implementiert wurde oder wenn Anwender Fehler gemacht haben. Wenn wir Methoden finden, dann stellen wir sie unseren Kunden zur Verfügung. Wir ändern übrigens nichts an der Kryptopolitik der Bundesregierung. Es geht hier nicht um eine Schwächung von Kryptoverfahren.« (Behörden Spiegel, 2018)

Neben der Umgehung von Verschlüsselung ging mit den Aufgaben von ZITiS auch einher, dass gefundene Schwachstellen in Software aus staatlichen Sicherheitsinteressen ggf. offengehalten werden. Im Gegensatz zu anderen Staaten (bspw. den USA oder dem Vereinigten Königreich), gab es aber noch kein definiertes Verfahren, durch das die Geheimhaltung oder Offenlegung von Sicherheitslücken geregelt wurde. Die Gestaltung dieses Entscheidungsprozesses war am Ende des Untersuchungszeitraumes noch im Gange. Die Regierung hat aber bekanntgegeben, dass ZITiS bis 2018 noch keine Schwachstellen aus externen Quellen eingekauft hatte (Deutscher Bundestag, 2018d, S. 13).

Die neue Institution wurde von Seiten der Netzgemeinschaft und der politischen Opposition scharf kritisiert. Ein Anlass für Kritik war bspw. der fehlende Kriterienkatalog zur Entscheidung über die Offenlegung von Sicherheitslücken (derartige Abwägungen werden zumeist als Vulnerabilities Equities Processes bezeichnet). Hierauf wurde bspw. durch den ehemaligen Datenschutzbeauftragten Peter Schaar oder durch Digitalcourage hingewiesen (Digitalcourage, 2017; heise.de, 2018a). Parlamentarisch wurde von der Linkspartei sogar gefordert, ZITiS wieder aufzulösen. Die neue Institution gefährde »die Datensicherheit und Grundrechte aller Bürgerinnen und Bürger« und verletze das »Trennungsgebot zwischen Polizei und Geheimdiensten« (Deutscher Bundestag, 2019).

Das Bestreben der Bundesregierung, die Beschützer-Rolle durch den Aufbau eigener technischer Fähigkeiten auszubauen und unabhängiger zu gestalten, ist wiederum herausgefordert worden. Auch wenn die Bundesregierung betonte,

dass sie an starker Verschlüsselung festhalte und keine Unterminierung der Technik anstrebe, bemängelte die Opposition, dass die Regierung die Rolle nicht klar genug definierte und bspw. keinen Prozess für die Offenlegung von Schwachstellen definierte. Mit dem Verweis auf das Trennungsgebot bezogen sich KritikerInnen wiederum auf das negative historische Selbst der Bundesrepublik.

Die domestischen Prozesse der Rollenkontestation, insbesondere mit Bezug auf die Rolle als Garant liberaler Grundrechte, begünstigten auch eine zurückhaltende außenpolitische Rollenübernahme der Bundesrepublik. Aktuelle Bestrebungen in der EU mit Regelungen zu digitalen Beweismitteln (E-Evidence) den Zugriff auf Daten in anderen Staaten jenseits internationaler Rechtshilfe zu erleichtern und Diensteanbieter direkt gegenüber externen Strafverfolgungsbehörden auskunftspflichtig zu machen, werden von der Bundesrepublik skeptisch beurteilt. In einem Brief an die Kommission äußerte die Regierung zusammen mit sieben weiteren EU-Mitgliedstaaten Bedenken mit Blick auf die extraterritoriale Geltung der Beschützer-Rolle. Die Bundesregierung bemängelte dabei, dass die vorgesehene Neuregelung den Empfängerstaaten keine Möglichkeit einräume, die externen Datenanfragen abzulehnen. Dies sei besonders vor dem Hintergrund einer fehlenden beiderseitigen Strafbarkeit problematisch, da so Ermittlungen möglich wären, die unter deutschem Recht nicht durchführbar wären. Ferner bedürfe es in einem solchen System Vorkehrungen zum Schutz der Bürgerrechte (Justizministerium, 2018).

Auch die Absicht zwischen EU und USA ein solches Abkommen zum erleichterten Zugriff auf Meta- und Inhaltsdaten zu etablieren, wurde von der Bundesregierung aufgrund bürgerrechtlicher Bedenken kritisch beurteilt. Die Bundesrepublik hat den Vorschlägen daher nicht zugestimmt, sie wurde aber von der Mehrheit im Rat überstimmt (heise.de, 2019). In einem von Netzpolitik.org veröffentlichten Hintergrundpapier äußerte die Bundesregierung besondere Bedenken gegen eine Ausweitung der EU-Regelungen mit den USA. Diese sehen im CLOUD Act nicht nur die Abfrage gespeicherter Daten vor, sondern auch den Zugriff auf laufenden Datenverkehr – also das unmittelbare Abfangen übertragener Kommunikation (Bundesregierung, 2019b, S. 3). Damit ist eine Facette der Beschützer-Rolle berührt, die die deutsche Bundesregierung für die eigenen Strafverfolgungsbehörden noch nicht stabil etablieren konnte.

Da die Bundesregierung die Beschützer-Rolle domestisch noch nicht sicher etablieren konnte, ist die extraterritoriale Teilung der Rolle derzeit kaum möglich. Die besonderen Bedenken und die damit verbundenen Kontestationsprozesse der domestischen Gegenrollenträger sorgen dafür, dass anderen Strafverfolgungsbehörden kein freier Zugriff auf die Daten deutscher Firmen gewährt wird.

## 4.2 Vereinigtes Königreich

### 4.2.1 Das britische IT-Strafrecht: Domestische Etablierung eines neuen Rechtsrahmens

In Großbritannien wurde 1990 mit dem Computer Misuse Act (CMA) die Grundlage zur strafrechtlichen Verfolgung von Cyberkriminalität gelegt. Im Gegensatz zur deutschen Entwicklung des Computerstrafrechts wurde im Vereinigten Königreich aber durch einen Angriff auf das interaktive Videotextangebot der British Telecom deutlich, dass die Beschützer-Rolle im Zeitalter der Vernetzung neu definiert werden musste. Robert Schifreen und Stephen Gold waren Ende 1984 in das Prestel-System der BT eingedrungen und hatten dabei auch Zugriff auf den persönlichen Posteingang von Prinz Philip. Von diesem Account aus verschickten sie Mails, die dazu führten, dass Angestellte der BT auf den Angriff aufmerksam wurden. Im April 1985 wurden sie identifiziert und unter dem Forgery and Counterfeiting Act 1981 angeklagt. Sie wurden in erster Instanz zu geringen Geldstrafen verurteilt (Murray, 2016, S. 358 f.). Beide entschieden sich jedoch dazu, das Urteil anzufechten und wurden in der Folge freigesprochen, da das Gesetz nicht die erforderliche Grundlage für eine Verurteilung liefere. Diese Entscheidung wurde im April 1988 durch das House of Lords bestätigt (House of Lords, 1988).

Vor diesem Hintergrund veröffentliche die Law Commission im August 1988 ein Working Paper, das die neuen Probleme der Computerkriminalität eingehend diskutierte, Regulierungsdefizite des bestehenden Rechts aufwarf und verschiedene Reformoptionen aufzeigte.[7] Hierbei wurde auch auf Erfahrungen in anderen Staaten (darunter Deutschland) sowie auf die Entwicklungen in der OECD verwiesen (The Law Commission, 1988, S. 109-128). Die Kommission identifizierte zwar legislativen Handlungsbedarf beim unbefugten Zugriff auf Computersysteme – ein Problem, das durch den Angriff von Schifreen und Gold offengelegt wurde – diskutierte die Möglichkeiten einer Kriminalisierung aber auch kritisch.

Die Etablierung eines neuen Straftatbestandes zum Eindringen in Computersysteme wurde unter anderem deshalb kritisch gesehen, weil ein Zugriff nicht in gleichem Maße als Verletzung der Persönlichkeitsrechte interpretiert wurde, wie in Deutschland:

---

7 Bereits 1987 hatte die Scottish Law Commission ein Working Paper zur Regulation von Computerstraftaten publiziert. Da das schottische Rechtssystem noch stärker auf dem Fallrecht beruht, war diese Kommission etwas skeptischer, was eine gesetzliche Neuregelung anging. Die Möglichkeit das Recht durch neue Fälle und die richterliche Auslegung weiterzuentwickeln schien aus dieser Perspektive noch nicht gänzlich ausgeschöpft (Wasik, 2010, S. 402).

> »No general right of privacy exists in English law even in the law of tort, and while obtaining unauthorised access to a computer may appear to be akin to the tort of trespass, such behaviour is not generally subject to criminal sanction without some further aggravating feature. Information is not property in English law [...] and it is no offence, as such, to read someone else's correspondence or files.« (Ebd., S. 81)

Die Beschützer-Rolle fand in der Folge eine deutlichere Referenz (Schutz für wen?) zum wirtschaftlichen Schutzgut, als auch zur physischen Sicherheit. Dem Working Paper folgte ein offener Konsultationsprozess in dem sowohl die Zivilgesellschaft als auch Wirtschaftsunternehmen zu Stellungnahmen aufgefordert waren. Ziel der Kommission war es, einen Eindruck von der empirischen Dringlichkeit des Problems zu erhalten, um dann fundierte Empfehlungen auszusprechen. Nach Auswertung der Rückmeldungen gelangte die Kommission im Oktober 1989 zu der Einschätzung, dass Hacking ein akutes wirtschaftliches und sicherheitspolitisches Problem geworden war und dass legislative Maßnahmen daher angebracht waren (The Law Commission, 1989, S. 6).

Dem Papier folgte 1989 der Vorschlag, drei neue Straftatbestände in einem Gesetz zu etablieren. Im Gegensatz zur deutschen Entwicklung wurde die Beschützer-Rolle in Großbritannien bereits in dieser Phase auch durch verstärkte sicherheitspolitische Erwägungen geprägt. Diese Dynamik zeigte sich in Verweisen auf Vorfälle, in denen Personen durch falsch programmierte Fertigungsanlagen physisch verletzt wurden (ebd., S. 3). Ähnlich wie in Deutschland wurde die Beschützer-Rolle aber auch durch wirtschaftliche Erwägungen, wie bspw. hohe Kosten zur Wiederherstellung der Systeme, ermöglicht (ebd., S. 6). Die Kommission erkannte die Regelungsnotwendigkeit aber nicht, weil Informationen als besonders schützenswert erachtet wurden, sondern, um die Integrität der Systeme und deren Funktionsfähigkeit zu wahren:

> »[...] the main argument in favour of a hacking offence does not turn on the protection of information, but rather springs from the need to protect the integrity and security of computer systems from attacks from unauthorised persons seeking to enter those systems.« (The Law Commission, 1988, S. 7)

Der Entwurf für den Computer Misuse Act wurde durch den Konservativen Abgeordneten Michael Colvin in das Unterhaus eingebracht. Auch er wies explizit darauf hin, dass das Gesetz nicht in erster Linie Informationen schützen sollte, sondern die Integrität der Systeme. Dieser Fokus blieb nicht ohne Kritik (insbesondere mit Blick auf Gesundheitsdaten), im Unterhaus wurde daher explizit hervorgehoben, dass, wenn der unberechtigte Zugang für weitere strafbare Handlungen genutzt würde, bspw. zur Informationsgewinnung und Erpressung, dies unter Section 2 ebenfalls erfasst sei (House of Commons, 1990b, S. 1138).

Der Fokus der Beschützer-Rolle auf folgenreiche Cyberangriffe findet Ausdruck in der expliziten Ablehnung eines Hacker-Privilegs, das die deutsche Regierung zunächst noch anerkannte. Im Gegensatz zur deutschen Beschützer-Rolle fand die britische einen der ersten Referenzpunkte (Schutz vor wem?) daher nicht im technisch interessierten Freizeithacker, sondern sanktionierte alle unbefugte Zugriffe (The Law Commission, 1988, S. 12). Dieser Standpunkt wurde im Parlament geteilt und fand Eingang in das Gesetz, auch wenn die Frage einer Überkriminalisierung debattiert wurde, wurden HackerInnen doch prinzipiell als gefährlich betrachtet, so dass deren Verhalten stets als strafbar erachtet wurde (House of Commons, 1990b, S. 1147). Diese Referenz auf potenziell folgenreiche Angriffe zeigte sich auch in den debattierten Szenarien, die bspw. Angriffe auf Krankenhäuser, militärische Einrichtungen oder Verkehrsleitsysteme umfassten (House of Commons, 1990b; House of Lords, 1990).

Die Kommission empfahl die Etablierung von drei neuen Straftatbeständen, die dann in den Computer Misuse Act übernommen wurden: »1. Unauthorised access to computer material. 2. Unauthorised access with intent to commit or facilitate commission of further offences. 3. Unauthorised modification of computer material« (The Stationery Office, 1990, Sections 1, 2, 3). Aus der Ablehnung einer/s potenziell wohlwollenden Hackerin/s und der daraus folgenden Referenz (Schutz vor wem?) auf gefährliche AngreiferInnen folgte auch, dass der Computer Misuse Act in Section 14 neue Kompetenzen zur Beschlagnahme und Durchsuchung bereits für den eigentlich als Ordnungswidrigkeit (summary offences) eingestuften Tatbestand »Unauthorised access to computer material« definierte (ebd., Section 14). Diese Ausweitung der Befugnisse der Strafermittlungsbehörden wurde im House of Commons besonders kritisch diskutiert, letztlich aber mehrheitlich akzeptiert (House of Commons, 1990b; House of Lords, 1990).

In der parlamentarischen Debatte wurde zur Rechtfertigung der neuen Regelungen, wie in der Kommission, wiederholt auf die wirtschaftlichen Kosten der Computerkriminalität, die steigenden Fallzahlen sowie die vermutlich hohe Dunkelziffer verwiesen (House of Commons, 1990b, S. 1134 bzw. 1143). Auch WirtschaftsvertreterInnen (bspw. der Arbeitgeberverband CBI) betonten unter Bezugnahme hierauf die Regulierungsnotwendigkeit (House of Commons, 1990a, S. 1291). Ähnlich wie in Deutschland wurde auch hier von VertreterInnen unterschiedlicher Parteien auf die rasante Verbreitung der Technik und damit die wachsende gesellschaftliche Bedeutung hingewiesen:

> »Government computerisation has made us all a great deal more vulnerable, as has company computerisation. The City of London money markets, Lloyd's and all sorts of financial organisations that have made Britain financially great and far advanced depend upon computers.« (House of Commons, 1990b, S. 1154)

Insgesamt wurde der Gesetzesentwurf daher überparteilich unterstützt. Dies wurde auch dadurch begünstigt, dass er als *private member's bill* eingebracht wurde (ebd., S. 1158). Es wurde aber auch kritisiert, dass die Regierung nicht selbst einen Vorschlag zur Regulierung vorgelegt hatte. Im Gegensatz zur Entwicklung in Deutschland, in der die (unterschiedlichen) Regierungen die Entwürfe maßgeblich vorangetrieben haben, war die Etablierung der Beschützerrolle in Großbritannien Ergebnis parlamentarischen Regulationsstrebens.

Wie bereits angedeutet, zeigt sich hier ein Unterschied zu der Entwicklung in Deutschland. Wie in Deutschland lag die Referenz (Schutz für wen?) zwar auf dem Schutz ökonomischen Wohlstands. Die Rolle als Wohlstandsmaximierer wirkte somit katalytisch auf die Etablierung der Beschützer-Rolle. Im Unterschied zu Deutschland stand in Großbritannien aber bereits in der Frühphase nicht das Verhalten von FreizeithackerInnen zur Debatte. Diskussionen befassten sich vielmehr bereits zu diesem Zeitpunkt mit physischen Folgen von Cyberangriffen, sodass die Referenz der Rolle (Schutz vor wem) von Beginn an eine andere war.

Da in Großbritannien erst vergleichsweise spät über eine Kriminalisierung von Computerstraftaten debattiert wurde (auch im Vergleich zu Deutschland), wurde die Etablierung der Beschützer-Rolle in stärkerem Maße durch internationale Erwartungen begünstigt. Die Abgeordneten befürchteten, dass das Vereinigte Königreich ohne eine Kriminalisierung der Computerstraftaten international zum Rückzugsort für HackerInnen werden könnte (ebd., S. 1135). Es galt also internationale Reputationsverluste aufgrund einer fehlenden bzw. defizitären Beschützer-Rolle zu vermeiden. Der internationale Rollenbezug wurde dabei auch durch die Devolution des Vereinigten Königreichs und potenziell unterschiedliche Regelungen selbst befördert (House of Lords, 1990, S. 231).

Die internationale Ausrichtung ist auch deshalb bemerkenswert, weil damit verbunden die Rolle als Garant liberaler Grundrechte einen zusätzlichen Bezugspunkt hat, nämlich auf der neu entstehenden Infrastruktur. Zum Zeitpunkt der Gesetzesverabschiedung wurde in Großbritannien bereits auf die Notwendigkeit eines international koordinierten Vorgehens verwiesen, um auch langfristig ein freies Internet zu gewährleisten:

> »Without legislation that is agreed internationally, to the effect that unauthorised access is a crime, there is a real danger that owners of computer network systems will be encouraged to erect ring fences of security around their systems. One has in mind university systems that are useful for sharing information and data. Without the law to convict unauthorised users of those systems, there is a danger that the systems will be less open and less available and that society will suffer as a result.« (House of Commons, 1990b, S. 1159)

Die Beschützer-Rolle ist in diesem Kontext also auch durch die Rolle als Garant liberaler Grundrechte begünstigt. Die Referenz (Schutz für wen?) liegt aber nicht

nur auf dem Schutz der eigenen Wirtschaft bzw. Bevölkerung, sondern auch auf dem Erhalt des freien Netzes. Dies ist besonders bemerkenswert, da das globale Internet zu dieser Zeit noch nicht in seiner späteren Form erkennbar war. Es ist damit auch die internationale Rollenausrichtung, die für die britische Etablierung der Beschützer-Rolle bedeutend war. Sie weist von Beginn an stärkere extraterritoriale bzw. internationale Bezüge auf.

Ferner adressierte die britische Rolle bereits im Jahr 2000 terroristische Gefahren, während die deutsche Beschützer-Rolle eine terroristische Referenz (Schutz vor wem?) erst später, nach den Anschlägen des 11. Septembers, fand. Mit dem Terrorism Act 2000 wurden explizit auch solche Cyberangriffe unter Strafe gestellt, die darauf ausgerichtet waren »to interfere with or seriously to disrupt an electronic system« (The Stationery Office, 2000c, Section 1(2)(e)). Mit bis zu zehn Jahren Freiheitsstrafe war auch das Strafmaß im Vergleich zu Deutschland deutlich höher, wo zu dieser Zeit die Referenz zu Terrorismus noch nicht gesetzlich hergestellt wurde. Diese Ausrichtung der britischen Beschützer-Rolle wurde durch die Bezugnahme auf historische Erfahrungen, insbesondere mit dem irischen Terrorismus, erleichtert. Die Referenz ist damit auf den domestischen Terrorismus bezogen und findet sich in verschiedenen Debatten sowohl auf Seiten der Regierung als auch in beiden Kammern des Parlaments (House of Commons, 1999a, 2000a; House of Lords, 2000). Der Bezug zum historischen Selbst als Opfer terroristischer Anschläge ermöglichte damit bereits früher eine sanktionsbewährtere Beschützer-Rolle, die auch domestisch weniger herausgefordert wurde als in Deutschland (The Stationery Office, 2000c).

### 4.2.2 Kryptopolitik

Auch in Großbritannien wurde Mitte der 1990er Jahre eine Debatte um die Regulation von Verschlüsselung geführt. In diesem Kontext wiesen VertreterInnen der Tory-Regierung, ähnlich wie in der Bundesrepublik, darauf hin, dass die Ermittlungsbehörden durch starke Verschlüsselung nicht in ihrer Arbeit eingeschränkt werden dürften. Es galt also die Funktionsfähigkeit der Beschützer-Rolle zu gewährleisten. Eine Regelung müsse daher darauf zielen »to preserve the ability of the intelligence and law enforcement agencies to fight serious crime and terrorism« (Department of Trade and Industry, 1997).

Nach interministeriellen Konsultationen veröffentlichte das Department for Trade and Industry 1996 ein Strategiepapier, das die Pläne der Regierung skizzierte. Die Beschützer-Rolle, die in diesen ersten Entwürfen dargelegt wurde, war deutlich von der amerikanischen Rolle inspiriert. Die Regierung beabsichtigte ein System aus gewerblichen Trusted Third Partys (TTPs) zu installieren, die die Verschlüsselung staatlich lizenziert übernehmen sollten. Die TTPs sollten gesetzlich dazu verpflichtet werden, eine Schlüsseldublette zu verwahren,

um diese den Sicherheitsbehörden zu Ermittlungszwecken zur Verfügung stellen zu können. Wie die amerikanische Administration, wollte auch die britische Regierung an Exportbeschränkungen für Verschlüsselungslösungen festhalten, die keine Key-Recovery-Funktionalität beinhalteten (ebd.). Ferner wurde darüber debattiert, dass auch die Schlüssel, die nicht bei TTPs hinterlegt waren, verfügbar sein sollten (House of Commons, 1999c). Um Zugriff auf die Schlüssel zu erhalten, die nicht bei britischen TTPs hinterlegt würden, sollten internationale Abkommen zur Kooperation bei der Strafverfolgung geschlossen werden (Trade and Industry Select Committee, 1999).

Im Gegensatz zur Bundesrepublik wurde in Großbritannien ein umfassendes und potenziell globales Key-Escrow-System von der Tory-Regierung nicht abgelehnt (ebd.). Zwar wurde eine amerikanische Dominanz und die extraterritoriale US-Beschützer-Rolle in diesem Kontext ebenfalls kritisch gesehen. Dies hatte aber keine strikte Ablehnung der Key-Recovery zur Folge, sondern führte zu Debatten darüber, wie ein solches System besser ausgestaltet werden könne. Stimmen aus der Regierung befürworteten daher grundsätzlich Lösungen zur Schlüsselhinterlegung auch unter Verweis auf deren potenziell positive Effekte für die wirtschaftliche Entwicklung. Nur mit einer (globalen) Schlüsselinfrastruktur könne auch das Vertrauen der Unternehmen und KundInnen in die Verschlüsselung der GeschäftspartnerInnen erhalten werden (Hickson, 1997, S. 584).

Kritik erfuhren diese Pläne aus der Wirtschaft und Zivilgesellschaft, auch Teile der zu diesem Zeitpunkt oppositionellen Labour Party lehnten das Vorhaben als zu weitreichend ab. Nur wenige Stimmen unterstützten die Pläne der Regierung ohne substanzielle Einschränkungen (Trade and Industry Select Committee, 1999). Die KritikerInnen warfen der Regierung unter anderem vor, mit einer Schwächung der Verschlüsselung nicht nur Wirtschaftsgeheimnisse zu gefährden, sondern auch weitreichende Überwachungsmöglichkeiten zu schaffen (Akdeniz, 1997; Hickson, 1997). Die Ablehnung erfolgte also vornehmlich im domestischen, nicht im internationalen Rollenspiel als Abgrenzung zur USA. Dies hilft zu verstehen, warum britische Regierungen international immer wieder die Regulation von Kryptographie offen diskutiert haben.

Als bei den Wahlen 1997 die konservative Regierung von John Major durch die Labour-Administration von Tony Blair ersetzt wurde, hielt die neue Regierung nach dem Wahlsieg trotz voriger Kritik an den Plänen zur Key-Recovery fest. Im Unterschied zur Vorgängerregierung sollten die Regelungen aber nicht mehr verpflichtend sein, sondern auf freiwilliger Kooperation mit den TTPs basieren (Trade and Industry Select Committee, 1999).

Im Vorwort einer Analyse unterschiedlicher Möglichkeiten zum Umgang mit dem Problem, konstatierte der neue Premierminister Tony Blair: »there is already evidence that criminals, such as paedophiles and terrorists, are using encryption to conceal their activities. […] If powers of interception and seizure are rende-

red ineffective by encryption, all society will suffer« (Cabinet Office, 1999, S. i). Ähnlich wie in Deutschland wurde damit auf die potenziellen Beschränkungen der Beschützer-Rolle verwiesen, die dazu führen würden, dass Strafverfolgung nicht mehr effektiv gewährleistet werden könne. Anders als in der Bundesrepublik führte aber die ausbleibende Referenz auf ein negatives historisches Selbstbild und die damit verbundenen Bedenken zu liberalen Freiheitsrechten dazu, dass die Regelung zur Schlüsselhinterlegung mit Plänen zu einem neuen Electronic Communications Act im Vereinigten Königreich für fünf Jahre implementiert wurden (The Stationery Office, 2000a). Deutliche Kritik aus der Wirtschaft und aus dem Parlament sorgten aber dafür, dass die Regelung – anders als von der Vorgängerregierung geplant – freiwillig war und dass weitere sicherheitspolitische Maßnahmen zum Umgang mit Verschlüsselung aus dem Gesetz gestrichen wurden (Trade and Industry Select Committee, 1999).

Stimmen, die darauf hinwiesen, dass sich die Politiken der internationalen Partner mit Blick auf Key-Escrow verändert hatten, dass die OECD-Guidelines dazu aufriefen NutzerInnen die freie Wahl der Verschlüsselung zu überlassen und die daher dafür plädierten, die Regelungen auch nicht auf freiwilliger Basis in Kraft zu setzen, konnten sich zunächst nicht durchsetzen. Wie in Deutschland wurde die Kritik auch hier unter Verweis auf die beiden Rollen als Wohlstandsmaximierer (von Akteure aus der Wirtschaft) und Garant liberaler Grundrechte (von Bürgerrechtsbewegungen und VertreterInnen der technischen Community) artikuliert (House of Commons, 1999b; Trade and Industry Select Committee, 1999).

Die Abgeordneten im Ausschuss für Handel und Industrie brachten ihre Enttäuschung über die Position der Regierung offen zum Ausdruck: »We are disappointed, however, that the Government should still hold a candle for key escrow and key recovery. […] We can foresee no benefits arising from Government promotion of key escrow or key recovery technologies« (Trade and Industry Select Committee, 1999, S. VIII – 90.). Grundsätzlich machten die Parlamentarier deutlich, das sie mit der Kooperation zwischen Regierung und Wirtschaft mit Blick auf Verschlüsselung nicht zufrieden waren und dass sie die Schuld dafür bei der Regierung sahen (ebd., S. VIII – 105.).

Auch wenn die Kritik nicht dafür gesorgt hat, dass das freiwillige System aus TTPs aufgegeben wurde, hat der Widerstand verschiedener Akteure doch dazu geführt, dass die Regelung zur freiwilligen Schlüsselhinterlegung mit einem fünfjährigen Verfallsdatum (sunset clause) versehen wurde, 2006 wurde die Regel endgültig ausgesetzt (House of Commons, 1999b). Die Regierung begründete die endgültige Abkehr von einer verpflichtenden Schlüsselhinterlegung dann auch mit den Bedenken, diese könnten die Internetwirtschaft in Großbritannien nachhaltig schädigen, insbesondere da die internationale Konkurrenz nicht durch derartige Arrangements beeinträchtigt worden war (House of Commons, 2000d, S. 775).

Die Rolle als Garant liberaler Grundrechte wirkte damit weniger begrenzend auf die Beschützer-Rolle als in Deutschland. Auch aufgrund der besonderen Beziehung zu den USA, wurde der Vorstoß der amerikanischen Regierung nicht rundum abgelehnt. Da die Referenz zu einem negativen historischen Selbst ebenfalls ausblieb, konnte die britische Regierung in der Folge immer wieder eine restriktivere Verschlüsselungspolitik verfolgen. Am folgenreichsten war letztlich die Kontestation der WirtschaftsvertreterInnen, die mit Bezug zur Rolle als Wohlstandsmaximierer, die besondere Bedeutung von Verschlüsselung für das Netz als Wirtschaftsraum herausstellte und betonte, dass starke Kryptografie für ein vertrauensvolles Verhältnis der Wirtschaftssubjekte essenziell sei. Den Wettbewerbsnachteil einer freiwilligen Schlüsselhinterlegung gab die Regierung daher auf. Sie suchte aber nach neuen Möglichkeiten die Beschützer-Rolle aufrechtzuerhalten.

Da es sich bei den Vorschriften im Electronic Communications Act um freiwillige Regelungen handelte, wurde für den Umgang mit Verschlüsselung der im Jahr 2000 verabschiedete Regulation of Investigatory Powers Act (RIPA) bedeutend – insbesondere, als die Sunset Clause 2006 zum Auslaufen der freiwilligen Regeln für Kryptographiedienstleister führte. Mit RIPA wurden einige der sicherheitspolitischen Maßnahmen etabliert, die bereits zuvor debattiert wurden, aber aufgrund des Drucks aus Parlament und Wirtschaft nicht mit dem Electronic Communications Act reguliert wurden. Um den Strafverfolgungsbehörden Zugriff auf verschlüsselte Kommunikation zu ermöglichen, ohne dabei Kritik für die Unterminierung von Kryptographie im Allgemeinen zu erfahren, wurde mit RIPA die Möglichkeit geschaffen, von Verdächtigen sanktionsbewährt die Herausgabe der privaten Schlüssel zu fordern. In den Debatten zu RIPA wurde der Konflikt zwischen den Rollen Wohlstandsmaximierer, Garant liberaler Grundrechte und Beschützer erneut deutlich (ebd.).

Auch die Regierungsseite erkannte die Probleme einer Unterminierung von Verschlüsselung an, sah es aber dennoch als unabdingbar, andere Möglichkeiten zur erzwungenen Schlüsselherausgabe zu etablieren. Die Regierung argumentierte, dass die neuen Regelungen nur dazu dienten, bereits existierende Kompetenzen im Angesicht technischer Entwicklungen zu erhalten. Es ging aus ihrer Sicht also nicht um den Ausbau der Beschützer-Rolle. Ferner versicherte Innenminister Jack Straw, dass die Ermittlungsbehörden nur Zugriff auf Schlüssel von rechtmäßig abgefangenen Daten verlangen könnten. Die Beschützer-Rolle wurde aus Sicht der Regierung durch die Rolle als Garant liberaler Grundrechte angemessen begrenzt. Die Forderung, den Ermittlungsbehörden die Möglichkeit zu geben, Schlüssel unter Androhung von Zwangsmaßnahmen zu fordern, wurde grundsätzlich auch von Teilen des Parlaments anerkannt (Trade and Industry Select Committee, 1999, S. VIII – 98.). Auch wenn es kritische Stimmen aus der Wirtschaft gab, stimmte auch der Ausschuss für Handel und Industrie der

Einschätzung zu, wonach die Befugnis zur Schlüsselherausgabe eine wichtige Kompetenz der Ermittlungsbehörden sei (House of Commons, 2000d, S. 775).

Allerdings machte die Opposition auch auf Probleme aufmerksam. Abgeordnete wiesen darauf hin, dass die Strafe für die Nichtherausgabe des Schlüssels möglicherweise geringer sein könnte als das Strafmaß für das verfolgte Delikt und dass daher ggf. eher Strafen für die Zurückhaltung der Schlüssel akzeptiert würden, als mit den Ermittlungsbehörden zu kooperieren. Ferner betonten sie, dass NutzerInnen nicht dafür belangt werden dürften, wenn Schlüssel automatisch geändert würden. Auch die Unschuldsvermutung würde durch die Regeln »auf den Kopf gestellt«, da Verdächtige nachweisen müssten, den Schlüssel nicht zu besitzen bzw. zu kennen. Weiterhin erschien es problematisch, von Beschuldigten Informationen zu verlangen, die sie selbst belasten könnten (Trade and Industry Select Committee, 1999, S. VIII). Punkte, die in der Debatte im Unterhaus wiederholt aufgegriffen und kritisiert wurden (House of Commons, 2000d). Allerdings ohne Erfolg, die Regierung etablierte mit RIPA die Möglichkeit, die Herausgabe von privaten Schlüsseln zu fordern, sofern Ermittlungsbehörden auf rechtmäßigem Wege an verschlüsselte Daten gelangten. Andernfalls drohten Freiheitsstrafen von bis zu zwei Jahren. War die nationale Sicherheit oder Kinderpornographie betroffen, reichte das Strafmaß bis zu fünf Jahren (Parliamentary Office of Science and Technology, 2006; The Stationery Office, 2000b). Part III Section 49 von RIPA sollte es Ermittlungsbehörden aus Gründen der nationalen Sicherheit, zur Strafverfolgung (bzw. -vereitelung) oder im Interesse des ökonomischen Wohlergehens des Vereinigten Königreichs ermöglichen, die Herausgabe von privaten Schlüsseln bzw. die lesbare Form der verschlüsselten Daten zu fordern. Die Betroffenen konnten ferner dazu verpflichtet werden, die Anordnung geheim zu halten. Von Kommunikationsdienstleistern verlangte RIPA, die Möglichkeiten zum Abfangen von Kommunikationsinhalten vorzuhalten und daher Verschlüsselung zu entfernen, sofern diese von den Communication Service Providern (CSP) selbst implementiert wurde (Severson, 2017, S. 6f.). Die Definition von CSPs ist dabei im Vereinigten Königreich umfassender als in Deutschland. Während in Deutschland Telekommunikationsdienstleister von Telemedien unterschieden werden, kennt die britische Rechtslage diese Differenzierung nicht. Damit werden bspw. auch Betreiber von Messengerdiensten erfasst und die Beschützer-Rolle ist dementsprechend umfassender (Home Office, 2015a, S. 6). Außerdem ist die Beschützer-Rolle in Großbritannien enger mit der Rolle als Wohlstandsmaximierer verbunden. Hierdurch entstehen auch katalytische Wechselwirkungen, wenn es bspw. um die Schlüsselherausgabe zum Erhalt des ökonomischen Wohlergehens des Vereinigten Königreiches geht.

Die neuen Regelungen wurden letztlich von einer überparteilichen Mehrheit als angemessen beurteilt. Sogar die oppositionellen Liberal Democrats konstatierten, dass es Umstände gebe, in denen derartige Kompetenzen zur Entschlüsselung

notwendig seien, um Schaden von der britischen Bevölkerung abzuwenden und die Sicherheit zu gewährleisten: »it would be a very serious omission to have no means of intercepting and reading encrypted communications between dangerous criminals embarking on a very serious crime, or between people attempting to threaten the lives of the people of this country« (House of Commons, 2000b, S. 1206).

Aufgrund der vorgetragenen Kritik, wurde Part III allerdings bei der Verabschiedung des Gesetzes noch außer Kraft gesetzt und sollte zu einem späteren Zeitpunkt aktiviert werden, sofern die zunehmende Nutzung von Verschlüsselung zu einem maßgeblichen Problem der Strafverfolgungsbehörden werden würde. Dass dieser Fall irgendwann eintreten würde, betonte der Innenminister bereits bei den ersten Parlamentsdebatten:

> »The gloomy prognosis, though, is that whatever is done, law enforcement will take a hit over encryption. [...] Introducing the measures in part III is the least that we can do to minimise the effect of that hit. They form an important part of the package of measures that we are putting in place if we are to have any hope of dealing successfully with the threat from the criminal use of encryption.« (House of Commons, 2000d, S. 777)

Aus Sicht der Regierung war der kritische Punkt im Juni 2006 erreicht. Die Administration kündigte daher Konsultationen zur Aktivierung der Befugnisse an. Die Pläne, dass die Regierung die Einführung der sogenannten Section 49 Notices erwog, führte bei Bürgerrechtsbewegungen zu vehementer Kritik (EDRi, 2006). Das Innenministerium rechtfertigte die Konsultationen und letztlich die Aktivierung der neuen Befugnisse damit, dass die Ermittlungsbehörden immer häufiger auf verschlüsselte Daten stießen und dass deren Arbeit hierdurch signifikant beeinträchtigt würde. Neben Kriminalität verwies das Innenministerium wiederholt auf die Gefahr terroristischer Aktivitäten, die unter dem Deckmantel von Verschlüsselung potenziell unentdeckt bleiben könnten. Aus Sicht der Regierung wurde dieses Problem zwischen 2003 und 2006 immer deutlicher, sodass zwingender Handlungsbedarf bestand, da die Funktion der Beschützer-Rolle nicht mehr gewährleistet werden konnte (Home Office, 2006, S. 3). Die Konsultationen mit VertreterInnen aus Wirtschaft, Zivilgesellschaft und Wissenschaft führten, trotz anhaltender Kritik, dazu, dass die entsprechenden Befugnisse im Oktober 2007 in Kraft gesetzt wurden (Home Office, 2007).

Der praktische Umgang mit diesen neuen Kompetenzen führte in der Folge immer wieder zur Kontestation der Regierung. Insbesondere der offensive Umgang mit den neuen Befugnissen sorgte schnell für Kritik. Die ErmittlerInnen nutzten die Kompetenzen aus Sicht der KritikerInnen bereits bei vergleichsweise geringen Anschuldigungen. So wurden bspw. gegen Tierschutz-AktivistInnen

oder psychisch Kranke Haftstrafen verhängt, da sie sich weigerten mit den Behörden zu kooperieren (Brunst, 2012, S. 336f.). Auch der Fall eines jungen Hackers, der im Sommer 2014 versucht hatte Zugriff auf eine Webseite zu erlangen und der die Polizei von Newcastle durch Scherzanrufe störte, wurde durch eine Section 49 Notice zu sechs Monaten Freiheitsstrafe verurteilt, da er sich weigerte die Schlüssel für seine kryptierte Festplatte preiszugeben. Auch dies wurde aus den Reihen der Netzgemeinde und von Bürgerrechtsbewegungen kritisiert. Einer der weiteren Hauptkritikpunkte war, dass die Anordnungen zur Schlüsselherausgabe nicht durch RichterInnen ausgesprochen werden mussten, sondern durch entsprechende Beamte der Ermittlungsbehörden (GCHQ, MI6, MI5, die Polizei und die National Crime Agency) (Vice, 2014).

Diese Kritik wurde mit dem Investigatory Powers Act (IPA) 2016 aufgegriffen. Das Gesetz sah erstmalig eine richterliche Befugnis für die Anordnung zur Schlüsselherausgabe vor.[8] Zwar blieben die Befugnisse unter Part III Section 49 weitgehend erhalten, mit dem Investigatory Powers Commissioner (IPC) etablierte die Regierung aber eine neue Kontrollinstanz, die die Praxis der Ermittlungsbehörden überwachen und regelmäßig Bericht erstatten sollte. Dies war aber die einzige Beschränkung der Beschützer-Rolle. Denn auch aufgrund der durch Terroranschläge in Paris erweiterte der IPA die Einsatzmöglichkeiten für Anordnungen zur Schlüsselherausgabe. Waren diese zuvor nur dann möglich, wenn ErmittlerInnen auf rechtmäßigem Weg (lawful interception) verschlüsselte Inhaltsdaten abgegriffen hatten, war der Einsatz durch den IPA auch dann möglich, wenn Behörden verschlüsselte Metadaten nutzten (Severson, 2017, S. 8).

Die Erweiterung exekutiver Kompetenzen wurde dabei maßgeblich durch die Anschläge auf die Redaktion von Charlie Hebdo im Januar 2015 in Paris ermöglicht. In diesem Kontext setzte sich der britische Premierminister David Cameron wiederholt dafür ein, nicht überwachbare Kommunikationsräume nicht zu dulden:

> »whether it has been about looking at letters, or about fixed telephone communications or mobile communications, we have always believed that, in extremis, on the production of a signed warrant from the Home Secretary, it should be possible to look at someone's communications to try and stop a terrorist outrage. The decision we have to take is: are we prepared to allow in future, as technology develops, safe spaces for terrorists to communicate? The principle I think we should adopt is that we are not content for that to happen, and as a result we should look to legislate accordingly.« (House of Commons, 2015b, S. 862)

8 Die neue gesetzliche Regelung wurden maßgeblich durch die Snowden-Enthüllungen ermöglicht.

Mit dieser Position sorgte Cameron international für Aufsehen, da in diesen Aussagen eine Forderung nach dem Verbot oder der substanziellen Schwächung von Verschlüsselung gesehen wurde (The Guardian, 2015b). KritikerInnen sahen in der Stellungnahme den einseitigen Versuch, die Beschützer-Rolle über Gebühr auszudehnen, ohne dabei die Implikationen für die Rollen als Wohlstandsmaximierer und Garant liberaler Grundrechte zu berücksichtigen.

Auch wenn der Premierminister nach heftiger Kritik darauf hinwies, dass er nicht beabsichtige, Verschlüsselung zu verbieten, blieben die Vorschläge zu einem restriktiveren Umgang umstritten. Bei der Vorstellung des IPA wies Innenministerin Theresa May aber explizit darauf hin, dass die Regierung nicht plane Verschlüsselung zu verbieten, sondern, dass sie darin auch ein wichtiges Werkzeug für die funktionierende Onlinewirtschaft sowie den Datenschutz der BürgerInnen sah. Dennoch seien die neuen Kompetenzen notwendig, um den sicherheitspolitischen Gefahren auch weiterhin effektiv begegnen zu können (House of Commons, 2015e, S. 975). Die Regierung erkannte damit die Bedenken der KritikerInnen an und wies selbst auf die Spannungen zwischen den drei Rollen hin. Die Exekutive ging davon aus, mit dem neuen Gesetz eine gute Balance zwischen den Rollen gefunden zu haben.

Durch den IPA wurde den zuständigen MinisterInnen, nach richterlicher Prüfung, die Möglichkeit eingeräumt, durch sogenannte »technical capability notices« die Entfernung technischer Schutzmaßnahmen gegenüber CSPs zu veranlassen (Science and Technology Committee, 2016, S. 16). Aufseiten der Bürgerrechtsbewegungen sorgte diese Praxis für erhebliche Kritik. Privacy International sah darin »an indirect attack on end-to-end encryption« (ebd., S. 16). Diese Sorge teilten auch andere NGOs. Sie befürchteten, dass durch die Vorgaben eine Verbreitung von Ende-zu-Ende-Verschlüsselung unterbleiben würde, da die Anbieter einer solchen Aufforderung zur Entschlüsselung nicht mehr nachkommen könnten, weil die Schlüssel direkt zwischen den NutzerInnen ausgetauscht werden. Eine verlangsamte Verbreitung von Ende-zu-Ende-Verschlüsselung habe sowohl negative Effekte für die Privatheit der Kommunikation als auch auch für den Wirtschaftsstandort (ebd., S. 17f.). Auch der mit dem Gesetz betraute Parlamentsausschuss teilte die Sorge über potenziell schädliche Effekte für die Verbreitung von Ende-zu-Ende-Verschlüsselung:

> »The Government still needs to make explicit on the face of the Bill that CSPs offering end-to-end encrypted communication or other un-decryptable communication services will not be expected to provide decrypted copies of those communications if it is not practicable for them to do so.« (UK Government, 2016b, S. 50)

Das Parlament forderte von der Regierung ferner klarzustellen, dass diese nicht beabsichtige, Hintertüren in Verschlüsselung vorzuschreiben oder die Technologie

grundlegend zu schwächen. Ferner wiesen die Abgeordneten darauf hin, dass die gesetzlichen Regelungen mit dem britischen und europäischen Datenschutz konform sein müssten (UK Government, 2016b, S. 50 bzw. 92).

Die Administration erkannte einige dieser Punkte an und stellte in diesem Kontext klar, dass CSPs nur die Verschlüsselung aufheben mussten, die sie selbst zur Verfügung gestellt bzw. implementiert hatten (ebd., S. 80). Ein expliziter Bezug zur Ende-zu-Ende-Verschlüsselung blieb aber aus. Mit Blick auf den Vorwurf, die Exekutive unterminiere Verschlüsselung im Allgemeinen, wiesen RegierungsvertreterInnen wiederholt darauf hin, dass bereits RIPA Telekommunikationsanbieter dazu verpflichtet hatte, Verschlüsselung zu entfernen soweit sie von den Dienstleistern selbst zur Verfügung gestellt wurde und dass der IPA diese Kompetenzen nicht erweitert habe (UK Government, 2016e). Die neuen Regelungen wurden dennoch von KritikerInnen als eine umfassende Kompetenzerweiterung gedeutet, da die Unternehmen noch unter RIPA nur dabei mitwirken mussten, Daten zu entschlüsseln, nachdem Ermittlungsbehörden diese rechtmäßig erhoben hatten. Durch den IPA jedoch wurde von den Dienstleistern verlangt prophylaktisch Kapazitäten zur Entschlüsselung vorzuhalten. Dies wurde wiederholt als ein Angriff auf Verschlüsselung im Allgemeinen gesehen, da die Unternehmen bspw. Hintertüren in ihren Produkten platzieren müssten (Severson, 2017, S. 10f.).

Zur Begrenzung der Beschützer-Rolle kam es damit nur mit Bezug zur Rolle als Wohlstandsmaximierer, da eine Überforderung der Dienstleister durch eine grundsätzliche Pflicht zur Entschlüsselung drohte.

Hervorzuheben ist ferner, dass die Regierung in diesem Kontext beanspruchte, Technical Capability Notices zur Dekryptierung auch für Unternehmen im Ausland erlassen zu können. Damit ging die teilweise extraterritoriale Geltung der Beschützer-Rolle einher, sofern britische Sicherheitsbelange berührt wurden (ebd., S. 9). Diese expansive Kompetenzaneignung wurde von zahlreichen (vornehmlich amerikanischen) Internetunternehmen kritisch gesehen (Science and Technology Committee, 2016, S. 18f.). Auch im Parlament wurde darauf hingewiesen, dass Unternehmen durch diese Regelungen in Konflikte zwischen widersprüchlichen gesetzlichen Regelungen verstrickt werden könnten (House of Commons, 2016b, S. 917). Aber auch nach dem Konsultationsprozess gab die Regierung diese Bestrebungen der Entterritorialisierung nicht auf. Die Regierung präzisierte im finalen Gesetzestext aber die Anforderungen, die mit einer extraterritorialen technical capability notice verbunden sind. So ist bei der Anordnung, wie auch im domestischen Gebrauch, zunächst abzuwägen, »whether it is reasonably practicable for a telecommunications operator« einer solchen Forderung nachzukommen (The Stationery Office, 2016, Section 85 (4)). Ferner ist bei ausländischen Unternehmen die Rechtslage im jeweiligen Land zu berücksichtigen und ob es für das Unternehmen möglich ist, der Anordnung folge zu leisten,

ohne dabei Gesetze zu verletzen (ebd., Section 85 (4)(a)(b)). Die britische Regierung trug damit die domestische Beschützer-Rolle nach außen und versuchte ihr mit dem IPA zumindest teilweise extraterritoriale Wirkung zu verschaffen.

Von vielen KritikerInnen aus dem Parlament wurden die Einschränkungen aber als zu undefiniert und kaum überprüfbar gesehen (Severson, 2017). Das Parlament vertrat in diesem Kontext aber keine eindeutig kritische Position, denn im legislativen Prozess wurde durch Abgeordnete einerseits darauf hingewiesen, dass die extraterritorialen Befugnisse prinzipiell problematisch sein könnten, andererseits forderten die MPs auch, die Möglichkeiten zum internationalen Datenaustausch zu verbessern (UK Government, 2016b, S. 63 bzw. 89).[9] Daher konnte die Regierung ihre Position im Gesetzestext letztlich verwirklichen und die Beschützer-Rolle teilweise über die territorialen Grenzen hinweg erweitern. Die Regierung griff dabei auch die Forderung nach internationaler Kooperation auf und betonte mit Blick auf die Rolle als Garant liberaler Grundrechte, dass es in diesem Kontext zunächst darauf ankomme, mit internationalen PartnerInnen grundlegende Regeln zum Datenaustausch festzulegen, die auch einen hohen Schutz der Privatsphäre der BürgerInnen gewährleisteten (ebd., S. 63).

Weitere VertreterInnen aus der Netzcommunity sahen in den Bestrebungen auch eine verzweifelte staatliche Reaktion auf die Weigerung Apples im Fall des Attentäters von San Bernardino ein verschlüsseltes iPhone zu entschlüsseln (Naked Security, 2019). Ferner wurde die im IPA definierte Praxis auch in einem wissenschaftlichen Gutachten kritisiert, das der UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression in Auftrag gegeben hatte. In dieser Studie wurde bemängelt, dass die Vorgaben zu vage gehalten waren und dass die Regelungen als Verpflichtung zum Einsatz von Hintertüren interpretiert werden könnten. Ferner problematisierte die Untersuchung, dass Großbritannien damit zu einem negativen Vorbild für andere Staaten geworden sei – bspw. China (United Nations Human Rights Special Procedures, 2018). Die Einführung gesetzlicher Restriktionen für Verschlüsselung

9 Die Forderungen nach einem verbesserten internationalen Datenaustausch erfolgte unter Verweis auf den Mord an Lee Rigby durch zwei islamistische Terroristen. Der Fall steht aber nicht unmittelbar mit der Verschlüsselungsproblematik in Verbindung. Dennoch löste er umfassende Kritik an Facebook aus, weil Informationen über die Täter und deren Pläne nicht frühzeitig an die britischen Sicherheitsbehörden übermittelt worden waren. In diesem Zusammenhang entwickelte sich im Vereinigten Königreich eine Debatte darüber, inwiefern Betreiber sozialer Medien dazu verpflichtet seien, die eigenen Seiten nach Anzeichen für terroristische Planungen zu durchsuchen und proaktiv Maßnahmen zu ergreifen (The Telegraph, 2014). Im Bericht des Intelligence and Security Committees wurde das extraterritoriale Defizit von RIPA explizit problematisiert (Intelligence and Security Committee, 2014e, S. 141f.).

könnte so Autokratien inspirieren und dazu genutzt werden, diese Praktiken zu legitimieren.

Damit wurde auch auf internationaler Ebene Kritik vorgetragen, die die britische Regierung aber bereits domestisch nicht daran gehindert hatte, Dienstleister dazu zu verpflichten, Möglichkeiten zur Entschlüsselung vorzuhalten. Die britische Exekutive hat in der Folge wiederholt versucht andere Staaten von dieser Praxis zu überzeugen und dabei im Kreis der 5-Eye-Staaten die meisten Fortschritte erzielt. Die Gruppe ruft seit mehreren Jahren regelmäßig zu einem restriktiveren Umgang mit Verschlüsselung auf.

Die deutlich kritischere Position gegenüber Verschlüsselung, die domestisch etabliert werden konnte, ermöglichte der britischen Regierung auch im Außenverhalten einen offensiveren Umgang mit der Thematik. Insbesondere zu dem Zeitpunkt als auch innenpolitisch über den IPA verhandelt wurde und nachdem sich eine Erweiterung der Beschützer-Rolle realisierte hatte, intensivierte die britische Regierung auch international ihre Bemühungen, Verschlüsselung stärker zu reglementieren. Im Rahmen der Five-Eyes problematisierte die britische Regierung zusammen mit den Partnerstaaten nach 2016 wiederholt die verschlüsselte Kommunikation. In einem gemeinsamen Kommuniqué machten die RegierungsvertreterInnen 2016 deutlich, dass sie Verschlüsselung zwar als wichtig für die Bürgerrechte im digitalen Zeitalter ansahen, aber gleichzeitig befürchteten, dass die Technik die Strafverfolgungsbehörden zunehmend bei ihrer Arbeit beeinträchtigen könnte (U.S. Department of Homeland Security, 2016). Die Regierungen befürchteten ein unausgeglichenes Verhältnis zwischen einem liberalen und unregulierten Internet und den nationalen Beschützer-Rollen, das maßgeblich durch die Verschlüsselung erzeugt werde.

Diese Sorgen wurden ein Jahr später konkreter formuliert und von Versuchen begleitet, zusammen mit den entsprechenden Dienstleistern, Möglichkeiten zum Umgang mit diesem Problem zu finden (Government of Canada, 2017). Die technische Community war aber nicht zu einer umfassenden Kooperation mit den Regierungen bereit, da sie die Einschätzung vertrat, dass eine Schwächung von Verschlüsselung die IT-Sicherheit des gesamten Netzes gefährden könnte und so sowohl aus bürgerrechtlicher als auch wirtschaftlicher Sicht nicht angemessen sei. Die Regierungen der 5-Eyes mussten auch 2018 eine mangelnde Kooperationsbereitschaft der Digitalwirtschaft akzeptieren. Führende UnternehmensvertreterInnen hatten es abgelehnt, an Gesprächen über die terroristische oder kriminelle Nutzung von Onlinekommunikationsräumen teilzunehmen (Australian Government, 2018).

Da die Bestrebungen des Geheimdienstverbundes in der Netzgemeinde nicht aufgegriffen wurden, formulierten die 5-Eyes 2018 eigene Prinzipien zur Verschlüsselung. Hierin vertraten die Regierungen die Position, dass:

> »Many of the same means of encryption that are being used to protect personal, commercial and government information are also being used by criminals, including child sex offenders, terrorists and organized crime groups to frustrate investigations and avoid detection and prosecution. Privacy laws must prevent arbitrary or unlawful interference, but privacy is not absolute.« (Ebd.)

Die Regierungen akzeptierten in ihrer Erklärung, dass es Fälle geben könne, in denen eine Entschlüsselung technisch unmöglich sei. Dies sollten aber Ausnahmen bleiben und um dies zu gewährleisten, riefen sie die Internetunternehmen zur freiwilligen, nationalen wie internationalen Kooperation mit den Ermittlungsbehörden auf. Die Unternehmen sollten in diesem Kontext freiwillig eigene Konzepte zur Überwachung von Kommunikation erarbeiten. Weiterhin betonten sie, dass der Zugriff auf kryptierte Daten nur unter Einhaltung rechtsstaatlicher Prozesse und unter Wahrung der bürgerlichen Freiheitsrechte erfolgen dürfe. Sie verliehen damit den Bestrebungen Ausdruck, die Beschützer-Rolle durch die Rolle als Garant liberaler Grundrechte einzuhegen.

Zum Abschluss machten die Regierungen aber auch deutlich, dass sie Einschränkungen ihrer sicherheitspolitischen Handlungsfähigkeit aufgrund technischer Hürden nicht dauerhaft tolerieren würden:

> »Should governments continue to encounter impediments to lawful access to information necessary to aid the protection of the citizens of our countries, we may pursue technological, enforcement, legislative or other measures to achieve lawful access solutions.« (Ebd.)

Eine Position, die die britische Regierung domestisch bereits mit dem IPA eingenommen hatte. 2019 erneuerten die fünf angelsächsischen Regierungen ihre Forderungen nach mehr Kooperation mit der Wirtschaft. Allerdings wiesen sie auch darauf hin, dass andere Unternehmen gezielt nur solche Technologien einsetzten, die sie selbst nicht mehr entschlüsseln könnten. Dieses Vorgehen wurde von den Regierungen als fahrlässig und riskant für die Gesellschaften gesehen (UK Government, 2019c, S. 2f.). Auch auf Ebene der Vereinten Nationen wies die britische Regierung immer wieder auf die Risiken hin, die aus ihrer Sicht mit einer weitgehenden Verbreitung nicht dekryptierbarer Verschlüsselung einhergeht (UK Government, 2017b).

Ebenfalls Ende 2018 hatten Vertreter des GCHQ in einem Lawfare-Gastbeitrag zwar betont, dass Verschlüsselung sowohl aus wirtschaftlicher als auch bürgerrechtlicher Perspektive bedeutend sei und dass Eingriffe nur unter strengen Auflagen durchgeführt werden dürften. Der IPA biete aus ihrer Sicht »world class oversight«, um diese Maßnahmen zu kontrollieren (Levy und Robinson, 2018). Um mit Verschlüsselung umzugehen, ohne sie zu brechen, brachten sie den Vorschlag ein,

bspw. bei Ende-zu-Ende verschlüsselten Messengern Nachrichtendienste als unsichtbare dritte Partei in die Kommunikation zwischen Verdächtigen einzubinden und so ein Abhören möglich zu machen. Dies könnten die Betreiber der Dienste ohne Probleme implementieren und die Verschlüsselung werde hierdurch nicht systematisch unterminiert (Levy und Robinson, 2018). Im Mai 2019 reagierten VertreterInnen der Netzgemeinde, Wissenschaft und Wirtschaft in einem offenen Brief auf diese Vorschläge. Sie betonten, dass der Vorschlag sowohl bürgerrechtlich als technisch problematisch sei. Eine Implementierung des »ghost protocols« unterminiere das Vertrauen in Authentifizierungsprozesse wodurch grundlegend infrage gestellt wäre, mit wem kommuniziert würde. Weiterhin müssten sämtliche Applikationen angepasst werden, um zu verhindern, dass die mitlesende Partei für KommunikationsteilnehmerInnen sichtbar würde. Hierdurch könnten neue Sicherheitslücken entstehen, die dann alle NutzerInnen beträfen (Access Now, 2019).

Aus der Netzgemeinde gab es vehemente Kritik an all diese Forderungen. Die Electronic Frontier Foundation sah in den Bestrebungen der 5-Eyes einen Export der britischen Überwachungspolitik und eine Aushöhlung der Bürgerrechte im Netz (EFF, 2017). In einem offenen Brief an die RegierungsvertreterInnen formulierten 83 Bürgerrechtsorganisationen und VertreterInnen der Netzgemeinschaft aus verschiedenen Ländern ihre Kritik an den Forderungen. Sie riefen die Staaten dazu auf:

> »[…] to protect the security of your citizens, your economies, and your governments by supporting the development and use of secure communications tools and technologies, by rejecting policies that would prevent or undermine the use of strong encryption, and by urging other world leaders to do the same.« (Human Rights Watch, 2017, S. 1)

Pläne, wodurch Hintertüren in Verschlüsselung vorgesehen werden müssten, waren aus Sicht der UnterzeichnerInnen schädlich für die Sicherheit im Netz allgemein. Diese Ansicht bekräftigten die KritikerInnen mit dem utilitaristischen Hinweis, dass Verschlüsselung sehr viel mehr Positives als Negatives ermögliche und dass Kriminelle und Terroristen im Extremfall immer auf Software zurückgreifen könnten, die außerhalb des Einflussbereichs der 5-Eye-Staaten liege (ebd., S. 2). Der Verweis aus der Netzgemeinde, dass das Netz selbst ein schützenswertes Gut sei und dass die staatliche Beschützer-Rolle ein sicheres Netz durch Eingriffe in Verschlüsselung oder das Zurückhalten von Schwachstellen unterminiere, wurde in verschiedenen Kontexten cybersicherheitspolitischer Debatten angeführt. Diese Bezüge blieben aber folgenlos, da die Regierung das Netz selbst als Schutzgut nicht prinzipiell anerkannte, sondern die Beschützer-Rolle auf die nationalen Systeme bezogen blieb.

Wie bei der Etablierung des domestischen Rechtsrahmens, zeigt sich auch in diesem Kontext, dass der britischen Regierung aufgrund ausbleibender Kontestationen eine umfassendere Rollenübernahme erleichtert wurde. In der domestischen Sphäre zeigt sich das daran, dass die Herausforderungen mit Verweis auf die Rolle als Garant liberaler Grundrechte nicht so folgenreich waren wie in der Bundesrepublik – auch aufgrund eines ausbleibenden negativen historischen Selbstbezugs. Die britische Regierung konnte daher stets eine striktere Kryptopolitik verfolgen als das deutsche Pendant. Diese ermöglichte auch eine verschlüsselungskritischere Rollenübernahme nach außen, die dort bei den signifikanten Anderen im 5-Eye-Verbund anschlussfähig war. Die Bestrebungen der Gruppe, eine technische Begrenzung der Beschützer-Rolle durch die rasche Verbreitung von (Ende-zu-Ende-)Verschlüsselung zu vermeiden, wurden stets durch die britische Regierung unterstützt.

### 4.2.3 Internationalisierung: Strafrechtliche Harmonisierung

Wie die Bundesrepublik, gehörte auch das Vereinigte Königreich 2001 zu den ersten Unterzeichnern der Convention on Cybercrime des Europarates. Forderungen nach internationaler Kooperation zur Bekämpfung von Cyberkriminalität wurden in Großbritannien aber bereits in den frühen 1990er Jahren laut.

> »Of couse [sic!], computer crime is often international crime. It is all very well for us to have an effective law in Britain, but we must ensure that similar laws exist in other major countries. The really serious criminal activities are likely to be netted through international co-operation across frontiers rather than by laws which are limited to activities in Britain.« (House of Commons, 1990b, S. 1147)

Die Limitationen einer territorial gebundenen Beschützer-Rolle wurden in diesem Kontext bereits früh problematisiert. Die Regierung erkannte in der Konvention dann einerseits eine Möglichkeit, die britischen Ambitionen im Kampf gegen Cyberkriminalität international zu dokumentieren und andererseits von der verbesserten Kooperation der unterzeichnenden Staaten zu profitieren (Foreign & Commonwealth Office, 2011). Ferner wurde die Konvention als Mittel zum Schutz der Digitalwirtschaft gesehen, da auf diesem Weg das Vertrauen der VerbraucherInnen gestärkt werden könne (Ofcom, 2009). Die internationale Harmonisierung der Beschützer-Rolle wurde damit durch das katalytische Zusammenspiel mit der Rolle als Wohlstandsmaximierer ermöglicht.

Ratifiziert wurde die Konvention aber erst 2011 als mit dem Police & Justice Act 2006 und dem Serious Crime Act 2007 alle erforderlichen Vorgaben umgesetzt waren (Foreign & Commonwealth Office, 2010). Mit diesen Gesetzen wurde einerseits die Strafbarkeit für DoS-Angriffe etabliert und andererseits das Strafmaß

für den Zugriff auf IT-Systeme angeglichen. Die gesetzliche Weiterentwicklung wurde dabei aber nur begrenzt durch die internationalen Vorgaben der Konvention und des Rahmenbeschlusses 2005/222/JI ermöglicht (Home Office, 2004). Zunächst wurden Ergänzungen des CMA durch domestische Entwicklungen angestoßen.

Da der Computer Misuse Act eine direkte Reaktion auf den Angriff von Schifreen und Gold war, adressierte er zunächst nicht alle Teilaspekte der IT-Sicherheit. Insbesondere die Strafbarkeit der Beeinträchtigung der Verfügbarkeit von Daten war zunächst noch nicht im Gesetz angelegt. Diese Regulierungslücke wurde durch den Terrorism Act 2000 für terroristische Vergehen geschlossen (The Stationery Office, 2000c). Für kriminelle Angriffe blieb das Defizit aber bestehen. Bereits 2002 wurde zwar im Parlament eine Erweiterung des CMA um DoS-Angriffe debattiert, der Vorschlag (der wieder als private member's bill eingebracht wurde) konnte aber keine Mehrheit im Parlament finden und blieb daher folgenlos (House of Lords, 2002a). Dies ist bemerkenswert denn zu diesem Zeitpunkt war Großbritannien bereits Unterzeichner der Europaratskonvention on Cybercrime. Die daraus folgende Notwendigkeit, auch DoS-Angriffe unter Strafe zu stellen, wurde auch im House of Lords betont. Ferner war absehbar, dass der Rahmenbeschluss 2005/222/JI empfehlen würde, ein Vergehen für derartige Vorfälle einzuführen. Bei einer Begutachtung des CMA durch das Internet Crime Forum der All Party Internet Group wurden diese Aspekte wiederum aufgeworfen (Home Office, 2004). Auch im Parlament wurde in diesem Kontext darüber diskutiert. Letztlich führten diese Debatten aber nicht unmittelbar zu einer gesetzlichen Anpassung (House of Lords, 2002b, S. 981). Während der Rahmenbeschluss bzw. die Europaratskonvention in Deutschland gesetzliche Anpassungen ermöglicht hat, wurde die britische Beschützer-Rolle durch einen domestischen Vorfall weiterentwickelt.

Im Jahr 2004 wurde deutlich, dass für Kriminelle die DoS-Regulationslücke nach wie vor offen stand. Ein Angeklagter wurde in erster Instanz für den massenhaften Versand von E-Mails und die daraus resultierende Überlastung eines Mailservers freigesprochen, da das Gericht in diesem Verhalten kein Vergehen nach dem Computer Misuse Act erkannte. Mit Blick auf kriminelle DoS-Angriffe bestand daher noch immer Regulierungsbedarf (Fafinski, 2006). Mit dem Police and Justice Act wurde dieses Defizit adressiert und ein neuer Straftatbestand im CMA etabliert, der auch die Beeinträchtigung von IT-Systemen unter Strafe stellte und damit auch den Anforderungen aus der Europaratskonvention und dem EU-Rahmenbeschluss gerecht wurde. Wie in Deutschland, schuf auch die britische Regierung in diesem Zuge einen Tatbestand für die Bereitstellung von Software, die Angriffe gegen Computersysteme ermöglicht (The Stationery Office, 2006, Section 3 bzw. 3a).

Während der Rahmenbeschluss 2005/222/JI noch zu keinen größeren Anpassungen der Beschützer-Rolle führte, wurde die Richtlinie 2013/40/EU umfassend

im Parlament diskutiert, da die Regierung beschlossen hatte, sich in diesem Kontext der EU-Regelung anzuschließen (opt-in) (House of Commons, 2011a, S. 1051).[10] Die Notwendigkeit internationaler Kooperation wurde in dieser Debatte besonders betont, »because the problem is an international one and online criminals do not respect international borders« (ebd., S. 1051). Der Opt-In wurde in diesem Kontext als Ausdruck des britischen Bemühens gesehen, den internationalen Kampf gegen Cyberkriminalität entschlossen zu führen. Ferner würden auf diesem Weg potenzielle Rückzugsorte für Kriminelle verschlossen, da alle Mitgliedsstaaten einen gesetzlichen Mindeststandard einhalten müssten (ebd., S. 1051). Die Regierung konstatierte daher:

> »The aims of the directive are consistent with the aims of the Government in protecting our country, our economy, our businesses and our citizens from those who seek to misuse the online environment.« (Ebd., S. 1052)

Diese Postion wurde im Parlament auch von den Abgeordneten der Opposition geteilt, die das Vorhaben grundsätzlich unterstützten. Allerdings wiesen KritikerInnen darauf hin, dass die britische Regierung die Entscheidung zum Opt-in zu spät getroffen habe und dass dadurch die Gestaltungsmöglichkeiten für Großbritannien begrenzt seien. Ferner wurde betont, dass eine europaweite Regulierung zwar wünschenswert sei, dass diese aber der Kooperation mit anderen Commonwealth-Staaten oder den USA nicht im Wege stehen dürfe. Die britische Regierung dürfe durch die Richtlinie nicht in ihrer Souveränität eingeschränkt werden, weitere Abkommen zu schließen (ebd., S. 1055 f.). Für die britische Regierung war es also bedeutsam, die Beschützer-Rolle möglichst unabhängig zu definieren. Die EU wurde zwar als wichtiger signifikanter Anderer anerkannt und die Richtlinie 2013/40/EU wurde übernommen. Es war aber stets bedeutsam, dass die Kooperation mit anderen Partnern hierdurch nicht negativ beeinflusst würde. Die souveräne Verfügung über die eigene Beschützer-Rolle sorgt damit dafür, dass diese aus britischer Sicht nicht delegiert werden kann.

Während in Deutschland ein weitgehend unkontrollierter Datenaustausch von digitalen Beweismitteln, wie er derzeit in der EU im Rahmen eine E-Evidence-Richtlinie debattiert wird, aufgrund der begrenzenden Wirkung der Rolle als Garant liberaler Grundrechte kritisch gesehen wird, begann die Regierung des Vereinigten Königreichs offensiv damit über extraterritoriale Abhör- und Entschlüsselungsanordnungen zu verhandeln. Insbesondere mit den USA wurde in diesem Kontext über erleichterte Kooperationsmodi gesprochen, die nicht auf

10 Mit dem Vertrag von Amsterdam 1997 hat sich die britische Regierung das Recht zusichern lassen, darüber zu entscheiden, ob sich das Vereinigte Königreich Regelungen im Bereich Freedom, Security and Justice unterwirft (opt-in) oder nicht (opt-out). Diese Regelung besteht auch nach dem Vertrag von Lissabon weiter (House of Commons, 2011b).

den mitunter langfristigen Wegen der Rechtshilfeverträge beruhen (Washington Post, 2016).

Hier zeigt sich, dass die domestisch weniger stark herausgeforderte Beschützer-Rolle in Großbritannien auch im Außenverhalten eine expansivere Rollenübernahme ermöglicht. Der fehlende Kontestationsmechanismus des negativen historischen Selbstbezugs sowie die Referenz (Schutz vor wem?) auf den domestischen Terrorismus erlaubte der britischen Regierung domestisch bereits früher höhere Strafmaße, eingreifendere Ermittlungsbefugnisse und weitreichendere Maßnahmen nach außen zu fordern. Dies wird bei dem folgenden Blick auf die Etablierung der domestischen Beschützer-Rolle deutlich. Weiterhin hat die Regierung, aufbauend auf die domestische Beschützer-Rolle, Kooperationen mit den USA geschlossen.

### 4.2.4 Neue Ermittlungswerkzeuge: Die Etablierung der offensiven domestischen Beschützerrolle

Die britische Regierung begann schon früher als die deutsche damit, die Beschützer-Rolle mit offensiven Mitteln zur Strafverfolgung auszustatten. Dies führte aufgrund der historischen Erfahrungen mit Terrorismus aber zu weniger intensiven Kontestationsprozessen, so dass die Regierung die Rolle einfacher stabilisieren konnte.

Mit dem Police Act 1997 wurde im Vereinigten Königreich bereits früh die Grundlage dafür gelegt, Polizeibehörden den Zugriff auf IT-Systeme zu gewähren. Section 93 erlaubt den ErmittlerInnen »interference with property or with wireless telegraphy […]« (The Stationery Office, 1997). Diese Befugnis war anwendbar, wenn zur Prävention oder Aufklärung schwerer Straftaten andere Ermittlungsmethoden nicht ausreichend waren. In den Debatten um den Police Act standen die digitalen Ermittlungsmethoden aber noch nicht im Zentrum der Aufmerksamkeit. Dennoch verwies die britische Regierung zur Legitimierung von Eingriffen in IT-Systeme immer wieder auf diese Regelung (UK Government, 2016c).[11] Im Parlament rekurrierte die Regierung zur Rechtfertigung des Police Acts explizit auf die gesellschaftliche Bedrohung durch (domestischen) Terrorismus. Diese Referenzen wurden auch von vielen Abgeordneten der Opposition geteilt.

> »We know from reading newspapers, watching television and listening to the radio how an increasing threat of crime affects the lives of more and more of our citizens. At the same time, there is no doubt that we have to be conscious

11 Während die Praxis des polizeilichen Eingriffs in IT-Systeme im Police Act 1997 noch als property interference bezeichnet wurde, änderte sich die Bezeichnung später zu *Equipment Interference*.

of the return of a terrorist threat to this country.« (House of Commons, 1997, S. 379)

Diese Bedenken bezüglich terroristischer Gefahren wurden auch im House of Lords wiederholt geäußert und zur Rechtfertigung der neuen Kompetenzen herangezogen (House of Lords, 1997, S. 412 bzw. 426). Die Anordnung der property interference oblag dabei leitenden BeamtInnen der Strafverfolgungsbehörden, sodass eine richterliche Kontrolle nicht vorgesehen war. Dies sorgte insbesondere bei Bürgerrechtsbewegungen für Kritik. Eine frühe Referenz (Schutz vor wem?) auf den domestischen und internationalen Terrorismus ermöglichte es der britischen Regierung aber schon früh, polizeiliche Befugnisse zum Eingriff in IT-Systeme zu etablieren. Der Widerstand gegen diese neuen Ermittlungsmethoden fokussierte sich hauptsächlich darauf, die Bürgerrechte angemessen zu schützen (House of Commons, 1997, S. 387 bzw. 392). Allerdings wurde in den Debatten nicht über die informationstechnischen Möglichkeiten der neuen Befugnisse debattiert, sodass deren Implikationen erst wesentlich später öffentlich bekannt wurden. Denn erst zwanzig Jahre nach Verabschiedung des Police Acts bekannte die Regierung, dass Polizeibehörden unter dieser Ermächtigung Eingriffe in IT-Systeme vornahmen.

Im Gegensatz zu Deutschland wurde der Analogieschluss aus der bestehenden polizeilichen Praxis auch nicht substanziell herausgefordert und durch Gerichte untersagt. Bürgerrechtsorganisationen wiesen in einer intensiven Debatte um staatliches Hacking 2016 (s.u.) aber auf die problematische Rechtsgrundlage hin und vertraten die Position, dass ein polizeiliches Eingreifen in IT-Systeme durch den Police Act nicht gedeckt sei (Liberty, 2016b, S. 5). Wie in Deutschland trat auch in Großbritannien die Beschützer-Rolle in Spannung mit der Rolle als Garant liberaler Grundrechte. Durch den anderen historischen Selbstbezug als Opfer von Terrorismus wurden die Maßnahmen aber nicht grundlegend hinterfragt bzw. abgelehnt.

1999 konstatierte die Regierung unter Tony Blair, dass die rasche technologische Entwicklung die bestehenden Regelungen zum Abfangen von Kommunikation vor neue Herausforderungen stelle. »This revolution in communications technology is one of the imperatives for change in the law« (UK Government, 1999, Foreword). In einem Konsultationspapier argumentierte die Regierung, dass TerroristInnen und Kriminelle die neuen Möglichkeiten nutzten und dass daher eine Novellierung insbesondere des Interception of Communications Act 1985 (IOCA) nötig sei. Das Innenministerium identifizierte Handlungsbedarf bspw. mit Blick auf den wachsenden E-Mailverkehr, der effizienter bei den Internet Service Providern (ISP) abgefangen werden könne und der nicht notwendigerweise über einen Public Telecommunication Operator geleitet wird. Folglich sollten auch ISPs zur Kooperation beim Abfangen von Daten verpflichtet werden. Hierfür war aber eine

Neufassung des Gesetzes nötig (UK Government, 1999, S. 14 bzw. 17). Die Regierung beabsichtigte damit die Regelungen des IOCA signifikant zu erweitern:

> »The intention is to provide a single legal framework which deals with all interception of communications in the United Kingdom, regardless of the means of communication, how it is licensed or at which point on the route of the communication it is intercepted. This means that the scope of the Bill will be wider than that of the Interception of Communications Act 1985 [...]« (Ebd., S. 16)

Der Innenminister betonte in diesem Kontext aber stets auch, dass hierbei die Bürgerrechte gewahrt werden würden (ebd.).

Vor diesem Hintergrund etablierte die Regierung mit dem Regulation of Investigatory Powers Act 2000 (RIPA) neue Regelungen, die den Polizeibehörden das Abfangen von Kommunikationsinhalten erlaubten. RIPA regelte Kompetenzen in sechs unterschiedlichen Bereichen neu: »the interception of communications; the acquisition of communications data; intrusive surveillance; directed surveillance; the use of covert human intelligence sources; and demands for decryption« (House of Commons, 2000d, S. 768). Neben den bereits debattierten Kompetenzen zur Entschlüsselung, waren mit Blick auf Informationstechnik und das Internet die Maßnahmen zum Abfangen von Kommunikation einschlägig, da es sich hierbei um Praktiken handelte, die besonders mit Blick auf die neuen Kommunikationswege etabliert wurden. Hierbei handelte es sich um Eingriffe in die Kommunikationsübertragung, die die Inhalte für Strafverfolgungsbehörden zugänglich macht (The Stationery Office, 2000b, Section 2 (2)).

Section 5(3) von RIPA erlaubte der/dem zuständigen MinisterIn mit Verweis auf drei Gründe, Anordnungen zum Abfangen von Kommunikation zu erlassen: die Nationale Sicherheit, die Aufklärung oder Verhinderung schwerer Kriminalität sowie den Erhalt des wirtschaftlichen Wohlergehens des Vereinigten Königreichs. Die/Der MinisterIn muss hierbei abwägen, ob die Maßnahme verhältnismäßig ist und ob die Informationen nicht auch auf anderem Weg erlangt werden könnten. Über die Anordnung oder die Beendigung der Maßnahme ist sodann ein/e Surveillance Commissioner zu informieren. Diese/r prüft die Anordnung und gibt sie frei, sofern sie/er sie für rechtmäßig hält. Beantragen können solche interception warrants die LeiterInnen der Geheimdienste sowie der übergeordneten Polizeibehörden bzw. des Zolls und National Criminal Intelligence Service (ebd., Section 6 (2)). Um die Kommunikationsinhalte abzufangen, können durch die Anordnungen auch Dritte (die Telekommunikationsanbieter) zur Kooperation verpflichtet werden. Sie sind dazu verpflichtet, alle Maßnahmen zu ergreifen, die »reasonably practicable« sind (ebd., Section 11 (6)). Ferner werden die Unternehmen verpflichtet, den Inhalt sowie die Existenz der Überwachungsanordnung geheim zu halten (ebd., Section 19 (3)).

In diesem Kontext zeigt sich erneut die enge, katalytische Verbindung zwischen der Beschützer-Rolle und der Rolle als Wohlstandsmaximierer. Denn die Eingriffsrechte beziehen sich nicht nur auf sicherheitspolitische Erwägungen, sondern können auch aus wirtschaftlichen Gründen erfolgen.

Die durch die/den MinisterIn ausgestellten Anordnungen zum Abfangen der Kommunikation wurden vom neu etablierten Interception of Communications Commissioner geprüft. Dieser wurde durch den Premierminister bestellt und musste zuvor ein hohes juristisches Amt bekleidet haben (ebd., Section 57). Zusätzlich etablierte RIPA mit dem Investigatory Powers Tribunal (IPT) ein neues Gericht, das die mit dem Gesetz verbundenen Kompetenzen und deren Angemessenheit mit Blick auf die Bürgerrechte überwachen sollte (ebd., Section 65).

Die Regierung verwies zur Rechtfertigung der Neuregelungen durch RIPA neben den neuen Gefahren der kriminellen und terroristischen Nutzung der neuen Kommunikationswege auch darauf, dass das Gesetz keine grundsätzlich neuen Befugnisse schaffe, sondern lediglich bestehende Regeln zusammengeführt würden, um dem technischen Wandel angemessen begegnen zu können. Ferner profitiere hiervon auch der Grundrechtsschutz der betroffenen BürgerInnen. Mit RIPA werde auch den Vorgaben des Human Rights Acts 1998 entsprochen. Wiederholt versicherte Home Secretary Jack Straw, dass eine angemessene Balance zwischen den Kompetenzen der Ermittlungsbehörden und den Bürgerrechten hergestellt werde (House of Commons, 2000d, S. 767).[12]

Eine Überarbeitung der bestehenden Regelungen war aus Sicht der Regierung aber unter anderem zur Bekämpfung von Geldwäsche, Menschenhandel, Pädophilie, Zigarettenschmuggel und anderen Delikten notwendig (ebd., S. 768). Prinzipiell stimmte die Tory-Opposition der Einschätzung der Regierung zu, dass der IOCA angesichts technischer Entwicklungen überarbeitet werden müsse, um die Sicherheit der britischen Bevölkerung nach wie vor zu gewährleisten. Auch die Erweiterung der Beschützer-Rolle auf die Überwachung der neuen Kommunikationswege wurde akzeptiert (ebd., S. 778). Die Liberal Democrats unterstützten das Gesetz letztlich ebenfalls. Auch sie wiesen auf die besonderen Gefahren hin, die durch die Verbreitung der Informationstechnik ermöglicht würden und betonten die Verantwortung des Parlaments, die britischen BürgerInnen zu schützen:

12 1998 wurde der Human Rights Act (HRA) beschlossen, um die Rechte aus der Europäischen Menschenrechtskonvention in britisches Recht zu übertragen. Der HRA stellt aber auch sicher, dass Akte der Primärgesetzgebung nicht durch Urteile außer Kraft gesetzt werden können. Gerichten bleibt nur die Formulierung einer Erklärung der Inkompatibilität, die aber keine Auswirkung auf die bestehenden britischen Gesetze hat (The Stationery Office, 1998). Der HRA wurde wiederholt kritisiert und immer wieder wurde auch über eine britische Bill of Rights als Alternative bzw. Ergänzung debattiert (House of Lords und House of Commons, 2008).

> »[…] we must ensure that serious threats to the physical safety of the people of this country, whether from criminals, hostile powers or terrorists, can be countered by the judicious and regulated use of such powers. We must do so in a way that does not disrupt an industry that has great earning power for the country and potential for the future.« (House of Commons, 2000b, S. 1206)

Diese Einschätzung teilten auch die meisten Labour-Abgeordneten. Die Referenz auf Terrorismus bzw. die Anschlagsfolgen, die Großbritannien bereits erfahren hat, wurden überparteilich geteilt. In diesem Kontext wurde ferner betont, dass die britische Bevölkerung kein Verständnis dafür aufbringen würde, wenn die erforderlichen Maßnahmen zur Prävention solcher Angriffe nicht ergriffen würden (bspw. House of Commons, 2000d, S. 784f.).

Der Ausbau der Beschützer-Rolle wurde daher maßgeblich durch das historische Selbst ermöglicht. Sowohl Regierung als auch Opposition fürchteten im Falle erneuter Terroranschläge, dafür verantwortlich gemacht zu werden, diese nicht verhindert zu haben.

RIPA erfuhr aber von Seiten der Zivilgesellschaft und von VertreterInnen der Internetwirtschaft Kritik. Wirtschaftliche Einwände gegen das neue Gesetz betonten, dass durch die Neuregelung auch kleinere ISPs zur Kooperation beim Abhören von Kommunikation verpflichtet seien. Dies könne mit empfindlichen Kosten verbunden sein, die die Unternehmen nur schwer tragen könnten (ebd., S. 779 f.). Kritik an den potenziellen Kosten und entsprechende Forderungen nach Kompensation für die betroffenen Unternehmen wurde sowohl von Branchenverbänden als auch Tory-Abgeordneten formuliert (House of Commons, 2000c).

Von den Liberal Democrats wurde wiederholt negativ hervorgehoben, dass keine transparente und unabhängige richterliche Kontrolle der Maßnahmen vorgesehen wurde (House of Commons, 2000b, S. 1206). Zwar wurde mit dem IPT ein neues Kontrollgremium etabliert, das die zuvor für unterschiedliche Behörden zuständigen Kontrollinstanzen ersetzte (das Interception of Communications Tribunal, das Security Service Tribunal und das Intelligence Services Tribunal), bemängelt wurde aber die Intransparenz und insbesondere der Umstand, dass keine Auskünfte zu Überwachungsmaßnahmen veröffentlicht werden sollten. Auch dass unter dem Freedom of Information Act 2000 keine weiteren Informationen angefordert werden konnten, wurde in diesem Kontext kritisiert (JUSTICE, 2000). Die Regierung argumentierte, dass Offenlegungen dazu führen könnten, tatsächlich Überwachte zu warnen und so Maßnahmen zu gefährden:

> »It is logically a difficult position to explain to individuals, and it is difficult for people to understand that they may make a complaint to the tribunal […] that they may be being intercepted even though it is not possible to tell them whether they are being intercepted. Because it is secret, people are bound to

> be suspicious, but—to repeat the point [...] the powers are operated in a strong ethical and legal framework.« (House of Commons, 2000d, S. 774)

Letztlich führte die Sorge vor Terroranschlägen mit Verweis auf die historischen Erfahrungen dazu, dass RIPA rasch durch das Parlament verabschiedet wurde. Das Gesetz wurde in der Folge wiederholt zum Ziel bürgerrechtlicher Kritik. Erst als durch die Enthüllungen von Edward Snowden 2013 staatliche Überwachungspraktiken öffentlich bekannt wurden, kam es zu einer Überarbeitung der Regelungen. 2014 wurde auch eingehend darüber diskutiert, dass die Regelungen genutzt wurden, um gezielt journalistische Quellen zu identifizieren und abzuhören (The Guardian, 2014c). Aus rollentheoretischer Perspektive transportierte diese Kritik den Vorwurf, die Exekutive habe die Beschützer-Rolle im Geheimen deutlich überdehnt. Unter diesem wachsenden domestischen wie internationalen Druck, legte die Regierung den Investigatory Powers Acts 2016 (IPA) vor.

Mit dem IPA wurde explizit über die Thematik staatlichen Hackens diskutiert. In diesem Kontext bekannte die britische Regierung auch erstmals, dass staatliche Eingriffe in IT-Systeme zu den gängigen Ermittlungspraktiken der Polizeibehörden zählten. Der IPA sollte den kurz nach den Snowden-Veröffentlichungen erlassenen Data Retention and Investigatory Powers Act 2014 ablösen, der aufgrund einer sunset-clause auszulaufen drohte. Mit dem IPA etablierte die Regierung neue Kompetenzen der Strafverfolgungsbehörden unter dem Begriff *Equipment Interference* erstmals explizit und sorgte dafür, dass die Regelungen aus dem Police Act nur noch eingeschränkt für den Eingriff in Computersysteme genutzt werden konnten (The Stationery Office, 2016, Section 14). Zur Rechtfertigung der Eingriffe verwies die Regierung darauf, dass aufgrund des technischen Wandels und insbesondere der voranschreitenden Nutzung von Verschlüsselung, Informationen nur noch auf diesem Weg zugänglich seien:

> »Equipment interference plays an important role in mitigating the loss of intelligence that may no longer be obtained through other techniques, such as interception, as a result of sophisticated encryption. It can sometimes be the only method by which to acquire the data.« (UK Government, 2016b, S. 23)

Diese jetzt explizit gemachte und durch den IPA gestützte Praxis sorgte im Rahmen eines öffentlichen Konsultationsprozesses für erhebliche Kritik. KritikerInnen wiesen darauf hin, dass die neuen Befugnisse nicht nur in Form eines Code of Conduct formuliert werden sollten, sondern dass es einer eigenen gesetzlichen Grundlage für derart invasive neue Kompetenzen geben sollte. Ferner bemängelten Bürgerrechtsbewegungen, dass der Eingriff in Systeme grundlegend die IT-Sicherheit unterminiere (Home Office, 2015c). Auch Bemühungen der Polizei, Schadsoftware auf dem freien Markt zu erstehen und sich damit bei der Aus-

übung der Beschützer-Rolle von Unternehmen wie Hacking Team abhängig zu machen, wurden scharf kritisiert (Liberty, 2016b, S. 5).

Im Gegensatz zur deutschen Politik, ist die Beschützer-Rolle in Großbritannien in diesem Kontext weniger spezifisch. Während in Deutschland zwischen den unterschiedlich intrusiven Praktiken der Online-Durchsuchung bzw. Quelle-TKÜ. unterschieden wird, gibt es im Vereinigten Königreich nur Regeln zur Equipment Interference. Allerdings gibt es auch hier Unterschiede in den Anordnungsanforderungen je nachdem, ob es sich um »live« mitgeschnittene oder gespeicherte Daten handelt. Für Kommunikation, die auf dem Transportweg abgefangen werden soll, bedarf es einer eigenen interception warrant (Home Office, 2018a, S. 12). Equipment Interference darf auch zur Überwachung eingesetzt werden. Das beinhaltet »monitoring, observing or listening to a person's communications or other activities, or recording anything that is monitored, observed or listened to.« (ebd., S. 13)

Die Regierung definierte die Kompetenzen zur Equipment Interference im IPA folgendermaßen:

> »Equipment interference describes a range of techniques used by the equipment interference authorities that may be used to obtain communications, equipment data or other information from equipment. Equipment interference can be carried out either remotely or by physically interacting with the equipment.« (Ebd., S. 10)

Equipment Interference umfasst damit eine Reihe verschiedener Praktiken, die es den Ermittlungsbehörden (im Geheimen) erlauben, Zugriff auf gespeicherte Daten zu erlangen. Sie reichen vom physischen Zugriff bis zur Ausnutzung von Softwareschwachstellen. In diesem Kontext sicherte die Regierung aber auch zu, dass die neuen Kompetenzen mit dem 1998 verabschiedeten Human Rights Act konform gestaltet würden (ebd., S. 10f.). Im Gegensatz zu den Geheimdiensten ist es den Polizeibehörden bspw. nur erlaubt targeted Equipment Interference einzusetzen. Den Geheimdiensten steht daneben die umfassendere bulk Equipment Interference offen (ebd., S. 67).

Mit dem IPA wurde den Ermittlungsbehörden die Befugnis zur Equipment Interference zur Aufklärung und Prävention schwerer Kriminalität erteilt. Ferner erlaubt der IPA den Polizeien den Eingriff, wenn dadurch der Tot oder die physische bzw. mentale Gesundheit von Personen geschützt werden kann (ebd., S. 24). Die Anordnung der Equipment Interference obliegt bei den Polizeibehörden einer/einem leitender/n Beamtin/en (law enforcement chief). Außer in besonders dringenden Fällen ist zudem die vorherige Genehmigung durch einen Judicial Commissioner nötig. Besonders akuter Handlungsbedarf liegt vor, wenn bspw. eine unmittelbare Gefahr für Leib und Leben besteht oder wenn für die Informationsbeschaffung nur ein kleines Zeitfenster offen ist. Die Anordnung muss

aber spätestens nach drei Werktagen durch einen Judicial Commissioner überprüft und bestätigt werden (ebd., S. 51). Wenn zur Ausübung der Beschützer-Rolle die staatlichen Kapazitäten nicht ausreichen und daher ein Telekommunikationsdienstleister zur Kooperation verpflichtet wird, bedarf es einer ministeriellen Anordnung (ebd., S. 48). Bei der Genehmigung der Equipment Interference muss stets abgewogen werden, ob die gleichen Informationen nicht auch durch weniger invasive Maßnahmen gewonnen werden können. Nur wenn dies nicht der Fall ist, ist die Maßnahme gerechtfertigt (ebd., S. 45).

Ähnlich wie in Deutschland sind die besonders invasiven Maßnahmen der Beschützer-Rolle damit an besonders schützenswerte Güter (Leib und Leben) gebunden und durch demokratische Kontrollinstanzen eingehegt. Auf diesem Weg versuchte die britische Regierung die Balance zwischen der Beschützer-Rolle und der Rolle als Garant liberaler Grundrechte zu gewährleisten.

Die explizite Legitimierung der Equipment Interference wurde aber im öffentlichen Konsultationsprozess besonders durch Bürgerrechtsbewegungen kritisiert. Privacy International wies, wie viele andere[13], darauf hin, dass die neuen Regelungen sehr weitreichende Folgen für die IT-Sicherheit haben könnten. Insbesondere die Unterstützung durch Telekommunikationsdienstleister sei in hohem Maße problematisch, da es in diesem Kontext denkbar sei, dass diese als Sicherheitsupdates getarnte Hintertüren in ihre Software integrieren könnten, um den staatlichen Anordnungen Folge zu leisten. Dies sei sowohl bürgerrechtlich bedenklich, da viele NutzerInnen persönlichste Daten auf IT-Systemen speicherten als auch aus wirtschaftlicher Sicht abzulehnen, da hierdurch auch Hintertüren für Kriminelle offen blieben: »This weakening of systems leads to sacrificing the security of the communications that we all rely on for banking, commerce and other everyday transactions […]« (Privacy International, 2015b).

Auch VertreterInnen der Wirtschaft sahen die neuen Befugnisse als zu weitreichend. Der Industrieverband techUK verwies in einer Stellungnahme ebenfalls darauf, dass es problematisch sei, Unternehmen dazu zu verpflichten, Schwachstellen in die eigenen Produkte zu integrieren. Die WirtschaftsvertreterInnen sahen in dieser Praxis auch erhebliche Probleme bezüglich der Haftung für Schäden, die durch diese Hintertüren bei anderen Kunden (auch im Ausland) entstehen könnten (techUK, 2015).

Die Regierung rechtfertigte die neuen Befugnisse vor dem Parlament unter Verweis auf die veränderte Gefahrensituation in der das Risiko eines Terroranschlags jederzeit gegeben sei. TerroristInnen nutzten zu ihrer Koordination und zur Vorbereitung von Anschlägen immer häufiger das Internet (House of Com-

13 Ähnlich wie Privacy International argumentierten Big Brother Watch (2015), die Electronic Frontier Foundation (2015) und Liberty (2016).

mons, 2016c). Equipment Interference sei in diesem Bereich oftmals die einzige Möglichkeit diese Gefahren aufzuspüren und zu bekämpfen.

> »It allows the security and intelligence agencies to keep pace with terrorists and serious criminals, who increasingly use sophisticated techniques to communicate, to evade detection in dark places, and to plan and plot what they do. Equipment interference has been instrumental in disrupting credible threats to life, including those against UK citizens.« (Ebd., S. 5)

Die Einschätzung, dass die Regierung die Möglichkeit haben müsse, auf Informationen auf IT-Systemen zuzugreifen, wurde auch von der Opposition nicht grundsätzlich in Abrede gestellt. Ferner wurden auch die etablierten Kontrollen und die Abwägung mit bürgerrechtlichen Bedenken weitgehend für ausreichend erachtet (House of Commons, 2016c, S. 6f.).

Die Abgeordneten erkannten damit im Gegensatz zu den AktivistInnen kein Defizit bei der Rolle als Garant liberaler Grundrechte. Das Argument, der Staat unterminiere durch die Beschützer-Rolle die Sicherheit im globalen Netz wurde wiederum nicht aufgegriffen bzw. akzeptiert. Der nationale Rahmen blieb Referenzpunkt (Schutz für wen?) der Beschützer-Rolle.

Es waren letztlich die aus der Rolle als Wohlstandsmaximierer folgenden Bedenken zur Beeinträchtigung der wirtschaftlichen Wettbewerbsfähigkeit, die den zuständigen Parlamentsausschuss dazu veranlassten, die Regierung aufzufordern, die praktische Anwendung der neuen Befugnisse genau zu überwachen und ggf. zu überarbeiten:

> »As ever, the fight against serious crime should be appropriately balanced with the requirement to protect and promote the UK's commercial competitiveness. We believe the industry case regarding public fear about 'equipment interference' is well founded.« (House of Commons, 2016d, S. 21)

In Großbritannien war also nicht die Rolle als Garant liberaler Grundrechte maßgeblich für die Einschränkung bzw. Kontrolle der exekutiven Kompetenzen, sondern die Rolle als Wohlstandsmaximierer. Da zusätzlich zum teilweise katalytischen Zusammenwirken der beiden Rollen im britischen Fall auch ein Bezug zum historischen Selbst als Opfer von Terrorismus hergestellt wird, ist der Exekutiven die Übernahme einer umfassenderen, weniger kontestierten Beschützer-Rolle im Bereich der polizeilichen Strafverfolgung möglich.

Diese umfassendere Beschützer-Rolle überträgt sich auch auf die internationale Ebene. Die extraterritoriale Qualität der Beschützer-Rolle zeigt sich im Anspruch ausländische Dienstleister zur Entschlüsselung zu verpflichten. Im Gegensatz zur Bundesrepublik hat das Vereinigte Königreich mit dem Crime (Overseas Production Orders) Act 2019 die Voraussetzungen dafür geschaffen, dass,

nach Abschluss eines internationalen Abkommens, britische Strafverfolgungsbehörden ohne den Weg über gegenseitige Rechtshilfe direkt an Diensteanbieter im Zielland herantreten und die Herausgabe von Daten verlangen können (The Stationery Office, 2019).

Aus Sicht der Regierung war dieser neue Weg und die damit verbundene Extraterritorialisierung der Beschützer-Rolle notwendig geworden, da die bestehenden Prozesse der Rechtshilfe mit einer Dauer von bis zu zwei Jahren nicht ausreichten, um akuten Gefahren durch schwere Kriminalität und Terrorismus zu begegnen. Hinzu komme, dass Daten immer häufiger im Ausland gespeichert seien und dass die domestischen Regelungen somit nicht mehr angemessen seien. Bereits in den ersten parlamentarischen Beratungen des Gesetzentwurfs ließ die Regierung keinen Zweifel daran, dass das erste Abkommen mit den USA geschlossen werden solle, da dort die Mehrheit wichtiger Diensteanbieter beheimatet sei (House of Commons, 2018b, S. 587f.). Dieses Abkommen wurde im Oktober 2019 geschlossen und umfasst nicht nur die Herausgabe von gespeicherten Meta- und Inhaltsdaten, sondern ermöglicht britischen Strafverfolgungsbehörden auch die Anordnung von unmittelbaren Abhörmaßnahmen zum Abfangen laufender Kommunikation, wobei US-BürgerInnen gegen alle Abfragen geschützt sind (UK Government, 2019a, S. 4f.). Bürgerrechtsorganisationen kritisierten diese neuen Regelungen und sahen darin ein beginnendes »Race to the Bottom« mit Blick auf die liberalen Grundrechte (EFF, 2019).

Auf internationaler Ebene äußert sich die weniger herausgeforderte Beschützer-Rolle in Großbritannien folglich auch in offeneren Kooperationen. Die Referenz der Beschützer-Rolle (Schutz für wen?) auf das nationale Gemeinwesen bleibt jedoch erhalten, da die jeweils eigenen StaatsbürgerInnen besonders geschützt werden.

## 4.3 Zwischenfazit

Die Analyse der Cybersicherheitspolitik im Bereich der Kriminalitätsbekämpfung zeigt einige Ähnlichkeiten aber auch deutliche Unterschiede zwischen den beiden Untersuchungsstaaten. In beiden Fällen wurde die Beschützer-Rolle zuerst durch ein katalytisches Zusammenspiel mit der Rolle als Wohlstandsmaximierer ermöglicht. In beiden Fällen wurde die Beschützer-Rolle damit zuerst mit Bezug auf das Referenzobjekt (Schutz für wen?) Wirtschaft etabliert. Die Kontestation einer zu weitgehenden Beschützer-Rolle erfolgte in beiden Staaten unter Verweis auf die wirtschaftlichen Folgen einer zu umfassenden Regulierung vornehmlich durch VertreterInnen der Wirtschaft sowie des Parlaments. In Deutschland war die Beschützer-Rolle zunächst auch dadurch begrenzt, dass FreizeithackerInnen nicht kriminalisiert werden sollten. Diese Beschränkung gab es in Großbritannien

nicht, da hier bereits früher über die potenziellen physischen Folgen von Cyberangriffen debattiert wurde. Die britische Regierung konnte die Beschützer-Rolle in der Folge umfassender gestalten als die deutsche, die die Referenz (Schutz vor wem?) erst später auf professionelle AngreiferInnen legte.

Mit Blick auf die Etablierung auch offensiver Beschützer-Rollen haben beide Regierungen versucht, den Ermittlungsbehörden neue Werkzeuge zur Gewährleistung der Sicherheit zur Verfügung zu stellen. Damit wurde die Beschützer-Rolle aus Sicht von AktivistInnen selbst zum Problem für (globale) IT-Sicherheit. Dies wurde von den Regierungen jedoch nicht aufgegriffen. Die Referenz (Schutz für wen?) der Rollen blieb dem nationalen Rahmen verhaftet.

Bei der Etablierung der offensiven Beschützer-Rolle gab es deutliche Unterschiede zwischen den beiden Untersuchungsstaaten. Die britische Regierung etablierte umfassendere Kompetenzen bspw. zur Verschlüsselung und zur extraterritorialen Reichweite. Es gab zwar auch in Großbritannien Bedenken von Bürgerrechtsorganisationen und Abgeordneten, dass die Regierung die sicherheitspolitischen Befugnisse überdehne, aber diese Einwände wurden begünstigt durch das Ausbleiben negativer historischer Selbstbezüge nicht so einflussreich in der Beschränkung der Beschützer-Rolle. Die Rolle als Wohlstandsmaximierer wirkte ambivalent auf die britische Beschützer-Rolle. So wurde die Beschützer-Rolle bspw. unter Verweis auf das volkswirtschaftliche Wohlergehen erweitert, allerdings bemängelten WirtschaftsvertreterInnen immer wieder die negativen Implikationen für Unternehmen oder KonsumentInnen. Die britische Regierung konnte daher aus einer relativ stabilen domestischen Beschützer-Rolle heraus auch international agieren. Die deutsche Regierung sieht sich dagegen mit anhaltenden Kontestationsprozessen konfrontiert, die meist auf historische Erfahrungen verweisen und die teilweise durch die Judikative gestützt wurden. Insbesondere Urteile des Verfassungsgerichts haben die Regierung wiederholt dazu veranlasst, das Verhältnis zwischen Beschützer-Rolle und der Rolle als Garant liberaler Grundrechte zu korrigieren. Hinzu kommt, dass die Bundesregierung lange nicht in der Lage war, die Beschützer-Rolle alleine auszufüllen. Bei der technischen Umsetzung musste sie auf kommerzielle Anbieter von Überwachungssoftware zurückgreifen. Auch das hat zu Widerständen aus der Netzgemeinschaft geführt.

Unterschiede in der internationalen Kooperation erwachsen aus diesen unterschiedlich stabilen domestischen Rollenbeziehungen. Während diese Beziehung im Vereinigten Königreich verhältnismäßig stabil ist, wird in Deutschland um die richtige Balance zwischen Beschützer-Rolle und der Rolle als Garant liberaler Grundrechte nach wie vor gerungen. Auf Grundlage der stabileren domestischen Rollenbeziehung konnte das Vereinigte Königreich eine Kooperationsvereinbarung mit den USA schließen, die den unmittelbaren Zugriff der Ermittlungsbehörden auf Daten in den USA ermöglicht. Deutschland steht einer ähnlichen EU-weiten Regulation skeptisch gegenüber. Beide Staaten sehen eine weitreichende

Delegation der Beschützer-Rollen skeptisch. Im Fall der Bundesrepublik liegt dies aber an den fehlenden Zusagen bürgerrechtlicher Standards, in Großbritannien an den Bestrebungen die Beschützer-Rolle möglichst souverän zu bestimmen und daher bilaterale Abkommen zu bevorzugen.

In der Verschlüsselungspolitik wird deutlich, dass die deutsche Regierung sowohl aufgrund innen- als auch außenpolitischer Erwägungen eine liberalere Linie verfolgte und damit die Beschützer-Rolle beschränkt hat. Hier zeigen sich Effekte im Sinne des »second image reversed«, die mit klassischen rollentheoretischen Ansätzen schwerer greifbar sind. Einerseits lehnte die Regierung ein US-geprägtes internationales System der Schlüsselhinterlegung ab, weil sie dadurch negative Folgen für die Rollen als Wohlstandsmaximierer und Garant liberaler Grundrechte fürchtete. Amerikanische Behörden sollten nicht auf die geschützten Daten deutscher BürgerInnen oder Unternehmen zugreifen können. Ferner wurde diese Ablehnung im domestischen Rollenspiel aufgegriffen und zudem immer wieder auf die demokratische Bedeutung von Verschlüsselung rekurriert sowie auf die Wichtigkeit für die Rolle als Garant liberaler Grundrechte hingewiesen. Hierbei wurden wiederholt Bezüge zum negativen historischen Selbst hergestellt. Aus diesen Gründen war eine restriktive Verschlüsselungspolitik auch domestisch erschwert. Die britische Regierung konnte ihre verschlüsselungsskeptische Beschützer-Rolle domestisch besser stabilisieren als die deutsche Bundesregierung. Dies wurde durch das historische Selbstbild – Opfer von (domestischem) Terrorismus – und die daraus resultierende geringere Kontestation mit Bezug zur Rolle als Garant liberaler Grundrechte ermöglicht. International wurde das auch durch die Einbindung in die ebenfalls verschlüsselungsskeptische Gruppe der 5-Eyes erleichtert.

Die wesentlichen Einflüsse, die die Entwicklung der Cybersicherheitspolitiken geprägt haben, sind in den Tabellen 3 und 4 schematisch dargestellt.

*Tabelle 3: Schematische Darstellung der Einflüsse auf die Politikentwicklung im Bereich der Strafverfolgung in der Bundesrepublik Deutschland: Wirkung auf die Beschützer-Rolle, – = kontestierend, + = katalytisch. Quelle: Eigene Darstellung*

| | **domestische Ebene** | | | | **internationale Ebene** | |
|---|---|---|---|---|---|---|
| | Historisches Selbst | Wirkung | Rollenbezüge | Wirkung | signifikante / organisierte Andere | Wirkung |
| Domestische Etablierung (bis 1999) | | | Wohlstandmaximierer | + | | |
| Kryptopolitik (1994 - 2019) | Autokratische Erfahrungen | – | Garant liberaler Grundrechte | – | USA | – |
| Internationalisierung (1995 - 2005) | | | | | CoE / EU | + |
| Neue Ermittlungswerkzeuge (2005 - 2019) | Autokratische Erfahrungen | – | Garant liberaler Grundrechte | – | | |

*Tabelle 4: Schematische Darstellung der Einflüsse auf die Politikentwicklung im Bereich der Strafverfolgung im Vereinigten Königreich: Wirkung auf die Beschützer-Rolle, – = kontestierend, + = katalytisch. Quelle: Eigene Darstellung*

| | **domestische Ebene** | | | | **internationale Ebene** | |
|---|---|---|---|---|---|---|
| | Historisches Selbst | Wirkung | Rollenbezüge | Wirkung | signifikante / organisierte Andere | Wirkung |
| Domestische Etablierung (bis 1999) | Opfer von Terrorismus | + | Wohlstandsmaximierer | + | | |
| Kryptopolitik (1994 - 2019) | Opfer von Terrorismus | + | | | USA / 5-Eyes | + |
| Internationalisierung (1995 - 2005) | | | | | CoE / EU | |
| Neue Ermittlungswerkzeuge (2005 - 2019) | Opfer von Terrorismus | + | | | USA | + |

# 5. Die Snowden-Enthüllungen: Das Netz und die Nachrichtendienste

Mit der schnellen Diffusion von IT in unterschiedlichste gesellschaftliche Bereiche einhergehend, wurden immer größere Datenmengen digital gespeichert. Das Internet ist dabei in den letzten 20 Jahren zu einer globalen Informationsinfrastruktur geworden, über die Daten von Staaten, Unternehmen und BürgerInnen versendet werden oder abrufbar sind. Die Enthüllungen von Edward Snowden im Juni 2013 haben gezeigt, dass diese neue Informationsquelle von Geheimdiensten besonders intensiv genutzt wurde bzw. wird. Die offengelegten Praktiken betrafen dabei sowohl die Beziehungen zwischen Regierungen und ihren Bevölkerungen als auch die zwischenstaatlichen Gepflogenheiten. Die Enthüllungen warfen dabei Licht auf die problematischen Beziehungen zwischen (verbündeten) Staaten – welche geheimdienstlichen Praktiken sind international erlaubt? – als auch das Verhältnis zwischen Regierung und Bevölkerung – welchen Schutz genießen (die eigenen oder verbündete) StaatsbürgerInnen? Sie irritierten auf beiden Ebenen und zwangen die Regierungen sowohl domestisch als auch international ihre Beschützer-Rollen neu bzw. erstmals explizit zu definieren. Die Enthüllungen bieten die Möglichkeit, einen Einblick in die sonst weitgehend klandestinen Praktiken der Geheimdienste zu erlangen und die Politiken beider Untersuchungsstaaten zu vergleichen. Im Zentrum des folgenden Kapitels stehen daher die geheimdienstlichen Praktiken, die durch die Veröffentlichungen einer gesellschaftlichen Debatte zugänglich wurden. Untersucht wird, wie Regierungen ihre Beschützer-Rollen mit Blick auf den Auslandsgeheimdienst bzw. im britischen Fall das für Signal Intelligence zuständige GCHQ definiert haben und welche Kompetenzen den Diensten zugesprochen wurden, um die Beschützer-Rolle auszufüllen bzw. welche Kontestationsprozesse erfolgten.

Durch die veröffentlichten Dokumente sowie durch weitere journalistische Recherchen und parlamentarische Untersuchungen wurde deutlich, dass die Regierungen ihre Beschützer-Rollen im Geheimen weiter definiert hatten, als öffentlich bekannt war. Die Enthüllungen bilden aufgrund ihrer innerstaatlichen sowie internationalen Implikationen den zentralen Kristallisationspunkt, an dem die Beschützer-Rollen im Bereich der Geheimdienste untersucht werden. Der Un-

tersuchungsbereich unterscheidet sich wesentlich von der Kriminalitätsbekämpfung, da es hier nicht um die Regulation nichtstaatlicher Akteure (Krimineller) geht, sondern um die Praktiken staatlicher Institutionen.

Die Entwicklungen im Kontext der Snowden-Enthüllungen sind einerseits besonders relevant, da hierdurch verschiedene problematische Praktiken aufgedeckt wurden. Hierzu zählt die im Internet erschwerte Unterscheidung zwischen innerstaatlicher und ausländischer Kommunikation. Mit dem Vereinigten Königreich und der Bundesrepublik werden ferner zwei Staaten verglichen, die sich auf unterschiedlichen Seiten der Enthüllungen wiederfanden. Während Großbritannien zusammen mit den USA für expansive Geheimdienstaktivitäten vielfach kritisiert wurde, zählte Deutschland zu den prominentesten KritikerInnen der enthüllten Praktiken.

## 5.1 Deutschland

### 5.1.1 Die Snowden-Enthüllungen: Die Bundesregierung zwischen Verunsicherung, Abhängigkeit und zaghafter Selbstbehauptung

Die Reaktion der Bundesregierung auf die Enthüllungen und die berichtete Ausspähung von sowohl Teilen der Regierung als auch der deutschen Bevölkerung war durch zwei Bestreben gekennzeichnet. Erstens versuchte sich die Regierung der eigenen Beschützer-Rolle zu versichern und zu evaluieren, inwiefern diese durch die Nachrichtendienste der Partnerstaaten unterminiert worden war. In diesem Kontext untersuchte die Regierung bspw., ob es domestisch zu einer (physischen) Beeinträchtigung der deutschen Internetinfrastruktur gekommen war. Weiterhin richtete die Bundesregierung die eigene Beschützer-Rolle partiell neu aus und legte deren Referenz (Schutz vor wem?) auch auf die Aktivitäten verbündeter Staaten. Zweitens war die Regierung auf internationaler Ebene bestrebt, die enthüllten Praktiken zu verändern und für mehr staatliche Zurückhaltung zu werben. Hier versuchte die deutsche Exekutive, bspw. durch die Unterstützung einer UN-Resolution, eine restriktivere Praxis zu etablieren sowie bilateral Abkommen zur Beschränkung von Spionage abzuschließen. Als dieses Ansinnen absehbar scheiterte, beförderte dieses internationale Rollenspiel und die resultierende Frustration die domestische Neuausrichtung bzw. Erweiterung der Beschützer-Rolle. Beide Bestrebungen wurden aber stets durch die Abhängigkeit der Beschützer-Rolle, insbesondere von amerikanischen Geheimdienstinformationen, moderiert, sodass eine direkte Konfrontation ausblieb.

Unmittelbar nach den Veröffentlichungen der Dokumente von Edward Snowden machte die deutsche Regierung deutlich, dass sie die expansiven Überwachungspraktiken der US-amerikanischen NSA und des britischen GCHQ nicht

für angemessen hielt. Prominenter Ausdruck dieser Haltung war die Aussage der Bundeskanzlerin »Ausspähen unter Freunden – das geht gar nicht« im Oktober 2013 (Spiegel, 2013a). Mit dieser Aussage kritisierte Angela Merkel die Überwachung ihres Handys. Diese Maßnahme war unmittelbar zuvor bekannt geworden. Sie war also Ausdruck des Unbehagens, dass die deutsche Exekutive selbst zum Ziel der alliierten Geheimdienste geworden war. Aber auch die Überwachung der deutschen Bevölkerung wurde durch die Regierung kritisiert. Allerdings wollte die Regierung in bilateralem Austausch zunächst aufklären, inwiefern die Anschuldigungen gegen die Verbündeten zutrafen.

Die kritische Abwägung zwischen sicherheitspolitischen Maßnahmen und der Gewährleistung der Bürgerrechte wurde bereits in der Frühphase im Juni 2013 deutlich, als Innenminister Friedrich mit der Proklamation eines »Supergrundrechts« Sicherheit die spannungsvolle Beziehung zugunsten sicherheitspolitischer Erwägungen zu entscheiden versuchte und die Überwachungstätigkeiten damit zumindest teilweise rechtfertigte (Welt, 2013). Eine Tendenz, die auch in der Fraktion der CDU/CSU immer wieder geteilt wurde (Deutscher Bundestag, 2013i, S. 58). Damit versuchte die Regierung zu vermeiden, dass die Beschützer-Rolle zu sehr beschränkt wurde.

In einer der ersten internationalen Reaktionen auf die Enthüllungen formulierte die Bundesregierung einen Fragenkatalog, den sie am 11. bzw. 24. Juni an die amerikanische sowie britische Botschaft übermittelte und mit dem sie auf Aufklärung insbesondere mit Blick auf die Programme PRISM und TEMPORA drängte. Die Antworten auf die Fragen beschränkten sich aber weitgehend darauf, dass die adressierten Regierungen die gesetzlichen Bestimmungen ihrer Nachrichtendienste erläuterten und deren Rechtmäßigkeit betonten (Deutscher Bundestag, 2013c, S. 5f.). Die parlamentarische Opposition und auch VertreterInnen aus der Netzgemeinschaft forderten ein nachdrücklicheres Vorgehen gegen die USA und Großbritannien und die Vernehmung von Edward Snowden in Deutschland. Die Bundesregierung lehnte eine konfrontativere Haltung mit der Begründung ab, dass die beiden Staaten »demokratische Rechtsstaaten und enge Verbündete Deutschlands« seien und dass der gegenseitige Respekt die Aufklärung gemäß »internationaler Gepflogenheiten« erfordere (ebd., S. 12). Die Regierung teilte offiziell die Sorgen über die enthüllten Praktiken, mäßigte ihr Verhalten nach außen aber mit Verweis auf die guten Beziehungen zu den USA und Großbritannien.

Unter dem Titel »Stop watching us« kam es Ende Juli zu ersten großen öffentlichen Protesten in deutschen Städten, die unter anderem von der parlamentarischen Opposition, aber auch von Bürgerrechtsorganisationen unterstützt wurden (Spiegel, 2013b). Diese Demonstrationen setzten sich im September fort und kritisierten die ausufernde Überwachung durch die amerikanischen und britischen Geheimdienste (Spiegel, 2013c). Damit geriet die Bundesregierung domestisch

immer stärker unter Druck, gegen Überwachungsmaßnahmen vorzugehen. Die Erwartung, die deutsche Bevölkerung vor massenhafter Überwachung zu schützen, artikulierte damit die domestischen Erwartungen an die Rolle als Garant liberaler Grundrechte.

Ebenfalls im Juli stellte die Kanzlerin ein Acht-Punkte-Programm vor, mit dessen Maßnahmen den publik gewordenen Praktiken begegnet werden sollte. Bei dieser Gelegenheit betonte die Bundeskanzlerin »Deutschland ist kein Überwachungsstaat«, äußerte aber auch Verständnis für ein höheres Sicherheitsbedürfnis der USA nach den Anschlägen vom 11. September 2001 (Bundesregierung, 2013b). Das Programm umfasste unter anderem das Vorhaben, Verwaltungsvereinbarungen von 1968/69 zwischen der Bundesrepublik und den USA, Großbritannien sowie Frankreich zu kündigen. Die Vereinbarungen regelten Sonderrechte bei der Überwachung des Post-, Brief- und Fernmeldeverkehrs. Dieses Vorhaben wurde zeitnah umgesetzt, bereits im August waren die Vereinbarungen außer Kraft (Auswärtiges Amt, 2013a,b). Allerdings wurde diese Maßnahme von VertreterInnen der Netzgemeinde als Symbolpolitik kritisiert, da auf die entsprechenden Regelungen seit 1990 nicht mehr zurückgegriffen worden war (Netzpolitik.org, 2014b).

Mit diesem Schritt dokumentierte die Regierung das Bestreben, die deutsche Bevölkerung nicht den Sicherheitsbehörden anderer Staaten (auch langjähriger Verbündeter) zu unterwerfen und versicherte sich ihrer eigenen Beschützer-Rolle. Keine anderen Akteure sollten legitim massenhaft deutsche BürgerInnen überwachen können. Zu dieser Art der Selbstvergewisserung der eigenen Rolle gehörte auch, dass der Generalbundesanwalt prüfte, ob die Enthüllungen die Eröffnung eines Verfahrens nach §99 StGB (Geheimdienstliche Agententätigkeit) erforderten (Deutscher Bundestag, 2013c). Dieser Prüfvorgang wurde allerdings 2017 nach Ermittlungen und parlamentarischer Untersuchung aus Mangel an Beweisen eingestellt (Generalbundesanwalt, 2017).

Weitere Punkte des Programms sahen unter anderem eingehende Konsultationen mit den USA zur Aufklärung der Situation, eine UN-Resolution zum Schutz der Privatsphäre sowie die schnelle Verabschiedung der europäischen Datenschutzgrundverordnung vor (Bundesregierung, 2013b).

Ein nachdrückliches internationales Vorgehen gegen die enthüllten Überwachungspraktiken forderten auch die Oppositionsparteien in verschiedenen parlamentarischen Anträgen. Sie rekurrierten dabei auf die »Schutzpflichten« der Bundesregierung gegenüber der deutschen Bevölkerung, die Wahrung der Grundrechte sowie auf die Verpflichtung zum Schutz der deutschen Wirtschaft (Deutscher Bundestag, 2013b, S. 1). Um den Schutz der politischen Souveränität zu gewährleisten, forderte die SPD ferner einen Ausbau der Spionageabwehr auch mit Blick auf die Aktivitäten verbündeter Staaten (ebd., S. 1).

Die Abgeordneten machten die Bundesregierung damit auf ihre aus der Beschützer-Rolle erwachsende Pflicht aufmerksam, die gleichsam durch Referenzen zur Rolle als Wohlstandsmaximierer und als Garant liberaler Grundrechte gestützt wurde. Die Bundesregierung könne nicht zulassen, dass amerikanische oder britische Nachrichtendienste die Geschäftsgrundlagen deutscher Unternehmen oder die Grundrechte deutscher BürgerInnen unterminierten.

Aber auch die Praktiken der deutschen Geheimdienste und die entsprechenden gesetzlichen Regelungen rückten in den Fokus der parlamentarischen Aufmerksamkeit. Die Grünen forderten eine umfassende Überprüfung der bestehenden legislativen Grundlagen für alle Überwachungspraktiken (Deutscher Bundestag, 2013f,h). Diese Forderung teilte auch die Linke, sie forderte zudem, die strategische Fernmeldeaufklärung durch den BND sofort zu suspendieren und erst nach einer Evaluation ggf. wiederaufzunehmen (Deutscher Bundestag, 2013g, S. 2). Auch die Grünen forderten eine Reform der Regelungen zur Geheimdienstkontrolle (Deutscher Bundestag, 2013i, S. 57). Die Bundesregierung erwiderte ggü. den Vorwürfen in dieser Phase noch, dass die Tätigkeiten des BND ausreichender Kontrolle unterlägen (ebd., S. 43).

Die Opposition war nicht überzeugt, dass die deutsche Regierung von den enthüllten Aktivitäten überrascht war und warf die Frage auf, ob die Exekutive im Geheimen möglicherweise ähnliche Programme unterhielt und ob so ggf. die Beschützer-Rolle ohne parlamentarische Kontrolle ebenfalls signifikant erweitert worden war. Hier deuteten sich bereits Kontestationsprozesse an, die dann im Parlamentarischen Untersuchungsausschuss zum Tragen kamen.

Auf internationaler Ebene begann der Austausch mit den USA und Großbritannien unmittelbar nachdem die Enthüllungen die Schlagzeilen bestimmt hatten. Nach ersten Konsultationen mit den USA vertrat die Regierung die Auffassung, dass es keine Anhaltspunkte für »eine flächendeckende Überwachung deutscher oder europäischer Bürger durch die USA« gäbe (Deutscher Bundestag, 2013a, S. 2). Durch Rückfragen bei deutschen Dienstanbietern versicherte sich die Bundesregierung wiederum der eigenen Beschützer-Rolle. Auch nach Rücksprache mit deutschen ISPs konnte die Regierung keine Ausspähung durch die NSA an Internetinfrastrukturen auf deutschem Territorium feststellen. Um ferner dem Verdacht nachzugehen, ausländische Geheimdienste hätten Zugriff auf den großen deutschen Internetknoten DE-CIX, konsultierte die Bundesregierung den betreibenden Branchenverband eco. Dieser schloss aus, dass es einen physischen Zugang amerikanischer oder britischer Geheimdienste gegeben habe, der eine unbemerkte Ausleitung von Datenverkehr ermöglicht haben könnte (ebd., S. 18).

Das BSI bzw. BMI überprüften ferner die Dienstleister, die Verträge mit der Bundesregierung unterhielten und evaluierten, inwiefern diese ausländischen Nachrichtendiensten Daten zur Verfügung stellten oder zum Ziel der Überwa-

chungsmaßnahmen geworden waren. In diesem Zuge wurde auch physisch überprüft, wo ggf. Zugriff auf Leitungen genommen werden konnte. Aber auch diese Ermittlungen ergaben keine Hinweise auf Angriffe gegen deutsche Regierungsnetze (Deutscher Bundestag, 2017c, S. 390 bzw. 394). Trotzdem wurden unter Federführung des BMI eine Reihe von Maßnahmen zur Verbesserung der Sicherheit der Regierungskommunikation ergriffen. Diese umfassten bspw. die erleichterte Nutzung von Verschlüsselung durch Regierungsstellen sowie eine Stärkung des BSI. In einer Stellungnahme zum Maßnahmenpaket hieß es:

> »Eine Verstärkung der Maßnahmen zur Verbesserung der Regierungskommunikation ist vor dem Hintergrund der aktuellen Vorfälle zwingend erforderlich. Es ist davon auszugehen, dass fremde Nachrichtendienste auch in Zukunft von allen technischen Möglichkeiten des Ausspähens bspw. Abhörens elektronischer Kommunikation […] Gebrauch machen werden.« (Ebd., S. 393)

Diese Anpassungen waren damit zuvorderst ein Selbstschutz des Beschützers. Die Bundeskanzlerin kritisierte dementsprechend die Ausrichtung der britischen und amerikanischen Geheimdienste, »wenn es zum Schluss gar nicht mehr allein um die Abwehr terroristischer Gefahren geht, sondern darum, sich auch gegenüber Verbündeten, zum Beispiel für Verhandlungen bei G-20-Gipfeln oder UN-Sitzungen, Vorteile zu verschaffen«, dann sei das nicht mehr hinnehmbar (Deutscher Bundestag, 2014b, S. 569).

Da der physische Eingriff in deutsche Infrastrukturen aber unwahrscheinlich erschien, rückten die großen amerikanischen Internetunternehmen in den Fokus der Aufmerksamkeit, da zahlreiche Deutsche die Dienste von Google, Microsoft, Apple und Facebook etc. nutzten. Die Bundesregierung forderte die Unternehmen daher zu Stellungnahmen auf. Diese versicherten in der Folge, dass sie den Geheimdiensten Daten nur nach Anordnung durch den FISA-Court zur Verfügung stellten (Deutscher Bundestag, 2013a, S. 19). Eine weiterführende Kooperation bei der Aufarbeitung der Vorwürfe, auch im Rahmen des späteren Untersuchungsausschusses des Bundestages, lehnten die amerikanischen Unternehmen aber ab (Deutscher Bundestag, 2017a). Damit offenbarten sich auf internationaler Ebene die begrenzten Möglichkeiten, die der Regierung bei der Erfüllung ihrer Beschützer-Rolle blieben.

In der Folge betonte die Bundesregierung, es gebe keine massenhafte Überwachung deutscher StaatsbürgerInnen. Die Regierung führte bspw. die, in den Medien diskutierte, Zahl von 500 Millionen abgefangenen Daten pro Monat auf eine Kooperation zwischen BND und NSA zurück, die aber Ziele im Ausland (genauer in Afghanistan) beträfe, die Daten deutscher StaatsbürgerInnen würden in dieser Zusammenarbeit besonders geschützt und nicht an die NSA oder andere Partnerdienste weitergegeben. Die Kooperation in diesem Rahmen diene auch

dem Schutz deutscher Soldaten in Afghanistan und sei daher richtig und notwendig. Nur in zwei Fällen sei, nach strenger Prüfung der Vorgaben durch das G10-Gesetz, eine Weitergabe von Daten deutscher StaatsbürgerInnen an die NSA erfolgt (Deutscher Bundestag, 2013a, S. 2). Die Position der Bundesregierung, wonach viele der erhobenen Vorwürfe unzutreffend seien, wurde im Parlament von den Unionsfraktionen gestützt (Deutscher Bundestag, 2013i, S. 61).

Mit dieser Linie wies die Bundesregierung darauf hin, dass die öffentliche Berichterstattung ein potenziell verzerrtes Bild der Lage transportierte. Tatsächlich seien einige der enthüllten Tatbestände Teil rechtmäßiger Aktivitäten. Allerdings machte die Exekutive gegenüber dem Parlament auch deutlich, dass einige Anliegen nicht öffentlich bzw. teilweise auch nur ohne Parlamentsbeteiligung erörtert werden könnten. In diesem Kontext wies die Bundesregierung bereits früh einerseits darauf hin, dass die öffentliche Beantwortung einiger parlamentarischer Fragen nicht möglich sei, da auf diesem Weg Informationen über die nachrichtendienstlichen Praktiken publik würden und sich Überwachungsziele in der Folge besser auf diese Maßnahmen einstellen könnten. Andererseits argumentierte die Regierung mit Bezug zu den signifikanten Kooperationspartnern, dass die Vertraulichkeit zentraler Baustein geheimdienstlicher Zusammenarbeit sei und dass auch aus Rücksicht auf die Nachrichtendienste der Partnerstaaten eine öffentliche Informationsweitergabe nicht erfolgen könne (Deutscher Bundestag, 2013a, S. 3f.).

In dieser Reaktion wurde deutlich, dass die deutsche Beschützer-Rolle in diesem Bereich maßgeblich von den Fähigkeiten der Partnerdienste abhängig war bzw. dass sich die Regierung nicht allein im Stande sah, Schutzziele zu erreichen und dass sie folglich die Geheimdienstkooperation für unerlässlich für die Gewährleistung der Sicherheit in Deutschland hielt:

> »Eine öffentliche Bekanntgabe von Informationen zu technischen Fähigkeiten von ausländischen Partnerdiensten und damit einhergehend die Kenntnisnahme durch Unbefugte würde erhebliche nachteilige Auswirkungen auf die vertrauensvolle Zusammenarbeit haben. Würden in der Konsequenz eines Vertrauensverlustes Informationen von ausländischen Stellen entfallen oder wesentlich zurückgehen, entstünden signifikante Informationslücken mit negativen Folgewirkungen für die Genauigkeit der Abbildung der Sicherheitslage in der Bundesrepublik Deutschland sowie im Hinblick auf den Schutz deutscher Interessen im Ausland. Die künftige Aufgabenerfüllung der Nachrichtendienste des Bundes würde stark beeinträchtigt. Insofern könnte die Offenlegung der entsprechenden Informationen die Sicherheit der Bundesrepublik Deutschland gefährden oder ihren Interessen schweren Schaden zufügen.« (Ebd., S. 4)

Die Einschätzung, dass die Sicherheit der Bundesrepublik maßgeblich von der Kooperation mit den USA abhänge, wurde auch im Parlament debattiert. Hier wiesen insbesondere Abgeordnete der Union darauf hin, dass Deutschland die amerikanische Administration nicht davon überzeugen könne, weniger Überwachung durchzuführen, wenn die Bundesrepublik im nächsten Atemzug stets nach den neuesten Geheimdiensterkenntnissen fragen müsse. Konkreter Bezugspunkt hierfür waren unter anderem die Hinweise zur sogenannten Sauerlandgruppe, die einen Anschlag in Deutschland geplant hatte und die durch Hinweise amerikanischer Dienste ausgehoben werden konnte (Deutscher Bundestag, 2013i).

Die Abhängigkeit der deutschen Beschützer-Rolle in diesem Kontext wurde auch in Aussagen der Bundesregierung deutlich. Angesichts anderer Gefahren bspw. durch den internationalen Terrorismus konnte die Kooperation schwer infrage gestellt werden. Die Bundesregierung befand sich in einem Dilemma, die amerikanische Unterminierung der Rollen der Bundesregierung einzugestehen und ggf. zu sanktionieren und damit nicht mehr an der Beschützer-Rolle der amerikanischen Regierung partizipieren zu können.

Die Regierung entschied sich dazu, eine offene Konfrontation mit den USA um jeden Preis zu vermeiden. Exemplarisch hierfür steht die Aussage von Innenminister Friedrich in einer Debatte zu den Snowden-Enthüllungen:

> »Aber über allem […] steht, dass wir die enge Partnerschaft mit unseren amerikanischen Freunden und Partnern brauchen, auch um die Sicherheit der Bürger in diesem Land in der Zukunft gewährleisten zu können.« (Ebd., S. 45)

In diesen Erklärungen zeigen sich klare Anzeichen für die asymmetrische Beziehung zwischen der Bundesrepublik und den Partnerdiensten. Gute Beziehungen mit den USA waren daher zur Erfüllung der Schutzfunktion aus Sicht der deutschen Regierung essenziell. Das Verprellen der Partner war daher bereits in dieser Phase unwahrscheinlich, um einen »sicherheitspolitischen Blindflug« zu vermeiden (ebd., S. 58).

Auch die Bundeskanzlerin betonte den besonderen Stellenwert der geheimdienstlichen Kooperation mit den USA, in Frage stehe aber die Ausrichtung bzw. Zielauswahl der amerikanischen und britischen Dienste (Deutscher Bundestag, 2014b, S. 569). Eine Sichtweise, die auch von großen Teilen der Opposition nicht grundsätzlich infrage gestellt wurde (Deutscher Bundestag, 2013i, S. 56). Ferner wurde von VertreterInnen der Geheimdienste immer wieder betont, dass die Fähigkeiten der amerikanischen PartnerInnen in Deutschland nicht vorhanden seien und dass daher eine vertrauensvolle Zusammenarbeit besondere Bedeutung habe. Eine zu rigorose Aufklärung wurde folglich kritisch gesehen, denn es wären bereits Zeichen erkennbar, dass die Kooperation mit dem BND eingeschränkt würde und dass ein Informationsverlust drohe (Deutscher Bundestag,

2017c, S. 518-520). Ein Vertreter des BND beschrieb die Beziehung zur NSA ähnlich. Die NSA versorge den BND mit der Technik sowie dem notwendigen Wissen zu deren Nutzung, um im Gegenzug an den Erkenntnissen des deutschen Nachrichtendienstes teilzuhaben. Die Defizite des deutschen Auslandsgeheimdienstes bei der Überwachung paketvermittelter Kommunikation wurden durch die Kooperation mit den USA gelindert (ebd., S. 586-588 ebenso 709f.).

Auch mit dem Bundesamt für Verfassungsschutz bestand eine ähnliche Kooperationsbeziehung. Um bspw. mit der technischen Entwicklung der rasch zunehmenden Internetkommunikation schritthalten zu können und die Überwachung und Analyse von diesen Informationen effizient gewährleisten zu können, nutzte das BfV das amerikanische Programm XKeyscore (ebd., S. 584). Parlamentarische Fragen, ob bspw. die Nutzung der amerikanischen Software XKeyscore zur Erfassung und Analyse von Internetverkehr an Bedingungen geknüpft war, beantwortete die Bundesregierung nicht öffentlich, um bei Kooperationspartnern kein Vertrauen zu verspielen (Deutscher Bundestag, 2013a, S. 21). Kritische Stimmen, die auch die Praktiken des BND adressierten, wurden von der Regierung in dieser Phase noch als unbegründet zurückgewiesen (Deutscher Bundestag, 2013e, S. 11).

Neben den Hinweisen darauf, dass die Beschützer-Rolle ohne die Kooperation mit den USA nicht ausreichend erfüllt werden könne, wurde die Zurückhaltung auch durch Verständnis für das Sicherheitsbedürfnis der USA moderiert. Ähnlich wie die Kanzlerin argumentierte bspw. der Bundesaußenminister als er im Rahmen eines bilateralen Cyber-Dialogs mit den USA deutlich machte, dass durch die Enthüllungen Vertrauen zwischen den Partnern beschädigt worden sei. Im Zentrum der Debatte stehe nun die Frage nach der angemessenen »Abwägung von Freiheit und Sicherheit« (Auswärtiges Amt, 2014). Frank-Walter Steinmeier äußerte aber auch Verständnis für die Praktiken der NSA, da die USA mit den Terroranschlägen vom 11. September 2001 erfahren mussten, dass die ausgreifende Vernetzung auch neue Risiken mit sich bringe (ebd.).

Eine direkte Konfrontation mit der US-Regierung vermied die deutsche Exekutive auch mit Blick auf domestische Forderungen aus der Opposition, Edward Snowden in Deutschland Asyl zu gewähren bzw. eine Anhörung auf deutschem Boden zu ermöglichen. Beide Forderungen wurden von der deutschen Regierung abgelehnt (Deutscher Bundestag, 2013d, 16f.). In einer Stellungnahme argumentierte die Bundesregierung, dass bei einer Befragung von Edward Snowden in Deutschland mit »einer Beeinträchtigung der Kooperation mit US-Sicherheitsbehörden zu rechnen sei, die für die Sicherheit Deutschlands von grundlegender Bedeutung sei« (Deutscher Bundestag, 2017c, S. 1278). Eine Klage gegen die Ablehnung einer Anhörung auf deutschem Boden lehnte das Bundesverfassungsgericht im Dezember 2014 ab (Bundesverfassungsgericht, 2014). Der Streitfall wurde sodann vor dem Bundesgerichtshof weitergeführt und endete

dort im März 2017 ebenfalls zugunsten der Regierung (Deutscher Bundestag, 2017c, S. 1281).

Ebenso negativ beschied die Bundesregierung die Forderung, das europäische Abkommen zur Übermittlung von Fluggastdaten mit den USA (EU-USA-PNR-Abkommen) zu kündigen, die gleiche Haltung wurde mit Blick auf das SWIFT-Abkommen vertreten.[1] Die Bundeskanzlerin sah in diesen Forderungen eine nicht zielführende »Trotzhaltung«, die die amerikanische Regierung nicht zur Kooperation veranlassen könne (Deutscher Bundestag, 2014b, S. 570). Das Safe-Harbor-Abkommen sollte aber im Zuge der neuen Datenschutzgrundverordnung überarbeitet und ein neues, höheres Datenschutzniveau in Drittstaaten erreicht werden (Deutscher Bundestag, 2013c, S. 35f.). Das Safe-Harbor-Abkommen bzw. die Datenschutzgrundverordnung war aus Sicht der Regierung damit die einzige Möglichkeit, auf die Enthüllungen zu reagieren und den Unmut deutlich zu machen, ohne damit den Kern der Snowden-Enthüllungen zu adressieren.

In dieser ersten Phase war die Bundesregierung noch zuversichtlich, dass die USA kooperativ bei der Aufarbeitung der Enthüllungen mitwirken würden. Die britische Regierung reagierte bereits früh zurückhaltender auf deutsche Bestrebungen, die Enthüllungen aufzuklären (Deutscher Bundestag, 2013a, S. 4). Die Bundesregierung versuchte bereits kurz nach den Enthüllungen, ein Abkommen mit den USA zu schließen, das die Überwachungspraktiken zwischen beiden Staaten reglementieren sollte. Berichte, wonach es Bestrebungen gäbe, dass Deutschland selbst Teil der 5-Eyes werden wolle, wurden aber bestritten. Bemühungen zur Etablierung neuer geheimdienstlicher Standards wurden ferner mit EU-Mitgliedsstaaten debattiert. Wobei die Regierung hier auch darauf hinwies, dass die EU im Bereich der Nachrichtendienste nicht zuständig sei (Deutscher Bundestag, 2013e, S. 2f.). Im August 2013 wurde ein Fortschrittsbericht zum Acht-Punkte-Plan veröffentlicht. Hierin äußerte sich die Regierung zuversichtlich zur Aushandlung eines No-Spy-Abkommens mit den USA und vermeldete erste Erfolge. So habe es von amerikanischer Seite bereits eine »mündliche Zusage« zum Abschluss gegeben. Die Vereinbarung solle dafür sorgen, dass sich Deutschland und die USA nicht gegenseitig ausspähten, auch Wirtschaftsspionage sollte verboten werden (Bundesregierung, 2013a). Im Parlament wurden die Bemühungen zum Abschluss einer solchen Vereinbarung weithin begrüßt. Es wurde aber darauf hingewiesen, dass hierdurch nicht nur die Regierung sowie die Wirtschaft

1 Die beiden Abkommen regeln den Informationsaustausch zwischen der EU und den USA zum Zweck der Verhinderung, Aufklärung und Verfolgung terroristischer Aktivitäten. Das Abkommen zur Übermittlung von Fluggastdaten (Passenger Name Records (PNR)) regelt die Übermittlung von Informationen zu Reisenden aus der EU in die USA. Das SWIFT-Abkommen bezieht sich auf den Austausch von Daten zu Finanztransaktionen (für weitere Informationen zu den Abkommen, s. bspw. Kaunert/Léonard/MacKenzie (2012))

geschützt werden dürfe, vielmehr müsse auch die Bevölkerung von flächendeckender Überwachung ausgenommen werden (Deutscher Bundestag, 2013i, S. 52 sowie 55).

Da die Bundesregierung die Zielauswahl der amerikanischen und britischen Nachrichtendienste für verfehlt hielt, versuchte sie mit diesem Vorgehen die Referenz der Beschützer-Rollen (Schutz vor wem?) zu verändern und das Ausspähen verbündeter Staaten zu beenden. Begünstigt wurde dieses Bestreben durch die Rollen als Wohlstandsmaximierer und Garant liberaler Grundrechte.

Zwischen Juli und August 2013 kam es zu einer Reihe von Gesprächen zwischen VertreterInnen der deutschen und amerikanischen Seite (Deutscher Bundestag, 2017c, S. 444-455). Am 12. August verkündete Kanzleramtsminister Ronald Pofalla in einer Pressekonferenz, dass die NSA ein No-Spy-Abkommen angeboten habe und dass Verhandlungen hierüber beginnen würden. Aus der Bereitschaft, ein Abkommen zu verhandeln, leitete er ferner ab, dass sich die amerikanischen Dienste, wie von der Regierung gefordert, in Deutschland an deutsches Recht hielten (ebd., S. 458). Eine Schlussfolgerung, die von der Opposition wiederholt heftig kritisiert wurde (Deutscher Bundestag, 2013i, S. 47-67). In der Folge wurde auf Ebene der Geheimdienste und Regierungen über die konkrete Gestalt einer solchen Vereinbarung diskutiert (Deutscher Bundestag, 2017c, S. 464). Am 23. Oktober berichteten deutsche Medien, dass das Handy der Bundeskanzlerin durch die NSA abgehört worden war. In der Folge wurden die Verhandlungen um ein Abkommen intensiviert (Deutscher Bundestag, 2013i, S. 473).

Dass die Bestrebungen, ein Abkommen zur Beschränkung der Überwachungsmaßnahmen abzuschließen, schwierig werden würden, war Ende 2013 abzusehen. Denn sowohl die USA als auch Großbritannien reagierten nicht wie gewünscht auf Gesprächsangebote und Nachfragen. Die Bundesregierung hielt zunächst aber dennoch an dem Ziel fest (Deutscher Bundestag, 2013d, S. 14f.). Sie gab aber bereits Ende des Jahres 2013 zu, dass die Konsultationen nicht nach den Vorstellungen der Bundesregierung verliefen und dass der Informationsaustausch nicht zufriedenstellend erfolgte (Deutscher Bundestag, 2013i, S. 43f.).

Als deutlich wurde, dass die deutsche Regierung mehr wollte, als eine nicht bindende Absichtserklärung, wurden die Verhandlungen Mitte November 2013 komplizierter und die amerikanische Seite wurde zurückhaltender (ebd., S. 470f. sowie 475). Ende November signalisierte die amerikanische Regierung, dass sie den Abschluss einer Vereinbarung ablehne, da sie damit einen unerwünschten Präzedenzfall etablieren würde. Im Januar 2014 erkannte die Bundesregierung, dass die amerikanische Seite die deutschen Forderungen nicht erfüllen würde. Wiederholt zeigte sich die Bundesregierung enttäuscht von der amerikanischen Informationspolitik und der mangelnden Transparenz (Deutscher Bundestag, 2014d, S. 366). Ende Januar gab auch die Bundeskanzlerin öffentlich zu verstehen, dass es substanzielle Differenzen zwischen der amerikanischen und

deutschen Regierung gebe. Im März 2014 signalisierte die US-Regierung, dass ein Abkommen nicht zustande kommen würde. Im April gab schließlich die Bundesregierung das Bestreben auf (Deutscher Bundestag, 2013i, S. 477-501). Aus Sicht von Angela Merkel erreichten die Verhandlungen daher nie die erforderliche Konkretisierung, die einen Abschluss realistisch gemacht hätte (Deutscher Bundestag, 2017c, S. 456). Verhandlungen mit der britischen Regierung führten ebenfalls zu keinem Ergebnis. Auch hier wurde auf unterschiedlichen Ebenen verhandelt und Ronald Pofalla gab am 12. August bekannt, dass ein Abkommen mit der britischen Seite auf einem guten Wege sei. Aber auch hier scheiterten die deutschen Bemühungen (Deutscher Bundestag, 2013i, S. 480f.).

Im Parlament wurde den USA, auch von Seiten der Regierungsparteien vorgeworfen, nicht aufrichtig mit den deutschen Stellen zu kooperieren und so einen substanziellen Informationsaustausch zu unterminieren (ebd., S. 62). Die Opposition warf der Regierung in diesem Kontext vor, gegenüber der amerikanischen Regierung zu nachsichtig zu sein und die Bedenken nicht nachdrücklich genug zu vertreten. Außerdem forderten sie, die Maßnahmen zur Spionageabwehr auch mit Blick auf befreundete Staaten auszubauen (ebd., S. 50f.).

Frustriert von den Reaktionen der amerikanischen und britischen Partnern gab die Bundesregierung bald das Ansinnen auf, ein No-Spy-Abkommen zu verhandeln. Die Bundeskanzlerin bekannte 2015, dass dieser Prozess aufgrund der amerikanischen und britischen Position nicht zu einem für die Bundesregierung akzeptablen Ergebnis geführt werden konnte. Die Regierung habe aber stets nach bestem Kenntnisstand informiert (Bundesregierung, 2015b). Vorwürfe der Opposition, wonach die Regierung die Bevölkerung und das Parlament über die Möglichkeit einer Vereinbarung belogen habe und es schon früh klar gewesen sei, dass die amerikanische Seite einer solchen nicht zustimmen würde, wurde von der Bundesregierung bestritten (Deutscher Bundestag, 2017c, S. 1397). Die Opposition warf der Regierung vor, die Verhandlungen nur zu Wahlkampfzwecken genutzt zu haben, obwohl sofort deutlich geworden sei, dass die amerikanische Seite nie den Abschluss eines Abkommens in Aussicht gestellt habe (ebd., S. 1619f.).

Auf internationaler Ebene war die Bundesregierung mit dem Ziel gescheitert, eine Norm zur Nicht-Überwachung zwischen Verbündeten zu etablieren. In der Folge wendete sie sich domestischen Maßnahmen zu, um eine weitere Unterminierung der eigenen Schutzfunktion entgegenzuwirken.

Nachdem ein Jahr nach den Enthüllungen absehbar war, dass die USA und Großbritannien ihre Überwachungspraktiken nicht signifikant beschränken würden, entschied die Bundesregierung, Verträge mit dem US-amerikanischen ISP Verizon zu kündigen und durch Kontrakte mit der Deutschen Telekom zu ersetzen. Dieser Schritt erfolgte allerdings erst nachdem die Problematik der Einbindung des amerikanischen Dienstleisters in sensible Regierungsnetze öffentlich diskutiert wurde (Netzpolitik.org, 2014a). Als Grund für den Wechsel führte die

Regierung an, dass »die im Zuge der NSA-Affäre aufgezeigten Beziehungen von fremden Nachrichtendiensten und Firmen gezeigt [hätten; Anm. d. Verf.], dass für die sicherheitskritische Kommunikationsinfrastruktur der Bundesregierung besonders hohe Anforderungen zu stellen sind« (Bundesministerium des Innern, 2014a). Beweggrund für den Wechsel war damit auch, dass ein deutsches Unternehmen leichter zur Einhaltung der Sicherheitsstandards verpflichtet werden und dass so ein unerwünschter Datenabfluss besser vermieden werden konnte (Deutscher Bundestag, 2017c, S. 398).

Zusätzlich nutzte die Bundesregierung die aus der Beschützer-Rolle erwachsenden defensiven Kompetenzen, um gegen die Überwachungspraktiken befreundeter Staaten vorzugehen und so auch eine Unterminierung der Rollen als Garant liberaler Grundrechte und Wohlstandsmaximierer zu verhindern.

In der Folge wurde das Bundesamt für Verfassungsschutz (BfV) angewiesen, vermehrt nach Aktivitäten befreundeter Nachrichtendienste zu suchen und die Spionageabwehr in diesem Bezug zu stärken. Die neue Bundesregierung schrieb dieses Ziel explizit im Koalitionsvertrag fest (CDU/CSU, 2013, S. 104). Im Zuge der parlamentarischen Untersuchung der Enthüllungen wurde deutlich, dass die deutsche Spionageabwehr zuvor bei befreundeten Nachrichtendiensten nur beim Vorliegen eines konkreten Verdachtsmoments tätig wurde (Deutscher Bundestag, 2017c, S. 415). Nach den Enthüllungen wurde beim BfV eine Untersuchung eingeleitet, die nach Zeichen der Spionage von amerikanischen und britischen Diensten suchen sollte. Konkrete Beweise für Überwachungsmaßnahmen konnte das BfV in diesem Zuge aber nicht identifizieren (ebd., S. 423, 425). Maßnahmen umfassten bspw. die Suche nach Abhörvorrichtungen an amerikanischen oder britischen Liegenschaften in der Bundesrepublik. Um Aktivitäten des Special Collection Services (SCS)[2] aufzudecken wurde bspw. das amerikanische Generalkonsulat in Frankfurt am Main aus der Luft inspiziert (ebd., S. 433f.). Anfragen, ob die amerikanische Botschaft in Berlin oder das Generalkonsulat in Frankfurt am Main auch durch Beamte des BfV besichtigt werden dürften, wurden von der amerikanischen Administration negativ beschieden (ebd., S. 437).

Die Anpassung der Spionageabwehr wurde dabei als Reaktion auf die »Aufhebung der klassischen ›Freund-Feind-Schemata‹« gesehen (ebd., S. 423). Der Innenminister Thomas de Maizière machte aber auch deutlich, dass die Bemühungen zwar gestärkt werden müssten, dass das Hauptaugenmerk aber nach wie vor auf den Diensten gegnerischer Staaten liege. Dies sei mit Blick auf die aufwändigen Praktiken geboten (ebd., S. 425). Im Verfassungsschutzbericht für das Jahr 2014 hieß es hierzu:

2 Über den SCS berichteten deutsche Medien im Zuge der Enthüllungen vermehrt. Beim SCS handelt es sich um eine Einheit der NSA und CIA, die diplomatische Vertretungen Amerikas für Überwachungszwecke nutzt (Deutscher Bundestag, 2017c, S. 430).

> »Im Bereich dieser sogenannten 360°-Bearbeitung wurden im Jahr 2014 die Weichen für eine Neuausrichtung der Spionageabwehr gestellt, die darauf abzielt, mittels Ressourcenverstärkung und fortentwickelter Methodik zukünftig eine umfängliche Bearbeitung illegaler nachrichtendienstlicher Aktivitäten sonstiger Staaten zu gewährleisten.« (Bundesamt für Verfassungsschutz, 2015, S. 153)

Die Opposition kritisierte diese Neuausrichtung als nicht ausreichend und argumentierte, dass eine effektive Spionageabwehr gegenüber den westlichen Partnern durch die Abhängigkeit des BND konterkariert werde (Deutscher Bundestag, 2017c, S. 1397f.). Die Grünen forderten gar, das BfV ganz aufzulösen und durch zwei neue Institutionen zu ersetzen (ebd., S. 1701). Zum Schutz der deutschen Wirtschaft betonte die Regierung immer wieder die Notwendigkeit, vermehrt gegen »Wirtschaftsspionage« vorzugehen (Deutscher Bundestag, 2013a, S. 31, Deutscher Bundestag, 2013d, S. 14). Verstärkte Aktivitäten gegen die staatliche Spionage gegen Wirtschaftssubjekte wurden in diesem Kontext auch unter Bezugnahme auf die Rolle als Wohlstandsmaximierer ermöglicht.

Diese veränderte Referenz (Schutz vor wem?) der Beschützer-Rolle war unmittelbar durch das internationale Rollenspiel begünstigt, in dem sich die USA nicht dazu bereit erklärt hatten, die eigene Rolle weniger expansiv zu definieren. Die Bundesregierung verlegte domestisch in der Folge zumindest einen Teil der Aufklärungskapazitäten auch auf Aktivitäten von Partnerstaaten.

Auf internationaler Ebene unterstützte die Bundesregierung weitere Maßnahmen mit Bezug zur globalen Internetinfrastruktur. Offiziell gab sie zwar an, nicht zu wissen, ob das transatlantische Telekommunikationskabel 14, das laut Snowden-Enthüllungen im britischen Bude vom GCHQ überwacht wurde (Süddeutsche Zeitung, 2013), tatsächlich kompromittiert war (Deutscher Bundestag, 2013c, S. 9). Die niedersächsische Landesregierung hielt diesen Verdacht 2014 für begründet:

> »Eine Überwachung der Kommunikation, die über dieses Seekabel erfolgt, an der Anlandungsstelle des Kabels in Bude (Großbritannien) und/oder den Endstellen in Manasquan und Tuckerton (beide USA) dürfte indes sehr wahrscheinlich sein.« (Niedersächsischer Landtag, 2014, S. 3)

Eine Einschätzung, die, wenn auch nicht derart explizit, von der Bundesregierung geteilt wurde. Denn die Bestrebungen, zusammen mit Brasilien (auch die brasilianische Regierung war prominentes Opfer der Überwachung) ein neues transatlantisches Kabel zu etablieren, das sowohl den USA als auch Großbritannien den physischen Zugriff auf die Infrastruktur erschwert, verdeutlichten die Absicht, insbesondere den privilegierten Zugang der USA zum Internetbackbone

zu schwächen (Spiegel, 2014a). Das teilweise auch von der EU-Kommission finanzierte Projekt soll den Internetverkehr ab 2020 direkt zwischen Portugal und Brasilien übermitteln (Golem.de, 2014). Das Projekt wurde dabei 2014 auch explizit mit dem besseren Schutz der Kommunikation begründet (Council of the European Union, 2014, S. 4).

Der Aufbau dieser neuen Infrastruktur wurde folglich nicht nur durch den Bezug zur Beschützer-Rolle begünstigt, sondern beinhaltete sowohl Referenzen zur Rolle als Garant liberaler Grundrechte als auch zur Rolle des Wohlstandsmaximierers. Sie spiegelt auf internationaler Ebene die domestischen Bestrebungen, Kontrakte mit amerikanischen Dienstleistern in kritischen Bereichen zu kündigen, um einen privilegierten Datenzugang zu unterbinden.

Da inländischer Internetverkehr potenziell immer über Knoten im Ausland geleitet werden kann, wurden in diesem Zuge auch weitere domestische Maßnahmen zur Wahrung der digitalen Souveränität debattiert. Durch ein verändertes Routing sollte die deutsche Kommunikation geschützt und dem Zugriff externer Geheimdienste entzogen werden. Hierzu führte das BSI Gespräche mit verschiedenen ISPs (Deutscher Bundestag, 2013e, S. 12). Die Bundesregierung prüfte auch die Möglichkeiten, Internetverkehr nur über europäische Infrastrukturen im Schengenraum zu leiten und so den physischen Zugriff auf diese Daten zu erschweren (Deutscher Bundestag, 2013i, S. 45). Diese Pläne wurden von Beginn an durch die Opposition und die Netzgemeinde kritisch gesehen (ebd., S. 47, Netzpolitik.org, 2013). Derartige Überlegungen standen aber auch von Beginn an in Widerspruch zum Ziel der Regierung, ein offenes und nicht fragmentiertes Internet als Raum des freien Meinungsaustausches zu erhalten und zu schützen (Auswärtiges Amt, 2014), da auf diesem Weg ein separates Deutschland- oder Schengen-Netz entstanden wäre. Die Regierung war sich dieser Problematik bereits früh bewusst und verfolgte den Ansatz nicht mit Nachdruck (Deutscher Bundestag, 2017c, S. 391). Ein stärker territorial gebundenes Netz wurde mit Blick auf die Wahrung eines freien Internets nicht angestrebt. Weitere Bestrebungen zur digitalen Souveränität wurden durch die Rolle als Garant liberaler Grundrechte, die sich auch auf das Internet im Ganzen bezog, unterlassen.

Ein Teil des Acht-Punkte-Plans sah vor, an der internationalen Normentwicklung bezogen auf umfassende Überwachungspraktiken mitzuwirken. Hiermit wurde dem Unbehagen über eine extraterritorial ausgedehnte Spionage Ausdruck verliehen und der Anspruch der eigenen (nationalen) Beschützer-Rollen geäußert. Ferner wurden die Forderungen mit der Rolle als Garant liberaler Grundrechte verknüpft.

Zunächst versuchte die Bundesregierung eine Erweiterung des Paktes über Bürgerliche und Politische Rechte zu erreichen. Dies scheiterte aber an Bedenken der USA, Großbritanniens und anderer EU-Staaten, die mit Verweis auf Autokratien deutlich machten, dass ein solcher Prozess von diesen Staaten zur Legi-

timierung ihrer restriktiven Internetpolitiken genutzt werden könnte (Deutscher Bundestag, 2017c, S. 1387). Daher verfolgte die Bundesregierung zusammen mit der brasilianischen Regierung das Ziel, eine Resolution zum Schutz der Privatsphäre im digitalen Zeitalter voranzutreiben (The Guardian, 2013c). Allerdings wurden auch die Formulierungen der Resolution nach Austausch mit den USA und Großbritannien gemäßigt, um deren Zustimmung zu gewinnen und eine direkte Konfrontation zu vermeiden (Reuters, 2013). Die Resolution wurde am 18. Dezember 2013 ohne Abstimmung von der Generalversammlung verabschiedet. Hierin heißt es:

> »[…] that unlawful or arbitrary surveillance and/or interception of communications, as well as unlawful or arbitrary collection of personal data, as highly intrusive acts, violate the rights to privacy and to freedom of expression and may contradict the tenets of a democratic society.« (United Nations, 2013c)

Damit versuchte die Bundesregierung zumindest in Form einer nicht-bindenden Resolution auf die Veränderung enthüllter Praktiken hinzuwirken.

Diese internationale Haltung stand aber mitunter in Spannung zum innenpolitischen Verhalten der Bundesregierung, wo sie ihre eigene Beschützer-Rolle verteidigen musste. Domestisch verweigerte auch die Bundesregierung bei zentralen Fragen und Kritikpunkten an den Praktiken des deutschen Bundesnachrichtendienstes dem Parlament die Antwort. Sie rechtfertigte diese Zurückhaltung mit der besonderen Schutzbedürftigkeit der erfragten Informationen:

> »[…] die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass eine auch nur geringfügige Gefahr ihres Bekanntwerdens unter keinen Umständen hingenommen werden kann, weshalb nach konkreter Abwägung des parlamentarischen Informationsrechts mit dem Staatswohl hier ausnahmsweise Letzteres überwiegt.« (Deutscher Bundestag, 2013c, S. 16)

Die Informationsverweigerung gegenüber dem Parlament erfolgte unter Verweis darauf, dass die Rolle als Garant liberaler Grundrechte durch Aktivitäten der Regierung nicht unterminiert würden. So betonte sie die geographische Begrenzbarkeit der Beschützer-Rolle, die eine Distinktion unterschiedlicher Überwachungsziele im Internet erlaube und den Schutz von deutschen GrundrechtsträgerInnen gewährleiste. Die Frage der Opposition, wie der BND sicher zwischen inländischer, internationaler und ausländischer Kommunikation differenziere, blieb von Seiten der Regierung unbeantwortet. Diese Unterscheidung war mit Blick auf die strategische Fernmeldeaufklärung aber von zentraler Bedeutung. Mit dieser Ermittlungsmaßnahme, über die nur der BND verfügt, werden Verdachtsmomente unabhängig von Einzelfällen generiert, indem großflächig Daten erhoben und

analysiert werden. Für die Anwendung dieser Maßnahme galten unterschiedliche rechtliche Schutzniveaus, die eine eindeutige Unterscheidung zwischen drei Kategorien zwingend erforderten. Für innerdeutsche Kommunikation durfte die strategische Fernmeldeaufklärung nicht angewendet werden, für internationale Kommunikation (ein Endpunkt in Deutschland, einer im Ausland) galten die Beschränkungen des G10-Gesetzes und für ausländische Kommunikation fanden die Bestimmungen des BND-Gesetzes Anwendung (Deutscher Bundestag, 2017c, S. 783). Die Opposition stellte grundsätzlich infrage, dass diese Differenzierung in einem paketvermittelten Netzwerk gewährleistbar sei. Ein Umstand, den auch die Regierung weitgehend einräumte. Aus diesem Grund werde die Kommunikation nach innerdeutschen Kommunikationen durchsucht und diese bereinigt (Deutscher Bundestag, 2013c, S. 14).

Mit der Frage, inwiefern die deutsche Regierung bei der Kommunikationsüberwachung die geografische Referenz der Beschützer-Rolle sicherstelle, eröffnete sich die domestische Kontestation der Politik der Bundesregierung.

Die Praktiken des BND und die Kooperation mit den ausländischen Partnerdiensten rückte so Ende des Jahres 2013 immer mehr in das Zentrum der domestischen Kritik. Forderungen, einen parlamentarischen Untersuchungsausschuss mit der Aufklärung der Vorwürfe zu betrauen, wurden in diesem Kontext lauter (Deutscher Bundestag, 2013i, bspw. S. 47 sowie 57). Diese Verschiebung der Aufmerksamkeit wurde maßgeblich durch das internationale Rollenspiel – die stockenden internationalen Verhandlungen – ermöglicht.

> »Wir haben also viele Fragen, und wir haben viele Fragen, die sich in erster Linie an ausländische Dienste richten und die mit unseren parlamentarischen Mitteln nur schwer aufzuklären und zu beantworten sind. Wir haben aber auch viele Fragen, die in Richtung unserer Nachrichtendienste gehen, die ihr Wissen, ihre Arbeitsweise und ihre mögliche Beteiligung betreffen.« (Ebd., S. 61)

Da die Aufarbeitung der internationalen Praktiken nicht erfolgversprechend erschien, wurde im Folgenden in der domestischen Auseinandersetzung die Kontrolle der Geheimdienste und deren Kompetenzen eingehend diskutiert. Hier ergibt sich damit ein direkter rückwirkender Interaktionseffekt zwischen internationalem und domestischem Rollenspiel.

### 5.1.2 Die Bundesregierung unter Druck: Die domestische Aufarbeitung der Enthüllungen

Im März 2014 setzte der Bundestag in fraktionsübergreifendem Konsens einen parlamentarischen Untersuchungsausschuss zur Aufarbeitung der von Edward Snowden enthüllten Praktiken ein. Das Mandat des Ausschusses umfasste dabei

sowohl die internationale als auch die domestische Dimension der Überwachung. Neben den (Kooperations-)Praktiken des BND sah der Aufgabenkatalog im domestischen Kontext auch vor, zu klären, ob die Bundesregierung ihren Informationspflichten gegenüber dem Parlament angemessen nachgekommen war (Deutscher Bundestag, 2014a). Im Zuge dieser Aufklärung wurde erstens deutlich, dass es erhebliche Unsicherheiten über die rechtlichen Grundlagen der Praktiken des BND gab. Zweitens zeigte die parlamentarische Aufarbeitung, dass die Exekutive in der Folge der Unsicherheit ihre Beschützer-Rolle mitunter sehr weitreichend definierte und Maßnahmen ergriffen hatte, die potenziell nicht durch bestehende gesetzliche Regelungen gedeckt waren. Drittens offenbarte die Untersuchung, dass die Kooperation mit der NSA zur Ausspähung deutscher und europäischer Ziele genutzt worden war. All dies führte dazu, dass die Beschützer-Rolle zunehmend infrage gestellt und in letzter Konsequenz eine gesetzliche Neuregelung der Kompetenzen des BND notwendig wurde.

Der Ausschuss musste sich auf die Aufarbeitung der innerdeutschen Vorgänge beschränken, da Bemühungen mit der US-Administration in Gespräche einzutreten, nicht aufgegriffen wurden (Deutscher Bundestag, 2017c, S. 1380). Bei der Aufarbeitung der Praktiken des BND zeigte sich zunächst, dass die Differenzierung zwischen innerdeutschen, internationalen und ausländischen Kommunikationsverkehren problematisch war. So wurden vom BND bspw. die sogenannten »Funktionsträger-« bzw. »Weltraumtheorien« vertreten (ebd., S. 755 bzw. 856). Der Funktionsträgertheorie folgend ging der BND davon aus, dass Kommunikationen natürlicher Personen, sofern sie für ausländische juristische Personen tätig waren, nicht den gesamten Schutz des G-10-Gesetzes genießen würden und daher potenziell Ziel von weniger restriktiven Überwachungsmaßnahmen werden könnten. Eine Einschätzung, die von JuristInnen bezweifelt wurde (ebd., S. 755-758). Auch die Bundesdatenschutzbeauftragte beurteilte das Vorgehen als verfassungswidrig (Süddeutsche Zeitung, 2016a).

Das Parlamentarische Kontrollgremium konstatierte in einer Stellungnahme lediglich, dass die rechtliche Lage unklar sei (Deutscher Bundestag, 2016b, S. 5). Unklar war zudem, wie der BND mit Daten umgehen sollte, die zwar zwischen KommunikationsteilnehmerInnen im Ausland ausgetauscht wurden, aber über Kabel in Deutschland geleitet wurden. Hierfür erfand der BND die Formulierung des »virtuellen Auslands«, das einen Zugriff auf Kabel in Deutschland rechtfertigen sollte (Deutscher Bundestag, 2017c, S. 759). In diesem Kontext entwickelte der BND eine weitere kritisierte Vorgehensweise, die mit der sogenannten »Weltraumtheorie« gerechtfertigt wurde, um auch diese Kommunikation nicht einem höheren Schutzniveau unterwerfen zu müssen und die Daten leichter mit anderen Nachrichtendiensten teilen zu können (ebd., S. 856f.). Drei juristische Gutachter konstatierten in der Folge substanzielle Defizite bei den gesetzlichen Grundla-

gen der strategischen Auslandsaufklärung (Bäcker, 2014; Hoffmann-Riem, 2014; Papier, 2014).

Die parlamentarische Aufarbeitung zeigte damit zunächst, dass die geografische Referenz der deutschen Beschützer-Rolle ebenfalls nicht klar war. Aufgrund der Paketvermittlung ist die Unterscheidung zwischen in- und ausländischer Kommunikation erschwert. Der BND hatte diesen Umstand genutzt, um möglichst viel Kommunikation unter möglichst wenig restriktiven Regelungen zu erheben und zu verarbeiten.

Zusätzlich zu den gesetzlichen Unklarheiten, wurde ferner bekannt, dass gemeinsame Überwachungsmaßnahmen mit den USA auch gegen Ziele in Deutschland und Europa gerichtet waren. Konkret ging es hierbei um Daten, die in Bad Aibling bei der Aufklärung von Satellitenkommunikation abgefangen wurden. Strittig war, ob diese Daten den Schutz der §§2 ff. des BND-Gesetzes genießen oder ob es sich um reine Auslandskommunikation handle, die diese Bevorzugung nicht genießt. Die Leitung des BND argumentierte, dass Satellitenaufklärung stets außerhalb des deutschen Staatsgebietes stattfinde und daher die entsprechenden Paragraphen nicht anwendbar seien. Diese Ansicht wurde von anderen JuristInnen bezweifelt und war auch zwischen Bundeskanzleramt und BND nicht unstrittig. Der Chef des Kanzleramtes Pofalla schloss sich aber der Auffassung des BND an und argumentierte, dass allein der Ort der Datenerhebung entscheidend für die Verfahrensweise sei (Deutscher Bundestag, 2017c, S. 856-859). Diese Praxis wurde insbesondere mit Blick auf die Kooperation mit den NSA in Bad Aibling problematisch, da der BND die Vorschriften zur Datenweitergabe an Dritte damit umgehen konnte (ebd., S. 1568). Der BND vertrat die Ansicht:

> »Die an die NSA weitergeleiteten Metadaten werden zum einen im Ausland durch eine dortige Satellitenempfangsanlage und durch dortiges Abgreifen von Richtfunkstrecken erhoben, so dass es sich um eine Datenerhebung im Ausland handelt. Die Satellitenempfangsanlagen in Bad Aibling greifen von Telekommunikationssatelliten Datenströme ab und leiten sie nach Bad Aibling. Die Erhebung findet somit an Telekommunikationssatelliten statt, also ebenfalls außerhalb des Geltungsbereichs des BNDG.« (Ebd., S. 860)

MitarbeiterInnen des Bundesbeauftragten für den Datenschutz beurteilten diese als »Weltraumtheorie« bekanntgewordene Interpretation jedoch als unhaltbar (ebd., S. 883). Auch der Untersuchungsausschuss des Bundestages und die Datenschutzbeauftragte des BND kritisierten diese Argumentationslinie (ebd., S. 1324 sowie 1567f.).

All diese Unsicherheiten und die expansiven Interpretationen durch den Nachrichtendienst traten im Zuge des parlamentarischen Untersuchungsausschusses zutage. Der BND hatte die mit dem Internet einhergehenden neuen Überwachungsmöglichkeiten aus Sicht der Opposition unverhältnismäßig weit

genutzt, da stets die Interpretation mit den geringsten Kontrollinstanzen angewendet wurde. Damit war die Beschützer-Rolle der Regierung, die bereits international durch die Überwachung durch befreundete Staaten beeinträchtigt wurde, auch domestisch herausgefordert. Der Vorwurf gegen die Regierung lautete hier, die Exekutive habe die Beschützer-Rolle ohne Wissen des Parlaments und der Öffentlichkeit systematisch überdehnt und rechtliche Unsicherheiten gezielt ausgenutzt.

Zu diesen Vorwürfen kamen neue Erkenntnisse über die Zusammenarbeit mit der NSA. Im Rahmen der Kooperation in Bad Aibling sollten sowohl die Daten deutscher als auch amerikanischer StaatsbürgerInnen nicht analysiert werden. Auch der Ringtausch von Informationen von StaatsbürgerInnen der jeweils anderen Partei wurde explizit untersagt. Auch für Ziele in Europa und Mitglieder der 5-Eyes galten Beschränkungen. Die Distinktion erfolgte dabei unter anderem über Top-Level-Domains und komplette URLs (Deutscher Bundestag, 2017c, S. 776-782). Da mit der strategischen Fernmeldeaufklärung verdachtsunabhängig Kommunikationsvorgänge überwacht werden, müssen, zur Verdachtsgewinnung, bestimmte Inhalte zur weiteren Analyse herausgefiltert werden. Dies erfolgt mittels sogenannter Selektoren, hierbei kann es sich um inhaltliche Schlagwörter (bspw. zum Terrorismus) oder sonstige Telekommunikationsmerkmale (bspw. IP- oder E-Mail-Adressen, Protokollfamilien oder Hashwerte) handeln (ebd., S. 783-786). An der prinzipiellen Unterscheidbarkeit der unterschiedlichen Kommunikationsformen (inländisch, international und ausländisch) wurde sowohl in der Netzgemeinschaft als auch von Datenschutzbeauftragten gezweifelt, da bspw. auch deutsche NutzerInnen E-Mailadressen unter der TLD .com unterhalten könnten (ebd., S. 880).

Das Memorandum of Agreement (MoA), das die Kooperation regelte und das nach den Anschlägen auf das World Trade Center sowie das Pentagon im April 2002 geschlossen wurde, sieht ferner vor, dass der BND die Kontrolle über die Operationen erhält und keine eigenständigen Maßnahmen von deutschem Boden aus stattfinden. Ferner betonte Frank-Walter Steinmeier, der als Chef des Bundeskanzleramtes maßgeblich an der Ausarbeitung beteiligt war:

> »Es gibt keinen Souveränitätsrabatt für die USA. Lassen Sie mich ganz klar sagen, was das MoA deshalb nicht ist: Es ist kein Freifahrtschein für die NSA, in Deutschland Daten über Deutsche zu erfassen. Das Gegenteil ist der Fall. Das Erfassen von Telekommunikation von Deutschen war explizit ausgeschlossen.« (Ebd., S. 771)

Das MoA adressierte maßgeblich die kooperative Satellitenüberwachung. Allerdings war auch das Ausspähen von Internetverkehr an zentralen deutschen Infrastrukturen bereits vorgesehen. Auch diese wurden im Rahmen des Untersuchungsausschusses problematisiert (ebd., S. 775). Die parlamentarische Oppositi-

on erkannte das MoA aber nicht als legitime Grundlage für die Kooperation und die damit einhergehenden Praktiken an (ebd., S. 1446f.).

Im April 2014 wurde öffentlich bekannt, dass sich spätestens seit 2008 Selektoren, die von der NSA eingebracht (gesteuert) wurden, gegen Ziele in Deutschland und Europa richteten und dass dies dem BND auch bewusst gewesen wäre. Diese Selektoren wurden sowohl für die Satelliten- als auch Kabelüberwachung verwendet. Seit 2006 wurde durch den BND eine Negativliste geführt, die diese Suchkriterien ausschloss. Hierunter befanden sich Selektoren zur Überwachung von EADS und Eurocopter, die sowohl auf die Telekommunikation über Satellit als auch Kabel gerichtet waren (ebd., S. 789-796 sowie 802-805). Diese Suchfilter legten auch den Verdacht der Wirtschaftsspionage nahe (Spiegel, 2014c). Die Opposition argumentierte, dass die Bundesregierung von diesen Aktivitäten bereits zuvor gewusst habe und dass das Parlament hierüber falsch informiert worden sei (Deutscher Bundestag, 2017c, S. 1631).

Bei der Aufarbeitung wurde damit deutlich, dass die NSA die Beschützer-Rolle der Bundesregierung substanziell unterminiert hatte. Die Kooperation in Bad Aibling wurde vom amerikanischen Geheimdienst gezielt dazu genutzt, europäische und deutsche Ziele zu überwachen. Zumindest der BND muss von diesen Praktiken gewusst haben, da eine Negativliste mit diesen Suchkriterien angelegt wurde. Wann bzw. inwiefern diese Vorgänge dem zuständigen Bundeskanzleramt gemeldet worden waren, blieb in der politischen Auseinandersetzung umstritten. Die parlamentarische Opposition und VertreterInnen der netzpolitischen Community äußerten massive Kritik an der Bundesregierung. Auch um die Form einer angemessenen Aufarbeitung der Vorwürfe gab es erheblichen Dissens zwischen der Opposition und der Regierung.

Die Regierung wollte auf internationaler Ebene eine Konfrontation mit den USA vermeiden und fragte daher offiziell, ob die Selektorenliste zur Prüfung freigegeben werden könnte. Dies wurde von der Opposition als Unterwürfigkeit interpretiert und als Indiz dafür, »dass die Geheimdienstkontrolle nicht mehr im Kanzleramt stattfindet, sondern gleich bei der NSA« (Deutscher Bundestag, 2015e, S. 9759 ähnlich 9761). Ferner kritisierte die Opposition die Haltung der Bundesregierung gegenüber dem Parlament. Denn die Regierung habe in unangemessener Weise wegen der Weitergabe vertraulicher Informationen mit dem Tatbestand des Geheimnisverrats gedroht, da zuvor Informationen an die Presse weitergeleitet worden waren (ebd., S. 9760f.). Die Regierung begegnete diesem Vorwurf mit dem Verweis auf die Notwendigkeit der Geheimhaltung zur Gewährleistung der Sicherheit in der Bundesrepublik und prangerte die gezielte Verbreitung vertraulicher Informationen an (ebd., S. 9765). Kritik von der Opposition erfuhr weiterhin die aus ihrer Sicht fehlgeleitete Ausrichtung der Geheimdienste, die nicht mehr dem Ziel der Terrorismusprävention diente, sondern zu einer anlasslosen Mas-

senüberwachung unschuldiger BürgerInnen geworden sei (Deutscher Bundestag, 2015e, S. 9760f. ebenso 9763).

In der parlamentarischen Auseinandersetzung um die Zusammenarbeit mit der NSA warf die Opposition der Regierung vor, das Parlament systematisch getäuscht und die Praktiken im Rahmen der Kooperation geduldet zu haben. Ferner insinuierte die Opposition, die Regierung habe entweder wissentlich das MoA aus dem Jahr 2002 nicht durchgesetzt und so dazu beigetragen, dass eigentlich ausgenommene Ziele dennoch überwacht wurden, oder die Kontrolle über den Geheimdienst verloren zu haben (ebd., S. 9756, 9758 sowie 9764). Rollentheoretisch formuliert, war der Bundesregierung entweder die Kontrolle über eigene Beschützer-Rolle entglitten oder sie hatte sie gezielt überdehnt.

In der Debatte um diese internationale Zusammenarbeit betonten RegierungsvertreterInnen, dass die deutschen Geheimdienste an Recht und Gesetz gebunden seien und dass der Austausch mit den amerikanischen Diensten essenziell sei. Zur Illustration wurde in diesem Kontext auf den vereitelten Anschlag der sogenannten Sauerlandgruppe verwiesen (ebd., S. 9754). Die Regierung gab aber auch zu, dass eine verbesserte Aufsicht über die strategische Fernmeldeaufklärung geboten sei und dass in dieser Hinsicht Reformbedarf bestehe (ebd., S. 9755):

> »Wir können nicht immer nur empört mit dem Zeigefinger über den Atlantik zeigen und Standards für den Schutz deutscher Bürger und Unternehmen einfordern und selber genau das nicht leisten. […] Wir müssen hier in Vorleistung gehen. Wenn dieser Untersuchungsausschuss ein Ergebnis haben sollte, dann ist es das, dass wir als Deutsche bereit sind, diese Pionierarbeit zu leisten. In globalen Zeiten […] macht der Unterschied zwischen Inländern und Ausländern überhaupt keinen Sinn mehr, schon gar nicht in Bezug auf unsere europäischen Partner.« (Ebd., S. 9757)

Zusätzlich befeuert wurde die Debatte als die Verhandlungen mit den USA ins Stocken gerieten, die auf eine Freigabe der Selektorenliste für den NSA-Untersuchungsausschuss zielten, und die Bundesregierung vorschlug, die Liste anstatt durch das Parlament, durch einen Sonderermittler prüfen zu lassen (Süddeutsche Zeitung, 2015). Dies wurde von der Opposition als Aushöhlung der parlamentarischen Kontrollbefugnis und damit als Unterminierung der Rolle als Garant liberaler Grundrechte interpretiert (Deutscher Bundestag, 2015f, S. 10096 ebenso 10099). Auch der Bundesbeauftragten für den Datenschutz und ihren MitarbeiterInnen wurde die Einsicht in die Selektorenliste unter Verweis auf das Staatswohl verweigert (Deutscher Bundestag, 2017c, S. 883f.). Mit den Stimmen der Regierungsmehrheit setzte die Regierung, gegen die Stimmen der Opposition, Dr. Kurt Graulich als Sonderermittler zur Prüfung der Selektoren ein (Handelsblatt, 2015).

Die Opposition und die G 10-Kommission legten gegen dieses Vorgehen Klage beim Bundesverfassungsgericht ein. Das Gericht bestätigte mit seiner Entscheidung am 13. Oktober 2016 aber den Kurs der Regierung und teilte die Einschätzung, »eine nicht konsentierte Herausgabe dieser Listen könne die Funktions- und Kooperationsfähigkeit deutscher Nachrichtendienste erheblich beeinträchtigen« wodurch »auch die außen- und sicherheitspolitische Handlungsfähigkeit der Bundesregierung« unverhältnismäßig eingeschränkt werden könne (Bundesverfassungsgericht, 2016a). Mit diesem Beschluss war die Einsetzung eines Sonderermittlers auch rechtlich abgesichert. Die Opposition kritisierte aber noch im Abschlussbericht des NSA-Untersuchungsauschusses, dass hierdurch der Öffentlichkeit lediglich eine Aufklärung »vorgegaukelt« worden sei (Deutscher Bundestag, 2017c, S. 1396). Später wurde öffentlich berichtet, dass die USA einer parlamentarischen Untersuchung der Selektoren nicht prinzipiell widersprochen, sondern vielmehr zur Bedingung gemacht hatte, dass diese nicht öffentlich werden durfte. Die Regierung wollte hierauf offenbar nicht eingehen und verfolgte daher weiter das Ziel, die Liste durch einen Sonderermittler prüfen zu lassen (Spiegel, 2015a). Aus rollentheoretischer Sicht, wurde in diesem Kontext über die angemessene parlamentarische Kontrolle der Beschützer-Rolle verhandelt. Die Opposition konnte sich mit ihren Forderungen allerdings nicht durchsetzen.

Graulich kam in seiner Untersuchung zu dem Ergebnis, dass die NSA mit Blick auf Ziele in Europa, das MoA klar verletzt habe (Deutscher Bundestag, 2017c, S. 854). In seinem Bericht führte der Sonderermittler aus:

> »Insbesondere die Verstöße gegen die Europa-Einschränkung im MoA JSA sind vielmehr bündnispolitisch prekär. Denn die NSA hat auf diese Weise aus der Tarnung des Gemeinschaftsprojekts nachrichtendienstliche Aufklärung gegen Mitgliedsländer der Europäischen Union unternommen. Die NSA hat sich damit nicht nur vertragswidrig verhalten, sondern auch ohne Abstimmung in der Kooperation die deutsche Position gegenüber ihren europäischen Partnern potentiell gefährdet.« (Graulich, 2015, S. 211f.)

Die Selektoren, die auf die Regierungen von Partnerstaaten zielten, seien dabei nicht durch das Auftragsprofil des BNDs gerechtfertigt. So wurden bspw. auch die E-Mails zahlreicher RegierungsmitarbeiterInnen in befreundeten Staaten überwacht (ebd., S. 186 bzw. 207).

Durch diese Enthüllungen über die Defizite der eigenen Beschützer-Rolle brüskiert, veranlasste die Bundesregierung in der Folge, dass die Kooperation in Bad Aibling zunächst eingefroren wurde (Deutscher Bundestag, 2017c, S. 845). Im Januar 2016 wurde sie wieder aufgenommen (Süddeutsche Zeitung, 2016b).

Zu den Erkenntnissen von Graulich wurde der Druck auf die Bundesregierung noch größer, da bekannt wurde, dass der BND um die fraglichen Selektoren

wusste. Der BND selbst hatte unmittelbar nach Veröffentlichung der Snowden-Dokumente im Juli/August 2013 damit begonnen, die Liste zu prüfen. In diesem Zuge wurden 2.000 neue, problematische Suchkriterien identifiziert (zumeist mit Bezug zu Europa). Insgesamt wuchs die Zahl der Negativselektoren auf etwa 40.000. Danach wurden auch diese Selektoren aus der Erfassung gelöscht, über die Erkenntnisse wurde aber weder die Leitung des BND noch das zuständige Bundeskanzleramt informiert. Erst im März 2015 wurden beide Stellen sowie anschließend die Bundeskanzlerin informiert (Deutscher Bundestag, 2017c, S. 831-836 sowie 848). In einer Pressemitteilung gab die Regierung im April bekannt, dass durch die Aufarbeitung der Snowden-Enthüllungen beim BND »technische und organisatorische Defizite« festgestellt worden seien, die durch das zuständige Bundeskanzleramt behoben würden (Bundesregierung, 2015a). In der BND-internen Aufklärung wurde die mangelnde Bereitschaft, Missstände zu melden und damit evtl. das kooperative Verhältnis mit der NSA zu beschädigen, unter anderem auf die Abhängigkeit des BND von der NSA zurückgeführt (Deutscher Bundestag, 2017c, S. 843). Die Bundesregierung gab in diesem Zusammenhang zu, die Kontrolle über den BND zumindest partiell verloren zu haben.

Eine Prüfung der BND-eigenen Selektoren durch das Parlamentarische Kontrollgremium kam ferner zu dem Ergebnis, dass der BND mit diesen Suchfiltern selbst Ziele überwacht hatte, die nicht zum Auftragsprofil des Dienstes passten. Hierzu gehörten PolitikerInnen und Institutionen von EU- und NATO-Mitgliedsstaaten sowie Institutionen der EU (Deutscher Bundestag, 2016c, S. 14). Im Zuge der Aufklärung wurde bekannt, dass der BND Selektoren der NSA als eigene verwendet hatte, wenn diese aus Sicht der MitarbeiterInnen dem Aufgabenprofil des Dienstes entsprachen (Deutscher Bundestag, 2017c, S. 1019f.). In diesem Kontext hatte sich innerhalb des BNDs aufgrund weitreichender Freiheiten eine Eigendynamik bei der Einstellung von Selektoren ergeben (ebd., S. 1023-1027). Die Leitungsebene erkannte die bisherige Handhabung der BND-eigenen Selektoren als problematisch und Ende September 2013 erging eine Weisung, die ein kontrollierteres Verfahren zur Aufnahme von Selektoren definierte (ebd., S. 1037). Außerdem wurden im Oktober 2013 etwa 700 Selektoren deaktiviert (ebd., S. 1042). Der Präsident des BND wurde, kurz nachdem die Bundeskanzlerin öffentlich das Ausspähen unter Freunden verurteilt hatte, über die problematischen Selektoren mit EU- und NATO-Bezug unterrichtet. Anschließend informierte er Ronald Pofalla über die kritischen Vorgänge. Da diese Praxis von allen Beteiligten als politisch sensibel betrachtet wurde, erging im Folgenden die Anweisung, diese Überwachungen umgehend einzustellen (ebd., S. 1044-1048). Bei den Überwachungszielen handelte es sich zumeist um Botschaften von Partnerstaaten, die in aufklärungsrelevanten Regionen lagen bzw. um europäische Unternehmen, die im Kontext der Proliferation beobachtet wurden (ebd., S. 1108).

Die Aufarbeitung hatte damit gezeigt, dass der BND selbst Aufklärung gegenüber befreundeten Staaten durchführte und dass die von der Bundesregierung zunächst öffentlich kritisierte internationale Fehlausrichtung der Nachrichtendienste in Deutschland ebenfalls Praxis war. Inwiefern das politisch gewollt war, oder ob es sich um ein Versagen der Aufsicht handelte, ist nach wie vor umstritten.

Bis März 2015 erhielt das Bundeskanzleramt offiziell keine Rückmeldung über den Verlauf der Selektorenlöschung. Bei Besuchen in Pullach ordnete Kanzleramtsminister Altmaier erneut die Prüfung und Löschung der Selektoren an und wies den BND an, dafür zu sorgen, dass sich derartige Vorfälle nicht wiederholten (ebd., S. 1072-1084). Ferner wurde im Kanzleramt die mit der Aufsicht über den BND beauftragte Abteilung personell verstärkt sowie das Auftragsprofil des Dienstes angepasst. Im Oktober 2015 informierte Peter Altmaier die Kanzlerin über die kritischen BND-eigenen Selektoren (ebd., S. 1099-1002). Die Kanzlerin musste vor dem Untersuchungsausschuss folglich eingestehen, dass die enthüllten Praktiken des BND gegen die von ihr vertretene Linie standen, dass Partnerstaaten nicht abgehört werden sollten:

> »Da sind wir dann ja im Zuge der weiteren Zeitabläufe – und daran hat der Untersuchungsausschuss ja auch mitgewirkt, muss man sagen, durch seine Beweisbeschlüsse – auf Dinge gestoßen, die gegen diesen Satz verstoßen. […] Wenn dieser Satz im BND, wie Sie jetzt sagen, zum Nachdenken geführt haben sollte, dann war er noch richtiger platziert, als er sowieso platziert war. Er erschien mir damals eher als eine Trivialität aus deutscher Perspektive.« (Ebd., S. 1001)

Strittig blieb hierbei die Frage, inwiefern die Informationspolitik erst durch begleitende Aktivitäten der Presse verfolgt wurde (ebd., S. 1009).

Eine weitere besonders kritisch diskutierte Kooperation zwischen BND und NSA betraf die ebenfalls selektorengesteuerte Erfassung von Kommunikation an deutschen Glasfaserkabeln. Diese Zusammenarbeit wurde unter der Bezeichnung Operation EIKONAL geführt und später auch prominent in der Öffentlichkeit diskutiert. Im Oktober 2014 wurde berichtet, dass der BND zwischen 2005 und 2008 an einem Internetknoten in Frankfurt am Main große Mengen Kommunikationsdaten abgefangen und Teile davon an die NSA weitergeleitet habe. 2007 sei diese Kooperation von deutscher Seite aufgrund der politischen Brisanz unter Protest der NSA beendet worden (Süddeutsche Zeitung, 2014a). Auch in diesem Kontext zeigte sich, dass der BND wissend zum Mitläufer der NSA geworden war. Aus rollentheoretischer Perspektive war der Regierung die Kontrolle über die eigene Beschützer-Rolle temporär abhanden gekommen.

Auch diese Kooperation beruhte auf dem MoA aus dem Jahr 2002. Betroffen hiervon war sowohl leitungsvermittelte als auch paketvermittelte Telekommuni-

kation. Motiviert war die Kooperation mit der NSA durch die Anschläge vom 11. September, die sowohl in Deutschland als auch in den USA das Bedürfnis nach einer weitreichenderen Überwachung von Auslandskommunikation erhöht hatte. Die deutsche Regierung suchte daher aktiv die Zusammenarbeit mit der NSA. Der BND verfolgte mit der Operation zwei Ziele: zum Einen die Aufklärung internationaler terroristischer Aktivitäten sowie zum Anderen den Aufbau eigener Kapazitäten zur effektiven großflächigen Überwachung von Internetkommunikation (besonders über Glasfaserkabel). Die NSA hat den BND durch das Zurverfügungstellen von Technik und Know-How maßgeblich ertüchtigt, in diesem Bereich tätig zu werden. Im Gegenzug wurde die NSA an den gewonnenen Erkenntnissen beteiligt. Zur Wahrung der eigenen Beschützer-Rolle wurde festgelegt, dass die NSA selbst keinen physischen Zugang zu den Kabeln erlangte und dass Informationen erst nach einer Überprüfung weitergegeben wurden. Ferner sollte nur Hard- und Software von der NSA verwendet werden, die für den BND transparent war (Deutscher Bundestag, 2017c, S. 890-894 sowie 948-950). Bei der Überprüfung der Hardware wurde aber deutlich, dass die Kontrolle der Komponenten mitunter nicht gewährleistet werden konnte. Im Zuge dieses Kontrollverlusts war es der NSA möglich, auf G10-geschützte Daten zuzugreifen. Der BND selbst wusste nach einer internen Begutachtung der Technik um dieses Defizit, unternahm aber zunächst nichts (ebd., S. 1512).

Erste Formen nahm die Operation 2003 an, als der BND sich erstmals an die Deutsche Telekom wendete, um Kommunikation in Frankfurt a.M. abzugreifen. Das Unternehmen reagierte aber zunächst skeptisch und fürchtete durch das Gewähren des Zugriffs gegen geltendes Recht zu verstoßen. Diese Zweifel wurden durch einen Brief des Bundeskanzleramts Ende 2003 ausgeräumt. In diesem Schreiben wurde das Unternehmen aufgefordert, den BND bei der Umsetzung der Überwachung zu unterstützen. Am 1. März 2004 wurde zwischen dem BND und der Deutschen Telekom der sogenannte Transit-Vertrag geschlossen. In diesem wurde die Übertragung von ausländischen Kommunikationsdaten geregelt (ebd., S. 899-902). Die Opposition ging davon aus, dass die Telekom das Schreiben des Bundeskanzleramts nicht hätte akzeptieren dürfen und dass das Unternehmen mit der Ausleitung der Daten daher Rechtsbruch begangen hat (ebd., S. 1476-1482).

Problematisch wurde diese Regelung als der Anteil paketvermittelter Kommunikation 2005 zunahm und aus Sicht der Deutschen Telekom eine zweifelsfreie Distinktion zwischen ausländischen, inländischen und internationalen Daten nicht mehr gewährleistbar war, da über die Leitungen bis zu 90 Prozent deutsche Verkehre geleitet wurden. In der Folge musste der BND eine Anordnung zur Überwachung gemäß Artikel 10-Gesetz erwirken (ebd., S. 906). Diese Anordnung erging nach Prüfung durch die G 10-Kommission am 20. Oktober 2005. Damit ging der Fokus auf ausländische Verkehre verloren und auch die G

10-geschützte Kommunikation wurde durch den BND zur Informationsgewinnung genutzt (ebd., S. 926-930). Nach einer Testphase wurden von Ende 2007 bis Juni 2008 paketvermittelte Kommunikationsdaten an den BND ausgeleitet (ebd., S. 943). Die Daten wurden auf ihr Schutzniveau überprüft und anhand von Selektoren des BNDs und der NSA gefiltert. Die für die NSA interessanten Inhaltsdaten wurden anschließend weitergeleitet (ebd., S. 954-958). Im Juni 2008 wurde die Operation aufgrund der Unergiebigkeit sowie der unkalkulierbaren Risiken eingestellt. Die Risiken resultierten aus dem Umstand, dass die technische Filterung von G 10-Verkehren nicht verlässlich funktionierte. Daher mussten die Daten nochmals »händisch« geprüft werden. Dies führte, neben der Datenreduktion, zu einem zeitlichen Verzug, der für die amerikanische Seite nicht akzeptabel war. Dies trug ebenfalls zur Einstellung des Projekts bei (ebd., S. 958-963). Dass die technischen Filter zur Unterscheidung deutscher Kommunikation zu keinem Zeitpunkt verlässlich funktionierten, war auch Gegenstand erheblicher Kritik (ebd., S. 1511).

Besonders kritisch wurde weiterhin darüber debattiert, ob der BND die G 10-Kommission darüber getäuscht habe, dass er mit dieser Anordnung auch sogenannte Routineverkehre (reine Auslandskommunikation) überwachen wollte, da es sonst keine rechtliche Grundlage für die Kabelerfassung in Deutschland gab (ebd., S. 1388). Die Opposition erkannte in dem Vorgehen eine gezielte Täuschung der Kontrollinstanz. Auch Mitglieder der G 10-Kommission sagten bei der parlamentarischen Untersuchung, dass sie über die doppelte Nutzungsabsicht der Anordnung nicht informiert waren. Die Opposition ging ferner davon aus, dass nach dem Urteil des BVerfG zur Auslandsaufklärung aus dem Jahr 1999 aufgrund der Datenerfassung in Deutschland, eine eigene neue Gesetzesgrundlage notwendig gewesen wäre. Der Zugriff auf die Kabel in Frankfurt erfolgte aus Sicht der Opposition damit ohne rechtliche Basis. Der BND habe gezielt versucht, zu vermeiden, dass es zur Etablierung einer neuen rechtlichen Regelung hierzu komme, um weiter mit möglichst wenig Restriktionen agieren zu können (ebd., S. 1397 sowie 1497-1502).

Die Regierung hatte aufgrund der mangelnden technischen Fähigkeiten des BND also nicht nur die Kontrolle über die sicherheitspolitische Kooperation verloren, sondern aus Sicht der Opposition auch die demokratische Kontrolle des Geheimdienstes teilweise umgangen bzw. darauf hingewirkt, dass ein Regulationsdefizit nicht erkennbar wurde. Aus rollentheoretischer Perspektive war damit fraglich, ob die Regierung die Kontrolle über die Beschützer-Rolle verloren hatte.

Öffentlich wurde in diesem Kontext ferner eine weitere Besonderheit paketvermittelter Kommunikation debattiert. Eigentlich war der BND laut G 10-Gesetz nur dazu befugt 20% der bestehenden Leitungskapazität zu überwachen. Dies sollte einer flächendeckenden Überwachung entgegenwirken. Da das Internet aber so gestaltet ist, dass möglichst nie eine Auslastung von 100% vorliegt,

sondern, dass immer Reserven in den Kapazitäten vorhanden sind, bestanden Zweifel daran, ob die Begrenzung tatsächlich zu einer Limitierung der Überwachung führt oder ob auch bei 20% praktisch alle Kommunikationsvorgänge erfasst werden könnten. Außerdem sind datenintensive Anwendungen (bspw. das Streaming von Videoangeboten) potenziell nicht überwachungsrelevant, so dass auch bei einer Begrenzung auf 20% noch sämtliche E-Mail-Kommunikation erfasst werden könnte, da diese im Vergleich kaum Leitungskapazität verbrauchen (Bäcker, 2014, S. 12f.). Es stand folglich infrage, inwiefern alte Regularien zur Begrenzung der Beschützer-Rolle aufgrund der technischen Entwicklung noch begrenzende Wirkung auf die Rolle hatten.

Die Regierung gestand ein, dass es offenbar Missstände bei der Kooperation zwischen BND und NSA gegeben habe. Allerdings dürfte die partnerschaftliche Zusammenarbeit mit den USA nicht durch eine Überreaktion gefährdet werden, da sonst negative Folgen für die Sicherheitslage in Deutschland zu fürchten seien (Deutscher Bundestag, 2015f, S. 10099f. ebenso 10101f.). Denn »Wer diese internationale Kooperation grundsätzlich infrage stellt […] spielt mit der Sicherheit dieses Landes.« (ebd., S. 10111). Die Regierung merkte ferner an, dass Partner aus Sorge vor der Veröffentlichung geheimer Informationen bereits intensiv ihre Kooperation mit dem BND prüften (Deutscher Bundestag, 2015g, S. 10371). Die Bundesregierung wollte diese Abhängigkeit der Beschützer-Rolle folglich auch nicht substanziell infrage stellen.

Eine weitere Kooperation mit den USA wurde unter dem Namen GLOTAIC geführt. In dieser Operation wurden die Leitungen eines deutschen Telekommunkationsproviders überwacht und Telefongespräche abgehört (Deutscher Bundestag, 2017c, S. 965-970). Die Initiative für das Projekt ging nach Aussagen des BND vom nicht näher spezifizierten amerikanischen Partnerdienst aus. Die Operation dauerte dann von 2004 bis 2006 und richtete sich gegen einen Provider, der besonders viel Kommunikation aus dem Nahen und Mittleren Osten abwickelte und die damit nach den Terroranschlägen in New York und Washington besonders bedeutsam erschien (ebd., S. 976f.). Auch in diesem Kontext wurde die Informationspraxis des BNDs kritisiert. Inwieweit das Bundeskanzleramt von der Operation GLOTAIC informiert war, wollte der damalige BND-Präsident Hanning nicht explizit beantworten. In der Befragung durch den Untersuchungsausschuss sage er:

> »Wissen Sie, mit dem Bundeskanzleramt gibt es eine formelle Schiene, und es gibt eine informelle Schiene, und es wird natürlich informell sicher sehr viel mehr mitgeteilt als formell. Aber wie das da genau abgelaufen ist, das kann ich Ihnen jetzt nicht mehr sagen aus meinem Gedächtnis heraus.« (Ebd., S. 973)

Frank-Walter Steinmeier sowie Thomas de Maizière, zu den fraglichen Zeiten Chefs des Bundeskanzleramts, bestritten, Kenntnis von der Operation gehabt zu haben. Betonten aber, dass dies ein Fehlverhalten des BNDs gewesen sei (ebd., S. 973f.).

Ähnlich verlief die Informationspolitik des BND bei einer geplanten Kooperation mit dem britischen GCHQ, die erst nach der Veröffentlichung der Snowden-Dokumente eingestellt wurde. Unter dem Operationsnamen Monkeyshoulder plante der BND zusammen mit dem GCHQ an einem zentralen Internetknoten in Frankfurt a.M. Internetverkehr zu überwachen. Auch hier stand der Verdacht im Raum, der deutsche Nachrichtendienst hätte eine Meldung an das Bundeskanzleramt systematisch zu verschleppen versucht (ebd., S. 990-993).

Durch die domestische Aufarbeitung der Snowden-Enthüllungen und das Bekanntwerden der Praktiken des BND wurde zunehmend deutlich, dass mit Blick auf den Auslandsnachrichtendienst Reformbedarf bestand. Die Regierung sah sich durch die parlamentarische Aufklärung mit mehreren Problemen konfrontiert, die eine gesetzliche Neuregelung nötig machten. Die Aufarbeitung hatte gezeigt, dass der BND seine Aufgaben angesichts rechtlicher Unklarheiten sehr expansiv interpretiert hatte. Die Untersuchung verdeutlichte weiterhin, dass der BND selbst Partnerstaaten abgehört hatte. Die Bundesregierung stand daher vor der Entscheidung, internationale Forderungen nach nachrichtendienstlicher Zurückhaltung zu kodifizieren oder selbst expansive Überwachungsmaßnahmen durchzuführen und diese zu verteidigen. Es galt also neue Vorgaben für die Beschützer-Rolle und deren Aufsicht zu formulieren.

In der Folge wurde Mitte 2015 mit der Arbeit an einem neuen BND-Gesetz begonnen. Das neue Gesetz sollte den aufgedeckten Defiziten Rechnung tragen, die Kooperation mit anderen Nachrichtendiensten regeln und auch die Aufsicht über den BND verbessern (ebd., S. 1388f.). Die wesentlichen Neuregelungen sowie die Auseinandersetzung um diese Neudefinition werden im folgenden Abschnitt dargestellt.

### 5.1.3 Die Etablierung einer neuen Beschützer-Rolle: Reform des BND-Gesetzes

Die Bundesregierung argumentierte von Beginn an, dass die Arbeit der Nachrichtendienste angesichts der zunehmend diffuseren Gefahrenlage in der Welt immer wichtiger werde.

> »Das hängt damit zusammen, dass der Prozess der Globalisierung, der uns so viele Vorteile im Hinblick auf Wohlstand und Freiheiten bringt, eben auch dazu führt, dass die Gewährleistung unserer inneren und äußeren Sicherheit

> immer mehr vorverlagert wird, weil die Bedrohungen, mit denen wir es zu tun haben, internationaler werden. Für den Bereich des internationalen Terrorismus kann das jeder nachvollziehen; das gilt aber auch für den Bereich der Cybersicherheit und vieles andere mehr.« (Deutscher Bundestag, 2016e, S. 18274)

Aus diesem Grund ging es aus Sicht der Regierung mit dem neuen BND-Gesetz explizit nicht darum, die Fähigkeiten und Kompetenzen des BND zu begrenzen, sondern transparenter zu gestalten. Auch die Kooperation mit anderen Nachrichtendiensten sollte nicht gefährdet werden (ebd., S. 18274, 18277f., 18280f.). Allerdings betonten auch RegierungsvertreterInnen, dass ein »Eigenleben« des Dienstes nicht akzeptabel sei (ebd., S. 18280 sowie 18283). Daher wurden auch neue Kontrollmechanismen implementiert. Die Gesetzesreform sorge dadurch dafür, dass das Sicherheitsbedürfnis und die Grundrechte in angemessenem Verhältnis gewahrt würden. Weiterhin sah die Bundesregierung im neuen BND-Gesetz eine Möglichkeit durch einen stärkeren Nachrichtendienst bestehende Abhängigkeiten zu reduzieren (Deutscher Bundestag, 2016f, S. 19625).

Es ging der Regierung folglich nicht um eine Beschränkung der Beschützer-Rolle, sondern um deren Erhalt bzw. die offenere Darstellung. Mit besseren Kontrollmechanismen sollte auch der Rolle als Garant liberaler Grundrechte genüge getan werden.

Die Opposition beklagte dementsprechend, dass das Gesetz all das legitimiere, was vorher unzulässig oder unreguliert gewesen sei (Deutscher Bundestag, 2016e, S. 18276). Eine Sichtweise, die auch in der Netzgemeinde weitverbreitet war (Netzpolitik.org, 2016a). Ferner bemängelten die Oppositionsparteien, dass das Gesetz zu unklar gehalten sei und dass das Ausspähen von EU-BürgerInnen sowie von Partnerstaaten nicht pauschal verboten worden sei (Deutscher Bundestag, 2016e, S. 18276).

Durch die Ermächtigung zur Kabelerfassung in Deutschland wurde dem BND die Kompetenz übertragen, Eingriffe zur Überwachung von Auslandskommunikation, wie im Rahmen der Operation Eikonal, auf Grundlage des BND-Gesetzes durchzuführen. Somit war der BND nach der Reform nicht mehr auf die freiwillige Kooperation der Unternehmen angewiesen, sondern konnte deren Kooperation gesetzlich erzwingen (Deutscher Bundestag, 2017c, S. 1388f.). Diese Verpflichtung zur Kooperation wird in §8 des neuen BND-Gesetzes geregelt. Die Unternehmen bzw. MitarbeiterInnen werden ferner dazu verpflichtet über die Maßnahmen Stillschweigen zu wahren (Bundesgesetzblatt, 2016a, §17). Damit schuf die Bundesregierung Klarheit mit Blick auf die Kabelüberwachung in Deutschland. Die Beschützer-Rolle wurde in diesem Kontext also an der vorherigen Praxis ausgerichtet.

Das Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes vom 23. Dezember 2016 ermächtigt den BND in den §§ 6ff. explizit, in Deutschland auf Kommunikationsnetze zuzugreifen, um dort Auslandskommunikation zu erheben und zu analysieren. Der BND darf dies, um

> »1. frühzeitig Gefahren für die innere oder äußere Sicherheit der Bundesrepublik Deutschland erkennen und diesen begegnen zu können, 2. die Handlungsfähigkeit der Bundesrepublik Deutschland zu wahren oder 3. sonstige Erkenntnisse von außen- und sicherheitspolitischer Bedeutung über Vorgänge zu gewinnen, die in Bezug auf Art und Umfang durch das Bundeskanzleramt im Einvernehmen mit dem Auswärtigen Amt, dem Bundesministerium des Innern, dem Bundesministerium der Verteidigung, dem Bundesministerium für Wirtschaft und Energie und dem Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung bestimmt werden.« (Ebd., §6(1))

Die Anordnung hierzu ergeht durch das Bundeskanzleramt. Aus welchen Netzen diese Informationen gewonnen werden dürfen, wird ebenfalls durch das Kanzleramt bestimmt (ebd., §6(1)). Bereits hierin erkannten KritikerInnen eine Ausweitung der Kompetenzen des BNDs, denn zuvor war der Nachrichtendienst an eine Begrenzung der Überwachung auf 20% der Leitungskapazität beschränkt. Von nun an aber, wurde das Ausspähen ganzer Netze ermöglicht (Netzpolitik.org, 2016a).

VertreterInnen und Institutionen von Mitgliedsstaaten der Europäischen Union dürfen nur dann überwacht werden, wenn dies den Vorgaben aus dem G 10-Gesetz entspricht und es der Aufklärung von Unternehmen dient, die im Verdacht der Proliferation stehen sowie zur Erkennung eines bewaffneten Angriffs auf die Bundesrepublik oder die Aufklärung internationaler Terroranschläge, sofern dabei nur Informationen über Drittstaaten und Nicht-EU-Mitglieder erhoben werden. Ferner dürfen UnionsbürgerInnen überwacht werden, wenn diese im Verdacht stehen schwere Straftaten begangen zu haben bspw. Straftaten gegen die Landesverteidigung (Bundesgesetzblatt, 2016a, §6(3)). Die Verwendung von Selektoren, die auf EU-Mitgliedsstaaten zielen, muss durch den Präsidenten/die Präsidentin des BNDs selbst angeordnet werden und das Kanzleramt ist hierüber zu informieren (ebd., §9(2)). Die Opposition beklagte, dass die Bestimmungen zur Überwachung dieser Ziele zu weitreichend seien und dass damit keine effektive Restriktion der Praktiken verbunden sei (Deutscher Bundestag, 2016e, S. 18277).

Die Überwachung deutscher StaatsbürgerInnen und Unternehmen ist dem BND weiterhin untersagt. Ebenso ist die Aufklärung mit dem Ziel der Erlangung von Wettbewerbsvorteilen verboten (Bundesgesetzblatt, 2016a, §6(4)(5)). Außerdem wird der BND verpflichtet, die Implementierung der technischen Maßnahmen mit einer Dienstanweisung zu regeln und diese durch das Bundeskanzleramt genehmigen zu lassen, das wiederum das Parlamentarische Kontrollgremium

informiert (Bundesgesetzblatt, 2016a, §6(7)). Das ausdrückliche Verbot der Wirtschaftsspionage wurde dabei als unabdingbar für Deutschland mit seiner starken, exportorientierten Wirtschaft gesehen (Deutscher Bundestag, 2016f, S. 19628). Die Regierung argumentierte, dass mit diesen Beschränkung weltweit erstmals effektive Restriktionen der Überwachung ergehen (Deutscher Bundestag, 2016e, S. 18284).

Mit Blick auf die Referenz der Beschützer-Rolle ist damit eine zweifache Restriktion verbunden. Die Aussage der Bundeskanzlerin, die Überwachung unter Partnerstaaten verurteilte wurde zumindest für die Europäische Union teilweise eingelöst. Die Bundesregierung beschränkt die eigene Beschützer-Rolle in diesem Kontext weiter als dies zuvor der Fall war. Außerdem verbietet die Bundesregierung dem BND ausdrücklich die Wirtschaftsspionage. Auch dies ist eine neue Beschränkung der Beschützer-Rolle, die maßgeblich durch die Rolle als Wohlstandsmaximierer ermöglicht wurde, da die Regierung hoffte, damit zu einer internationalen Norm zum Verzicht auf Wirtschaftsspionage beitragen zu können.

Mit dem neuen Gesetz wurde ferner eine neue Institution zur Kontrolle der strategischen Fernmeldeüberwachung installiert. Im sogenannten Unabhängigen Gremium prüfen und entscheiden drei Mitglieder sowie drei stellvertretende Mitglieder über die Anordnungen zur Telekommunikationsüberwachung aus dem Bundeskanzleramt sowie über die Selektoren mit Bezug zur EU. Zwei der drei Mitglieder müssen RichterInnen am Bundesgerichtshof, ein stellvertretendes Mitglied muss Bundesanwältin bzw. Bundesanwalt beim Bundesgerichtshof sein. Das Unabhängige Gremium wird für die Dauer von sechs Jahren durch das Bundeskabinett berufen. Das Gremium erstattet dem Parlamentarischen Kontrollgremium mindestens alle sechs Monate Bericht (Bundesgesetzblatt, 2016a, §16). KritikerInnen aus der Opposition und der Netzgemeinschaft bemängelten, dass das Gremium nur dem Namen nach unabhängig sei, da es durch das Bundeskabinett bestellt wird (Netzpolitik.org, 2016b). Auch die Opposition kritisierte das Gremium als potenziell untauglich zur Kontrolle des BND (Deutscher Bundestag, 2016e, S. 18276 sowie Deutscher Bundestag, 2017c, S. 1689). Die SPD-Regierungsfraktion sah das Gremium ebenfalls skeptisch und präferierte eine ausgebaute Kontrolle durch die G 10-Kommission, trug letztlich aber die neue Regelung als akzeptablen Kompromiss mit (Deutscher Bundestag, 2016e, S. 18278).

Zusätzlich zum Unabhängigen Gremium wurde mit dem neuen Gesetz auch das Parlamentarische Kontrollgremium gestärkt. Durch eine/n Bevollmächtige/n und einen Stab von MitarbeiterInnen soll das Kontrollgremium effektiver in die Lage versetzt werden, die Aufsicht über den BND besser auszuüben. Der/die Bevollmächtigte wird auf Weisung des Kontrollgremiums tätig und führt Untersuchungen beim BND durch. Diese Funktion wurde mit §5 des ebenfalls Ende 2016 erlassenen Gesetz zur weiteren Fortentwicklung der parlamentarischen Kon-

trolle der Nachrichtendienste des Bundes geschaffen. Mit dem Gesetz wurden weiterhin die Informationspflichten der Bundesregierung gegenüber dem Parlamentarischen Kontrollgremium spezifiziert sowie ein Schutz für Whistleblower geschaffen, die dem Kontrollgremium direkt Missstände offenbaren (Bundesgesetzblatt, 2016b). Diese neue Konstruktion wurde von KritikerInnen, analog zum Sonderermittler zur Untersuchung der NSA-Selektoren, als Schwächung der parlamentarischen Kontrolle interpretiert, da die Mitglieder des Kontrollgremiums Informationen nicht mehr selbst einsehen könnten und sich vielmehr auf die Einschätzungen Dritter verlassen müssten (Deutscher Bundestag, 2017c, S. 1692 sowie Deutscher Bundestag, 2016e, 18266 bzw. 18268).

Schließlich wurde mit §13 der Austausch von Informationen mit Partnerdiensten explizit erlaubt und geregelt. So ist für jede Datenweitergabe zu spezifizieren, wozu die Kooperation genutzt wird. Der BND behält sich das Recht vor, Informationen über die Nutzung der Daten zu verlangen und ggf. deren Löschung beim Partnerdienst zu veranlassen. Ferner ist das Parlamentarische Kontrollgremium über die Zusammenarbeit und die damit verfolgten Ziele zu unterrichten (Bundesgesetzblatt, 2016a).

Diese Neuregelungen wurden von den Fraktionen der Regierungskoalition im Parlament als Beitrag zur verbesserten Kontrolle der Nachrichtendienste gesehen und als substanzieller Fortschritt interpretiert. Explizit wurde in diesem Kontext von VertreterInnen der Regierungskoalition auch damit argumentiert, dass mit den neuen Regelungen die nachrichtendienstliche Beschützer-Rolle transparenter und auch für die Öffentlichkeit sichtbarer werden sollte, wozu unter anderem eine jährliche öffentliche Anhörung der drei PräsidentInnen der Geheimdienste des Bundes vorgesehen wurde (Deutscher Bundestag, 2016e, S. 18267). Ermöglicht wurde die gesetzliche Neuregelung der Befugnisse des Parlamentarischen Kontrollgremiums auch durch die Arbeit des NSU-Untersuchungsausschusses, der ebenfalls Defizite bei der Kontrolle der Geheimdienste offenbart hatte und wiederholt angeführt wurde. Weitergehende Reformvorschläge der Opposition lehnte die Regierung aber unter Verweis auf die negativen Implikationen für die Arbeitsfähigkeit der Dienste ab (ebd., S. 18271).

Prinzipiell bemängelte die Opposition, dass das G 10-Gesetz nicht im neuen Gesetz erwähnt werde (Deutscher Bundestag, 2016f, S. 19630). Die RegierungsvertreterInnen vertraten die Ansicht,

> »für uns gilt der Geltungsbereich unseres Grundgesetzes nicht universell, sondern er gilt auf Deutschland bezogen – auf unser Staatsgebiet, auf die Deutschen und die Staatsgewalt.« (Ebd., S. 19635)

Die Regierung hielt damit an einem territorial gebundenen Verständnis des Grundgesetzes fest. Sie betonte aber den besonderen Schutz für BürgerInnen

der Europäischen Union. Die Notwendigkeit zur Unterscheidung zwischen unterschiedlichen Sicherheitssphären wurde mit Verweis auf die kritische weltweite Gefahrenlage gerechtfertigt und die Wichtigkeit der Nachrichtendienste betont: »[…] wir leben zum Glück nicht in Zeiten von Krieg in Europa. Wir leben aber in Zeiten von Krieg im Rest der Welt, in Zeiten von Terror, von fürchterlichem Terror […]« (Deutscher Bundestag, 2016e, S. 18272).

Aus Sicht der Opposition war das neue Gesetz ein weitgehendes Zugeständnis an den Bundesnachrichtendienst, der hierdurch vom »kleinen Bruder« der NSA zu deren »Zwilling« würde (Deutscher Bundestag, 2016f, S. 19626). Die Linke forderte auch in der parlamentarischen Auseinandersetzung die Abschaffung des Nachrichtendienstes (ebd., S. 19627).

Unter Verweis auf die Rolle als Garant liberaler Grundrechte legte der Betreiber des Internetknotens DE-CIX in Frankfurt am Main eine Klage vor dem Bundesverfassungsgericht ein, nachdem eine erste Klage vom Bundesverwaltungsgericht abgelehnt worden war (DE-CIX, 2018). Hierbei stützten sich die Betreiber auch auf ein Gutachten des ehemaligen Präsidenten des Bundesverfassungsgerichts Hans-Jürgen Papier, in dem er konstatiert, dass die Regulation der Überwachung paketvermittelter Kommunikation aufgrund der technischen Gegebenheiten unverhältnismäßig sei (Papier, 2016, S. 14). Auch auf internationaler Ebene wurde das neue BND-Gesetz kritisiert. So bemängelten drei UN-SonderberichterstatterInnen, dass die neue Regelung einen unverhältnismäßigen Eingriff in das Recht zur freien Meinungsäußerung darstelle (United Nations, 2016a).

Die Gesetzesnovelle, die aus rollentheoretischer Perspektive die Festschreibung der Beschützer-Rolle darstellt, hat zu anhaltenden Kontestationsprozessen geführt. Bereits in der parlamentarischen Aufarbeitung der Snowden-Enthüllungen wurde offenbar, dass der BND JournalistInnen im Ausland abgehört hatte (Deutscher Bundestag, 2017c, S. 1611). Reporter ohne Grenzen reichten gegen diese Überwachung von BerufsgeheimnisträgerInnen im Ausland Klage vor dem Bundesverfassungsgericht ein. Die BeschwerdeführerInnen kritisieren dabei vor allem die unterschiedlichen Schutzniveaus für Kommunikation in Deutschland, der EU und dem sonstigen Ausland. In Kombination mit der neuen expliziten Kompetenz zur Informationsweitergabe an andere Nachrichtendienste führe dies zu einem gefährlichen System des Ringtausches, durch das der Schutz besonders geschützter Kommunikation systematisch ausgehöhlt werde (Reporter ohne Grenzen, 2018). Diese Kritik wurde auch von der parlamentarischen Opposition geteilt (Deutscher Bundestag, 2016e, S. 18277).

Das Bundesverfassungsgericht beurteilte das neue BND-Gesetz am 19. Mai 2020 als teilweise verfassungswidrig. Das Gericht beanstandete zwar nicht grundsätzlich die Überwachungskompetenzen des Nachrichtendienstes, forderte aber Nachbesserungen bei dessen Kontrolle. Zudem machte das Gericht deutlich, dass

die deutsche Staatsgewalt auch im Ausland an die Grundrechte gebunden ist. Das Gericht widersprach damit direkt der Interpretation der Bundesregierung. Dementsprechend forderten die RichterInnen die Regierung auf, das BND-Gesetz bis zum Ende des Jahres 2021 grundgesetzkonform zu gestalten (Bundesverfassungsgericht, 2020).

Mit dem neuen BND-Gesetz hat die Bundesregierung die Beschützer-Rolle entlang der enthüllten Praktiken gestaltet. Dies wurde einerseits durch die mit dem internationalen Terrorismus verbundene Gefahrenlage sowie durch die internationale Abhängigkeit ermöglicht. Der Rolle als Garant liberaler Grundrechte wurde aber durch neue Kontrollbefugnisse sowie das neue Unabhängige Gremium und die Stärkung des Parlamentarischen Kontrollgremiums ebenfalls entsprochen. Die Gegenrollenträger haben dies aber als unzureichend betrachtet und das Bundesverfassungsgericht hat die Bundesregierung zur Überarbeitung des Gesetzes verpflichtet.

## 5.2 Vereinigtes Königreich

### 5.2.1 Die Snowden-Enthüllungen: Die britische Regierung zwischen Kritik und Selbstbehauptung

Nach den Veröffentlichungen der Snowden-Enthüllungen geriet die britische Regierung durch die weltweite Berichterstattung in die Kritik. In den ersten Stellungnahmen verurteilten RegierungsvertreterInnen daher die Veröffentlichung der Dokumente als schädlich für die Gewährleistung der Sicherheit im Vereinigten Königreich und damit als unangemessene Beeinträchtigung der Beschützer-Rolle. Zudem führten sie aus Sicht der Regierung zu einer verzerrten öffentlichen Wahrnehmung der nachrichtendienstlichen Praktiken.

Außenminister William Hague betonte daher, dass die Regierung zwar daran interessiert sei, dafür zu sorgen, dass die BürgerInnen Vertrauen in die Arbeit der Nachrichtendienste und deren rechtmäßige Praktiken hätten, dass aber in diesem Kontext keine Informationen öffentlich werden dürften, die Kriminellen, TerroristInnen oder ausländischen Nachrichtendiensten Aufschluss über die Fähigkeiten des GCHQ offenbaren könnten. Um die Praktiken domestisch aufzuklären, wurden dem mit der Kontrolle der Nachrichtendienste betrauten Intelligence and Security Committee des Parlaments zusätzliche Informationen des GCHQ zur Verfügung gestellt (House of Commons, 2013c, S. 31). International verbat sich die Regierung jede Einmischung, so betonte Premierminister Cameron mit Blick auf die EU, dass die Regelungen geheimdienstlicher Praktiken alleinige nationalstaatliche Prärogative seien (UK Government, 2013c).

In dieser ersten Phase war die britische Regierung bemüht, die eigene Beschützer-Rolle gegen Kritik von innen und außen zu behaupten. Hierzu versuchte sie einerseits weitere Enthüllungen zu vermeiden und andererseits betonte sie die rechtsstaatliche Kontrolle der enthüllten Praktiken und damit die eigene Rolle als Garant liberaler Grundrechte sowie die Notwendigkeit geheimdienstlicher Aktivitäten. Durch den Druck zeigte sie auch die Bereitschaft, die Beschützer-Rolle etwas transparenter zu machen.

Bereits in der ersten parlamentarischen Debatte im Juni 2013 wurde von der Regierung sogar die Frage aufgeworfen, ob das GCHQ alle notwendigen Kapazitäten habe, um die Sicherheit bestmöglich zu gewährleisten. Der Außenminister gab schon in dieser Frühphase zu bedenken, dass die gesetzlichen Regelungen angesichts der technischen Entwicklung und der vielfältigen Gefahren (insbesondere des Terrorismus') ausgebaut werden müssten (House of Commons, 2013c, S. 41 bzw. 48). Immer wieder finden sich in den Debatten zudem Verweise auf die Vorgängerinstitution des GCHQ, die Government Code and Cypher School, die von einem Anwesen in Bletchley Park maßgeblich zur Entschlüsselung der deutschen Kommunikation im Zweiten Weltkrieg beitrug. Diese Referenz auf das positive historische Selbst des Nachrichtendienstes findet sich sowohl bei VertreterInnen der Regierung als auch der Opposition (ebd., S. 38f. ebenso 46).[3]

Auf internationaler Ebene vertrat die britische Regierung die Position, dass die Menschenrechte on- wie offline Gültigkeit hätten. RegierungsvertreterInnen machten aber auch deutlich, dass die enthüllten Überwachungsbestrebungen nicht substanziell begrenzt werden würden. Auf einer Konferenz in Seoul sagte Außenminister Hague nur wenige Monate nach Veröffentlichung der ersten Dokumente aus den Snowden-Files:

> »We do all face sophisticated and persistent threats in cyberspace from terrorists or organised criminals. We will not compromise on the United Kingdom's security or give free rein in cyberspace to those who wish to harm our country. With my full support our security and intelligence agencies will continue to address threats in cyberspace and to help our allies and partners to do the same – and the UK will remain at the centre of the debate on how we tackle those threats more effectively. But countries who seek to hide behind firewalls and erect artificial barriers on the internet will ultimately reduce their security, not enhance it.« (Foreign & Commonwealth Office, 2013a)

In diesem Kontext wurde auch betont, dass Staaten, die eine stärkere staatliche Kontrolle des Internets anstrebten, riskierten den digitalen Wirtschaftsraum

3 Die Referenzen zum positiven historischen Selbst des Nachrichtendienstes und dessen Einfluss auf die britische Cybersicherheitspolitik wurde durch den Verfasser kursorisch in einem Aufsatz dargestellt (Steiger, 2017).

nachhaltig zu beschädigen (ebd.). Auf diese Weise versuchte die britische Regierung den Vorwürfen zu begegnen, dass sie mit ihren Überwachungspraktiken selbst weitgehende Kontrolle ausübe und die Sicherheit anderer Staaten bzw. deren BürgerInnen unterminiere. Sie rechtfertigte die eigene Sicherheitspolitik mit aus ihrer Sicht legitimen Bedenken um die (physische) Sicherheit im Vereinigten Königreich und kritisierte zugleich die staatlichen Kontrollen autokratischer Staaten.

Weiterhin betonte die Regierung, dass die Nachrichtendienste stets im Einklang mit den gesetzlichen Regeln arbeiteten und dass damit der Schutz der Bürgerrechte gewährleistet sei. Rollentheoretisch gesprochen, bekräftigte die Regierung damit, dass es kein Defizit bei der Rolle als Garant liberaler Grundrechte gab. Zudem dürfe das GCHQ nur nach ministerieller Anweisung umfassende Überwachungsmaßnahmen ergreifen. Dies sorge insbesondere mit Blick auf die Überwachung britischer StaatsbürgerInnen für eine strenge Kontrolle. Der Prozess gewährleiste, dass der sicherheitspolitische Nutzen stets kritisch gegen die bürgerlichen Freiheitsrechte abgewogen werde. Zusätzlich dazu seien die Überwachungsanordnungen Gegenstand der Prüfung durch den/die Intelligence Services Commissioner und Interception of Communications Commissioner. Insgesamt verfüge das Vereinigte Königreich über eines der stärksten Kontrollsysteme für Nachrichtendienste (House of Commons, 2013c, S. 32 ebenso 38).

Zu diesen Kontrollen kam die positive Haltung gegenüber dem GCHQ, das nicht nur VertreterInnen der Regierung und des Dienstes selbst immer wieder betonten. Die positive Einstellung gegenüber den Nachrichtendiensten wurde in einer ersten Stellungnahme des britischen Premierministers David Cameron deutlich, in der er zur Rechtfertigung der enthüllten Praktiken auch die domestischen Erfahrungen mit Terrorismus aufgriff:

> »But we have every reason to be proud of our intelligences [sic!] services and the way in which they are properly constituted in this country. Since 2000, we have seen serious attempts at major acts of terrorism in Britain typically once or twice a year. […] This year alone, there were major trials related to plots including plans for a 7/7-style attack with rucksack bombs two plots to kill soldiers […]« (UK Government, 2013b)

Aus Sicht der Regierung bestand daher kein Anlass, die Nachrichtendienste in ihren Befugnissen zu beschränken, da die Gefahrenlage für das Vereinigte Königreich insbesondere aufgrund terroristischer Aktivitäten nach wie vor akut war. Die Referenz zum historischen Selbst als Opfer von Terroranschlägen findet sich in diesen Debatten ähnlich wie in den Debatten zu den polizeilichen Befugnissen.

Die Einschätzung wurde aber von Bürgerrechtsorganisationen sowie von Edward Snowden herausgefordert. Aus seiner Sicht waren die Befugnisse des britischen GCHQ sogar noch problematischer als die der amerikanischen NSA:

> »Their respect for the privacy right, their respect for individual citizens, their ability to communicate and associate without monitoring and interference is not strongly encoded in law or policy. And the result of that is that citizens in the United Kingdom and citizens around the world who are targeted by the United Kingdom […] they're at a much greater risk than they are in the United States.« (The Guardian, 2014b)

Die Snowden-Enthüllungen illustrierten in diesem Zusammenhang umfassende Überwachungspraktiken des GCHQ, wie bspw. das Programm Tempora in dessen Kontext transatlantische Glasfaserkabel am Übergabepunkt in Bude angezapft und Kommunikation überwacht wurde (The Guardian, 2013a).

Aus rollentheoretischer Perspektive bemängelten die KritikerInnen eine noch umfassendere und schlechter kontrollierte britische Beschützer-Rolle. Aus ihrer Sicht bestand damit ein Defizit bei der Rolle als Garant liberaler Grundrechte. Außerdem zeigten die Enthüllungen, dass die britische Beschützer-Rolle auch offensiv gegen Partnerstaaten gerichtet war.

Die Snowden-Enthüllungen offenbarten, dass die britische Regierung auch vor dem Hacken in verbündeten Staaten nicht zurückschreckte. Zwischen 2010/11 und 2013 infiltrierte das GCHQ die Systeme des belgischen Telekommunikationsdienstleisters Belgacom. Die als Operation Socialist bezeichnete Maßnahme diente dazu, dem Nachrichtendienst Zugriff auf Informationen insbesondere zu Kommunikationsvorgängen in Afrika und dem Mittleren Osten zu gewähren. Außerdem sollte der Zugriff dann ggf. über Belgacom auf andere Unternehmen ausgedehnt werden. Das GCHQ attackierte damit nicht nur ein Unternehmen im einem EU-Mitgliedsstaat, sondern auch einen wichtigen Dienstleister europäischer Institutionen sowie der NATO. Die belgische Regierung kam nach der Analyse des Angriffs 2018 in einem geheimen Papier zu der Einschätzung, dass der Angriff durch den britischen Geheimdienst ausgeführt wurde und vermutlich durch den Außenminister genehmigt worden war. Öffentlich machte die belgische Regierung diese Erkenntnisse aber nicht über offizielle Kanäle (heise.de, 2014; Spiegel, 2014b; The Guardian, 2018).

Die britische Regierung ging in der Folge zur Behauptung der Beschützer-Rolle offensiv gegen den Guardian vor, der die Dokumente von Edward Snowden erhalten hatte und die Berichterstattung in Großbritannien maßgeblich vorantrieb. Im Juli 2013 wurden JournalistInnen veranlasst, die Festplatten mit den Snowden-Dokumenten physisch zu zerstören. Andernfalls drohte die Regierung mit rechtlichen Konsequenzen (The Guardian, 2013b). Ein Vorgehen das von Bürgerrechtsorganisationen als schwerwiegender Eingriff in die Pressefreiheit scharf kritisiert wurde (Amnesty International, 2013) und auch von Mitgliedern des Unterhauses skeptisch bewertet wurde (House of Commons, 2013e, S. 350f.). Das Vorgehen wurde von Premierminister Cameron aber explizit gerechtfertigt:

> »As I said, we have a free press and it is very important that the press feels it is not pre-censored in what it writes. The approach we have taken is to try to talk to the press and explain how damaging some of these things can be. That is why The Guardian destroyed some of the information on disks it had, although it has now printed further damaging material. I do not want to have to use injunctions, D notices or other, tougher measures [...]« (House of Commons, 2013d, S. 666f.)[4]

Die Abwägung zwischen der Beschützer-Rolle und der Rolle als Garant liberaler Grundrechte war aus Sicht der Regierung damit eindeutig formuliert. Die freie Presseberichterstattung durfte die Beschützer-Rolle nicht unterminieren. Zu diesen Maßnahmen der Selbstbehauptung gehörte auch die kurzfristige Verhaftung und Durchsuchung von David Miranda[5] am Flughafen Heathrow im August 2013. Die Rechtmäßigkeit des Vorgehens wurde später auch gerichtlich bestätigt (The Guardian, 2014a). Das resolute Vorgehen gegen die britischen Medien wurde von internationalen JournalistInnen-Verbänden als flagranter Verstoß gegen die Pressefreiheit interpretiert (Committee to protect Journalists, 2013).

Die Veröffentlichungen der Snowden-Dokumente sorgten aber auch in Großbritannien für Kritik von BürgerrechtsaktivistInnen (Liberty, 2013). Drei britische Bürgerrechtsorganisationen reichten in der Folge, zusammen mit weiteren internationalen NGOs, eine Klage vor dem Investigatory Powers Tribunal (IPT) ein, dem mit der juristischen Bewertung geheimdienstlicher Praktiken betrauten Gremium. Konkret vertraten die KlägerInnen die Ansicht, dass die enthüllten Überwachungsmaßnahmen gegen die Artikel 8 bzw. 10 der Europäischen Menschenrechtskonvention verstießen (Investigatory Powers Tribunal, 2014).

Neben der prozeduralen Kontrolle der Nachrichtendienste verwiesen RegierungsvertreterInnen zur Entkräftung der Kontestationen immer wieder auf die Benevolenz des GCHQ und auf die positiven historischen Erfahrungen mit dem Dienst sowie mit der Kooperation mit der NSA, die seit den 1940er Jahren maßgeblich für die Sicherheit beider Nationen gewesen sei. Während in der deutschen Debatte häufig die einseitige Abhängigkeit von den USA betont wurde, wurde das Verhältnis zwischen dem Vereinigten Königreich und den USA von britischer Seite symmetrisch wahrgenommen und die Reziprozität der Beziehung akzentuiert (House of Commons, 2013c, S. 43). Auf internationaler Ebene wurde die Übernahme einer expansiven Beschützer-Rolle daher erleichtert, da das GCHQ auch

4 Mittels D Notice, mittlerweile DSMA Notice, kann die britische Regierung Medien darum bitten, bestimmte Informationen aus sicherheitspolitischen Gründen nicht zu publizieren. Die Entscheidung über die Veröffentlichung obliegt aber nach wie vor den Redaktionen (Defence and Security Media Advisory Committee, 2020)

5 Dem Lebensgefährten von Glenn Greenwald, der maßgeblich an der Veröffentlichung der Snowden-Dokumente beteiligt war.

weiterhin auf Augenhöhe mit der NSA kooperieren und als technisch versierter Partner wahrgenommen werden sollte.

Diese Kooperation sei nach wie vor für beide Seiten essenziell und die Prinzipien der Zusammenarbeit stünden auch nach Jahrzehnten nicht zur Disposition, sondern sollten weiter ausgebaut werden (House of Commons, 2013c, S. 45 bzw. 49). Die Regierung bestritt in diesem Kontext auch, dass das GCHQ durch den Austausch mit der NSA an Daten gelangt sei, die es laut britischem Recht nicht erheben dürfe (ebd., S. 32f.). Das unterschiedliche Schutzniveau für britische und amerikanische StaatsbürgerInnen durch die NSA wurde von der Opposition zwar problematisiert, die Kooperation allerdings nicht substanziell in Frage gestellt (ebd., S. 39 ebenso 43).

Im Gegensatz zu Deutschland, wo die Beschützer-Rolle als abhängig von der amerikanischen gesehen wurde, sah die britische Regierung eine Kooperation auf Augenhöhe. Außerdem verwies die Exekutive auf die positiven Erfahrungen der Kooperation mit den USA. Zudem betonte sie die Notwendigkeit einer starken Beschützer-Rolle. Die Regierung zeigte sich immer wieder stolz auf die Leistungen des Nachrichtendienstes und deren Fähigkeiten. In diesem Zusammenhang verwiesen RegierungsvertreterInnen wiederholt auch auf das positive historische Selbst des CGHQ und insbesondere die Erfolge während des Zweiten Weltkriegs. Diese positive Einstellung gegenüber dem Nachrichtendienst wurde auch von der parlamentarischen Opposition weitgehend geteilt.

Die Regierung betonte, die Arbeit der Nachrichtendienste sei in einer zunehmend komplexen Sicherheitslage von zentraler Bedeutung für die Gewährleistung der Sicherheit in Großbritannien:

> »There is no doubt that secret intelligence, including the work of GCHQ, is vital to our country. It enables us to detect threats against our country ranging from nuclear proliferation to cyber attack. Our agencies work to prevent serious and organised crime, and to protect our economy against those trying to steal our intellectual property. They disrupt complex plots against our country, such as when individuals travel abroad to gain terrorist training and prepare attacks. They support the work of our armed forces overseas and help to protect the lives of our men and women in uniform [...]« (Ebd., S. 33)

Die oppositionelle Labour Party verteidigte ebenfalls die Arbeit der Nachrichtendienste und verwies auf deren einwandfreien Leumund. Auch die Opposition betrachtete es als wichtiger, die gesetzlichen Vorgaben transparent zu kommunizieren und ggf. anzupassen, um das öffentliche Vertrauen zu stärken. Eine Veränderung der enthüllten Praktiken wurde dagegen kaum gefordert (ebd., S. 34-36).

Konservative Abgeordnete bezeichneten die Enthüllungen gar als »non-story«, die Selbstverständlichkeiten nachrichtendienstlicher Kooperation zwischen Ver-

bündeten unnötig problematisiere. Ferner vertraten VertreterInnen der Tories die Ansicht, dass sich das Vereinigte Königreich bereits in einem »cyber-war« befände und dass den Diensten aufgrund der besonderen Gefahr durch kinetisch folgenreiche Cyberangriffe weitgehende Freiheiten eingeräumt werden sollten (ebd., S. 43 bzw. 45). Auch Abgeordnete der Liberal Democrats konnten bspw. die Aufregung der deutschen Bundesregierung über die Überwachung des Mobiltelefons der Bundeskanzlerin nicht nachvollziehen und betrachteten die Reaktion entweder als Ausdruck tiefer Naivität oder als bloßes öffentliches Manöver (House of Commons, 2013e, S. 362).

Die Ausrichtung der Beschützer-Rolle und deren Umfang wurde im Vereinigten Königreich damit nicht so kritisch beurteilt wie in Deutschland. Während die enthüllten Praktiken in Deutschland als unangemessen empfunden wurden, teilten in Großbritannien viele PolitikerInnen die Ansicht, dass die Arbeit der Nachrichtendienste in dem veröffentlichten Umfang nicht grundsätzlich falsch seien. Dies wurde sowohl durch die als brisant empfundene Gefahrenlage als auch durch das historisch begründete Vertrauen in den Nachrichtendienst ermöglicht.

Zusätzlich zu den essenziellen sicherheitspolitischen Funktionen wurde den Praktiken des GCHQ auch zentrale Bedeutung für die Erreichung wirtschaftlicher Ziele zugesprochen, bspw. bei der offensiven Aufdeckung und Verfolgung von Steuerkriminalität und Wirtschaftsspionage (ebd., S. 356). Ein potenter Nachrichtendienst komplementiert aus dieser Sicht auch die Rolle als Wohlstandsmaximierer. Die Beschützer-Rolle hatte im Gegensatz zu Deutschland damit auch eine katalytisch wirkende Bezugnahme zu wirtschaftlichen Schutzobjekten über den defensiven Wirtschaftsschutz hinaus, die auch eine offensivere Rollenübernahme rechtfertigte.

Zwei Monate nach den ersten Enthüllungen gab das Intelligence and Security Committee (ISC) eine Bewertung zu den veröffentlichten Dokumenten ab. Im Mittelpunkt der parlamentarischen Untersuchung stand der Vorwurf, das britische GCHQ habe im Rahmen der Kooperation mit der NSA durch das PRISM-Programm Zugriff auf Daten britischer StaatsbürgerInnen erlangt, ohne über die dazu notwendigen Berechtigungen zu verfügen. Nach ihrer Untersuchung attestierten die Abgeordneten dem GCHQ, dass die Kooperation im Rahmen der gesetzlichen Regelungen erfolgt sei und dass für die Überwachungsmaßnahmen Anordnungen der zuständigen MinisterInnen vorlagen. Alle Maßnahmen seien durch RIPA 2000 und den Intelligence Services Act 1994 gedeckt gewesen. Die in der Presse geäußerten Verdachtsmomente seien daher unbegründet. Die MPs äußerten aber Bedenken, ob das gesetzliche Regelwerk, das die Auslandsüberwachung regelte, angesichts der technischen Entwicklungen noch angemessen sei. Diese Problematik wurde ferner durch den Interception of Communications Commissioner (IOCCO) untersucht (Intelligence and Security Committee, 2013a,

S. 2).[6] Die Regierung begrüßte diese Entlastung des Nachrichtendienstes explizit und betonte, dass die Überwachungspraktiken stets geltendem Recht entsprächen und angemessener demokratischer Kontrolle unterworfen seien (Foreign & Commonwealth Office, 2013b).

Mit dieser Einschätzung stützte das zuständige parlamentarische Kontrollorgan die Position der Regierung. Auch aus Sicht der Abgeordneten gab es keine systematische Überdehnung der Beschützer-Rolle zu Lasten der Rolle als Garant liberaler Grundrechte.

Im Oktober 2013 kam es zu ersten Kontestationsprozessen durch den kleinen Koalitionspartner gegen einen Ausbau der Überwachungsmaßnahmen. Abgeordnete der Liberal Democrats befürchteten, das Vereinigte Königreich befände sich auf einem Pfad, der »schlafwandlerisch« in einen ausgeprägten Überwachungsstaat führe und in dem die Balance zwischen Sicherheit und Freiheit nicht mehr gewahrt werde. Allerdings wurde auch von den skeptischen Abgeordneten nicht die Notwendigkeit oder Benevolenz der Nachrichtendienste infrage gestellt (House of Commons, 2013e, S. 333).

Mit Blick auf wirtschaftliche Schäden verwiesen britische Abgeordnete auf Deutschland. Überwachungskritische Stimmen aus dem Lager der Liberal Democrats betonten, dass durch die enthüllten Praktiken wirtschaftliches Vertrauen unterminiert werde und dass in Deutschland bereits Konzepte zur Wahrung der digitalen Souveränität (Schengen-Routing) debattiert würden (ebd., S. 338). Die Liberal Democrats forderten daher, wie das ISC, eine grundlegende Evaluation des bestehenden Rechtsrahmens (insbesondere RIPA 2000) – ein Anliegen, das auch von Abgeordneten der Labour Party geteilt wurde (ebd., S. 341 bzw. 364). Insbesondere das Programm Tempora sorgte für Besorgnis, ob die ergriffenen Maßnahmen verhältnismäßig und mit Artikel 8 der Europäischen Menschenrechtskonvention vereinbar seien (ebd., S. 342 ebenso 345). Auch die Beteiligung an Prism und der damit potenziell verbundene Datenaustausch wurden wiederholt problematisiert (ebd., S. 353f.). Generell bemängelten KritikerInnen, dass im Gegensatz zu anderen Staaten und auch den USA in Großbritannien keine wirkliche Debatte über die enthüllten Praktiken stattfinde (ebd., S. 333 ebenso 358f.).

Aber auch auf Seiten des überwachungsskeptischeren kleinen Koalitionspartners wurde auf die historischen Leistungen der »code breakers« sowie auf die Notwendigkeit der Geheimhaltung ihrer Aktivitäten hingewiesen (ebd., S. 361 bzw. 364). Die direkte Verbindung historischer Leistungen und aktueller sicherheitspolitischer Herausforderungen wurde bspw. vom Parteivorsitzenden Nick Clegg betont:

---

6 In seinem 2014 veröffentlichten Bericht kam auch der IOCCO zu der Einschätzung, dass bspw. eine längere Speicherung von erhobenen und nicht für relevant befundenen Daten nicht stattfinde (IOCCO, 2014, S. 15).

> »The security services are similarly awe-inspiring. […] GCHQ has an illustrious history, from the code-breakers who defeated the Enigma machine and shortened the Second World War by at least 2 years, through to the contemporary fight against terrorism.« (UK Government, 2014)

Ein zentraler Bezugspunkt zur Rechtfertigung der expansiven Überwachungsmaßnahmen und zum Nachweis der Benevolenz des GCHQ waren auch beim kritischen Koalitionspartner die historischen Erfahrungen mit dem Nachrichtendienst. Auch KritikerInnen der enthüllten Maßnahmen bezogen ihre Kontestationen damit nicht auf den Nachrichtendienst oder das Potenzial, Daten missbräuchlich zu verwenden, sondern auf das gesetzliche Regelwerk. Auch die Gefahrenlage für das Vereinigte Königreich wurde nicht grundlegend bestritten.

Die Abgeordneten der Tories erwiderten Kritiken mit dem Verweis auf die strenge Kontrolle der britischen Nachrichtendienste (House of Commons, 2013e, S. 367f. ebenso 372). Außerdem betonten sie, dass die Nachrichtendienste große Datenmengen benötigten, um hierin die relevanten Informationen finden zu können – großflächige Überwachungsmaßnahmen waren aus ihrer Sicht also notwendig, um aktuellen Gefahren zu begegnen (ebd., S. 375). VertreterInnen der Tories hielten KritikerInnen zudem entgegen, dass die Gefahrenlage diffuser denn je sei und rekurrierten auf die domestischen Erfahrungen mit Terrorismus, insbesondere die Anschläge in London am 7. Juli 2005 (ebd., S. 345).

Auf die Leistungen des Nachrichtendienstes verwies explizit der damalige Direktor des GCHQ Anfang November 2013. Er stellte in einer Rede ebenfalls eine direkte Verbindung zwischen historischen Erfolgen und aktuellen Praktiken her:

> »I've already spoken about the rich legacy of Bletchley Park for GCHQ: just as the work at Bletchley involved exploiting the adversary's information risk whilst minimising our own, today's internet provides a virtual battlespace for a similar struggle. […] The period we spent in Bletchley Park in World War Two showcases the successes possible when a technological and innovative mindset is allied to an in-depth understanding of the communications environment in which our targets operated.« (GCHQ, 2013)

Wie in diesem Fall und der Äußerung von Nick Clegg wurde in Aussagen immer wieder die direkte Verbindung zwischen historischer Leistung und aktueller Herausforderung hergestellt. Die nachrichtendienstlichen Aktivitäten im Internet wurden so auf eine Stufe mit den Herausforderungen während des Zweiten Weltkrieges gestellt, wobei die Referenz (Schutz vor wem?) der gegenwärtigen Beschützer-Rolle zwischen (internationalem) Terrorismus und feindseligen Staaten schwankt.

Referenzen zu negativen historischen Erfahrungen finden sich zwar im parlamentarischen Kontext, sie sind aber selten und wurden oft nicht aufgegriffen. RegierungsvertreterInnen erwiderten diese Bezugnahmen mitunter gar damit, dass sie aus der Zeit gefallen und nicht mehr mit der nachrichtendienstlichen Tätigkeit im 21. Jahrhundert vergleichbar seien (House of Commons, 2013c, S. 43). Verweise auf das positive historische Selbst des Nachrichtendienstes wurden damit praktisch von allen Parteien geteilt. Eine Position, die die nachrichtendienstliche Beschützer-Rolle gänzlich infrage stellte gab es daher kaum. Stattdessen bezogen sich kritische Stimmen auf die Evaluation des Rechtsrahmens. Beschränkungen der nachrichtendienstlichen Kompetenzen wurden dagegen nur vereinzelt gefordert.

Im Zuge der parlamentarischen Aufarbeitung der Enthüllungen hielt das ISC die erste öffentliche Anhörung seiner Geschichte ab. In diesem Rahmen gaben am 7. November 2013 die Direktoren der drei großen britischen Nachrichtendienste (MI5, MI6 und GCHQ) Auskunft über deren Aktivitäten. In seiner Stellungnahme wies der Direktor des MI6 auf die diffuse Gefahrenlage und die damit verbundenen wichtigen Aufgaben der Nachrichtendienste hin. Zu den Herausforderungen gehörten demnach in erster Linie Terrorismus aber auch Cyberangriffe oder Aktivitäten feindlicher Staaten in Gebieten, die für das Vereinigte Königreich von Relevanz seien. Dabei stellte er auch die enge Kooperation mit den Streitkräften heraus (Intelligence and Security Committee, 2013b, S. 1f.). Das Internet wurde von den Direktoren übereinstimmend als asymmetrische Domäne charakterisiert, die terroristische Bestrebungen tendenziell erleichtere und deren Verfolgung erschwere (ebd., S. 3f.). Aber auch staatliche Akteure versuchten mit dem Internet ihre begrenzten Ressourcen zu kompensieren und Ziele zu beeinträchtigen, die sie sonst nicht erreichen könnten (ebd., S. 12f.). Die Frage, warum die britische Öffentlichkeit erst durch die Snowden-Dokumente von flächendeckenden Maßnahmen erfahren habe, beantwortet der Direktor des GCHQ mit Verweis auf die Notwendigkeit, bestimmte Methoden zur Wahrung ihrer Effektivität geheim zu halten. Ferner gebe es bereits Hinweise darauf, dass TerroristInnen die Informationen aus den veröffentlichten Dokumenten gezielt nutzten um einer Überwachung zu entgehen.

> »What I can tell you is that the leaks from Snowden have been very damaging. They have put our operations at risk. It is clear that our adversaries are rubbing their hands with glee. [...] and our own security has suffered as a consequence.« (Ebd., S. 18)

Der Dienst betreibe weitgehende Überwachung nur zu dem Zweck, einen möglichst großen »Heuhaufen« mit potenziell sicherheitspolitischen Inhalten zu generieren und diesen dann auch nicht komplett, sondern nur partiell und gezielt zu durchsuchen. Ferner versicherte er, dass die Kooperation mit der NSA stets im

Einklang mit britischem Recht gestaltet wurde. Auch die Bedeutung des Dienstes für das ökonomische Wohlergehen des Vereinigten Königreichs wurde in diesem Kontext hervorgehoben (ebd., S. 13-17). Dass die Enthüllungen die Sicherheitslage verschlechtert habe, wurde 2014 auch durch den neuen Direktor des GCHQ, Robert Hannigan, bestätigt. In einem vielbeachteten Beitrag für die Financial Times attestierte er den Betreibern von Sozialen Netzwerken ferner zu »command-and-control networks of choice for terrorists and criminals« geworden zu sein, da sie nach den Enthüllungen starke Verschlüsselung zum Teil ihres Marketings gemacht und damit Ermittlungsbehörden den Zugriff auf Daten erschwert hatten (Financial Times, 2014).

Aus Sicht der Nachrichtendienste war eine umfassende Überwachung daher essenziell, um die Beschützer-Rolle in einer Domäne sicherzustellen, die den GegnerInnen potenziell einen Vorteil biete. Ferner verurteilten sie die Beeinträchtigungen der Rolle durch die Veröffentlichungen. In diesem Kontext wurde auch die wichtige Zusammenarbeit zwischen GCHQ und den britischen Streitkräften herausgestellt. Während die britische Regierung außenpolitisch kritisiert wurde, waren die domestischen Kontestationen zunächst weniger schwerwiegend. Das GCHQ und deren Aktivitäten wurden von VertreterInnen fast aller Parteien positiv bewertet. Dies wurde durch die Bezugnahme zum positiven historischen Selbst sowie die Erfahrungen mit Terrorismus ermöglicht. Kritische Stimmen bezogen sich auf den Rechtsrahmen der Beschützer-Rolle aber nicht auf den Nachrichtendienst. In der Folge geriet die britische Regierung dennoch vermehrt unter Druck, weil innerstaatliche Untersuchungen zu dem Ergebnis kamen, dass die gesetzlichen Regelungen den technischen Realitäten nicht mehr Rechnung trugen.

### 5.2.2 Die Regierung unter Druck: Selbstbehauptung unter wachsendem domestischen Druck

Die Bemühungen, neue gesetzliche Regelungen zu erlassen wurden zunächst intensiviert, als der Europäische Gerichtshof im April 2014 Regelungen zur Vorratsdatenspeicherung für unrechtmäßig erklärte (Europäischer Gerichtshof, 2014). Damit drohten aus Sicht der Regierung wichtige Informationen verloren zu gehen. Der Data Retention and Investigatory Powers Act 2014 wurde in der Folge zwar verabschiedet. Die Tories konnten ihre Vorstellungen allerdings nicht vollends umsetzen und der kleine Koalitionspartner beschränkte die Regelung, die die Vorratsdatenspeicherung weiterhin erlaubte, auf zwei Jahre (sunset clause). Diese Regelungen hatten zwar kaum direkte Bezüge zur IT-Sicherheit, aber hierdurch ergab sich für das Jahr 2016 zusätzlicher Handlungsdruck für die Regierung (s.u.), da sie weiterhin eine gesetzliche Grundlage für die Vorratsdatenspeicherung aufrecht erhalten wollte und diese im Investigatory Powers Act 2016 mit wei-

teren Kompetenzen der Nachrichtendienste verband (House of Commons, 2015d, S. 1084).

Innerstaatlich wurden die Überwachungsmaßnahmen zunächst aber gestützt. Im Dezember 2014 urteilte das IPT erstmals über die Klagen der Bürgerrechtsorganisation gegen die Überwachungspraktiken des GCHQ. In ihrem Urteil stellten die RichterInnen fest, dass die Nachrichtendienste ihre Kompetenzen nicht über Gebühr ausgedehnt hatten (Investigatory Powers Tribunal, 2014, S. 76). Nachdem weitere Informationen über die konkreten Programme bekannt geworden waren, revidierte das IPT im Januar 2015 aber einen Teil dieses Urteils. In einer Urteilsergänzung teilte das Tribunal mit, dass Teile der Kooperation mit der NSA, die den Umgang mit Daten britischer BürgerInnen betrafen, die von amerikanischer Seite erhoben worden waren, gegen die Artikel 8 bzw. 10 der Europäischen Menschenrechtskonvention verstoßen hatten. Durch das Publikwerden im Rahmen der Aufarbeitung der Enthüllungen seien sie doch seit Bekanntwerden legal (Investigatory Powers Tribunal, 2015c).

Nachdem das IPT 2014 Klagen gegen die umfassende Kommunikationsüberwachung im Internet abgelehnt hatte, reichten Bürgerrechtsorganisationen eine weitere Klage vor dem Europäischen Gerichtshof für Menschenrechte ein (Privacy International, 2018). Im September 2018 urteilte der Gerichtshof, dass Teile von RIPA gegen Artikel 8 und 10 der Europäischen Menschenrechtskonvention verstoßen hatten. Das Gericht beurteilte die Kontrolle der umfassenden Kommunikationsüberwachung für nicht angemessen, befand die Praxis aber nicht für grundsätzlich inkompatibel mit Artikel 8. Zudem bemängelte das Gericht einen fehlenden Schutz für die besonders sensible Kommunikation von JournalistInnen. Da sich das Urteil aber auf die Regelungen nach RIPA bezogen, wurden die neuen Praktiken nach dem IPA, mit dem aus Sicht des Gerichts substanzielle Veränderungen einhergegangen waren, nicht überprüft bzw. infrage gestellt. Die Praktiken des Informationsaustauschs zwischen Geheimdiensten befand das Gericht für vereinbar mit der EMRK (European Court of Human Rights, 2018). Die KlägerInnen sahen in dem Urteil einen Erfolg, interpretierten die Befugnisse im IPA aber als noch weitreichender:

> »This judgment is a vital step towards protecting millions of law-abiding citizens from unjustified intrusion. However, since the new Investigatory Powers Act arguably poses an ever greater threat to civil liberties, our work is far from over.« (English PEN, 2018)

Neben diesem späteren Erfolg vor einem internationalen Gericht, urteilte aber auch das IPT 2015 zugunsten der KlägerInnen. Im Februar bzw. April 2015 entschied das Gericht gegen den Nachrichtendienst. Nach Auffassung der RichterInnen hatte das GCHQ in einem Fall besonders geschützte juristische Kommunikation unrechtmäßig abgehört. Die RichterInnen urteilten, dass die Regelun-

gen zum Umgang mit besonders geschützter Kommunikation nicht mit Artikel 8(2) der Europäischen Menschenrechtskonvention vereinbar waren. Die Regierung musste in diesem Zusammenhang zugeben, dass die Regeln zum Umgang mit diesen Daten nicht transparent gemacht worden waren. In der Folge musste das GCHQ die Daten löschen und die Regierung musste den Umgang mit diesen Daten spezifizieren (Investigatory Powers Tribunal, 2015a). Weiterhin urteilte das IPT im November 2015, dass das GCHQ die Daten zweier Bürgerrechtsorganisationen zwar rechtmäßig abgehört hatte, dass die Daten dann aber zu lange gespeichert worden waren (Investigatory Powers Tribunal, 2015b).

Die Kontestation der Beschützer-Rolle wurde damit durch die Judikative zumindest teilweise unterstützt und die Regierung in der Folge zu einer Spezifizierung der Rolle veranlasst.

Der Druck auf die Regierung erhöhte sich im Laufe der Jahre 2015/16 weiter, da unabhängige Evaluationen durch das ISC und den Independent Reviewer of Terrorism Legislation zu der Auffassung gelangten, dass das gesetzliche Regelwerk reformbedürftig sei. Das ISC hatte unmittelbar nach den Enthüllungen mit der Untersuchung der Überwachungspraktiken begonnen und auch in öffentlicher Anhörung Stellungnahmen dazu eingeholt. Im März 2015 legten die Abgeordneten ihren Bericht »Privacy and Security: A modern and transparent legal framework« vor (Intelligence and Security Committee, 2015). Auch in diesem Bericht bekräftigten die ParlamentarierInnen fraktionsübergreifend zunächst die besondere Bedeutung der Nachrichtendienste für die Sicherheit und das wirtschaftliche Wohlergehen des Vereinigten Königreiches.[7] Weiterhin betonten die Mitglieder des Committees, dass sie der Überzeugung seien, die Nachrichtendienste versuchten nicht die gesetzlichen Regelungen zu umgehen (dies schloss explizit den Human Rights Act 1998 ein). Allerdings kritisierte der Bericht, dass die Überwachungspraktiken und die gesetzlichen Bestimmungen nicht in ausreichendem Maße Transparenz für die Öffentlichkeit generierten. Daher empfahl der Ausschuss, eine neue rechtliche Grundlage für die Arbeit der Nachrichtendienste zu schaffen, die die Kompetenzen der Dienste ebenso transparent mache wie die damit einhergehenden Kontrollmechanismen (ebd., S. 1f.).

Rollentheoretische formuliert, folgten die Abgeordneten damit der Linie der Judikative, die die mangelnde Transparenz kritisierte, die Beschützer-Rolle aber nicht grundsätzlich infrage stellte. Das GCHQ und dessen Aktivitäten standen daher nicht zur Disposition.

Wie im deutschen Fall, war es auch in Großbritannien die großflächige Überwachung der Internetkommunikation, die im Rahmen der Aufarbeitung besonde-

7 Das wirtschaftliche Wohlergehen gehört ebenso zum, mit dem Intelligence Services Act 1994 gesetzlich definierten, Schutzgut wie die nationale Sicherheit und die Prävention schwerer Straftaten (The Stationery Office, 1994, Section 3(2)).

re Aufmerksamkeit erfuhr. Das ISC befasste sich eingehend mit den Kompetenzen zur selektorengestützten Überwachung mit dem Ziel der Verdachtsgenerierung (»bulk interception«). In diesem Kontext konstatierten die Ausschussmitglieder, dass nur ein geringer Teil der erfassten Kommunikation durch menschliche Analysten ausgewertet werde, da zuvor technische Filter große Teile der Daten verwerfen würden. Wie groß die jeweiligen Anteile der überwachten und dann ausgewerteten Daten waren, wurde aber nicht veröffentlicht. Im Gegensatz zum deutschen BND, ist das GCHQ aber nach einer entsprechenden Anordnung (RIPA Section 8(1)) auch dazu berechtigt, gezielt die Kommunikation britischer StaatsbürgerInnen zu überwachen und auszuwerten. Für Datenverkehre mit einem Endpunkt im Vereinigten Königreich und einem außerhalb bestand eine andere Form der Anordnung, die auch die Überwachung großer Datenmengen erlaubt (RIPA Section 8(4)). Beide Anordnungen müssen durch zuständige MinisterInnen ergehen (Intelligence and Security Committee, 2015, S. 2-7). Wenn das GCHQ eine Kommunikation abfängt, die sowohl einen Endpunkt in Großbritannien als auch im Ausland hat, dürfen nur Informationen mit Bezug zum/zur ausländischen KommunikationspartnerIn ausgewertet werden. Sollen zusätzlich Daten über KommunikationsteilnehmerInnen innerhalb des Landes analysiert werden, ist dazu entweder eine Section 8(1) Anordnung nötig oder eine ergänzende Section 16(3) Erweiterung (ebd., S. 41).

Wie in Deutschland sorgte auch im Vereinigten Königreich die verlässliche Distinktion zwischen in- und ausländischer bzw. internationaler Kommunikation für Diskussionen, da eine Unterscheidung bei paketvermittelter Information aufgrund unterschiedlicher Routenwahl und der Architektur des Netzes schwer zu treffen ist. Die Abgeordneten stellten daher fest:

> »[…] in respect of internet communications, the current system of 'internal' and 'external' communications is confusing and lacks transparency. The Government must publish an explanation of which internet communications fall under which category, and ensure that this includes a clear and comprehensive list of communications.« (Ebd., S. 41)

Auch die Erweiterung um Section 16(3) sollte nach Meinung der Ausschussmitglieder entfallen und durch Anordnungen nach Section 8(1) ersetzt werden. Ferner regte das ISC an, dass die unterschiedlichen Schutzniveaus für in- und ausländische Kommunikation nicht nur geografisch gefasst werden sollten, sondern dass zudem britische StaatsbürgerInnen im Ausland den gleichen Schutz genießen sollten wie inländische Kommunikation und ebenfalls nur mit einer Section 8(1) Anordnung überwacht werden dürften (ebd., S. 43f.).

Grundsätzliche Kritik bzw. die Forderung nach einem Verbot großflächiger Überwachungsmaßnahmen, wie sie von den Bürgerrechtsorganisationen Big Brother Watch, JUSTICE, Liberty und Rights Watch vorgebracht wurden, teilten

die Abgeordneten im ISC nicht. Vielmehr kam es aus ihrer Sicht auf eine transparente Regelung sowie eine rechtsstaatliche Kontrolle an, um eine unangemessene Beeinträchtigung von Freiheitsrechten zu verhindern (ebd., S. 35). Forderungen wonach Überwachungsanordnungen durch RichterInnen und nicht MinisterInnen erlassen werden sollten, lehnten die Ausschussmitglieder ebenfalls ab. Sie argumentierten, dass hierdurch eine Prüfung der politischen Opportunität und eventueller internationaler Implikationen ausbleibe, was zu einer erhöhten Zahl von genehmigten Anordnungen führen könne, sowie, dass RichterInnen nicht durch das Parlament politisch verantwortlich gemacht werden könnten (ebd., S. 2-7 bzw. 75f.). Diese Einschätzung wurde von BürgerrechtsaktivistInnen nicht geteilt, sie forderten eine richterliche Prüfung und Anordnung von Überwachungsmaßnahmen (Intelligence and Security Committee, 2014c, S. 13). Das ISC empfahl dagegen, die Kontrolle durch die zuständigen Interception of Communications Commissioner bzw. den Intelligence Services Commissioner zu stärken und ihnen mehr Befugnisse zur Kontrolle der Überwachungsanordnungen bzw. deren Umsetzung einzuräumen (Intelligence and Security Committee, 2015, S. 45 bzw. 78).

Auch die Praxis des gezielten Hackens von Computersystemen im Ausland bemängelten die Abgeordneten. Das GCHQ war gemäß Section 7 Intelligence Services Act dazu berechtigt, IT-Systeme im Ausland zu infiltrieren. Der Ausschuss befand, dass die Zahl der IT-Operationen signifikant zugenommen habe und dass es hierzu außerhalb der »Interference with Property« (Sections 5 und 7 Intelligence Services Act) eine eigenständige gesetzliche Regelung für Eingriffe in IT-Infrastrukturen geben solle (ebd., S. 66f.). In öffentlichen Anhörungen des Ausschusses, wurde die Praxis, in IT-Systeme einzudringen und dabei auf Sicherheitslücken zurückzugreifen von Bürgerrechtsorganisationen grundsätzlich kritisiert, da hierdurch die IT-Sicherheit weltweit unterminiert werde und Risiken für alle NutzerInnen entstünden. Hieraus könnten nicht nur Schäden für die Privatsphäre, sondern auch für das Vertrauen in den Wirtschaftsraum entstehen (Intelligence and Security Committee, 2014d, S. 2). In ihrem Bericht nahmen die Abgeordneten diese Sorgen auf, erkannten aber an, dass das GCHQ für seine Arbeit auf Sicherheitslücken und deren Ausnutzung angewiesen sei. Sie mahnten an, dass die Praxis politisch strenger kontrolliert werden sollte (Intelligence and Security Committee, 2015, S. 69).

Mit Blick auf Eingriffe in die Grundrechte, gaben VertreterInnen des GCHQ dem Ausschuss gegenüber an, dass bei Überwachungsaktivitäten stets die Vorgaben des Human Rights Acts 1998 und damit die Regelungen der Europäischen Konvention für Menschenrechte beachtet würden (ebd., S. 85). Im Gegensatz zu Deutschland, wo dem BND Versagen bei der Einhaltung der Gesetze vorgeworfen wurde, wurde dem GCHQ durch die Abgeordneten attestiert, trotz eines vagen

und reformbedürftigen gesetzlichen Rahmens, vorbildlich und stets nach bestem Wissen gehandelt zu haben (Intelligence and Security Committee, 2015, S. 7).

Der Vorwurf des Ringtausches von Informationen mit der NSA wurde ebenfalls durch den Ausschuss überprüft. Die Abgeordneten konstatierten hierzu, dass das GCHQ prinzipiell durch die gesetzlichen Grundlagen zum Datenaustausch ermächtigt sei, dass die Ausgestaltung jedoch nicht ausreichend spezifiziert sei. Auch in diesem Kontext erkannten die Mitglieder des ISC daher legislativen Handlungsbedarf (ebd., S. 94).

Im Gegensatz zu VertreterInnen der Netzgemeinde forderten Parlament und Judikative die Beschützer-Rolle der Regierung damit nicht substanziell heraus. Auch sie erkannten das Internet nicht als zu schützendes Gut an, sondern beurteilten die Gewährleistung nationaler Sicherheit als wichtiger. Aus rollentheoretischer Perspektive war damit eine Begrenzung der Beschützer-Rolle abgelehnt, mit Blick auf die Rolle als Garant liberaler Grundrechte wurde das GCHQ selbst als unproblematisch und die Überwachungspraktiken grundsätzlich als notwendig beurteilt.

Dieses besondere Vertrauen in den Nachrichtendienst stützte sich auch in der Phase parlamentarischer Aufarbeitung auf dessen historische Erfolge, die immer wieder durch den Direktor des Nachrichtendienstes hervorgehoben (GCHQ, 2014) und ferner von einem wissenschaftlichen Gutachter im Anhörungsprozess angeführt wurden: »I seriously think we have to give our intelligence and security community the tools it says it needs, and rely that they will deal with it lawfully« (Intelligence and Security Committee, 2014b, S. 10).

Nachdem das ISC seinen Untersuchungsbericht im März 2015 vorgelegt und eine Reform der Regelungen empfohlen hatte, folgte im Juni 2015 der Bericht von David Anderson, dem Independent Reviewer of Terrorism Legislation (Anderson, 2015). Im Rahmen seiner Analyse holte er Stellungnahmen verschiedener Interessengruppen ein. VertreterInnen der Nachrichtendienste verwiesen ihm gegenüber wiederholt auf die Notwendigkeit starker Dienste, um den Gefahren durch (domestischen und internationalen) Terrorismus, Cyberangriffe oder militärische Konflikte zu begegnen (ebd., S. 41). Hierzu müsse das GCHQ international als angesehener Kooperationspartner wahrgenommen werden, da nur so gewährleistet werden könne, dass Kooperationen und damit Informationsaustausch stattfänden. Aus diesem Grund äußerten VertreterInnen des GCHQ gegenüber Anderson ferner den Wunsch nach einer klaren gesetzlichen Grundlage für den Datenaustausch mit ausländischen Nachrichtendiensten (ebd., S. 198-201). Technologieführerschaft und Kooperationsfähigkeit war aus Sicht des GCHQ zentral zur effizienten Wahrnehmung der Beschützer-Rolle (ebd., S. 198).

Die Internetunternehmen und Kommunikationsdienstleister betonten in ihren Stellungnahmen gegenüber Anderson, dass sie für ihre Geschäftsmodelle auf vertrauensvolle Kommunikation und Datenintegrität angewiesen seien. Durch die

Snowden-Enthüllungen sei dieses Vertrauen beschädigt worden. Die amerikanischen Internetunternehmen bekräftigten in ihren Ausführungen die Ansicht, dass Unternehmen nicht auf Druck von Regierungen Daten herausgeben sollten, insbesondere dann, wenn es sich um Daten anderer StaatsbügerInnen handelt (ebd., S. 203-206). Dieses Unbehagen formulierte ein/e UnternehmensvertreterIn anonym folgendermaßen: »We can't get into conversations that leave our customers on the outside …our priority is our brand, not UK intelligence« (ebd., S. 206).

Grundsätzliche Kritik an den großflächigen Überwachungsmaßnahmen wurde von Bürgerrechtsorganisationen vorgetragen. Sie sahen in der Kombination neuer technischer Überwachungsmöglichkeiten und der rasant wachsenden digitalen Kommunikation eine Gefahr für die Privatsphäre aller InternetnutzerInnen, die sich ohne demokratische Debatte entfaltet habe:

> »[…] communications methods in general have expanded and the digital world makes surveillance even easier. The expansion of this approach means we have slipped into a mass surveillance model without a democratic debate regarding the consequences.« (Ebd., S. 223)

Insbesondere die Möglichkeit das »digitale Schleppnetz« auszuwerfen und auf diesem Weg, ohne viel Aufwand, große Mengen von Daten zu erheben, sorgte für Kritik, da die gesetzlichen Regularien das Ausmaß dieser Praktiken zum Zeitpunkt ihrer Entstehung noch nicht vorhersehen konnten. Abwägungen der Verhältnismäßigkeit seien bei dem Ausmaß der Internetüberwachung nicht mehr plausibel zu treffen. Auch die Argumentation, dass große Mengen der Daten nicht durch menschliche AnalystInnen ausgewertet würden, überzeugte die KritikerInnen nicht, da aus ihrer Sicht ein Eingriff in die Privatsphäre bereits mit der Erfassung der Daten einherging (ebd., S. 223f.). Gegenüber Anderson formulierten Bürgerrechtsorganisation auch Kritik an der parlamentarischen Aufsicht der Nachrichtendienste. So sei das ISC nur mit Abgeordneten besetzt, die durch die/den PremierministerIn nominiert wurden, Berichte müssten zudem zunächst durch die/den RegierungschefIn freigegeben werden. Ferner dürften MinisterInnen Informationen vor dem Committee zurückhalten (ebd., S. 241).

Wie das ISC gelangte auch Anderson zu der Einschätzung, dass das bestehende gesetzliche Regelwerk nicht mehr angemessen war. Auch er forderte die Regierung auf, eine transparentere Regelung für die Überwachungsmaßnahmen der Geheimdienste zu etablieren. Mit Blick auf die Kapazitäten zur flächendeckenden Überwachung, schloss sich Anderson ebenfalls der Ansicht des ISCs an und empfahl, den Nachrichtendiensten diese Möglichkeit offen zu lassen (ebd., S. 285-288). Die Dienste hätten ihm gegenüber überzeugend dargelegt, dass diese Maßnahmen zur Bekämpfung terroristischer Aktivitäten insbesondere nach den Anschlägen im Juli 2005 notwendig seien (ebd., S. 269). Um die Kontrolle der

Überwachungsmaßnahmen zu vereinfachen, schlug Anderson aber vor, eine Independent Surveillance and Intelligence Commission zu etablieren und dadurch die Interception of Communications und die Intelligence Services Commissioner zu ersetzen (Anderson, 2015, S. 299). Außerdem sollte es auch bei Urteilen des IPT ein Berufungsrecht geben – eine Forderung, die von vielen BürgerrechtlerInnen vorgetragen wurde. Ob die Organisation des ISCs geändert werden sollte, bspw. so, dass die Mitglieder wie in anderen Ausschüssen gewählt werden, überließ Anderson dem Parlament (ebd., S. 305f.). Im Gegensatz zum ISC befürwortete Anderson aber die Anordnung von Überwachungsmaßnahmen durch RichterInnen (ebd., S. 300f.).

Neben dem ISC kam damit eine zweite Untersuchung zu dem Ergebnis, dass es legislativen Handlungsbedarf gebe. Wie das ISC forderte aber auch Anderson im Gegensatz zu AktivistInnen keine substanzielle Beschränkung der Maßnahmen. Aber auch er legte eine juristische Kontrolle der Überwachungsanordnungen nahe und empfahl die Kontrollinstanzen zu stärken. Die Notwendigkeit einer potenten Beschützer-Rolle wurde auch in diesem Kontext mit Verweis auf die Erfahrungen mit Terrorismus begründet. Die Vorschläge zielten folglich darauf, ein ausgewogenes Verhältnis zwischen den Rollen als Garant liberaler Grundrechte und der Beschützer-Rolle herzustellen, nicht auf eine substanzielle Beschränkung.

Im Juni 2015 wurden die Berichte und ihre jeweiligen Empfehlungen im Unterhaus debattiert. In diesem Rahmen betonten RegierungsvertreterInnen, dass die Untersuchungen sowohl die Wichtigkeit der nachrichtendienstlichen Aufklärung unterstrichen und den Verdacht ausgeräumt hätten, die Dienste unterminierten bewusst die gesetzlichen Regelungen (House of Commons, 2015d, S. 1081-1083). Die Innenministerin mahnte weiterhin an, dass bei weiteren Diskussionen stets die Gefahrenlage bedacht werden müsse:

> »[…] these powers are about protecting and saving people's lives. In any debate about the right balance between security and privacy, it is important that we remember the full context of the threats we face. They include the threat from terrorism — both from overseas and home-grown in the UK. […] We also face other threats from organised criminals and the proliferation of cybercrimes such as child sexual exploitation, and threats from hostile foreign states and from military and industrial espionage.« (Ebd., S. 1084f.)

Die Priorität der Regierung lag daher darauf, dem Nachrichtendienst die nötigen Werkzeuge an die Hand zu geben, um die Sicherheit des Vereinigten Königreichs zu gewährleisten und dies im Einklang mit den bürgerlichen Freiheitsrechten umzusetzen (ebd., S. 1085).

Abgeordnete der parlamentarischen Opposition betonten ebenfalls die Bedeutung der Nachrichtendienste und deren »quiet heroism«, sie hoben aber auch die Notwendigkeit hervor, einen neuen gesetzlichen Rahmen für die Tätigkeiten der

Dienste zu schaffen und dabei darauf zu achten, dass die Kontrolle sowie die Befugnisse der Dienste angemessen seien (ebd., S. 1086). Die Labour Party erkannte ferner, wie die Regierung, dass es angesichts der vielfältigen Gefahren nicht zu einem Auslaufen der Befugnisse des DRIPA 2014 kommen dürfe, so dass die zeitliche Dringlichkeit einer Neuregelung überparteilich anerkannt wurde (ebd., S. 1087). Wie David Anderson forderte die Labour Party eine richterliche Anordnung für Überwachungsmaßnahmen. In diesem Kontext wiesen Abgeordnete darauf hin, dass das Vereinigte Königreich mit seiner Regelung auch innerhalb der 5-Eyes exponiert sei. Außerdem versprachen sie sich hiervon eine erhöhte Kooperationsbereitschaft von amerikanischen Internetunternehmen (ebd., S. 1089).

Vor diesem Hintergrund entwarf die Regierung 2016 eine Reform der bestehenden gesetzlichen Regularien mit dem Ziel, die Bedenken auszuräumen, ohne nachrichtendienstliche Befugnisse aufzugeben. Die Neuregelung erfolgte, aufgrund der besonderen Einstellung gegenüber dem Nachrichtendienst und den Erfahrungen mit Terrorismus, vor dem Hintergrund einer domestisch wenig kontestierten Beschützer-Rolle.

### 5.2.3 Stabilisierung und Ausbau der Beschützer-Rolle: Der Investigatory Powers Act 2016

Der Investigatory Powers Act, der auch aufgrund der erweiterten Befugnisse bei der Strafverfolgung von KritikerInnen den Spitznamen »Snoopers' Charter« bekam, beinhaltete für den Bereich der Nachrichtendienste Kompetenzzuwächse sowie neue Kontrollarrangements. Im November 2015 legte die Regierung einen ersten Gesetzentwurf zum IPA vor. Dieser sorgte sowohl international als auch domestisch für erhebliche Kritik.

Edward Snowden sah in dem Entwurf das umfassendste und am wenigsten kontrollierte Überwachungsgesetz in der westlichen Welt (Snowden, 2015). Der konservative Abgeordnete David Davis bemängelte, dass der Debatte in Großbritannien die angemessene Kritik an den vorgeschlagenen Maßnahmen fehle. Er führte diesen Umstand auf eine fehlende historische Sensibilität zurück:

> »We have a wonderful illusion about our security services, a very comforting illusion. […] Because for the past 200 years we haven't had a Stasi or a Gestapo, we are intellectually lazy about it, so it's an uphill battle.« (The Guardian, 2015a)

Die beständige historische positive Bezugnahme auf das GCHQ wurde aber nur von wenigen PolitikerInnen kritisiert.

Der Gesetzentwurf wurde in der Folge von drei parlamentarischen Ausschüssen evaluiert und mit VertreterInnen der Zivilgesellschaft und Wirtschaft diskutiert. Aus Sicht der Regierung stand am Ende dieses Prozesses ein Entwurf, der

sicherstellte, dass die Sicherheitsbehörden über die notwendigen Kompetenzen verfügten, um die Sicherheit des Vereinigten Königreichs bestmöglich zu gewährleisten, ohne dabei andere Rechte über Gebühr zu beschränken (UK Government, 2016d, S. 2).

Nach diesem Konsultationsprozess wurde der überarbeitete Gesetzentwurf im März 2016 in zweiter Lesung im Unterhaus debattiert. Die Innenministerin betonte in dieser Sitzung, dass der Austausch mit den verschiedenen Interessengruppen zu einem neuen transparenten Gesetz geführt hätte, das sowohl die Sicherheit als auch die bürgerlichen Freiheiten in angemessener Weise miteinander verbinde. Insbesondere verwies Theresa May auf die Neuerungen zum Schutz besonders sensibler Berufsgruppen (bspw. von AnwältInnen und JournalistInnen) sowie auf das explizite Verbot, ausländische Nachrichtendienste um das Abfangen von Daten von Personen innerhalb des Vereinigten Königreichs zu bitten. Ferner wies die Innenministerin auf die neue Institution des Investigatory Powers Commissioners hin, die die Funktionen der Interception of Communications Commissioner, Intelligence Services Commissioner und Chief Surveillance Commissioner bündelte, sowie die neue Praxis zur Anordnung von Überwachungsmaßnahmen, wonach diese nur gemeinsam durch eine/n MinisterIn und eine/n Judicial Commissioner erlassen werden können (sog. double-lock) (House of Commons, 2016a, S. 812f.). Außerdem führte sie aus, dass das Gesetz erstmals die Wilson Doktrin expliziere und damit das Abhören von Mitgliedern des Parlaments nur nach Anordnung durch die/den PremierministerIn möglich sei (ebd., S. 819). Aus Sicht der Regierung bildete der Entwurf damit ein Vorbild für andere Staaten:

> »The Bill will provide world-leading legislation setting out in detail the powers available to the police and the security and intelligence services to gather and access communications and communications data. It will provide unparalleled openness and transparency about our investigatory powers, create the strongest safeguards, and establish a rigorous oversight regime.« (Ebd., S. 813)

Um Kritiken zuvorzukommen, verwies May aber auch darauf, dass aufgrund der Sunset-Clause im DRIPA 2014, schneller legislativer Handlungsbedarf bestünde, um den neuen Gefahren weiterhin begegnen zu können (ebd., S. 813).

Aus Sicht der Regierung erhielt das Gesetz damit das Gleichgewicht zwischen den Rollen Garant liberaler Grundrechte und der Beschützer-Rolle. KritikerInnen sahen in dem Vorhaben einen übermäßigen Ausbau der Beschützer-Rolle.

Besondere Kontestation erfuhren die Pläne zur flächendeckenden Kommunikationsüberwachung (bulk Interception) bzw. zum flächendeckenden Eindringen in zahlreiche Computersysteme (bulk Equipment Interference) (ebd., S. 817). Letztere Maßnahme wurde mit dem IPA erstmals eingeführt und daher besonders kritisch beurteilt. Bulk Equipment Interference ist nicht an ein direktes Ziel gebunden, sondern kann auch mehrere Systeme betreffen. Sie ist aber explizit

darauf beschränkt gegen Ziele im Ausland eingesetzt zu werden, britische BügerInnen dürfen durch diese Maßnahme nicht in erster Linie (primarily) betroffen sein (Home Office, 2018a, S. 67).

Die Regierung hatte zu beiden Praktiken bereits im Entwurfsstadium Erklärungen abgegeben und deren Notwendigkeit betont. Zur bulk interception führte die Regierung aus, sie sei »a vital tool designed to obtain foreign-focused intelligence and identify individuals, groups and organisations overseas that pose a threat to the UK« (UK Government, 2015c, S. 1). Die Regierung wollte damit den Regelungen nach Section 8(4) RIPA eine neue Grundlage geben. Mit Blick auf bulk Equipment Interference argumentierte die Regierung, dass durch die technologische Entwicklung das Abhören von Kommunikation nur noch begrenzt nützlich sei, da die Daten aufgrund von Verschlüsselung nicht mehr auswertbar seien. Aus diesem Grund sei es notwendig den Nachrichtendiensten die Möglichkeit einzuräumen, notfalls auch viele Geräte zu infiltrieren (UK Government, 2015b, S. 1f.). Sie führte ferner aus, dass zwar aufgrund der paketvermittelten Kommunikation in einem globalen Netz, nicht immer genau zwischen in- und ausländischer Kommunikation unterschieden werden könne, dass in beiden Fällen aber inländische Kommunikation nur dann analysiert werden dürfe, wenn eine ergänzende Anordnung durch die/den zuständigen MinisterIn vorläge, die durch eine/n Judicial Commissioner überprüft wurde (UK Government, 2015b,c).

Beide Praktiken wurden bereits in einem offenen Brief vor der parlamentarischen Debatte durch JuristInnen als unverhältnismäßig abgelehnt (The Guardian, 2016). Auch Bürgerrechtsorganisationen kritisierten die Praktiken mit dem Hinweis, dass etwa durch die Zurückhaltung von Sicherheitslücken das Netz insgesamt für alle NutzerInnen unsicherer werde (Big Brother Watch, 2016). Die Regierung argumentierte dagegen, dass diese Maßnahmen unerlässlich seien. Bei fast allen Terrorismusermittlungen sowie bei zahlreichen Einsätzen der Streitkräfte seien derartige Praktiken erfolgreich genutzt worden (House of Commons, 2016a, S. 822f.). Die DUP kritisierte als einzige Oppositionspartei den Regierungsentwurf nicht substanziell. Sie verwies hierzu auf die Erfahrungen mit Terrorismus in Nordirland (ebd., S. 842).

Bei der Abstimmung über das Gesetz enthielten sich die Abgeordneten der Labour Party, da sie einerseits die Notwendigkeit anerkannten, ein neues Gesetz zu erlassen um nicht durch die Sunset-Clause eine Situation zu generieren, in der das Handeln der Sicherheitsbehörden eingeschränkt wäre. Andererseits sahen sie im Vorschlag der Regierung Defizite bei der Wahrung der bürgerlichen Freiheitsrechte. Die neuen Kontrollarrangements waren für viele Abgeordnete nur »kosmetischer« Natur und nicht mit substanziellen Verbesserungen verbunden (ebd., S. 825 bzw. 828f.). Ferner kritisierten sie die zu vage Zielbestimmung des ökonomischen Wohlergehens. Sie vermuteten darin eine verdeckte Überdehnung der Beschützer-Rolle: »This raises the issue of what extra activities the Government

want to cover under this banner that are not covered by national security« (House of Commons, 2016a, S. 831).[8] Aus Sicht der Rollentheorie war dies die Forderung, die Rollenreferenz zu klären. Da in der Vergangenheit Gewerkschaftsmitglieder unter ähnlichen Rechtfertigungen zu Unrecht abgehört worden waren (ebd., S. 831 bzw. 834). Die Abgeordneten sahen zwar ebenfalls die von der Regierung angeführten Gefahren wie Terrorismus und organisierte Kriminalität, dennoch bestanden Zweifel, ob die Fähigkeiten zu bulk interception bzw. bulk Equipment Interference tatsächlich in diesem Maße notwendig waren, da hiermit eine neue Qualität der Überwachung verbunden sei (ebd., S. 833). Ähnlich argumentierten auch Abgeordnete der SNP (ebd., S. 838-844).

International stieß der Plan der Regierung, flächendeckende Überwachung sowie systematisches Hacken auf eine gesetzliche Grundlage zu stellen, ebenfalls auf Widerstand. Der UN-Sonderberichterstatter Joseph Cannataci kritisierte den Gesetzentwurf und forderte die britische Regierung auf:

> »to take this golden opportunity to set a good example and step back from taking disproportionate measures that may have negative ramifications far beyond the shores of the United Kingdom. More specifically, the Special Rapporteur invites the Government to show greater commitment to protecting the fundamental right to privacy of its own citizens and those of others and also to desist from setting a bad example to other States by continuing to propose measures, especially bulk interception and bulk hacking« (United Nations, 2016b, S. 14)

Diese Kritik wurde von Bürgerrechtsorganisationen geteilt (Liberty, 2016a; Open Rights Group, 2016b) und auch im Parlament erörtert (House of Commons, 2016a, S. 826). Die parlamentarische Opposition warf der Regierung vor, mit dem Gesetz autokratischen Bestrebungen zur Kontrolle des Internets zu folgen und damit einen gefährlichen Präzedenzfall zu etablieren (ebd., S. 844). Ferner argumentierten KritikerInnen, dass die Regierung mit dem Gesetz, im Gegensatz zu den USA, die falschen Schlussfolgerungen aus den Snowden-Enthüllungen zöge und nicht eine Begrenzung der flächendeckenden Überwachung einleite, sondern das Gegenteil hiervon verfolge (ebd., S. 863).

Trotz der Kontestationen aus Zivilgesellschaft und den Reihen der parlamentarischen Opposition wurde der Gesetzesentwurf im März in zweiter Lesung durch das Unterhaus mit der Regierungsmehrheit verabschiedet (ebd., S. 904).

8 Die Regierung hatte schon mit dem DRIPA 2014 versucht, die Verbindung zwischen ökonomischem Wohlstand und nationaler Sicherheit zu definieren. Sie stellte damit klar, dass es um das ökonomische Wohlergehen nur dann gehe, wenn dieses mit der nationalen Sicherheit verbunden sei (The Stationery Office, 2014, Section 3). Diese Festlegung wurde von der Opposition aber als defizitär betrachtet.

Aufgrund der Bedenken zu den besonders sensiblen »Bulk Powers« und auf Drängen der parlamentarischen Opposition, folgte im anschließenden Konsultationsprozess aber eine erneute kritische Auseinandersetzung mit deren Implikationen. Das Joint Committee on Human Rights gelangte bei der Prüfung zu dem Ergebnis, dass deren Einsatz nicht grundsätzlich gegen Artikel 8 der Europäischen Menschenrechtskonvention verstoße, obwohl ein deutliches Spannungsverhältnis konstatiert wurde (House of Lords und House of Commons, 2016, S. 12). Die Ausschussmitglieder forderten daher von der Regierung, den operativen Nutzen der Maßnahmen nachzuweisen und sie daher durch den Independent Reviewer of Terrorism Legislation (David Anderson) eingehend prüfen zu lassen (ebd., S. 13).

Diese Evaluation wurde im Juni 2016 abgeschlossen. In seinem Bericht kam Anderson zu der Einschätzung, dass eine umfassende, strategische Überwachung von Internetkommunikation (bulk Interception) essenziell zur Gewährleistung der Sicherheit im Vereinigten Königreich sei. Die Maßnahmen hätten sich in unterschiedlichen Einsatzszenarien als überaus hilfreich herausgestellt, darunter die Bekämpfung von Terrorismus, die Abwehr von Cyberangriffen oder die Unterstützung der Streitkräfte. Hierbei sei gleichermaßen der Zugriff auf Meta- wie Inhaltsdaten wichtig. Mit anderen, weniger invasiven, Maßnahmen sei ein ähnliches Ergebnis nicht zu erreichen. Daher war die Praxis aus Sicht von Anderson auch nicht ersetzbar. Er gab aber zu bedenken, dass durch die zunehmende Verbreitung von Verschlüsselung diese Maßnahme potenziell an Wirksamkeit verlieren könnte (Anderson, 2016, S. 91).

Die Fähigkeit zum umfassenden Hacken von Systemen (bulk Equipment Interference) wurde daher von Anderson als eine potenzielle Weiterentwicklung der Überwachung am Übertragungsweg gesehen. Auch wenn es zum Zeitpunkt der Prüfung noch keine Anwendungsfälle zur Evaluation der operativen Nützlichkeit gab (ebd., S. 109). Aufgrund des potenziell besonders tiefen Eingriffs in die Privatsphäre mahnte er aber an:

> »[…] that bulk EI will require, to an even greater extent than the other powers subject to review, the most rigorous scrutiny not only by the Secretary of State but by the Judicial Commissioners who must approve its use and by the IPC which will have oversight of its consequences.« (Ebd., S. 110)

Damit stützte Anderson die Einschätzung der Regierung wonach die Fähigkeiten zur Gewährleistung der Sicherheit notwendig seien. VertreterInnen aus Zivilgesellschaft und Wirtschaft hatten diese Position wiederholt kritisiert.

Im parlamentarischen Prozess wurde die Beschützer-Rolle zwar kontestiert, nach einer Prüfung durch Anderson wurden die Maßnahmen, insbesondere die bulk Equipment Interference, aber als notwendig beurteilt. Gegen die Pläne zum staatlichen Hacken gab es allerdings aus der Netzgemeinde bereits seit 2015 Widerstände, sodass es hier zu noch anhaltenden Kontestationsprozessen kam.

2015 wurde von der Regierung erstmals öffentlich eingeräumt, dass die Nachrichtendienste zur Erfüllung ihrer Aufgaben auf das Hacken von IT-Systemen zurückgriffen. Im Februar 2015 veröffentlichte die Regierung unter dem Druck eines laufenden Prozesses vor dem IPT eine offizielle Richtlinie zu dieser Praxis (Home Office, 2015b). Dies führte zu einer Klage verschiedener Bürgerrechtsorganisationen zusammen mit britischen Wirtschaftsunternehmen. Die KlägerInnen sahen die Hacking-Praktiken nicht durch bestehende gesetzliche Regelungen gedeckt und als tiefgreifenden Eingriff in die Privatsphäre, der sensiblere Bereiche betreffe als die Überwachung von Kommunikationsverkehren (Investigatory Powers Tribunal, 2015d, S. 4f.). Ein Vertreter des britischen ISP GreenNet äußerte Bedenken über das Ausmaß der CNE-Aktivitäten des britischen Nachrichtendienstes, die im Zuge des Prozesses aufgedeckt worden waren:

> »We remain extremely concerned that Ed Snowden was right about GCHQ having the most intrusive capabilities of any security agency, and about exactly how widespread their computer network exploitation may be, and the risks to network security and the privacy, freedom and safety of internet users around the world.« (Privacy International, 2015a)

Das IPT wies die Klage im Februar 2016 aber zurück und erkannte in den CNE-Operationen der Nachrichtendienste kein rechtswidriges Verhalten, sondern beurteilte die Praxis als prinzipiell rechtmäßig (Investigatory Powers Tribunal, 2016).

Die KlägerInnen reichten in der Folge Klage vor dem Europäischen Gerichtshof für Menschenrechte und dem Supreme Court ein. Das Verfahren vor dem Europäischen Gerichtshof für Menschenrechte ist noch anhängig. Im September 2019 schlossen sich weitere Bürgerrechtsorganisationen der Klage an (Article 19, 2019). Nachdem Liberty mit Klagen vor dem High Court und dem Court of Appeal gescheitert war, reichte die Bürgerrechtsorganisation zusammen mit sieben ISPs Klage vor dem Supreme Court ein. Ziel dieser Klage war es, dafür zu sorgen, dass Urteile des IPT weiterer juristischer Prüfung offenstehen sollten. Eine richterliche Prüfung war gesetzlich nicht vorgesehen und die vorigen Klagen waren mit Verweis hierauf abgelehnt worden. Der neue IPA sah zwar im Gegensatz zu RIPA prinzipiell eine begrenzte Möglichkeit zur Berufung vor (Section 241). Diese trat am 1. Januar 2019 in Kraft (Home Office, 2018c), wurde aber von KritikerInnen bereits während der Konsultation des Gesetzes als unzureichend bewertet (House of Commons, 2016a, S. 881). Im Mai 2019 urteilte der Supreme Court zugunsten der KlägerInnen und unterwarf damit die Entscheidung des IPT weiterer gerichtlicher Prüfung. Ein Argument, das die RichterInnen zur Begründung der Entscheidung anführten, war, dass sich die Gesetzesinterpretation des IPT losgelöst von Rechtsprechung in anderen Gebieten entwickeln könnte: »Consistent application of the rule of law requires such an issue to be susceptible in appropriate cases to review by ordinary courts« (The Supreme Court, 2019, S. 58).

Privacy International und andere VertreterInnen der Zivilgesellschaft feierten dies als Sieg für den Schutz der Bürgerrechte, da die Entscheidungen des IPT damit nicht mehr unanfechtbar waren und auch die Entscheidung zur CNE wieder vor Gericht überprüft werden kann:

> »Privacy International's tenacity in pursuing this case has provided an important check on the argument that security concerns should be allowed to override the rule of law. Secretive national security tribunals are no exception. The Supreme Court was concerned that no tribunal, however eminent its judges, should be able to develop its own ›local law‹. Today's decision welcomes the IPT back from its legal island into the mainstream of British law.« (Privacy International, 2019)

Andere JuristInnen sahen in dem mit vier zu drei Stimmen gefällten Urteil aber einen Bruch der Parlamentssouveränität, das mit der ursprünglichen Regelung eine weitere richterliche Prüfung ausschließen wollte (ouster clause) (The Guardian, 2019b). Inwiefern eine substanzielle Herausforderung der Bulk Powers erfolgversprechend ist, bleibt zweifelhaft, da der High Court im Juli 2019 urteilte, die Kompetenzen stünden nicht im Widerspruch zum Human Rights Act 1998 und eine Klage von Liberty damit ablehnten (High Court of Justice, 2019). Liberty kündigte aber an, trotz des Urteils weitere Klagen gegen das nachrichtendienstliche Hacking voranzutreiben (Liberty, 2019).

Während dieser laufenden Kontestationsprozesse hatte die Regierung die Praxis der bulk Equipment Interference aber zunehmend ausgebaut. Im November 2018 veröffentlichte das GCHQ zusammen mit dem 2016 gegründeten National Cyber Security Centre (NCSC) den sogenannten Equities Process, mit dem darüber entschieden wird, ob eine Sicherheitslücke für das Hacken von IT-Systemen zurückgehalten oder zum Schließen der Schwachstelle veröffentlicht wird.[9] In der Pressemitteilung wird die grundsätzliche Problematik des Umgangs mit ausnutzbaren Softwareschwachstellen thematisiert: »[…] we do not disclose every vulnerability we find. In some cases, we judge that the UK's national security interests are better served by ›retaining‹ knowledge of a vulnerability« (GCHQ, 2018b).

Bei diesem Prozess stünden stets zwei Ziele im Widerspruch, die sorgsam gegeneinander abgewogen werden müssten. Einerseits könne durch die Veröffentlichung der Information die Schwachstelle für alle NutzerInnen geschlossen und damit die Sicherheit des Netzes insgesamt erhöht werden. Andererseits könne eine Sicherheitslücke aber auch genutzt werden, um nachrichtendienstlich Informationen über Gefahren zu sammeln oder Aktivitäten potenziell feindseliger

9 Das National Cyber Security Centre ist Teil des GCHQ, soll aber öffentlich sichtbarer für die Cybersicherheit im Vereinigten Königreich sorgen.

Akteure (Terrorgruppen, Staaten oder Krimineller) zu vereiteln. Die Standardentscheidung sei dabei stets, Informationen zu veröffentlichen. Die Entscheidung über den Umgang mit einer Lücke treffen VertreterInnen der Nachrichtendienste und des NCSC. In besonders sensiblen Fällen werden die/der DirektorIn des GCHQ und die/der AußenministerIn in die Beurteilung einbezogen. Bei der Entscheidungsfindung wird unter anderem beurteilt, gegen welche Ziele die Schwachstelle eingesetzt werden kann und welche Informationen durch sie erlangt werden können. In die Gleichung fließt aber auch die Risikoeinschätzung ein, welche Ziele im Vereinigten Königreich durch diese Schwachstelle angreifbar wären (bspw. kritische Infrastrukturen) und wie hoch die Wahrscheinlichkeit ist, dass die Lücke durch andere gefunden und ausgenutzt wird (GCHQ, 2018d). Der mit dem IPA etablierte Investigatory Powers Commissioner kontrolliert diese Abwägung. Der neue Prozess sollte diese Entscheidungsfindung transparent und die angelegten Maßstäbe nachvollziehbar machen (GCHQ, 2018b).

Im Dezember 2018 unterrichtete die Regierung das ISC und den Investigatory Powers Commissioner, dass die bulk Equipment Interference deutlich häufiger eingesetzt werden würden als antizipiert. Zunächst war die Regierung davon ausgegangen, dass auf das systematische Hacken nur selten zurückgegriffen werden müsse. Diese Einschätzung hatte sich aber seit der Verabschiedung des IPA verändert. Diese Anpassung wurde mit technischen Veränderungen (Verschlüsselung) begründet, die dazu führten, dass andere Maßnahmen weniger effektiv geworden waren (Home Office, 2018b).

Die Beschützer-Rolle ist mit Blick auf die bulk Equipment Interference domestisch nach wie vor kontestiert und steht auch international in der Kritik. Insbesondere mit der bulk Equipment Interference konnte die britische Regierung die Beschützer-Rolle im Bereich der Nachrichtendienste ausbauen. Diese Erweiterung hat einen anhaltenden Kontestationsprozess ausgelöst, es ist aber unwahrscheinlich, dass diese Kontestationen domestisch folgenreich sein werden. Dies liegt daran, dass die Maßnahme nach der Prüfung durch David Anderson auch von großen Teilen des Parlaments akzeptiert wird und dass die britischen Gerichte bereits die Einschätzung vertreten haben, die Praxis sei grundsätzlich zulässig.

## 5.3 Zwischenfazit

Im Lichte der durch die Snowden-Enthüllungen entstandenen Öffentlichkeit, mussten die Regierungen beider Untersuchungsstaaten ihre Beschützer-Rollen evaluieren. Die Veröffentlichungen wurden in beiden Staaten allerdings unterschiedlich aufgenommen. Während die britische Regierung die Publikation der Dokumente verurteilte und offensiv gegen den Guardian vorging, um weitere

Publikationen zu unterbinden und so die eigene Beschützer-Rolle zu wahren, versuchte sich die Bundesregierung ihrer eigenen Rolle durch die Prüfung der Vorwürfe rückzuversichern. Beide Staaten erließen aufgrund des domestischen Drucks neue Regelungen für ihre Dienste. Bemerkenswert ist, dass in beiden Fällen eine substanzielle Beschränkung der Rollen ausgeblieben ist. In Deutschland erlaubte die Bundesregierung dem BND viele der enthüllten Praktiken. In Großbritannien erweiterte die Exekutive die Rolle mit der bulk Equipment Interference sogar. Ermöglicht wurde dies durch die Referenz (Schutz vor wem?) auf (internationalen) Terrorismus sowie in Großbritannien die Aktivitäten feindseliger Staaten.

Die britische Regierung konnte bei der Stabilisierung und dem Ausbau ihrer Beschützer-Rolle domestisch auf ein weithin geteiltes positives Selbst des GCHQ zählen. Die historischen Leistungen des Dienstes, insbesondere während des Zweiten Weltkriegs, und eine weitgehend geteilte Gefahreneinschätzung erleichterten es der Regierung, substanzielle Kontestationen zu vermeiden bzw. zu kontern. Das IPT und unabhängige Untersuchungen kritisierten zwar den intransparenten gesetzlichen Rahmen und forderten eine Reform. Die Praktiken der Überwachung selbst wurden allerdings kaum herausgefordert. Die Regierung konnte die enthüllten Praktiken so offensiver verteidigen und letztlich ausbauen, auch weil die Enthüllungen aus Sicht der Regierung und zahlreicher Abgeordneter nur die »normale« Praxis nachrichtendienstlicher Tätigkeiten dokumentiert hatten. Die Referenz der Beschützer-Rolle, die Prävention terroristischer Aktivitäten, rechtfertigte auch Maßnahmen gegen Unternehmen in verbündeten Staaten. Ferner erleichterte auch die Rolle als Wohlstandsmaximierer den Ausbau der Beschützer-Rolle, da die Nachrichtendienste explizit mit der Sicherung der ökonomischen Leistungsfähigkeit betraut sind. International stand die britische Regierung für die enthüllten Überwachungsmaßnahmen zwar in der Kritik, die Herausforderungen durch den internationalen Terrorismus und die Kooperation mit der NSA erleichterten aber auch in diesem Kontext die Übernahme einer expansiven Rolle. Für die Regierung war es dabei wichtig, dass das GCHQ international als besonders kompetenter Kooperationspartner mit großer technischer Expertise wahrgenommen wurde und dass das GCHQ auf Augenhöhe mit der NSA agieren konnte. Die besondere Beziehung zu den USA stabilisierte so die auch innenpolitisch nicht substanziell kontestierte Beschützer-Rolle. Hier zeigen sich damit ebenfalls Wirkungen eines »second image reversed«.

Die Rolle als Garant liberaler Grundrechte sorgte bei der gesetzlichen Neuregelung allerdings dafür, dass Kontrollmechanismen gestärkt und Praktiken transparenter gemacht wurden. Die richterliche Prüfung von Überwachungsanordnungen sowie die Einrichtung des IPC verbesserte die Aufsicht über die nachrichtendienstlichen Aktivitäten, der Vulnerabilities Equities Process stellte öffentlich die Kriterien vor, die die Sicherheitsbehörden bei der Zurückhaltung von Sicher-

heitslücken berücksichtigen müssen. Auch mit Blick auf die Kontestationen zeigen sich Rückwirkungen des internationalen auf das domestische Rollenspiel, da viele Klagen von internationalen Bürgerrechtsorganisationen getragen wurden.

Die deutsche Regierung wurde zunächst im internationalen Rollenspiel bei der Aufklärung der Enthüllungen durch die Reaktionen der amerikanischen und britischen Regierungen frustriert. Beide Partner wollten die eigenen Beschützer-Rollen nicht beschränken. Dies führte dazu, dass die Bundesregierung international Prozesse der Normgenese unterstützte und versuchte, die physischen Zugriffe auf die Internetinfrastruktur zu erschweren. Innenpolitisch spiegelte sich dieses Verhalten in der Kündigung von Verträgen mit amerikanischen Unternehmen. Ferner richtete die Regierung die eigene Beschützer-Rolle (Spionageabwehr) auch auf Tätigkeiten verbündeter Staaten aus. Eine offene Konfrontation mit den Verbündeten vermied die Bundesregierung aber.

Die domestische Aufarbeitung der Enthüllungen offenbarte, dass die Praktiken des BND aus Sicht vieler Abgeordneter nicht unproblematisch waren. In der parlamentarischen Aufarbeitung zeigte sich, dass der BND Mittel nutzte, die die Bundesregierung gegenüber den USA und Großbritannien kritisiert hatte. In der Folge wurde die Beschützer-Rolle in der Referenz (Schutz vor wem?) begrenzt und ein zusätzliches Schutzniveau für BürgerInnen und Staaten der Europäischen Union etabliert. Die Rolle als Wohlstandsmaximierer sorgte in Deutschland ferner dafür, dass Wirtschaftsspionage explizit verboten wurde. Die Bundesregierung hoffte, damit zu einer internationalen Norm beizutragen. Maßnahmen wie die strategische Fernmeldeaufklärung wurden allerdings weitgehend anhand der enthüllten Praktiken kodifiziert und die Beschützer-Rolle bspw. durch die Kabelerfassung in Deutschland ausgebaut. Dies wurde durch Verweise auf die sicherheitspolitischen Herausforderungen, insbesondere den Terrorismus, gerechtfertigt. Zur Rechtfertigung betonte die Regierung ferner die Bedeutung der Kooperation mit den USA für die Sicherheit in Deutschland. Diese Abhängigkeit und enge Verwobenheit der eigenen Beschützer-Rolle trat in der parlamentarischen Untersuchung deutlich zu Tage und sorgte mit dafür, dass die Beschützer-Rolle nicht beschränkt wurde.

Die Rolle als Garant liberaler Grundrechte sorgte auch in Deutschland für neue Kontrollmechanismen. So etablierte die Bundesregierung mit dem Unabhängigen Gremium ein neues Aufsichtsorgan.

Die wesentlichen Einflüsse, die die Entwicklung der Cybersicherheitspolitiken geprägt haben, sind in den Tabellen 5 und 6 schematisch dargestellt.

*Tabelle 5: Schematische Darstellung der Einflüsse auf die Politikentwicklung im Bereich der Nachrichtendienste in der Bundesrepublik Deutschland: Wirkung auf die Beschützer-Rolle, – = kontestierend, + = katalytisch. Quelle: Eigene Darstellung*

| | **domestische Ebene** | | | | **internationale Ebene** | |
|---|---|---|---|---|---|---|
| | Historisches Selbst | Wirkung | Rollenbezüge | Wirkung | signifikante / organisierte Andere | Wirkung |
| Die Snowden Enthüllungen (Juni - Dezember 2013) | | | Garant liberaler Grundrechte | – | USA / UK / UN | |
| Bundesregierung unter Druck (Januar 2014 - Dezember 2015) | | | Garant liberaler Grundrechte | – | USA | – |
| Etablierung einer neuen Beschützer-Rolle (Januar 2016 - 2019) | | | Garant liberaler Grundrechte | – | USA / EU | + |

*Tabelle 6: Schematische Darstellung der Einflüsse auf die Politikentwicklung im Bereich der Nachrichtendienste im Vereinigten Königreich: Wirkung auf die Beschützer-Rolle, – = kontestierend, + = katalytisch. Quelle: Eigene Darstellung*

| | **domestische Ebene** | | | | **internationale Ebene** | |
|---|---|---|---|---|---|---|
| | Historisches Selbst | Wirkung | Rollenbezüge | Wirkung | signifikante / organisierte Andere | Wirkung |
| Die Snowden Enthüllungen (Juni - März 2014) | GCHQ, Opfer von Terrorismus | + | Wohlstandsmaximierer | + | USA / 5-Eyes | + |
| Regierung unter Druck (April 2014 - Dezember 2015) | GCHQ, Opfer von Terrorismus | + | Wohlstandsmaximierer | + | USA / 5-Eyes | + |
| Etablierung einer neuen Beschützer-Rolle (Januar 2016 - 2019) | GCHQ, Opfer von Terrorismus | + | Wohlstandsmaximierer | + | USA / 5-Eyes | + |

# 6. Krieg im Cyberspace? Die militärische Nutzung des Netzes

Eine wachsende Zahl von Staaten hat damit begonnen, den Cyberspace auch als militärische Domäne zu erschließen und damit ihre Sicherheitspolitiken zu komplementieren (Lewis und Neuneck, 2013). Spätestens seit den Cyberangriffen auf Estland im Jahr 2007 wird immer wieder über die Möglichkeit eines Cyberwars debattiert. Dem Cyberspace wird dabei immer wieder eine Begünstigung konventionell unterlegener Akteure zugesprochen. Außerdem sei das Netz ein Ort in dem die Offensive der Defensive stets überlegen sei. Aufgrund des Attributionsproblems sei es ferner kaum verlässlich möglich, AngreiferInnen zu identifizieren. Durch diese strategischen Eigenschaften ist der Cyberspace ein sicherheitspolitischer Handlungsraum, der die internationalen Beziehungen und den Konfliktaustrag potenziell verändert. Wie die beiden Untersuchungsstaaten mit den militärischen Herausforderungen des Netzes umgegangen sind, wird im Folgenden näher untersucht.

Im folgenden Kapitel wird nachvollzogen, inwiefern die beiden Untersuchungsstaaten begonnen haben, offensive Fähigkeiten aufzubauen und durch welche Einflüsse dies ermöglicht wurde. Ferner wird in diesem Zusammenhang analysiert, welche (völker)rechtlichen Positionen die Staaten mit Blick auf den Einsatz von militärischen Cyberkapazitäten entwickelt haben.

## 6.1 Deutschland

### 6.1.1 Der Aufbau militärischer Kapazitäten: Defensive Ausrichtung und Schutz der eigenen Systeme

Verstärkte Aufmerksamkeit erfuhr die IT-Sicherheit der Streitkräfte, als Ende der 1990er Jahre die Sicherheit kritischer Infrastrukturen eingehender debattiert wurde. Die potenziellen Folgen der Beeinträchtigung von militärischer Infrastruktur durch Cyberangriffe wurde in diesem Kontext auch von einer Enquete-

Kommission des Bundestags problematisiert und die Komplexität der Gefahrenlage diskutiert:

> »Bedrohungen können von kriminellen Einzeltätern, von Terroristen, von kriminellen Organisationen oder auch von feindlichen Staaten ausgehen. Insofern wird die Unterscheidung zwischen ziviler und militärischer Bedrohung sowie zwischen innerer und äußerer Sicherheit immer verschwommener.« (Deutscher Bundestag, 1998b, S. 84)

In einer Auseinandersetzung im Cyberspace sei daher immer weniger zwischen Krieg und Frieden zu unterscheiden. Angriffe könnten das gezielte Handeln der gegnerischen Partei massiv einschränken, ohne die Schwelle eines bewaffneten Angriffs zu erreichen. Zu derartigen Angriffen könnten, so die Einschätzung der Kommission, auch weniger ressourcenstarke Akteure in der Lage sein, so dass asymmetrische Konfliktlagen entstünden. Um der neuen Verwundbarkeit vernetzter Gesellschaften und der Streitkräfte zu begegnen, solle auf Defensivmaßnahmen gesetzt werden, da etablierte Konzepte wie Abschreckung nur sehr begrenzt anwendbar seien (ebd., S. 84).

Die Bundeswehr setzte, wie viele andere Streitkräfte, auf das militärische Potenzial von IT, um in Gefechtssituationen informationelle Vorteile zu erlangen bzw. diese ausnutzen zu können. So wurde auch in der Bundeswehr unter der Bezeichnung vernetzte Operationsführung ein Konzept der network centric warfare entworfen (heise.de, 2006). Im Weißbuch von 2006 wurde die militärische Bedeutung des Cyberspace in einem zentralen militärischen Strategiedokument erwähnt. Hier betonte die Bundesregierung ebenfalls, dass Cyberangriffen vorrangig mit zivilen Mitteln begegnet werden müsse (Bundesministerium der Verteidigung, 2006, S. 19). Die militärische Beschützer-Rolle war damit zunächst defensiv angelegt und auf den Schutz der bundeswehreigenen Infrastrukturen bzw. (Waffen-)Systeme gerichtet.

In der Folge wurde aber auch die Möglichkeit erprobt, den Cyberspace zur Durchführung offensiver militärischer Operationen zu nutzen. Ersten institutionellen Ausdruck fanden die Bestrebungen zur offensiven militärischen Nutzung des neuen Handlungsraums im Jahr 2007 als im Kommando Strategische Aufklärung eine Einheit zur Durchführung von Computer Network Operations (CNO) gegründet wurde. Auftrag dieser neuen Einheit war und ist es, in gegnerischen Netzwerken zu wirken und ggf. konventionelle militärische Maßnahmen zu begleiten. Ein eigenständiges, losgelöstes Wirken im Sinne eines »Cyberwar« wurde durch das Verteidigungsministerium aber als unwahrscheinlich eingeschätzt (Deutscher Bundestag, 2014c, S. 1165). Damit legte die Bundesregierung den Grundstein zum Aufbau einer offensiven militärischen Beschützer-Rolle.

Die Bundesregierung sah in einem durch militärische Feindseligkeit geprägten Cyberspace aber auch ein erhebliches Risiko und plädierte dafür, internationa-

le Regeln zur Selbstbeschränkung zu fördern, um eine »Kultur der Zurückhaltung zu schaffen« (Deutscher Bundestag, 2010a, S. 5). Zu dieser Kultur der Zurückhaltung gehörte aus Sicht der Bundesregierung die Präzisierung völkerrechtlicher Vorgaben sowie die freiwillige Selbstbeschränkung der Staatengemeinschaft (ebd., S. 5). Die Bundesregierung unterstrich die eigene Zurückhaltung bspw. dadurch, dass die Bundeswehr keine Schadsoftware entwickeln sollte bzw. dass die Streitkräfte keine Cyberangriffe gegen Ziele im Ausland durchführten (ebd., S. 5). Diese Position stand in offensichtlichem Widerspruch zur Etablierung eigener CNO-Kräfte, die zur Infiltration gegnerischer Netze auf den Einsatz von Schadsoftware angewiesen sind.

Entsprechend den Einschätzungen im Weißbuch 2006, wurde in der ersten Cybersicherheitsstrategie der Bundesregierung 2011 deren zivile Ausrichtung betont:

> »Zivile Ansätze und Maßnahmen stehen bei der Cyber-Sicherheitsstrategie im Vordergrund. Sie werden ergänzt durch die Maßnahmen der Bundeswehr zum Schutz ihrer eigenen Handlungsfähigkeit und im Rahmen zugrunde liegender Mandate, um auf diese Weise Cyber-Sicherheit als Teil gesamtstaatlicher Sicherheitsvorsorge zu verankern.« (Bundesministerium des Innern, 2011, S. 5)

Dem Gedanken staatlicher Selbstbeschränkung folgend, wurde das Aufgabengebiet der Bundeswehr defensiv beschrieben. Im Fokus stand der Schutz der eigenen militärischen Netze. Diese Ausrichtung ist auch aus der Haltung der Bundesregierung ableitbar, dass die in der Strategie skizzierten Maßnahmen keine parlamentarische Mandatierung erforderten (Deutscher Bundestag, 2011a, S. 4). Dennoch wurde auch hier darauf hingewiesen, dass vernetzte Gesellschaften erheblichen Risiken aus dem Cyberspace ausgesetzt seien. Die neue Verwundbarkeit wurde wiederum insbesondere mit Bezug zu kritischer Infrastruktur hergestellt. Als Beispiel für eine solche Attacke wurde unter anderem auf den Wurm Stuxnet verwiesen, der in Iran Zentrifugen zur Urananreicherung manipuliert hatte (Bundesministerium des Innern, 2011, S. 3).[1]

Die Beschützer-Rolle blieb somit zwar defensiv ausgerichtet, allerdings rückte mit der kritischen Infrastruktur und dem Szenario eines potenziell folgenreichen Cyberangriffs ein neues Referenzobjekt sowie die Frage der Landesverteidigung in den Blick.

In den Verteidigungspolitischen Richtlinien 2011 wurde die militärische Gefahr, die von Cyberangriffen ausging, dann auch zentraler aufgegriffen. Hier heißt es:

---

1 Für weitere Informationen zu Stuxnet s. bspw. Zetter (2014).

> »Informationsinfrastrukturen gehören heute zu den kritischen Infrastrukturen, ohne die das private und öffentliche Leben zum Stillstand käme. Angriffe darauf können aufgrund ihrer engen Verflechtung zur Destabilisierung auch unseres Staates mit gravierenden Auswirkungen für die nationale Sicherheit führen. Mit der Bedrohung aus dem Informationsraum werden Staaten ihre bisherigen Vorstellungen über Konflikte und ihre Lösungsmöglichkeiten anpassen.« (Bundesministerium der Verteidigung, 2011, S. 9)

Insbesondere die Möglichkeit, die Urheberschaft von Angriffen ex post abstreiten zu können, wurde von der Regierung in diesem Kontext problematisiert, so entstünden potenziell asymmetrische Konfliktlagen, die es ohne diese neue Vulnerabilität nicht geben würde. Unter Bezugnahme auf Artikel 51 der UN-Charta, hat die Bundesregierung aber bereits 2011 die Einschätzung vertreten, dass auch ein Cyberangriff, der in seinen Folgen einem konventionellen Angriff vergleichbar ist, als bewaffneter Angriff bewertet werden und folglich das Recht zur Selbstverteidigung auslösen könne (Deutscher Bundestag, 2011a, S. 4).

Auf internationaler Ebene versuchte die Bundesregierung weiterhin, ein militärisches Wettrüsten zu vermeiden und auf staatliche Zurückhaltung hinzuwirken. Die Abschlusserklärung beim NATO-Gipfel in Lissabon, in der die Bedrohung durch Cyberangriffe prominent erwähnt wurde und in der von allen Mitgliedsstaaten mehr Engagement gefordert wurde, wurde von der Regierung und dem Bundestag debattiert (Bundesministerium der Verteidigung, 2011, S. 9 bzw. 17). Dass eine Cyberattacke automatisch unter Artikel 5 des Nordatlantik-Vertrags fallen könne, wurde in einer öffentlichen Anhörung des Auswärtigen Ausschusses kritisch beurteilt. Die Abgeordneten bevorzugten die Konsultation eines solchen Vorfalls unter Artikel 4 (Deutscher Bundestag, 2011c, S. 14-16). Diese Auffassung wurde gleichsam von der Bundesregierung und der Opposition in einer Debatte des neuen strategischen Konzepts der NATO im Bundestag zum Ausdruck gebracht (Deutscher Bundestag, 2010b, S. 7600, 7608 bzw. 7610). Auf internationaler Ebene setzte sich die Bundesregierung daher erfolgreich dafür ein, Cyberangriffe innerhalb der NATO nicht automatisch nach Artikel 5 zu behandeln. Ziel dieses Vorstoßes war es, einen dezidiert zivilen Ansatz beim Umgang mit diesen neuen Gefahren zu entwickeln (Deutscher Bundestag, 2010c, S. 8097).[2]

Im Rahmen der Vereinten Nationen plädierte die Bundesregierung wiederholt für die Etablierung internationaler Normen zum Umgang mit Cyberangriffen. Der Fokus lag hierbei einerseits auf Verbesserungen bei der Attribtution

2 Die Debatte um die Anwendbarkeit von Artikel 5 war nach den Angriffen auf Estland im April und Mai 2007 verstärkt geführt worden (The Guardian, 2007). 2014 legte die NATO fest, dass ein Cyberangriff potenziell Artikel 5 auslösen könne. Ein Automatismus wurde allerdings nicht etabliert ebenso wenig definierte die Allianz eine Schwelle für einen solchen Angriff (Reuters, 2016).

von Angriffen, die durch internationale Kooperation verlässlicher werden sollte, sowie auf der Sorgfaltsverantwortung der Staaten für den Cyberspace. Staaten sollten Angriffe unterbinden, die von ihrem Territorium ausgingen (United Nations, 2011, S. 10). Die Regierung wies in diesem Kontext darauf hin, dass Staaten dem Völkergewohnheitsrechts entsprechend Verantwortung trügen »for internationally wrongful cyber activity attributable to them, including the internationally wrongful activity in cyberspace of any State-backed proxies acting on the State's instructions or under its direction or control […]« (United Nations, 2013a, S. 9). Regierungen müssten daher darauf hinwirken, dass ihr Territorium nicht für Cyberangriffe genutzt werde (ebd., S. 9).

Auch wenn die Bundesregierung international versuchte, eine Kultur der Zurückhaltung zu fördern, wurden die eigenen Kapazitäten nach 2010 immer weiter ausgebaut und auch institutionell verankert. Weiterhin hat die Bundesregierung ihre Haltung zur militärischen Nutzung des neuen Handlungsraumes entwickelt. Bereits mit der Schaffung der CNO-Kräfte vertrat die Regierung die Auffassung, dass der Aufbau und Einsatz von Schadsoftware durch die Bundeswehr kein grundsätzliches rechtliches Problem darstelle. Eine Einschätzung die innerstaatlich später auch durch ein Gutachten des Wissenschaftlichen Dienstes des Bundestages prinzipiell bestätigt wurde (Deutscher Bundestag, 2015h). Eine erste theoretische Einsatzfähigkeit erreichten diese Kräfte 2012 (Augen Geradeaus!, 2012). Der Verteidigungsausschuss des Bundestages wurde von der Regierung über diese neuen Fähigkeiten 2012 bzw. 2013 informiert (Deutscher Bundestag, 2014c, S. 1165). Damit war auch ein relevanter Gegenrollenträger offiziell in die Entwicklung offensiver Fähigkeiten der militärischen Beschützer-Rolle eingebunden.

### 6.1.2 (Schonende) Offensive und aktive Verteidigung

Im Jahr 2015 wurde in Deutschland immer häufiger auch über offensive militärische Maßnahmen im Cyberspace debattiert. Auslöser hierfür war unter anderem die Einschätzung der Bundesregierung, dass Cyberangriffe immer häufiger durchgeführt würden und dass sie hierbei einen Qualitätssprung vollzogen hätten (Deutscher Bundestag, 2015d, S. 3). Diese Einschätzung fand auch in einem gewachsenen und immer deutlicher formulierten militärischen Schutzanspruch Ausdruck. Während der Aufgabenbereich der Bundeswehr in der ersten Cybersicherheitsstrategie noch zurückhaltend formuliert wurde und auf den Schutz der eigenen militärischen Infrastruktur bezogen blieb, zeigte sich in der Folgezeit deutlicher, dass die Bundeswehr den Cyberspace als weiteren militärischen Handlungsraum konzipiert hatte. Auch in diesem Raum sollte die Bundeswehr ihren verfassungsmäßigen Aufgaben nachkommen:

> »Die Verteidigung gegen Cyber-Angriffe, die einen bewaffneten Angriff auf Deutschland darstellen bzw. einen solchen vorbereiten oder begleiten können. Die Ausübung von Cyberfähigkeiten im Rahmen von Auslandseinsätzen nach Artikel 24 Absatz 2 des Grundgesetzes.« (Deutscher Bundestag, 2015d, S. 3)

Damit fand die Beschützer-Rolle erstmals konkrete offensive Bezüge. Im Falle eines bewaffneten Angriffs nach Artikel 51 der UN-Charta sollte die Bundeswehr die Landesverteidigung übernehmen. Außerdem sollten Cybermaßnahmen mandatierte Auslandseinsätze komplementieren.

Die Strukturen bei der Bundeswehr waren aus Sicht der Regierung diesen Herausforderungen nicht mehr gewachsen und mussten daher reformiert werden. Die Exekutive betonte hierbei aber, dass der Einsatz der Streitkräfte den gleichen Erfordernissen unterliege wie eine konventionelle Dislozierung. Die CNOs sollten aus Sicht der Regierung einerseits die eigenen Kräfte schützen sowie deren Wirken unterstützen (ebd., S. 3f.).

KritikerInnen aus der Netzgemeinde sahen in der zunehmend offensiven Ausrichtung der Bundeswehr ein Problem für das Netz allgemein, da Cyberangriffe wie »Streubomben« wirken könnten, die viele, auch unbeabsichtigte, Ziele treffen könnten. Diese Analogie wurde von der Bundesregierung aber als unangemessen zurückgewiesen, da die kinetischen Folgen deutlich unterschiedlich seien. Außerdem seien die Angriffe genau auf Zielsysteme zuschneidbar. Dies sei besonders wichtig, da die Bundeswehr durch das Völkerrecht verpflichtet ist, Kollateralschäden zu minimieren (ebd., S. 5).

Während KritikerInnen potenziell unbeherrschbare Folgen der Beschützer-Rolle bspw. durch das Überspringen von Malware auf Systeme jenseits des eigentlichen Ziels fürchteten, wurde der Cyberspace von der Regierung als besonders »schonende« Domäne für den militärischen Einsatz bewertet.

In der Folge gestand die Bundesregierung auch ein, dass die CNO-Kräfte zum Wirken in fremden Netzen auf Schwachstellen zurückgreifen müssten und daher Schadsoftware bzw. Exploits benötigten (Deutscher Bundestag, 2015b). Die Regierung argumentiert zwar, dass im Sinne eines Vulnerabilities Equities Process Sicherheitslücken, »deren Nutzung weitreichende Auswirkungen auf die Sicherheit der Bevölkerung bzw. des Staates haben, gemeldet werden sollen«, schränkte aber ein, dass dabei die zur Aufrechterhaltung der Schutzfunktion notwendigen Kapazitäten nicht negativ beeinträchtigt werden dürften (Deutscher Bundestag, 2018c, S. 10). Ob bzw. inwiefern die Bundeswehr beim Aufspüren und der Nutzbarmachung von Schwachstellen (Zero-Day-Exploits) mit privatwirtschaftlichen Unternehmen kooperiert bzw. diese Lücken dort bezieht, beantwortet die Regierung nicht öffentlich (ebd., S. 10).

In diesem Bereich wird die Ablehnung einer Beschützer-Rolle für das gesamte Internet besonders deutlich. Die Auswirkungen einer Sicherheitslücke werden mit Blick auf die nationalen Gegebenheiten evaluiert. Ein Schutz der globalen Infrastruktur, wie er zur Kontestation der Beschützer-Rollen in fast allen Bereichen von der Netzgemeinde gefordert wird, findet bei der Regierung keine Unterstützung.

Die Bundesregierung nutzte die neuen Kapazitäten der Beschützer-Rolle bereits im Herbst 2015. 2016 berichteten Medien darüber, dass die Bundeswehr 2015 den ersten Einsatz ihrer CNO-Kräfte durchgeführt habe. Im Rahmen der Befreiung einer in Afghanistan entführten Entwicklungshelferin, hatten sich die Streitkräfte, nach Anfrage aus dem Krisenstab des Auswärtigen Amts, in das Netz eines afghanischen Telekommunikationsdienstleisters gehackt und die Bewegungen der EntführerInnen mittels Handydaten verfolgt. Offiziell bestätigt wurde diese Operation allerdings nicht (Spiegel, 2016).

Bei einem Blick auf die Einsatzdoktrin der CNO-Kräfte der Bundeswehr wird ferner ein Trend deutlich, der, sofern er von allen Staaten geteilt wird, das Ziel einer internationalen Kultur der Zurückhaltung deutlich schwieriger erreichbar macht. Während das Völkerrecht für den Einsatz staatlicher Streitkräfte die sichtbare Unterscheidung zwischen Kombattanten und Nicht-Kombattanten vorsieht, betont die Bundesregierung, dass das völkerrechtliche Unterscheidungsgebot »bei der Nutzung technischer Einrichtungen und Aktivitäten im Cyber-Raum nicht [verlange, Anm. d. Verf.], die Zurechenbarkeit zu einem bestimmten Staat offenzulegen« (Deutscher Bundestag, 2015d, S. 11). Die SoldatInnen, die CNOs durchführen, tragen daher Uniformen mit Hoheitsabzeichen und sind damit als Kombattanten im Sinne des Völkerrechts erkennbar (Deutscher Bundestag, 2015a, S. 5), die technischen Infrastrukturen, über die ein Angriff erfolgt, attribuieren den Angriff aber nicht eindeutig. Die Nutzung falscher Identitäten, um den Verdacht bspw. auf andere Akteure zu lenken, ist aus Sicht der Bundesregierung aber untersagt (Deutscher Bundestag, 2015b, S. 2). Der Aufbau einer verifizierbaren Kultur der Zurückhaltung im Cyberspace ist dadurch dennoch erschwert. Insgesamt zeigt die Bundesregierung auch kein Interesse daran, offensive Fähigkeiten mit anderen Staaten zu teilen. Die Beurteilung von Cyberangriffen soll ebenfalls, auch innerhalb der EU, den Nationalstaaten überlassen bleiben (Deutscher Bundestag, 2018a).

Im Kontext der Debatte um den Aufbau offensiver Kapazitäten definierte die Bundesregierung weiterhin gegen welche Ziele die neuen Mittel eingesetzt werden dürften. Hierbei orientierte sie sich an etablierten völkerrechtlichen Normen. Ziele von militärischen Cyberangriffen können aus Sicht der Bundesregierung nur Objekte sein,

> »[…] die aufgrund ihrer Beschaffenheit, ihres Standorts, ihrer Zweckbestimmung oder ihrer Verwendung wirksam zu militärischen Handlungen beitragen und deren gänzliche oder teilweise Zerstörung, deren Inbesitznahme oder Neutralisierung unter den im betreffenden Zeitpunkt des Angriffs gegebenen Umständen einen eindeutigen militärischen Vorteil darstellen.« (Deutscher Bundestag, 2015a, S. 2)

Dies könne aber auch »nicht als militärisch klassifizierte Gegner« einschließen, sofern rechtlich zulässig mit militärischen Mitteln gegen diese vorgegangen werden dürfe (Deutscher Bundestag, 2015d, S. 6).

Die parlamentarische Opposition verlangte Auskunft darüber, ob aus Sicht der Bundesregierung offensive Cybermaßnahmen ein konstitutives Mandat des Bundestages benötigten. Die Regierung stellte in der Folge klar, dass für offensive Einsätze der CNO-Kräfte die gleichen Regeln wie für den konventionellen Einsatz deutscher Truppen gelten. Damit sicherte die Regierung dem Parlament die tradierten Kontrollrechte auch für CNOs zu:

> »Der Einsatz militärischer Cyber-Fähigkeiten durch die Bundeswehr unterliegt denselben rechtlichen Voraussetzungen wie jeder andere Einsatz deutscher Streitkräfte. Grundlagen für Einsätze der Bundeswehr sind die einschlägigen Regelungen des Grundgesetzes sowie des Völkerrechts, Maßnahmen des Sicherheitsrates nach Kapitel VII der VN-Charta (Mandate), völkerrechtliche Vereinbarungen mit dem betreffenden Staat und das Parlamentsbeteiligungsgesetz.« (Ebd.)

Damit bestätigte die Bundesregierung die Regelungen nach Artikel 87a GG. Außerdem betonte die Regierung, dass Artikel 26 GG Deutschland auch im Cyberspace einen Angriffskrieg verbiete (ebd., S. 7). Der Einsatz der neuen Fähigkeiten der militärischen Beschützer-Rolle sollte aus Sicht der Regierung damit domestisch wie international den etablierten rechtlichen Regeln folgen und parlamentarisch mandatiert werden.

Ebenfalls 2015 begann das Verteidigungsministerium mit der Arbeit an einem neuen Weißbuch zur deutschen Sicherheitspolitik. In diesem Zusammenhang wurde das Thema Cybersicherheit zu einem zentralen Themengebiet, das in einem eigenen Workshop bearbeitet wurde. Zur Eröffnung dieser Veranstaltung skizzierte die Verteidigungsministerin die Gefahrenlage im Cyberspace sowie die potenziellen Herausforderungen für die Streitkräfte. Sie betonte dabei, dass Cyberoperationen zu etablierten Komponenten militärischer Auseinandersetzungen geworden seien. In diesem Kontext habe insbesondere der Konflikt zwischen Russland und Georgien 2008 gezeigt, wie die beiden Komponenten verknüpft werden könnten. Das Attributionsproblem mache aber eine Kartierung der Konfliktparteien schwierig, dies liege an der grenzen- und hierarchielosen

Organisation des Netzes. Zur Illustration der vielfältigen Einsatzmöglichkeiten von Cyberangriffen wies die Ministerin auf den Bundestagshack 2015 hin. Mit Blick auf die Konfliktkonstellationen im Cyberspace betonte die Ministerin, Cyberangriffe ermöglichten konventionell unterlegenen Akteuren asymmetrisch gegen andere vorzugehen (Bundesministerium der Verteidigung, 2015a).

Die Aufgaben der Bundeswehr umfassten nach Einschätzung der Bundesregierung daher zwei wesentliche Bereiche: erstens den Schutz der bundeswehreigenen IT-Systeme. Dies sei auch mit Blick auf die zunehmend vernetzten Waffensysteme wie den Eurofighter von zentraler Bedeutung, um im Ernstfall das Funktionieren der konventionellen Streitkräfte sicherzustellen und den Schutzauftrag erfüllen zu können. Zweitens stelle der Cyberspace neben Land, See, Luft und Weltraum einen eigenen militärischen Handlungsraum dar, in dem die Bundeswehr agiere und daher die entsprechenden Fähigkeiten aufbauen und vorhalten müsse. Um dieses Ziel zu erreichen sollte ein eigener Organisationsbereich Cyber- und Informationsraum die vorhandenen Kapazitäten bündeln und Partnerstaaten als zentraler militärischer Ansprechpartner in Fragen der militärischen Cybersicherheit dienen. Die Ministerin setzte daher einen Aufbaustab ein, der mit der konzeptionellen Entwicklung dieses neuen Organisationsbereichs betraut wurde (ebd.). Zudem beschloss das Verteidigungsministerium schon im April 2015 die »Strategische Leitlinie zur Cyber-Verteidigung im Geschäftsbereich BMVg« (Bundesministerium der Verteidigung, 2015b). Der Spiegel berichtete im Juli 2015 über das eingestufte Dokument und Netzpolitik.org veröffentlichte zeitgleich den Volltext (Netzpolitik.org, 2015; Spiegel, 2015b).[3]

In den Leitlinien verwies das BMVg zunächst auf die gestiegene Abhängigkeit von IT, die staatliche, wirtschaftliche und gesellschaftliche Akteure gleichermaßen betreffe. Explizit leiste die Bundeswehr in diesem Zusammenhang »Beiträge zum Heimatschutz auch durch die Verteidigung gegen Cyber-Angriffe, die einen bewaffneten Angriff auf Deutschland darstellen, vorbereiten oder begleiten können« (Netzpolitik.org, 2015). Außerdem sei in künftigen Konfliktlagen davon auszugehen, dass komplementär zu konventionellen Operationen, die gegnerische Nutzung des Cyberspace beeinträchtigt oder ganz unterbunden werden müsse. Dabei müsse stets die eigene Handlungsfähigkeit gesichert werden. Die Notwendigkeit in diesem Bereich verstärkt aktiv zu werden, wurde neben der gewachsenen Vulnerabilität auf die gestiegene Angriffshäufigkeit sowie auf die qualitativ immer ausgefeiltere Durchführung zurückgeführt. Die Leitlinien weisen aber auch darauf hin, dass die Bundeswehr allein möglicherweise nicht dazu in der Lage sei, das nötige Know-How vorzuhalten, so dass evtl. auf Ressourcen aus der Reserve

3 Das veröffentlichte Dokument verfügt über keinerlei Paginierung mehr, weshalb in folgenden Referenzen auf den Text Verweise auf Seitenzahlen fehlen.

zurückgegriffen und Personal aus der Wirtschaft temporär eingebunden werden müsse (Netzpolitik.org, 2015).

Offensive Cyberoperationen stellten aus Sicht des BMVg besonders effektive Mittel zur Zielerreichung dar, da sie präzise gegen bestimmte Ziele eingesetzt werden könnten und zumeist keine kinetischen Folgen hätten, also keine Menschenleben gefährdet würden. Ferner seien deren Effekte nicht von Dauer:

> »Offensive Cyber-Fähigkeiten der Bundeswehr sind als unterstützendes, komplementäres oder substituierendes Wirkmittel anzusehen. Sie haben zum Einen das Potenzial, in der Regel nicht-letal und mit hoher Präzision auf gegnerische Ziele zu wirken, zum Anderen kann diese Wirkung im Gegensatz zu kinetischen Wirkmitteln unter Umständen sogar reversibel sein.« (Ebd.)

Rollentheoretisch gesprochen waren CNOs aus Sicht der Bundesregierung damit ein geeignetes Mittel, die militärische Beschützer-Rolle möglichst ohne Kollateralschäden und physische Zerstörung zu erfüllen. Cyberangriffe sind damit ein besonders »schonendes« und präzises Mittel zur Erreichung militärischer Ziele.

Die Leitlinien stießen sowohl bei der parlamentarischen Opposition als auch bei VertreterInnen der Zivilgesellschaft auf Kritik. Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) erkannte in der Bevorratung von Sicherheitslücken zur offensiven Nutzung eine Unterminierung der Sicherheit des Netzes im Allgemeinen. Außerdem wurde bemängelt, dass die Leitlinien erhebliche rechtliche Probleme aufwürfen, da sie ein Wirken gegen IT-Infrastrukturen vorsehen, die potenziell nicht in staatlicher Hand seien und ggf. keine legitimen Ziele für militärische Angriffe darstellten. Aus dieser Sicht verstieß die Bundesregierung mit den Plänen gegen die Genfer Konventionen und würde internationales Recht brechen (FIfF, 2015). Ferner wies sowohl das FIfF als auch die deutsche Gesellschaft für Informatik darauf hin, dass die Bundesregierung mit Blick auf den Bundestagshack 2015 gezeigt habe, dass der Schutz essenzieller Infrastrukturen nicht gewährleistet sei. Daher sei der Ausbau defensiver Maßnahmen begrüßenswert, der Ausbau offensiver Kapazitäten aber unangemessen (Gesellschaft für Informatik, 2015). Auch die Grünen bemängelten die zu offensive Ausrichtung der Leitlinien als kontraproduktiv, da Deutschland auf diesem Weg einer zunehmend konfliktiven Dynamik im Cyberspace folge (Brugger, 2015).

Diese Kontestationen wurden von der Bundesregierung aber nicht aufgenommen und blieben folgenlos. Im April 2016 legte der Aufbaustab Cyber- und Informationsraum seinen Abschlussbericht vor. Trotz der Kontestationsprozesse wurde in diesem Dokument der Ausbau der militärischen Kapazitäten befürwortet. Dabei wurde auf die nationale Sicherheit, auf die Manipulation von Wahlen sowie auf die wirtschaftliche Prosperität verwiesen: »Die zunehmend komplexeren Angriffe erfordern den Ausbau der staatlichen Handlungsfähigkeit zum Schutze

unseres demokratischen Systems und seiner wirtschaftlichen Grundlagen« (Bundesministerium der Verteidigung, 2016, S. 1).

Die militärische Beschützer-Rolle hatte im Zuge der Debatten um Wahlmanipulationen durch russische Cyberangriffe während des US-Präsidentschaftswahlkampfs mit dem demokratischen System ein zusätzliches neues Referenzobjekt erhalten. In diesem Kontext wirkte die Rolle als Garant liberaler Grundrechte katalytisch auf den Ausbau der Beschützer-Rolle, da die Freiheiten notfalls auch militärisch zu schützen seien.

Die Notwendigkeit, einen eigenen militärischen Organisationsbereich einzurichten, wurde neben einem »Qualitätssprung in der Bedrohungslage« mit dem Verweis auf internationale Partner sowie Entwicklungen in der NATO begründet (ebd., S. 1f. sowie 13f.). Die NATO hatte den Cyberspace 2016 auf dem Gipfel von Warschau als »a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea« definiert (NATO, 2016). Der Aufbaustab empfahl daher, entsprechend der Ankündigung der Ministerin, analog zu Verbündeten einen eigenen Organisationsbereich mit InspekteurIn zu etablieren (Bundesministerium der Verteidigung, 2016, S. 1).

Zur Verdeutlichung des gestiegenen Risikopotenzials verwies der Aufbaustab unter anderem auf Stuxnet, der die Angreifbarkeit von kritischen Infrastrukturen gezeigt habe sowie auf den OPM- und Bundestagshack, die potenziell sensible Informationen zum Ziel hatten.[4] Das Netz mit seinen technischen Besonderheiten und seiner globalen Architektur stelle dabei sowohl die Unterscheidung zwischen Krieg und Frieden als auch die Differenzierung innerer und äußerer Sicherheit vor Herausforderungen. Für den Einsatz der Streitkräfte im Cyberspace gelten aber dennoch die gleichen Regelungen wie für deren konventionellen Einsatz (Parlamentsbeteiligungsgesetz) (ebd., S. 5). Der Aufbaustab erklärte, es sei das Ziel mit dem neuen Organisationsbereich »Informationsdominanz im Operationsraum zu erreichen, um Entscheidungsprozesse zu optimieren und Einsatzwirkung zu maximieren« (ebd., S. 5). Dazu müsse sowohl das Personal besser geschult als auch das institutionelle Gefüge der Bundeswehr angepasst werden (ebd., S. 16f.). Im Oktober 2016 wurde dazu im Ministerium eine neue Abteilung Cyber- und Informationstechnik aufgestellt (Bundeswehr, 2020).

Neben dem Umgang mit qualitativ immer höherwertigen Angriffen, wurde mit der Reform der Beschützer-Rolle auch, die internationale Kooperationsfähigkeit verbessert. Ferner wurden zur Rechtfertigung des Aufbaus auch auf die eigenen Erfahrungen mit Cyberangriffen verwiesen.

---

4 2014/15 wurde das amerikanische Office of Personnel Management (OPM) Opfer eines Cyberangriffs bei dem persönliche Daten von mehr als 20 Millionen Bediensteten und BewerberInnen gestohlen wurden (The New York Times, 2015). Ebenfalls 2015 wurde der Bundestag zum Ziel eines Angriffs, auch hierbei wurden Daten entwendet (Spiegel, 2015c).

Aufgrund der Sorge vor folgenreichen Angriffen auf kritische Infrastrukturen arbeitete die Bundesregierung auf internationale Normen hin. Im Rahmen der OSZE setzte sich die Bundesregierung 2016 erfolgreich für eine Kultur der Zurückhaltung ein. Mit einem zweiten Bündel von vertrauensbildenden Maßnahmen wurde unter deutschem Vorsitz empfohlen, dass Staaten auf freiwilliger Basis dazu beitragen sollten, Cyberangriffe auf kritische Infrastrukturen zu vermeiden, da diese auch Folgen für benachbarte Staaten haben könnten (OSCE, 2016a,b). Diese Maßnahmen sind Teil der Bemühungen eine Norm des Nicht-Angriffs auf kritische Infrastrukturen zu etablieren, die allerdings bis heute nicht allgemein anerkannt ist. 2019 drängte der Bundesaußenminister erneut auf die Spezifizierung einer solchen Norm, die konkret Angriffe auf weltweite Handelsströme, das Bankensystem oder die zivile Luftfahrt ächten solle. Heiko Maas bemängelte, dass hierzu aber »der ernsthafte politische Wille« fehle (Auswärtiges Amt, 2019).

Eingeleitet durch den Prozess der Erarbeitung eines neuen Weissbuches, setzte sich auch der Verteidigungsausschuss des Bundestages Anfang 2016 mit der militärischen Nutzung des Internets auseinander. Hier wurde durch die Sachverständigen unter anderem auf Probleme bei der Parlamentsbeteiligung hingewiesen. Angeführt wurde bspw. der Umstand, dass der Einsatz von deutschen Tornados zur Aufklärung zustimmungspflichtig sei, obwohl kein Waffeneinsatz erfolge. Für Cyberoperationen bedeute das, dass auch die Aufklärung feindlicher Netze, also der erste Zugriff eigentlich durch den Bundestag mandatiert werden müsse (Deutscher Bundestag, 2016a, S. 25). Mehrere Gutachter sprachen sich ferner gegen die Entwicklung von Schadsoftware durch die Bundesrepublik aus. Dies berge stets das Risiko, dass diese Werkzeuge von Dritten zweckentfremdet würden, dass damit die globale Unsicherheit steige und dass gegnerische Systeme permanent ausgekundschaftet werden müssten, um die Zuverlässigkeit der Exploits sicherzustellen (ebd., S. 20 bzw. 27). Insbesondere letztgenannter Aspekt widerspreche »der deutschen Kultur der militärischen Zurückhaltung« (ebd., S. 27). Die Vertreterin des BMVg teilte diese Kritik allerdings nicht. Mit Blick auf die potenzielle Proliferation von Wissen über Schwachstellen sah die Staatssekretärin des BMVg aber keine Probleme, da die Bundeswehr die eigenen Wissensbestände »im Griff« habe (ebd., S. 40).

In dieser Anhörung wurde ferner darüber debattiert, wie weitreichend eine staatliche Sorgfaltsverantwortung für den Cyberspace reichen könne und ob damit ggf. umfassende Überwachungsmaßnahmen verbunden seien (ebd., S. 37f.). Eine umfassende Kontrolle von Internetverkehr, um Angriffe aufzuspüren, stand somit prinzipiell im Widerspruch zur Rolle als Garant liberaler Grundrechte.

Darüber hinaus bestanden bei der Opposition Bedenken, inwiefern Cyberoperationen überhaupt parlamentarisch kontrollierbar seien, da keine physischen Truppenbewegungen entständen und die Operationen stets klandestin ablaufen könnten. Ferner könne das Attributionsproblem auch gegen die parlamentari-

schen KontrolleurInnen verwendet werden (ebd., S. 50-54). Die Frage, ab wann die Bundesregierung einen Cyberangriff als bewaffneten Angriff werten und damit ein Recht auf Selbstverteidigung beanspruchen würde, wurde von der Vertreterin des Verteidigungsministeriums nicht beantwortet; auch unter Verweis, dass dadurch »die Grauzone« entfallen würde, die ggf. Entscheidungsspielraum gewähren oder abschreckend wirken könne (ebd., S. 53). Ähnlich argumentierte die Bundesregierung auch in der Antwort auf eine parlamentarische Anfrage. Konkrete Maßstäbe oder Schwellen zur Beurteilung eines Vorfalls nannte sie auch hier nicht (Deutscher Bundestag, 2015d, S. 10 bzw. 11). Sollte die Regierung zu der Auffassung gelangen, dass ein Angriff das Selbstverteidigungsrecht auslöse, würde sie sich aber vorbehalten, »mit allen zulässigen militärischen Mitteln [zu; Anm. d. Verf.] reagieren« (Deutscher Bundestag, 2018e, S. 6).

Sichtbar kulminiert ist der domestische Aufbau von Cyberkapazitäten im Jahr 2017 als die Bundeswehr das Kommando Cyber- und Informationsraum (Kdo CIR) mit etwa 14.500 Dienstposten etablierte. Diesem untersteht unter anderem das Kommando Strategische Aufklärung sowie das 2018 gegründete Zentrum Cyber-Operationen (Bundesministerium der Verteidigung, 2020; Bundeswehr, 2020). Ebenfalls 2018 wurde beschlossen in Kooperation zwischen dem BMI und BMVg die Agentur für Innovation in der Cybersicherheit zu gründen. Sie soll dazu beitragen die technologische Souveränität der Bundesrepublik bei Schlüsseltechnologien sicherzustellen (Bundesregierung, 2019a). Mit dem Kdo CIR wurde der Cyberspace als militärischer Handlungsraum auch institutionell fest verankert.

Einerseits hat sich die Bundesregierung bei diesem Schritt maßgeblich an den internationalen Partnern orientiert und die Kooperationsfähigkeit verbessert. Insbesondere die Entwicklungen und Erfordernisse in der NATO wurden in diesem Kontext immer wieder angeführt. Andererseits wurden die zunehmend häufiger auftretenden und in ihrer Qualität immer besseren Cyberangriffe zur Rechtfertigung der neuen Kapazitäten herangezogen. Gegen die internationalen Dynamiken blieben die domestischen Kontestationen folgenlos. Eine von der parlamentarischen Opposition (insbesondere den Grünen und Linken) immer wieder angemahnte Lücke bei der Kontrolle militärischer Cyberkapazitäten, wurde von der Bundesregierung ebenfalls bestritten (Deutscher Bundestag, 2018c, S. 3).

Trotz Kritik aus den Reihen des Parlaments konnte die Regierung auf die Zustimmung der Mehrheit der Abgeordneten zählen. So konnte die Regierung auch die parlamentarische Zustimmung zu einer Budgeterhöhung für den Aufbau des neuen Kommando Cyber- und Informationsraum gewinnen. Um die parlamentarische Kontrolle der CNO-Kräfte zu verbessern, wird darüber diskutiert, einen spezifischen parlamentarischen Unterausschuss zu etablieren (Deutscher Bundestag, 2017b, S. 53f.).

Besonders problematisiert wurde die, aus Sicht der Opposition, unklare Aufgabenteilung zwischen dem Bundesnachrichtendienst und der Bundeswehr beim

Einsatz in gegnerischen Netzen (Deutscher Bundestag, 2016a, S. 39). Diese Frage wurde explizit auch mit der Thematik eines digitalen Gegenschlags als Reaktion auf einen Cyberangriff (Hackback) debattiert. Da in diesem Kontext die Frage offen war, wer diese Maßnahme durchführen solle (ebd., S. 45). Die Regierung verwies in diesem Kontext auf das 2011 gegründete Nationale Cyber-Abwehrzentrum in dem die wesentlichen Akteure (BKA, Nachrichtendienste und Streitkräfte) vertreten seien und in dem eine Entscheidung über die angemessene Reaktion und die durchführende Stelle getroffen werden könne (ebd., S. 62).

Da aus Sicht der Bundesregierung zwischen Krieg und Frieden im Cyberspace nicht mehr eindeutig unterschieden werden konnte, weil die Angriffe praktisch nie die Schwelle eines bewaffneten Angriffs überschreiten und so das Selbstverteidigungsrecht gemäß Artikel 51 der UN-Charta auslösen könnten, plädierten VertreterInnen der Bundeswehr für eine neue gesetzliche Regelung zum »digitalen Verteidigungsfall«, die einen Einsatz der Streitkräfte im Cyberspace unterhalb der Schwelle eines bewaffneten Angriffs ermöglicht und die innerstaatlichen Prozesse zur Amtshilfe (Art. 35 GG) durch die Bundeswehr vereinfacht (Augen Geradeaus!, 2019). Aus Sicht des Inspekteurs des Kdo CIR, kommt es bei schwerwiegenden Cyberangriffen

> »[…] buchstäblich auf Minuten an. Die derzeitigen Prozesse des Bundes und der Länder sind darauf nicht ausgelegt. Allein die Unkenntnis des Angreifers und die damit verbundene Frage der Zuständigkeit, das bisher fehlende gesamtstaatliche Cyber-Lagebild und die Verfahren zur Anforderung von Amtshilfe oder die fehlende direkte Zusammenarbeit mit beispielsweise den Internet Service Providern ermöglichen aktuell keine optimale Reaktion in solch einem Szenario.« (Ebd.)

Im Juni 2019 konstatierte Verteidigungsministerin von der Leyen in einem Interview, dass die Möglichkeit zu digitalen Gegenschlägen »zur Abschreckung« benötigt werde, dass Reaktionen aber nicht zwangsläufig digital sein müssten, sondern bspw. durch Sanktionen erfolgen könnten (t-online.de, 2019).

Damit versuchte die Bundesregierung die Einsatzschwelle der militärischen Beschützer-Rolle zu senken. Dies war aus Sicht der Streitkräfte nötig, da die etablierten Voraussetzungen durch Cyberangriffe kaum erreicht werden. Einem Verschwimmen der Trennung zwischen Krieg und Frieden, wie er immer wieder debattiert wurde, würde dann durch eine niedrigere Schwelle zum Einsatz der militärischen Beschützer-Rolle korrespondieren.

Unklar ist die konkrete Aufgabe der Bundeswehr in diesem Kontext auch in einer maßgeblich vom Innenministerium im Mai 2019 angestoßenen, noch nicht beendeten, Debatte um digitale Gegenschläge im Falle eines Cyberangriffs – KritikerInnen sprechen in diesem Zusammenhang von Hackback, die Bundesregierung bezeichnet das Vorgehen als aktive Cyberabwehr. Im Ernstfall sollte

aus Sicht des Innenministers der BND auf einen Angriff bspw. auf kritische Infrastrukturen, wie im Falle WannaCry, reagieren und die entsprechenden Gegenmaßnahmen ausführen, dieser Vorstoß erfolgte Presseberichten zufolge nach Absprache mit dem Bundeskanzleramt. Um ein solches Vorgehen zu ermöglichen, bedürfte es aber einer Grundgesetzänderung, da es sich hierbei um polizeiliche Maßnahmen zur Gefahrenabwehr handelt, für die die Bundesländer zuständig sind (Deutschlandfunk, 2019a; ZDF, 2019). Ein Vertreter des Innenministeriums sagte dazu:

> »Wenn man bei solchen Szenarien zu dem Ergebnis kommt, dass es die Länder alleine nicht schultern können, gehört es zu unserer Pflicht, uns auf eine solche Situation rechtlich vorzubereiten. Wenn wir sie nie brauchen, wäre es mir am liebsten.« (Deutschlandfunk, 2019a)

Diese Position vertrat die Bundesregierung auch bei einer parlamentarischen Anfrage im November 2018. Inwiefern diese neue Herausforderung eine Neubalancierung zwischen Bund und Ländern erfordere, würde noch geprüft (Deutscher Bundestag, 2018e, S. 3). Eine Entscheidung zugunsten des BND könnte ferner das Trennungsgebot unterminieren (Deutschlandfunk, 2019a).

Ein Gutachten der Wissenschaftlichen Dienste des Bundestages kam zu dem Schluss, dass es völkerrechtlich zunächst nicht relevant sei, ob die Gegenmaßnahme durch einen Nachrichtendienst oder die Streitkräfte erfolge, da die Handlung dem Staat zugeschrieben würde. Allerdings dürften militärische Gegenmaßnahmen (also Angriffe, die signifikante Schäden verursachen) »nur durch Kombattanten, also Mitglieder der Streitkräfte, ausgeführt werden« (Deutscher Bundestag, 2018f). Die durchführende Instanz müsste also durch Art des Einsatzes bestimmt werden, ganz allgemein fehle den Nachrichtendiensten aber eine Befugnis jenseits der Aufklärung (ebd.).

In einem regierungsinternen Papier, aus dem der Bayerische Rundfunk zitierte, wurde ein vierstufiges Vorgehen beschrieben, um massiven Cyberangriffen aus dem Ausland zu begegnen. In einer ersten Reaktion (Stufen eins und zwei) könnten die Netzbetreiber oder Polizeien damit beginnen den Netzwerkverkehr zu blockieren oder die Routen zu verändern. Hierbei fände noch keine offensive Maßnahme außerhalb der eigenen Netze statt. Auf der dritten Stufe soll es der zuständigen Behörde erlaubt sein, auf fremde Netzwerke zuzugreifen und »Daten zu verändern oder Daten zu löschen« (Bayerischer Rundfunk, 2019). Dieser Schritt war ein Desiderat nachdem beim Bundestagshack 2015 sensible Daten abgegriffen worden waren, die später auf Rechnern in Osteuropa gefunden wurden. Aufgrund einer fehlenden Rechtsgrundlage, durften die Informationen dort aber nicht gelöscht werden. Die vierte Stufe der Reaktion sah dann ein Eingreifen in die Systemfunktionen des angreifenden Rechners vor, um einen laufenden Angriff zu beenden. Über das Vorgehen sollte im Cyber-Abwehrzentrum beraten

werden, inwiefern »ein erheblicher Cyber-Angriff aus dem Ausland vorliegt«, der nicht durch andere Maßnahmen beendet werden kann (Bayerischer Rundfunk, 2019). In der Folge sollte ein Gremium aus VertreterInnen des Kanzleramts, des Auswärtigen Amts, des Justiz-, des Verteidigungs- und des Innenministeriums über eine Reaktion entscheiden. Mit der Durchführung des Gegenangriffs sollte dann der BND betraut werden (ebd.).

Der Innenminister rechtfertigte die Maßnahmen unter Verweis auf die potenziell verheerenden Folgen eines umfassenden Cyberangriffs:

> »Wenn Sie sich einen größeren Angriff auf kritische Infrastruktur vorstellen – nicht nur Energieversorgung, sondern Krankenhäuser und ähnliches und alles gleichzeitig –, dann kann eine solche Situation eintreten, wo eben die herkömmlichen Abwehrmöglichkeiten nicht mehr ausreichen.« (Deutschlandfunk, 2019a)

Kontestationen gegen die Pläne gab es sowohl vom Koalitionspartner als auch von der parlamentarischen Opposition, die insbesondere vor einem Rüstungswettlauf warnte und das Risiko von Kollateralschäden hervorhob. Um die unerwünschten Folgen eines Cyberangriffs zu illustrieren, verwies ein Vertreter der FDP auf das Risiko eines »Cyber-Kundus« (ZDF, 2019).[5] Im September 2019 wurde über ein eingestuftes Gutachten des Wissenschaftlichen Dienstes des Bundestages berichtet, das ebenfalls mit Verweis auf potenzielle Eskalationsdynamiken Probleme bei den Plänen zu einem digitalen Gegenschlag feststellte (Zeit, 2019).

Bislang ist unentschieden, welche Institution, in welcher Form digitale Gegenschläge führen sollte. Die militärische Beschützer-Rolle der Bundeswehr wurde zwar ausgebaut, es bleibt aber unklar, wann diese Kapazitäten eingesetzt werden. Klar ist nur, dass dies bei einem bewaffneten Angriff, der das Selbstverteidigungsrecht nach Artikel 51 der UN-Charta evoziert und im Rahmen von mandatierten Einsätzen der Streitkräfte möglich wäre. Wie ein digitaler Verteidigungsfall aussehen könnte, der diese Hürden unterschreitet, ist dagegen noch nicht geklärt.

## 6.2 Vereinigtes Königreich

### 6.2.1 Der Aufbau militärischer Kapazitäten: Neue offensive Möglichkeiten

Offensive Cyberkapazitäten zum militärischen Einsatz wurden durch das GCHQ bereits Anfang der 2000er Jahre im Rahmen des Einsatzes in Afghanistan aufge-

5 Am 4. September 2009 befahl ein deutscher Oberst den Luftangriff auf zwei von den Taliban entführte Tanklaster. Bei diesem Angriff starben mindestens 90 ZivilistInnen (Deutschlandfunk, 2019b).

baut. Hierbei stützte sich der Nachrichtendienst auf eine erprobte Kooperation mit dem Verteidigungsministerium. Dabei sind offensive Cybermaßnahmen zum Einsatz gekommen, die direkte Folgen für den Konfliktverlauf in der realen Welt gehabt haben (GCHQ, 2018c). Diese Einsätze wurden aber erst weit nach deren Durchführung eingeräumt.

Entsprechend der offensiven Ausrichtung der militärischen Beschützer-Rolle sprach sich die britische Regierung international bereits 2004 explizit gegen ein Verbot der militärischen Nutzung des Netzes aus. Die völkerrechtlichen Vorgaben zum Einsatz militärischer Mittel seien zur Verhinderung eskalativer Dynamiken ausreichend. Außerdem könne ein solches Verbot im Widerspruch zum Prinzip des freien Informationsflusses im Netz stehen, da zur Verifikation Kontrollen von und ggf. Eingriffe in Datenströme notwendig werden könnten. In der ersten Risikoeinschätzung kam die britische Exekutive zu der Auffassung, dass Staaten keine maßgeblichen Gefahren im Netz darstellten (United Nations, 2004, S. 11).

Die militärische Beschützer-Rolle unterscheidet sich hier bereits deutlich von der deutschen. Schon in der Frühphase nutzte die britische Regierung offensive Cyberkapazitäten um die eigenen Streitkräfte zu unterstützen. Eine zusätzliche Kontrolle war aus Sicht der Exekutive nicht notwendig, da rechtliche Regelungen übertragbar seien. Eine Kontrolle der Rolle könne ferner im Widerspruch zum freien Fluss von Informationen im Netz stehen. Restriktionen der Beschützer-Rolle waren aus rollentheoretischer Sicht nicht mit der Rolle als Garant liberaler Grundrechte vereinbar.

Die Gefahreneinschätzung mit Blick auf staatliche Akteure revidierte die britische Regierung in ihrer ersten Cyber Security Strategy 2009 (Cabinet Office, 2009, S. 13). Da Staaten nun doch als Risiken für die nationale Cybersicherheit gesehen wurden, wurde dem Verteidigungsministerium bereits 2008 die Aufgabe zugeschrieben, die Entwicklungen im Bereich der Cybersicherheit zu überwachen und die potenziellen Risiken zu evaluieren (Cabinet Office, 2008, S. 44). Cybersicherheit wurde in der folgenden National Security Strategy (NSS) 2009 zu den emergenten Problemfeldern der Sicherheitspolitik gezählt. Die Regierung ging davon aus, dass Staaten zunehmend damit beginnen würden, militärische Kapazitäten in diesem Bereich zu entwickeln. Anstelle von militärischen Interventionen könnten dann Cyberangriffe genutzt werden, um Schäden zu verursachen (UK Government, 2009, S. 13, 65).

In der ersten Cyber Security Strategy von 2009 wies die Regierung darauf hin, dass der Cyberspace auch genutzt werden sollte, um gegen Gegner vorzugehen. Cyberangriffe gegen Großbritannien könnten sowohl von Staaten als auch Terrororganisationen ausgehen. Die Regierung müsse daher in der Lage sein, falls nötig, offensive Maßnahmen zu ergreifen (Cabinet Office, 2009, S. 13-16). Der Cyberspace sei die neue Domäne, die es zum Erhalt der Sicherheit und des Wohlstands zu verstehen und nutzen gelte:

> »Just as in the 19th century we had to secure the seas for our national safety and prosperity, and in the 20th century we had to secure the air, in the 21st century we also have to secure our position in cyber space.« (Cabinet Office, 2009, S. 21)

Die britische Beschützer-Rolle fand damit neben dem Schutz der eigenen Netze bereits früh eine Referenz (Schutz vor wem?) auf den (Cyber)Aktivitäten feindlicher Staaten und von Terrorgruppen. Ähnlich wie in der Bundesrepublik wurde die Notwendigkeit militärischer Handlungsfähigkeit auch durch potenzielle Angriffe auf kritische Infrastrukturen gerechtfertigt.

Die militärische Einschätzung verschärfte sich 2010 nach dem Wahlsieg der Tories. In diesem Kontext rückte die Offensive zunehmend in den Fokus der Aufmerksamkeit. In der neuen NSS sah der National Security Council in Cyberangriffen eine der vier größten sicherheitspolitischen Herausforderungen für das Vereinigte Königreich. Angriffe könnten dabei von Staaten, Terrororganisationen oder Kriminellen ausgehen (UK Government, 2010, S. 11 sowie 27). Zur Illustration möglicher Angriffe auf kritische Infrastrukturen und deren »potentially devastating real-world effect«, verwies die britische Regierung auf den Wurm Stuxnet (ebd., S. 30).

Die Kompetenzen des GCHQ sollten bei der Entwicklung offensiver Fähigkeiten genutzt werden, um auch militärische Kapazitäten auszubauen. In der Cyber Security Strategy von 2011 wurde dies institutionell verankert. Die Regierung etablierte hierzu eine Joint Cyber Unit, die die Kooperation zwischen dem Nachrichtendienst und den Streitkräften im Bereich der Cybersicherheit verstetigte. Zusätzlich zu dieser Einheit beim GCHQ etablierten die Streitkräfte eine weitere, eigene Joint Cyber Unit in Corsham. Auf militärischer Seite wurde die Verantwortung beim neuen Joint Forces Command angesiedelt. Etwa 320 Millionen britische Pfund erhielt das GCHQ für den Aufbau weiterer Cyberkapazitäten. Mit den neuen Fähigkeiten sollten Angriffe abgeschreckt und abgewehrt werden (Cabinet Office, 2011, S. 26f.).

Dieser Schritt wurde mit der wachsenden Verwundbarkeit und der gestiegenen Zahl immer komplexerer Angriffe gerechtfertigt. Mit Blick auf internationale Konflikte konstatierte die Regierung: »In times of conflict, vulnerabilities in cyberspace could be exploited by an enemy to reduce our military's technological advantage, or to reach past it to attack our critical infrastructure at home« (ebd., S. 15). Auch ein terroristischer Angriff auf kritische Infrastrukturen wurde in diesem Zusammenhang als potenzielles Risiko debattiert. Dies alles vollziehe sich in einem grenzenlosen Raum, in dem die Attribution von Angriffen und die Unterscheidung zwischen Gegnern schwierig sei. Der Cyberspace war aus Sicht der Regierung zu einem neuen Raum geworden, in dem auch entscheidende militärische Vorteile gewonnen werden könnten. Das Bestreben einiger Staaten, Angriffe

abstreitbar durchzuführen berge hierbei besonders große Risiken (ebd., S. 15 bzw. 17). Für das Vereinigte Königreich sei es daher notwendig, proaktiv im Cyberspace zu agieren und diesen für die eigene Sicherheitspolitik besser zu nutzen. Dies stimme auch mit den Vorgaben des neuen Strategischen Konzepts der NATO überein (ebd., S. 26). Die Regierung war zu diesem Zeitpunkt der Auffassung, dass ein Cyberangriff auf kritische Infrastrukturen verheerende Folgen nach sich ziehen könnte. Ein Vertreter des Verteidigungsministeriums verglich Cyberoperationen mit kinetischen Folgen mit dem Einsatz von Marschflugkörpern. Mit Blick auf die Kontrolle der neuen Kapazitäten betonte die Regierung, ähnlich wie die deutsche, dass die neuen Möglichkeiten durch die etablierten Regeln nationalen und internationalen Rechts reguliert werden sollten (UK Government, 2011).

Innerhalb kurzer Zeit rückte damit, begünstigt durch den Wechsel der RollenträgerInnen in der Exekutive sowie durch den Verweis auf die Aktivitäten anderer Staaten und die Folgen von Cyberangriffen, die offensive Ausrichtung der Beschützer-Rolle in den Vordergrund.

Ebenfalls 2011 wurde in britischen Medien darüber berichtet, dass die Regierung damit begonnen habe, die Fähigkeit zu Cyberangriffen auszubauen. Der Parlamentarische Staatssekretär im Verteidigungsministerium Nick Harvey gab gegenüber dem Guardian an, dass Cyberoperationen zu einem wichtigen Bestandteil des militärischen Arsenals geworden wären. Sorgen, dass diese Militarisierung des Netzes einen aggressiveren Einsatz dieser Kapazitäten zur Folge haben könnte, teilte er nicht:

> »I don't think that the existence of a new domain will, in itself, make us any more offensive than we are in any other domain. The legal conventions within which we operate are quite mature and well established.« (The Guardian, 2011)

Auch wenn die Unterscheidung zwischen Krieg und Frieden aus Sicht der britischen Regierung im Netz schwieriger wurde, sollte das nicht zu einem offensiveren Einsatz der entsprechenden Beschützer-Rolle führen.

Die Verantwortung für die Entwicklung der neuen Fähigkeiten wurde wiederum dem GCHQ übertragen, politisch war das Cabinet Office zuständig. Das Verteidigungsministerium sollte den Prozess begleiten und die militärischen Anforderungen einbringen. Harvey führte aus, dass der Westen seine Technologieführerschaft nicht als garantiert betrachten sollte und dass Staaten wie China vehement an der Modernisierung ihrer Streitkräfte arbeiteten (ebd.).

Diesen Aussagen folgend, verkündete der Verteidigungsminister im September 2013 öffentlich, dass Großbritannien »a full-spectrum military cyber capability, including a strike capability« aufbaue (UK Government, 2013a). Dabei würde auch auf die Expertise von ReservistInnen zurückgegriffen. Die britische Regierung war damit die erste, die die Entwicklung eines offensiven Cyberarse-

nals ankündigte (Financial Times, 2013). Im Dezember 2013 legte das Verteidigungsministerium ein erstes Strategiedokument vor, das sich ausschließlich mit militärischen Aspekten der Cybersicherheit befasste. Nachdem die Aufgabe des Militärs, ähnlich wie in Deutschland, zuvor primär im Schutz militärischer IT-Infrastruktur gesehen wurde, wies der Verteidigungsminister im Vorwort darauf hin, dass dies nicht mehr ausreiche:

> »Cyber is the new frontier of defence. For years, we have been building a defensive capability to protect ourselves against these cyber attacks. That is no longer enough. You deter people by having an offensive capability.« (Ministry of Defence, 2013, S. iii)

Die größte Gefahr für folgenschwere und komplexe Cyberangriffe ging zu diesem Zeitpunkt aus Sicht der Regierung von anderen Staaten aus, die mit ihren Fähigkeiten wirtschaftliche aber auch militärische Ziele verfolgten (ebd., S. 1-9). Eine Definition offensiver Maßnahmen oder wie diese eingesetzt werden könnten, beinhaltete dieses Dokument allerdings nicht. Betont wurde lediglich, dass der Einsatz den tradierten Vorgaben des Kriegsvölkerrechts entsprechen müssten (ebd., S. 1-24).

Die öffentliche Ankündigung, Cyberangriffskapazitäten aufzubauen, wurde in der Folge auch im Parlament diskutiert. Die Opposition sprach sich nicht prinzipiell gegen den Aufbau aus, forderte von der Regierung aber, eine klare Einsatzdoktrin vorzulegen. Ein gänzlich klandestines Vorgehen berge das Risiko, dass Maßnahmen als illegitim wahrgenommen würden. Außerdem wurde kritisiert, dass die parlamentarische Kontrolle der Exekutive im Bereich verdeckter Operationen nicht ausreichend sei. Die Zuständigkeit des ISC sei in diesem Kontext noch nicht definiert (House of Commons, 2014a, S. 794f., 816f.). Ferner ging es darum, deutlich zu machen, dass Maßnahmen stets verhältnismäßig seien:

> »Proportionality is at the gutes of the whole business of international law, human rights and legitimacy. We have to show that proportionality is there and that we have mechanisms and systems to ensure that it is. Simply claiming that it is there will not be good enough.« (Ebd., S. 795)

Die meisten Abgeordneten teilten aber die Einschätzung, dass die Regierung in diesem Bereich aktiv werden müsse, da das Gefahrenpotenzial durch die wachsende Vernetzung stark gestiegen sei. Ein Cyberangriff könne die wirtschaftliche Prosperität nachhaltig beschädigen und im Extremfall sogar zum partiellen Zusammenbruch der Gesellschaft führen (ebd., S. 796f. ebenso 806, 809, 812–815).

Ferner begrüßten Abgeordnete, dass Cyberangriffe zur Erreichung militärischer Ziele genutzt werden könnten, ohne dabei das Leben britischer Soldaten

zu riskieren (ebd., S. 796f.). Aus Sicht der Regierungsabgeordneten waren Cyberkapazitäten zu einem »battle-winning asset« geworden (ebd., S. 804). Das Parlament erwarte daher, dass die Exekutive die entsprechenden Fähigkeiten aufbaue. Russland, China, Nordkorea, Iran und Syrien seien bislang durch Cyberangriffe aufgefallen, die sowohl Regierungen als auch Unternehmen getroffen hätten. Die Exekutive könne diesem Trend nicht tatenlos begegnen (ebd., S. 805, 811).

Um die parlamentarische Kontrolle der neuen Fähigkeiten zu gewährleisten, legte die Regierung Ende 2014 in einem erneuerten Memorandum of Understanding mit dem Intelligence and Security Committee fest, dass das ISC auch mit der Kontrolle offensiver Cybermaßnahmen betraut sein sollte (Intelligence and Security Committee, 2014a, S. 12).

Die Entscheidung, kein eigenständiges Kommando für den Cyberspace zu etablieren, wie bspw. die USA, wurde vereinzelt kritisiert (House of Commons, 2014a, S. 814). Dies liegt maßgeblich darin begründet, dass das Militär eng mit dem GCHQ kooperiert und dass bspw. beim Kampf gegen den Islamischen Staat Cyberangriffe durch den Nachrichtendienst ausgeführt wurden. Die Regierung institutionalisierte die Kooperation zwischen Verteidigungsministerium und GCHQ 2014 in einem National Offensive Cyber Programme (NOCP) (The Times, 2018b). Die Regierung verwies darauf, dass sich diese Zusammenarbeit historisch bewährt habe und auch im Cyberspace erfolgreich sein werde (The Telegraph, 2018).

Die offensive Referenz (Schutz vor wem?) der Beschützer-Rolle wurde mit Verweis auf verschiedene Staaten konkretisiert und deren Notwendigkeit unterstrichen. Kontestationen aus dem Parlament bezogen sich auf die Kontrolle der neuen Fähigkeiten durch das ISC. Dieser Forderung kam die Regierung zügig nach und räumte dem ISC die Zuständigkeit ein. Damit wurde auch aus Sicht vieler Abgeordneter ein wichtiger Schritt zur Wahrung der Rolle als Garant liberaler Grundrechte vollzogen. Bei der konkreten Ausgestaltung des Programms zum Aufbau der Kapazitäten konnte die Regierung wiederum auf historische Erfolge der Streitkräfte und des Nachrichtendienstes hinweisen.

Bereits bei ersten parlamentarischen Fragen danach, wer im Ernstfall digitale Gegenmaßnahmen gegen einen Angriff ergreifen sollte, verwies die Regierung 2014 auf das GCHQ. Nach Analyse im Cyber Security Operations Centre und Rücksprache mit dem Cabinet Office, sollte der Nachrichtendienst ggf. die Reaktionen durchführen (House of Commons, 2013a, S. 41-43). In Anhörungen wurden von VertreterInnen der Streitkräfte darauf hingewiesen, dass Cyberangriffe ein potentes Mittel zu Erreichung militärischer Ziele sein könnten, dass für einen effizienten Angriff aber genaues Wissen über die Ziele vorhanden sein müsse, die daher vorher ausgespäht werden müssten. Ein schneller Gegenschlag könne daher schwierig sein, wenn nicht bereits zuvor in die Systeme eingegriffen wurde (ebd., Ev 14f.). In der Folge verlangten die Abgeordneten des Verteidigungsaus-

schusses von der Regierung eine klarere Positionierung darüber, unter welchen Bedingungen diese Fähigkeiten genutzt werden sollten:

> »There is clearly still much work to be done on determining what type or extent of cyber attack would warrant a military response. Development of capabilities needs to be accompanied by the urgent development of supporting concepts. We are concerned that the then Minister's responses to us betray complacency on this point and a failure to think through some extremely complicated and important issues.« (Ebd., S. 4)

Die Abgeordneten erkannten an, dass Cyberangriffe eine Möglichkeit darstellten militärische Operationen auszuführen, ohne dabei das Leben britischer Soldaten zu gefährden. Die Regierung müsse aber klarstellen, wie diese neue Fähigkeit genutzt werden solle. Außerdem wiesen die Mitglieder des Verteidigungsausschusses darauf hin, dass der Einsatz offensiver Cyberfähigkeiten problematisch werden könne, wenn es um die Abwägung der Verhältnismäßigkeit sowie die sichere Attribution der Angriffe gehe (House of Commons, 2014b, S. 41f.).

Die Regierung beantwortete Fragen nach dem Einsatz nicht direkt, sondern verwies darauf, dass Reaktionen im Einzelfall geprüft werden müssten. So sollte ein Ermessensspielraum gewahrt werden, der auch abschreckend wirken könne. Gegenmaßnahmen erfolgten aber immer unter Vorgaben des Kriegsvölkerrechts (House of Commons, 2013b, S. 7f.).

Bürgerrechtsorganisationen kritisierten den Aufbau militärischer Kapazitäten als eine unangemessene Militarisierung des Netzes, die zu erheblichen Kollateralschäden führen könnte. Ferner sei es bedenklich, dass die offensiven Kapazitäten klandestin entwickelt würden und sich so weitgehend parlamentarischer Kontrolle entzögen (Open Rights Group, 2016a, S. 1, 5).

Diese Kontestation blieb allerdings folgenlos, da sie auch vom Parlament nicht geteilt wurde. Bis Ende 2014 hatte die britische Regierung damit offensive Kapazitäten aufgebaut und dies auch öffentlich eingeräumt. Ermöglicht wurde dies, durch die Referenz (Schutz vor wem?) zu feindlichen Staaten sowie Terrororganisationen und Verweise auf potenzielle physische Folgen von Cyberangriffen. Mit dem Bezug zu Russland wurde die Referenz der Beschützer-Rolle ab 2015 weiter konkretisiert.

### 6.2.2 Einsatz der offensiven Kapazitäten und Russland als neuer Referenzpunkt

Die Notwendigkeit verstärkt auch offensiv im Cyberspace tätig zu werden, wurde 2015 von den Streitkräften unter Verweis auf die Verschränkung konventioneller und digitaler Maßnahmen durch Russland in Estland, Georgien und der Ukraine gerechtfertigt. Diese neue Situation lasse eine klare Unterscheidung zwischen

Krieg und Frieden nicht mehr zu (Ministry of Defence, 2015). Einen Monat nach diesen Aussagen wurde die Verantwortlichkeit für folgenschwere Cyberangriffe vom Cabinet Office auf das Verteidigungsministerium übertragen (House of Commons, 2015c, S. 650).

Die Mitglieder des Verteidigungsausschusses forderten im November 2015 von der Regierung, angesichts der russischen Cyberaktivitäten flexibel auf Angriffe zu reagieren und neue Konzepte zu entwickeln, da eine konventionelle Vergeltungsdrohung für Cyberangriffe, die zumeist keine kinetischen Folgen hätten, wenig glaubhaft sei. Russland habe seine feindseligen Absichten durch Angriffe auf Estland, Georgien, die Ukraine, Deutschland sowie den französischen Fernsehsender TV5 Monde deutlich gemacht (House of Commons, 2015a, S. 12f.). Die Aktivitäten zielten dabei stets darauf, unterhalb der Schwelle eines bewaffneten Angriffs zu bleiben und so auch Artikel 5 des Transatlantikvertrages zu unterlaufen bzw. dessen Anwendbarkeit infrage zu stellen (House of Commons, 2016e, S. 18, 26).

Im Gegensatz zu Deutschland, wo die Absenkung der militärischen Einsatzschwelle auch durch den Bundestag besonders kritisch gesehen wird, unterstützten in Großbritannien viele Abgeordnete ein flexibles digitales, notfalls auch militärisches, Vorgehen.

Auf die neuen offensiven Kapazitäten sowie deren Einsatz ging George Osborne ebenfalls im November 2015 in einer Rede vor MitarbeiterInnen des GCHQ ein. Er verknüpfte hierbei ausdrücklich die nationale und ökonomische Sicherheit: »[…] there will be no economic security for our country without national security. Nowhere is that more true than when it comes to cyber« (UK Government, 2015a). Osborne wies darauf hin, dass mit der gestiegenen Vernetzung und der wachsenden NutzerInnenschaft des Netzes das ursprüngliche vertrauensvolle Verhältnis zwischen den NutzerInnen nicht mehr bestünde. Dies werde durch die Aktivitäten feindlicher Staaten oder Terrororganisationen immer deutlicher. Mit Blick auf die Verantwortung für die Sicherheit des Vereinigten Königreichs, sei es für die Regierung unerlässlich offensive Cyberfähigkeiten zu entwickeln und vorzuhalten, da durch Cyberangriffe mittlerweile auch Menschenleben in Gefahr seien. Die Regierung nehme diese Verantwortung sehr ernst und begegne damit den immer ausgefeilteren Angriffen. Terrorgruppen seien zwar noch nicht in der Lage verheerende Angriffe gegen kritische Infrastrukturen durchzuführen, strebten diese Fähigkeit aber an. Nur die Regierung sei in der Lage, Schutz gegen diese besonders komplexen Angriffe zu gewähren. Der Cyberspace stelle aber einen Raum dar, in dem Angriff stets einfacher sei als Verteidigung. Daher sei es notwendig ein Abschreckungspotenzial aufzubauen. Hierzu gehöre es, ein möglichst schwer zu treffendes Ziel zu sein, Normen für Cyberangriffe zu entwickeln – bspw. die staatliche Sorgfaltsverantwortung – sowie im Ernstfall dazu in der Lage zu sein, zurückzuschlagen (ebd.).

> »We reserve the right to respond to a cyber attack in any way that we choose. And we are ensuring that we have at our disposal the tools and capabilities we need to respond as we need to protect this nation, in cyberspace just as in the physical realm. We are building our own offensive cyber capability – a dedicated ability to counter-attack in cyberspace.« (UK Government, 2015a)

Bei der Entwicklung dieser Fähigkeiten wurde weiterhin auf die Expertise des Verteidigungsministeriums und des GCHQs zurückgegriffen, um zu den besten Ergebnissen zu gelangen. Diese Kapazitäten seien für die Kriegführung im 21. Jahrhundert essenziell (ebd.).

Im Juli 2016 veröffentlichte das Verteidigungsministerium die zweite Auflage des sogenannten Cyber Primer in dem weitere militärische Aspekte der Cybersicherheitspolitik debattiert wurden. Fehlte in der vorangegangenen Auflage noch eine Definition offensiver Cyberoperationen, wurden diese nun erstmals beschrieben:

> »Offensive cyber operations include activities that project force to create, deny, disrupt, degrade and destroy effects in and through cyberspace. These operations may transcend the virtual domain into effects in the physical and cognitive domains.« (Ministry of Defence, 2016a, S. 54)

Die Cyberkapazitäten dienten dabei im Wesentlichen der Konfliktprävention, dem Schutz des Vereinigten Königreichs sowie dem Anspruch, schnell überall auf der Welt Einfluss nehmen zu können. So könnten Cyberangriffe dazu genutzt werden, Ziele zu erreichen die sonst nicht angreifbar wären, ohne eine massive Eskalation nach sich zu ziehen. Als Beispiel hierfür verwies die Regierung auf Stuxnet (ebd., S. 2 bzw. 65).

Die Fähigkeit zur digitalen Abschreckung wurde auch in der Cyber Security Strategy 2016 hervorgehoben. Angreifer müssten damit rechnen, dass die britische Regierung offensive Maßnahmen zur Abwehr von Cyberangriffen anwende (UK Government, 2016f, S. 9f.). Besonders besorgniserregend war aus Sicht der Regierung, dass es eine kleine aber wachsende Anzahl feindlicher Staaten gäbe, die auch destruktive Cyberangriffe entwickelten. Dies stelle eine neue Qualität in der Gefahrenlage dar:

> »[…] a small number of hostile foreign threat actors have developed and deployed offensive cyber capabilities, including destructive ones. These capabilities threaten the security of the UK's critical national infrastructure and industrial control systems. Some states may use these capabilities in contravention of international law in the belief that they can do so with relative impunity, encouraging others to follow suit.« (Ebd., S. 18)

Zur Illustration eines solchen Szenarios verwies die Regierung auf den Angriff auf ukrainische Energieversorger im Dezember 2015, durch den ein Stromausfall ausgelöst wurde, von dem etwa 220.000 BürgerInnen betroffen waren (ebd., S. 21). Die technischen Fähigkeiten von Terrororganisationen reichten nach Einschätzung der Exekutive noch nicht aus, um folgenschwere Angriffe gegen kritische Infrastrukturen durchzuführen (ebd., S. 50). Es sei daher die wichtigste Aufgabe der Administration, das Vereinigte Königreich vor den Angriffen feindlicher Staaten zu schützen, da deren Angriffe die nationale Sicherheit, politische Stabilität sowie wirtschaftliche Leistungsfähigkeit unterminieren könnten. Das NOCP und die Kooperation zwischen GCHQ und Streitkräften sollten daher ausgebaut werden. Weiterhin verfolgte die Regierung das Ziel, das Verhalten von Staaten durch eine offensive Attributionspraxis zu beeinflussen und so nicht-normkonformes Verhalten öffentlich anzuprangern (ebd., S. 26 bzw. 49-51).

Die offensiven Fähigkeiten wurden bei der Vorstellung der neuen Strategie dann direkt mit den Fähigkeiten zur Attribution verknüpft »because the ability to detect, trace and retaliate in kind is likely to be the best deterrent« (UK Government, 2016a). Würde das Vereinigte Königreich auf den Aufbau offensiver Kapazitäten verzichten, bliebe im Ernstfall nur die Wahl, entweder gar nicht zu reagieren oder konventionell zu vergelten. Da aus Sicht der Regierung zwischenstaatlichen Spannungen zukünftig immer Cyberangriffe zur Unterminierung der Verteidigungsfähigkeit vorausgehen würden, wäre der Verzicht auf Vergeltung durch Cyberangriffe unverantwortlich (ebd.).

Eine flexible militärische Beschützer-Rolle war damit sowohl aus Sicht des Parlaments als auch der Regierung essenziell, da die AngreiferInnen gezielt niedrigschwellige Operationen durchführten, die sonst nicht angemessen vergolten werden könnten. Die Aktivitäten Russlands dienten hierzu als mahnendes Beispiel.

Aus Sicht des Verteidigungsministeriums stellte der Cyberspace, den wegweisenden neuen Handlungsraum des 21. Jahrhunderts dar und damit die Nachfolge des Luftraums. Es sei nur eine Frage der Zeit, bis Großbritannien den ersten folgenschweren Cyberangriff erlebe, da eine Vielzahl verschiedener Akteure offensive Fähigkeiten entwickle. Daher sei es wichtig, offensiv handlungsfähig zu sein: »It is important that our adversaries know there is a price to pay if they use cyber weapons against us, and that we have the capability to project power in cyberspace as in other domains« (Ministry of Defence, 2016b).

Gegenüber dem ISC führten VertreterInnen des GCHQ aus, dass im Rahmen des NOCP verschiedene Fähigkeiten aufgebaut würden. Dies umfasse auch Angriffsoptionen mit schwerwiegenden Folgen, die gegen Staaten eingesetzt werden könnten, möglicherweise aber nie zum Einsatz kämen. Primärer Effekt sollte die Abschreckung potenzieller Angreifer sein. Mit Blick auf den Einsatz von Cyberangriffen führten VertreterInnen des GCHQ aus, dass offensive Cyberoperatio-

nen den gleichen rechtlichen Anforderungen unterlägen wie konventionelle militärische Einsätze. Die Abgeordneten stimmten den Einschätzungen des GCHQ weitgehend zu und befürworteten auch den Aufbau offensiver Kapazitäten (Intelligence and Security Committee, 2017, S. 44f.). Sachverständige hatten weiterhin die unklare parlamentarische Kontrolle der offensiven Fähigkeiten bemängelt. Um die Aufsicht zu verbessern, sollte das ISC aus Sicht der ExpertInnen unter anderem personell gestärkt und (auch schon vor Operationsbeginn) detaillierter unterrichtet werden (International Centre for Security Analysis, 2017, S. 3f. bzw. 6f.).

Aus Sicht der Abgeordneten waren die Bestrebungen der Regierung mit Blick auf die Aktivitäten Russlands aber nachvollziehbar, da bspw. Angriffe im Zusammenhang mit den amerikanischen Präsidentschaftswahlen dafür sprächen, dass die bisherige Zurückhaltung staatlicher Akteure zunehmend erodiere. Es sei daher für die Sicherheit unerlässlich gegen derartige Angriffe vorzugehen, weil auch Großbritannien zum Ziel von Angriffen werden könne. In diesem Kontext begrüßten die Abgeordneten ausdrücklich das Angebot des GCHQ Parteien und Abgeordneten bei der Sicherung ihrer Kommunikation zu unterstützen (Intelligence and Security Committee, 2017, S. 31-34).

Auf internationaler Ebene wies die britische Regierung auf drei Entwicklungen hin, die aus ihrer Sicht besonders besorgniserregend waren. Erstens nehme die staatliche Nutzung von Proxies zur Ausführung von Cyberangriffen zu. Zweitens nutzten Staaten Cyberangriffe immer häufiger in Verbindung mit anderen Mitteln des Konfliktaustrages. Dies würde drittens besonders häufig zur Destabilisierung von anderen Staaten eingesetzt und bleibe stets unterhalb der Schwelle eines bewaffneten Angriffs (Foreign & Commonwealth Office, 2017, S. 3).

Die Notwendigkeit im Cyberspace schlagkräftig zu sein, wurde von VertreterInnen der Regierung daher unter Verweis auf derartige staatliche Aktivitäten begründet. Nach der Vergiftung von Sergei Skripal im März 2018 in Salisbury verwies der Direktor des GCHQ explizit auf die Aktivitäten Russlands im Cyberspace:

> »For decades, we have collected intelligence on Russian state capabilities, on their intent and on their posture. And for over twenty years, we've monitored and countered the growing cyber threat they pose to the UK and our allies. […] We'll continue to expose Russia's unacceptable cyber behaviour, so they're held accountable for what they do.« (GCHQ, 2018c)

Mit Blick auf die russischen Aktivitäten konstatierte Fleming, dass die Maßnahmen die Distinktion zwischen Kriminalität und staatlichem Handeln zunehmend verwischten. Insbesondere wies er auf den Einsatz von NotPetya gegen Banken, Energieversorger und staatliche Einrichtungen in der Ukraine hin. Die Operationen Nordkoreas seien ein weiterer Beleg dafür, dass feindliche Staaten den

Cyberspace maßgeblich für ihre Belange einsetzten, WannaCry stehe beispielhaft hierfür. Das GCHQ arbeite daher auch weiterhin eng mit dem Verteidigungsministerium zusammen, um die eigenen Kapazitäten sukzessive zu erweitern (ebd.).

Die Sicht der britischen Regierung auf das Völkerrecht und den Einsatz von Cyberangriffen skizzierte Jeremy Wright im Mai 2018. Hierbei machte er deutlich, dass ein Cyberangriff unter der Schwelle eines bewaffneten Angriffs nicht illegitim sei und auch das staatliche Souveränitätsprinzip (Artikel 2(7)) nicht notwendigerweise verletze.

> »Some have sought to argue for the existence of a cyber specific rule of a ›violation of territorial sovereignty‹ in relation to interference in the computer networks of another state without its consent. […] Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is therefore that there is no such rule as a matter of current international law.« (UK Government, 2018b)

Diese Interpretation deckt auch die Praxis offensiven nachrichtendienstlichen Hackens, wie sie von Großbritannien praktiziert wird. Eine illegale Intervention liegt aus Sicht der britischen Regierung erst dann vor, wenn Staaten nicht mehr »free from external, coercive intervention in the matters of government« seien, sie also bspw. bei politischen Wahlen beeinflusst würden (ebd.).[6]

Außerdem betonte Wright die staatliche Sorgfaltsverantwortung für Angriffe auch von »individuals acting under its instruction, direction or control« (ebd.). Dieser Verantwortung könnten sich Staaten nicht durch die Nutzung von Proxies entziehen. Die Regierung verfolge daher die Praxis, Cyberangriffe öffentlich zu attribuieren, sofern sie dies für zielführend erachte, um regelgeleitetes Verhalten im Cyberspace zu fördern. Wright verwies in diesem Zusammenhang explizit auf den Wurm WannaCry, der das britische NHS substanziell beeinträchtigt hatte sowie auf die Ransomware NotPetya. Die britische Regierung forderte andere Staaten auf, sich diesen Bemühungen anzuschließen, um die Glaubwürdigkeit der Zuschreibungen zu erhöhen (ebd.). Die Regierung hatte bereits im Dezember 2017 offiziell die Lazarus Group bzw. Nordkorea für WannaCry verantwortlich gemacht. Aus Sicht der Exekutive nutzte das Regime in Pjöngjang Cyberangriffe, um Sanktionen zu umgehen. Ein Vertreter des britischen Außenministeriums

6 Diese Bezugnahme ist auch Ergebnis der britischen Erfahrungen während des Referendums zum Austritt aus der Europäischen Union. In diesem Kontext gab es den Verdacht, Russland habe die Abstimmung zu manipulieren versucht (The Guardian, 2019a; The New York Times, 2017).

betonte, dass dieses Verhalten inakzeptabel sei und dass die nordkoreanische Regierung dafür mit Gegenmaßnahmen zu rechnen habe (UK Government, 2017a).

Die britische Regierung vertrat ferner die Ansicht, dass auf einen Cyberangriff nicht in gleicher Weise reagiert werden müsse, sondern, dass alle Maßnahmen zulässig seien, die notwendig und verhältnismäßig seien (UK Government, 2018b). Das Risiko eines durch militärische Offensivkapazitäten geprägten Cyberspace, sah die britische Regierung nicht. Vielmehr betonte sie, dass es das Recht eines jeden Staates sei, solche Fähigkeiten aufzubauen, da die Staaten bei deren Einsatz an das Völkerrecht gebunden seien. Wright illustrierte dies am Beispiel eines Angriffs auf zivile Flugleitsysteme, der egal mit welchen Mitteln er ausgeführt würde, einen klaren Bruch des Völkerrechts darstelle. Genauso verhalte es sich bei Angriffen auf medizinische Einrichtungen. Legitim seien aber Angriffe im Rahmen bewaffneter Auseinandersetzungen wie bspw. gegen Terrororganisationen, um deren Kampffähigkeit zu beeinträchtigen (ebd.).

Wie die deutsche Regierung erkannte auch die britische Exekutive keine wesentlichen Regulierungslücken im internationalen Recht.

Der Ankündigung, Cyberangriffe künftig häufiger öffentlich zu attribuieren, folgten noch im gleichen Jahr mehrere Zuschreibungen. Im März hatte die US Regierung eine Gruppe iranischer HackerInnen beschuldigt, unter anderem Angriffe gegen Universitäten durchgeführt zu haben. Die britische Regierung teilte diese Einschätzung und begrüßte das Vorgehen der US-Administration (UK Government, 2018a). Im September 2018 wies Premierministerin Theresa May auf die russischen Cyberaktivitäten unter anderem zur Beeinflussung von demokratischen Wahlen hin (House of Commons, 2018c, S. 169). Medienberichten zufolge, plante die Regierung nach der Vergiftung von Sergei Skripal in Salisbury Vergeltungsmaßnahmen im Cyberspace. Treffen sollten diese Angriffe den russischen Militärgeheimdienst GRU sowie assoziierte (kriminelle) Gruppen. Sie sollten darauf ausgerichtet sein, deren Operationsfähigkeit einzuschränken oder den Zugang zu Finanzmitteln zu begrenzen (The Times, 2018a). Im Parlament räumte die Premierministerin diese Möglichkeiten zumindest theoretisch ein (House of Commons, 2018a, S. 633). Der Direktor des GCHQ bezeichnete die Bedrohung durch Russland als sehr real. Um Russland in seinen Bestrebungen, die internationale Ordnung zu unterminieren, zu stoppen, müsse der Herausforderung mit unterschiedlichen Maßnahmen begegnet werden (GCHQ, 2018a).

Im Oktober 2018 gab das NCSC bekannt, dass nach Auffassung der britischen Sicherheitsbehörden der russische Militärgeheimdienst GRU für eine Reihe prominenter Cyberangriffe verantwortlich war, darunter Attacken zur Destabilisierung von Demokratien. Nach Einschätzung der britischen Regierung war der GRU unter verschiedenen Namen bekannt, darunter APT 28, Fancy Bear, Sofacy, Pawnstorm, Sednit, CyberCaliphate, Cyber Berkut, Voodoo Bear, BlackEnergy Ac-

tors, STRONTIUM, Tsar Team, Sandworm.[7] Die Angriffe verstießen aus Sicht des Außenministers offensichtlich gegen internationales Recht:

> »The GRU's actions are reckless and indiscriminate: they try to undermine and interfere in elections in other countries; they are even prepared to damage Russian companies and Russian citizens. This pattern of behaviour demonstrates their desire to operate without regard to international law or established norms and to do so with a feeling of impunity and without consequences. [...] Our message is clear: together with our allies, we will expose and respond to the GRU's attempts to undermine international stability.« (UK Government, 2018d)

Im Dezember 2018 gab die britische Regierung ferner bekannt, dass die Gruppe APT 10, die für zahlreiche Spionageangriffe verantwortlich gemacht wurde, für die chinesische Regierung arbeite bzw. sehr enge Verbindungen zum Ministerium für Staatssicherheit habe. Mit den Angriffen verstoße die chinesische Regierung in flagranter Weise gegen ein bilaterales Abkommen mit dem Vereinigten Königreich sowie gegen Ziele der G20, die den Diebstahl geistigen Eigentums verbieten (UK Government, 2018c). Für Angriffe gegen Georgien im Oktober 2019 machte der britische Außenminister wiederum den russischen Militärgeheimdienst GRU verantwortlich (UK Government, 2020).

Die offensive Attribution wurde damit auch durch die Rollen als Garant liberaler Grundrechte und Wohlstandsmaximierer ermöglicht, die die Gewährleistung demokratischer Wahlen und die wirtschaftliche Wettbewerbsfähigkeit beinhalten. Sie wirkten damit katalytisch auf den Ausbau der Beschützer-Rolle. Die Fähigkeit zur Attribution und zur Vergeltung im Cyberspace wurden ferner zu einem wesentlichen Teil der flexiblen militärischen Beschützer-Rolle im Cyberspace. Die Regierung folgte damit den Praktiken der vermeintlichen Angreifer und versuchte deren Operationen zu kontern.

International war die britische Regierung in diesem Zuge die erste, die 2018 der NATO offensive Cyberfähigkeiten angeboten hat (House of Commons, 2019, S. 1200).

Für die Jahre 2018-2020 wurden dem Verteidigungsministerium zusätzlich 1,8 Mrd. Pfund zur Verfügung gestellt, die für die Entwicklung offensiver Cybermaßnahmen sowie die Bekämpfung von U-Booten und das Nuklearwaffenarsenal vorgesehen wurden (Treasury, 2018, S. 76).

---

7 Die deutsche Regierung schloss sich der Einschätzung, dass die russische Regierung für die Angriffe (darunter der Bundestagshack 2015) verantwortlich sei, offiziell an. Zuvor wurde dies nur in deutschen Geheimdienstkreisen für sehr wahrscheinlich gehalten (Spiegel, 2018; Zeit, 2018).

Ebenfalls 2018 wurde öffentlich bekannt, dass im Kampf gegen Daesh in Kooperation zwischen GCHQ und den Streitkräften systematisch offensive Cyberoperationen durchgeführt worden waren. Diese hätten sowohl die Kommunikations- als auch Operationsfähigkeit der Terrororganisation substanziell unterminiert: »This is the first time the UK has systematically and persistently degraded an adversary's online efforts as part of a wider military campaign« (GCHQ, 2018c). In diesem Kontext sei eine ganze Reihe unterschiedlicher Angriffstechniken zum Einsatz gekommen. Die Attacken reichten dabei von der Blockade von Diensten, bis zur Zerstörung von technischem Equipment.[8] Aus Sicht des GCHQ waren die Maßnahmen dabei sehr erfolgreich. Jeremy Fleming betonte, dass die Angriffe stets im Rahmen der nationalen und internationalen rechtlichen Regelungen durchgeführt wurden und dass die demokratische Kontrolle der Operationen gewährleistet sei. KritikerInnen, die dies bestritten hatten, warf er vor, die Wertvorstellungen sowohl im Geheimdienst als auch bei den Streitkräften nicht verstanden zu haben (ebd.).

Um auch in Zukunft offensiv im Cyberspace aktiv sein zu können, bedürfe es eines kontinuierlichen Trainings der eigenen Kräfte. Dies geschehe im Vereinigten Königreich regelmäßig in der Kooperation zwischen dem Verteidigungsministerium und dem GCHQ. Nur auf diesem Weg ließe sich lernen, wie die eigenen Fähigkeiten im Ernstfall am besten eingesetzt werden sollten. Letztlich ging es darum, die Sicherheit des Vereinigten Königreichs zu gewährleisten, Daher sei es wichtig, »[..] to make the UK harder to attack, better organised to respond when we are, and able to push back if we must« (ebd.). Mit Blick auf die Gefahrenlage verwies die Regierung erneut auf die russischen Aktivitäten (Foreign & Commonwealth Office, 2019). Die besondere Bedeutung der Abschreckung, insbesondere gegenüber Russland, betonte im März 2019 auch Außenminister Jeremy Hunt. Er verwies in diesem Kontext explizit darauf, dass die westlichen Staaten die Kapazitäten aufbauen müssten, um ihre demokratischen Systeme vor externen Einflussnahmen zu schützen. Vergeltung müsse dabei nicht immer durch Cyberangriffe erfolgen, eine erfolgreiche Abschreckung müsse aber verschiedene Optionen glaubwürdig abdecken können (UK Government, 2019b).

Die enge Kooperation zwischen dem Nachrichtendienst und den Streitkräften wird in naher Zukunft weiter ausgebaut. Die britische Regierung hat angekündigt, eine neue National Cyber Force bestehend aus VertreterInnen des GCHQ und den Streitkräfte zu gründen (Ministry of Defence, 2019). Die neue Einheit soll offensive Cybermaßnahmen entwickeln und durchführen. Der Kommandeur des Joint Forces Command betonte, dass der Aufbau der neuen Kräfte für die

8 Medienberichten zufolge führte das GCHQ im Zusammenspiel mit Spezialkräften bspw. Angriffe auf Systeme von IS-Kommandeuren aus, um deren Kommunikation zu manipulieren und sie dann in Hinterhalte zu locken (Sky News, 2018).

sicherheitspolitische Handlungsfähigkeit besonders wichtig sei: »By adopting offensive cyber techniques in the UK we are levelling the playing field and providing new means of both deterring and punishing states that wish to do us harm« (Sky News, 2018).

KritikerInnen bemängelten die geheime Natur der neuen Einheit und den fehlenden demokratischen Diskurs über den Einsatz von CNOs (The Guardian, 2020).

Neben der flexiblen militärischen Beschützer-Rolle, die durch die Maßnahmen hybrider Kriegführung Russlands ermöglicht wurde, hat die britische Regierung zudem die offensiven Kapazitäten zur Unterstützung militärischer Operationen ausgebaut und genutzt. Die Einsätze gegen den Islamischen Staat stehen exemplarisch hierfür.

## 6.3 Zwischenfazit

Beide Untersuchungsstaaten haben in den vergangenen 20 Jahren die militärischen Beschützer-Rollen ausgebaut und Kapazitäten zum offensiven Wirken in gegnerischen Netzen etabliert. Sowohl in der Bundesrepublik als auch in Großbritannien lag die Referenz (Schutz für wen?) der Rolle zunächst auf dem Schutz militärischer Infrastrukturen und verschob sich dann durch Bezugnahmen zur kritischen Infrastruktur zunehmend hin zur Landesverteidigung. Wie im Vereinigten Königreich wurde auch in Deutschland nach 2016 auf die Notwendigkeit des Schutzes des demokratischen Systems verwiesen, sodass der Ausbau der Beschützer-Rolle auch unter Verweis auf die Rolle als Garant liberaler Grundrechte begünstigt wurde.

Deutschland hat sich international früh für eine Kultur der Zurückhaltung im Cyberspace ausgesprochen. Im Rahmen der OSZE konnte die Bundesregierung erfolgreich für eine emergente Norm zum Nichtangriff von kritischen Infrastrukturen werben. Die Unterstützung einer Kultur der Zurückhaltung stand aber von Beginn an in einem Spannungsverhältnis zum Aufbau eigener CNO-Kräfte und der Etablierung der offensiven Beschützer-Rolle. Wie diese agieren sollten, ohne Schadsoftware zu entwickeln bzw. zu verwenden, blieb von Beginn an unklar. Auch die später von der Regierung entwickelte Einsatzdoktrin, die die Nutzung von Verschleierungstechniken zum verdeckten Operieren in gegnerischen Netzen vorsieht, konterkariert eine verifizierbare Kultur der Zurückhaltung. Mit Blick auf den Aufbau offensiver Kapazitäten hat die Regierung auf die besondere Präzision und die vergleichsweise geringen kinetischen Effekte von digitalen Maßnahmen verwiesen. Cyberangriffe sind aus dieser Perspektive ein besonders schonendes Mittel zur Erfüllung der militärischen Beschützer-Rolle, die sonst einen konventionellen Angriff nötig gemacht hätte. Die Etablierung des Kdo CIR wurde einer-

seits durch zunehmend ausgefeiltere Angriffe sowie andererseits durch Verweis auf die NATO-Partner ermöglicht, da die Bundesregierung die Kooperationsfähigkeit der deutschen Streitkräfte in diesem Gebiet verbessern wollte.

Die deutschen Bestrebungen zu einer insgesamt zurückhaltenden militärischen Nutzung des Netzes standen nicht nur in einem gewissen Spannungsverhältnis zum Aufbau eigener Kapazitäten, sie wurden auch international bspw. durch die britische Regierung herausgefordert, die sich früh gegen eine zu weitgehende Regulation militärischer Cyberkapazitäten stellte und als erste öffentlich die eigenen offensiven Kapazitäten bekanntgab. Die britische Regierung hat für sich stets in Anspruch genommen, alle Möglichkeiten nutzen zu können.

Beide Regierungen haben betont, dass für den Einsatz militärischer Cyberangriffe die gleichen Regelungen gelten sollten wie für konventionelle vergleichbare Einsätze des Militärs. In Deutschland hat die Bundesregierung dem Parlament versichert, dass ein konstitutives Mandat notwendig ist. In Großbritannien wurde das ISC mit der Kontrolle betraut. Mit Blick auf internationales Recht haben ebenfalls beide Regierungen darauf verwiesen, dass die völkerrechtlichen Vorgaben auch für den Einsatz von Cyberangriffen gelten. Sie haben in diesem Kontext ferner wiederholt das Prinzip der Sorgfaltsverantwortung betont und die Nutzung von Proxies verurteilt. Eine umfassende Kontrolle des Netzes zur Prüfung normkonformen Verhaltens wird aber durch die Rolle als Garant liberaler Grundrechte beschränkt.

Der Aufbau der Beschützer-Rolle wurde in beiden Staaten durch die Furcht vor folgenreichen Cyberangriffen und immer fähigeren AngreiferInnen begünstigt. Insbesondere nach Stuxnet wurde die Beschützer-Rolle durch Verweis auf diese Vulnerabilität gerechtfertigt. Beide Staaten waren in den letzten Jahren dann aber mit niedrigschwelligen Cyberangriffen staatlichen Ursprungs konfrontiert und haben hierauf unterschiedlich reagiert. Aufgrund der historischen Erfahrungen beim Einsatz der Streitkräfte, ist die Rolle der Bundeswehr jenseits der Landesverteidigung bzw. eines durch den Bundestag mandatierten Einsatzes nicht möglich. Debatten über einen niedrigschwelligeren Einsatz der Bundeswehr und einen neuen »Cyber-Verteidigungsfall« sind aufgrund verfassungsrechtlicher Bedenken und historischer Erfahrungen bislang ergebnislos geblieben. Außerdem ist die offensive Ausrichtung der Bundeswehr Kontestation auch aus dem Parlament ausgesetzt. Der deutschen Beschützer-Rolle fehlt eine klare Referenz (Schutz vor wem?) und Einsatzschwelle. Die Regierung scheint sich bisher noch nicht im Klaren darüber zu sein, ob bzw. wie sie die Kapazitäten angesichts niedrigschwelliger Angriffe verwenden soll und wie die Kompetenzen zwischen den unterschiedlichen Institutionen verteilt werden sollen. Die historisch gewachsene Ordnung der Beschützer-Rolle im deutschen Föderalismus sowie das Trennungsgebot stellen die Bundesregierung hier vor besondere Aufgaben.

In Großbritannien ist die militärische Beschützer-Rolle zwischen den Streitkräften und dem GCHQ geteilt. Dies wurde durch die positiven historischen Erfahrungen und den bereits im Bereich der Nachrichtendienste hervorgehobenen guten Ruf des GCHQs ermöglicht. Die britische Regierung hat im Rahmen dieser Kooperation Angriffstechniken entwickelt, die für folgenschwere Cyberangriffe genutzt werden können. Sie sieht diese Kapazitäten als Mittel zur Abschreckung. Um auf die niedrigschwelligen Angriffe verhältnismäßig zu reagieren, hat das GCHQ unterschiedliche Angriffsvarianten entwickelt. Die Referenz (Schutz vor wem?) der Rolle liegt mittlerweile auf Russland, das spätestens mit der Vergiftung von Sergei Skripal zu einem wesentlichen Referenzpunkt der Beschützer-Rolle wurde. Die britische Regierung hat die offensiven Kapazitäten aber auch zur Ergänzung des Einsatzes gegen den Islamischen Staat offensiv genutzt und sie so mit ihren konventionellen Fähigkeiten verschränkt.

Die wesentlichen Einflüsse, die die Entwicklung der Cybersicherheitspolitiken geprägt haben, sind in den Tabellen 7 und 8 schematisch dargestellt.

*Tabelle 7: Schematische Darstellung der Einflüsse auf die Politikentwicklung im Bereich des Militärs in der Bundesrepublik Deutschland: Wirkung auf die Beschützer-Rolle, – = kontestierend, + = katalytisch. Quelle: Eigene Darstellung*

| | **domestische Ebene** | | | | **internationale Ebene** | |
|---|---|---|---|---|---|---|
| | Historisches Selbst | Wirkung | Rollenbezüge | Wirkung | signifikante / organisierte Andere | Wirkung |
| Aufbau militärischer Kapazitäten (2000 - 2015) | Autokratische Erfahrungen | – | | | UN / OSZE / NATO | |
| (Schonende) Offensive und aktive Verteidigung (2015 - 2019) | Autokratische Erfahrungen | – | Garant liberaler Grundrechte | + | UN / NATO | + |

*Tabelle 8: Schematische Darstellung der Einflüsse auf die Politikentwicklung im Bereich des Militärs im Vereinigten Königreich: Wirkung auf die Beschützer-Rolle, – = kontestierend, + = katalytisch. Quelle: Eigene Darstellung*

| | **domestische Ebene** | | | | **internationale Ebene** | |
|---|---|---|---|---|---|---|
| | Historisches Selbst | Wirkung | Rollenbezüge | Wirkung | signifikante / organisierte Andere | Wirkung |
| Aufbau militärischer Kapazitäten (2000 - 2015) | GCHQ, MoD | + | | | UN / NATO | |
| Einsatz der offensiven Kapazitäten (2015 - 2019) | GCHQ, MoD | + | Garant liberaler Grundrechte | + | UN / NATO / USA / RUS | + |

# 7. Fazit: Cybersicherheit zwischen Innen- und Außenpolitik

Die Studie ist mit dem Ziel gestartet, zu untersuchen, wie sich die deutschen und britischen Cybersicherheitspolitiken zwischen 1995 und 2019 entwickelt haben und was diese Entwicklungen ermöglicht hat. Sie hat dazu ein rollentheoretisches Zwei-Ebenen-Spiel eingeführt, um die innen- und außenpolitischen Rollenspiele miteinander in Bezug zu setzen, ohne einem der beiden Priorität einzuräumen. Um ein differenziertes Bild der Cybersicherheitspolitiken zu zeichnen und pauschale Befunde der Sekuritisierung zu qualifizieren, hat die Arbeit die Cybersicherheitspolitiken entsprechend der rollentheoretischen Konzeption in drei Handlungskontexte unterteilt. Diese unterscheiden sich durch ihre Akteurskonstellationen. Im Bereich der Strafverfolgung steht die Regulation des Verhaltens nichtstaatlicher Akteure im Vordergrund. Im Bereich der Nachrichtendienste und des Militärs geht es dagegen um die Regelung staatlichen Verhaltens und damit um Selbstregulation der Regierungen. Dieses Kapitel wird im Folgenden die Ergebnisse der Untersuchung kurz zusammenfassen.

Dazu werden zunächst die empirischen Befunde vorgestellt. Im ersten Schritt wird dabei die Entwicklung der Cybersicherheitspolitiken kurz nachgezeichnet und die Unterschiede zwischen den beiden Untersuchungsstaaten herausgearbeitet. Insbesondere wird hierbei das dynamische Verhältnis von außen- und innenpolitischen Einflüssen betont. Im zweiten Schritt wird erörtert, welche Implikationen sich aus diesen Politiken für die internationale Ordnung der Cybersicherheit und das Netz ergeben. Im zweiten Teil des Fazits wird die Nützlichkeit des Zwei-Ebenen-Rollenspiels auch mit Blick auf theoretische Alternativen evaluiert. Abgeschlossen wird das Fazit mit einem Blick auf die Limitation der Untersuchung sowie einem Ausblick auf die weitere Forschung zu Cybersicherheitspolitiken.

## 7.1 Empirische Befunde

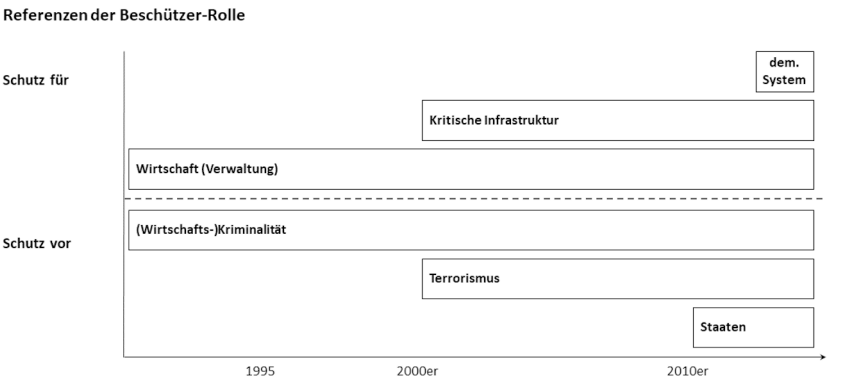
### 7.1.1 Entwicklung der Cybersicherheitspolitiken

Die Untersuchung hat gezeigt, dass die empirischen Sekuritisierungsbefunde, die lange die theoriegeleitete Analyse von Cybersicherheitspolitiken geprägt haben, durch die Unterscheidung zwischen drei Untersuchungsbereichen deutlich ausdifferenziert werden können. Die Studie konnte zeigen, dass die Politiken durch die unterschiedlichen (domestischen wie internationalen) signifikanten Anderen sowie durch unterschiedliche Referenzen auf das historische Selbst ermöglicht wurden. In den Untersuchungsstaaten haben sich dabei unterschiedliche Dynamiken zwischen dem domestischen und internationalen Rollenspiel ergeben. Die empirischen Befunde werden im Folgenden im Kontext der forschungsleitenden Annahmen kurz zusammengefasst.

1. *Die Regierungen beider Untersuchungsstaaten haben im Laufe des Untersuchungszeitraums ihre Beschützer-Rollen in der Cybersicherheitspolitik erweitert.*

In beiden Untersuchungsstaaten und über das gesamte Spektrum der drei Analysebereiche hinweg, ergibt sich über den Untersuchungszeitraum ein Aufwachsen der Beschützer-Rollen der Regierungen. Dies zeigt sich in der Inklusion zusätzlicher schützenswerter Referenzobjekte, im Bezug zu immer gefährlicheren AngreiferInnen und in den daraus folgenden Kompetenzzuwächsen der Sicherheitsbehörden. Damit hat sich die doppelte Referenz der Beschützer-Rollen (Schutz für wen/was bzw. Schutz vor wem) über den Untersuchungszeitraum verändert. Die Frage nach dem Schutz für wen wurde zunehmend universeller beantwortet. Der Katalog abzuwehrender AngreiferInnen erweiterte sich ebenfalls. Waren die Beschützer-Rollen zu Beginn noch auf den Schutz der Wirtschaft ausgerichtet, wurden durch die zunehmende Vernetzung und die damit verbundene (physische) Verwundbarkeit immer mehr Referenzobjekte schutzbedürftig. Die Entwicklung der Straftatbestände spiegelt so exemplarisch die Lösung vom Referenzobjekt Wirtschaft und die veränderte Einschätzung der Fähigkeiten von AngreiferInnen wider. In beiden Untersuchungsstaaten haben die Regierungen die Beschützer-Rollen durch Bezüge zu den kritischen Infrastrukturen und deren essenzieller gesellschaftlicher Bedeutsamkeit erweitert, da durch die Verknüpfung von Cyberangriffen mit kritischen Infrastrukturen kinetische Folgen realistischer wurden. Die Prävention von internationalem Terrorismus war ab den 2000er Jahren prägend. Nach dem Bekanntwerden von Stuxnet wiesen beide Regierungen ferner auch auf die Gefahr von staatlichen Cyberangriffen hin. Mit dem demokratischen System erhielt die Rolle zudem ein weiteres Schutzgut. Dies folgte insbesondere auf die Vorwürfe, Russland habe versucht den US-Präsidentschaftswahlkampf durch Cyberangriffe zu manipulieren. Die Entwicklung ist in der Abbildung 3

*Abbildung 3: Entwicklung der Referenzen der Beschützer-Rollen, Quelle: Eigene Darstellung*




schematisch dargestellt. Soweit entspricht dieser Befund den eingangs erwähnten Studien zur Sekuritisierung bspw. in den USA.

Beide Regierungen haben in allen drei Untersuchungsbereichen ferner damit begonnen, selbst offensive Fähigkeiten aufzubauen. In den drei Handlungskontexten unterminieren die Regierungen IT-Sicherheit zur Aufrechterhaltung der Beschützer-Rollen. Sie haben diesen Aufbau eingeleitet, um einerseits das klassische sicherheitspolitische Handlungsrepertoire zu erweitern und um andererseits neuen digitalen Angriffsformen zu begegnen. Im Bereich der Strafverfolgung nutzen die Polizeibehörden Schadsoftware zum Abhören von Kriminellen oder Terrororganisationen. Die Nachrichtendienste überwachen Kommunikationsvorgänge im Internet, um (externe) Gefahren zu identifizieren und die Streitkräfte greifen auf Sicherheitslücken zurück, um militärische Operationen zu flankieren oder zu ersetzen.

Die Entwicklungen in den drei Bereichen unterscheiden sich aber deutlich. Die Politiken wurden dabei sowohl durch das innen- als auch das außenpolitische Rollenspiel beeinflusst.

> *2. Die Beschützer-Rollen unterscheiden sich in den drei Untersuchungsbereichen aufgrund der Interaktion mit unterschiedlichen signifikanten Anderen (domestisch wie international) und aufgrund unterschiedlicher historischer Selbstbezüge. Die Regierungen müssen ihre Positionen in einem rollentheoretischen Zwei-Ebenen-Spiel einnehmen und sind dabei auf komplementäre Rollenübernahmen durch signifikante Andere angewiesen. Beide Rollenspiele stehen dabei in interaktivem Austausch und können sich gegenseitig beeinflussen.*

Im Bereich der Strafverfolgung etablierten beide Staaten neue Straftatbestände. Was als illegitimes Verhalten in diesem Bereich gewertet werden sollte, wurde daher relativ schnell festgelegt. Da diese Bezüge der Beschützer-Rollen unter vielen

demokratischen Staaten ähnlich waren und da Cyberkriminalität international ein wachsendes Problem darstellte, waren sie auch international anschlussfähig. Dies ermöglichte eine internationale Harmonisierung der gesetzlichen Regelungen im Europarat und in der EU. Die internationale Kooperation zur Strafverfolgung wurde vereinfacht, da die Referenz auf der Regulation nichtstaatlicher Akteure – also Dritter – lag.

Die Etablierung der Verhaltensstandards für nichtstaatliche Akteure und deren Explikation in Straftatbeständen verlief in beiden Untersuchungsstaaten relativ ähnlich. Die britische Regierung konnte aber bereits früher eine expansivere Beschützer-Rolle etablieren. Sie zeigt sich unter anderem in höheren Strafmaßen, in der Sanktionierung jeglicher Hackingaktivitäten und in den Bestrebungen, Verschlüsselung restriktiver zu regulieren. Dies wurde durch die Bezüge zum historischen Selbst – die Erfahrungen mit Terrorismus in Nordirland ermöglicht. Die Referenz der Rolle (Schutz vor wem?) lag damit schon von Beginn an auf gefährlicheren AngreiferInnen. Aufgrund der domestisch relativ stabilen Beschützer-Rolle, konnte die britische Regierung ihre Rolle sogar extraterritorial ausdehnen. Sie nimmt so in Anspruch, auch ausländische Dienstleister zur Entschlüsselung zu zwingen. Mit Blick auf die Regulation von Verschlüsselung verfolgte die deutsche Regierung eine liberalere Politik, da es substanzielle domestische Kontestationen, gestützt auf Bezüge zum negativen historischen Selbst, gab. Außerdem wurde diese Ablehnung auch durch das internationale Rollenspiel ermöglicht in dem die Bundesrepublik eine globalisierte Beschützer-Rolle der USA ablehnte, da diese die eigenen Rollen zu unterminieren drohte. Während die britische Regierung aus einer stabilen domestischen Beschützer-Rolle heraus auch international (insbesondere im Rahmen der 5-Eyes) für eine stärkere Regulation von Verschlüsselung warb bzw. noch wirbt, ist die deutsche Regierung sowohl durch das domestische als auch durch das internationale Rollenspiel einer solchen Regulation gegenüber skeptischer. Die deutsche Regierung konnte in der domestischen Sphäre ferner die eigene Beschützer-Rolle noch nicht stabilisieren. Kontestationsprozesse aus Zivilgesellschaft und Opposition sorgten, gestützt auf Gerichtsurteile, dafür, dass die Regierung die Beschützer-Rolle anpassen bzw. beschränken musste. Die domestischen Kontestationen und die Rolle als Garant liberaler Grundrechte begrenzen auch die außenpolitische Kooperationsbereitschaft der Bundesregierung, so steht die Bundesregierung europäischen Bemühungen skeptisch gegenüber, externen Ermittlungsbehörden Zugriff auf digitale Spuren in Deutschland zu gewähren. Die britische Regierung hat demgegenüber ein solches Abkommen zum gegenseitigen Datenzugriff mit den USA abgeschlossen. Dies wurde durch eine domestisch stabilere Beschützer-Rolle sowie die besonderen Beziehungen zu den USA erleichtert.

Im Bereich der Nachrichtendienste zeigt sich eine deutliche Differenz in der Einschätzung, was als akzeptables staatliches Verhalten gilt. Die deutsche

Bundesregierung versuchte sich nach den Snowden-Enthüllungen zunächst domestisch und international der eigenen Beschützer-Rolle zu versichern. Sie tat dies durch die innenpolitische Aufklärung der Vorwürfe sowie internationale Verhandlungen über ein Abkommen zur Begrenzung gegenseitiger Spionage. Durch die ablehnenden Reaktionen der amerikanischen und britischen Regierungen frustriert, versuchte die deutsche Administration domestisch durch die Kündigung kommerzieller Verträge mit amerikanischen Dienstleistern und international durch die Unterstützung neuer transatlantischer Internetkabel, den physischen Zugriff auf Internetkommunikation zu erschweren. Außerdem ergänzte die Regierung die Referenz der Beschützer-Rolle (Schutz vor wem?), um auch Aktivitäten befreundeter Nachrichtendienste aufzudecken und ggf. zu verfolgen. Eine innenpolitisch geforderte, konfrontative Haltung gegenüber den USA wurde durch die Regierung aber aufgrund der internationalen Abhängigkeit abgelehnt. Da eine internationale Aufarbeitung der Vorwürfe keine Erfolge zeigte und die Enthüllungen auch den Verdacht genährt hatten, der deutsche BND sei möglicherweise Komplize der NSA gewesen, wurden die Enthüllungen domestisch durch den NSA-Untersuchungsausschuss aufgearbeitet. Hierbei wurde deutlich, dass der BND selbst zahlreiche problematische Praktiken etabliert hatte. Das führte zu domestischen Kontestationsprozessen und der Forderung, neue gesetzliche Regelungen für den Auslandsnachrichtendienst zu erlassen. Diese Neuregelung führte in der Folge aber nicht zu einer Begrenzung der eigenen Beschützer-Rolle, sondern, unter Verweis auf bestehende Gefahren (insbesondere den internationalen Terrorismus) und die Notwendigkeit des Informationsaustauschs, zu einer Rechtfertigung zahlreicher zuvor enthüllter Praktiken. Allerdings beschränkte die Bundesregierung explizit die Tätigkeiten des BND mit Blick auf europäische Ziele so, dass der ursprünglichen Kritik der Kanzlerin am Ausspähen unter Freunden, eine Beschränkung der eigenen Beschützer-Rolle folgte. Sie begrenzte damit die Referenz (Schutz vor wem?) der Rolle und etablierte hohe Anforderungen für die Überwachung europäischer Ziele.

In Großbritannien reagierte die Regierung offensiv auf die Enthüllungen und suchte die Funktionsfähigkeit der Beschützer-Rolle unter anderem durch das Vorgehen gegen den Guardian zu wahren und weitere Publikationen zu verhindern. Die britische Regierung wurde domestisch mit weniger Kontestationen der Beschützer-Rolle konfrontiert als die deutsche. Die historischen Selbstbezüge erlaubten der Regierung im Vereinigten Königreich dabei gleich in doppelter Hinsicht eine expansivere Beschützer-Rolle. Einerseits konnte sie zum Nachweis der Notwendigkeit weitreichender sicherheitspolitischer Maßnahmen auf die historischen Erfahrungen mit Terrorismus verweisen. In diesem Kontext wurde der Auf- und Ausbau der Beschützer-Rolle unter Bezugnahme auf Terrorismus in Nordirland sowie auf die Anschläge vom 7. Juli 2005 in London gerechtfertigt. Damit war die Gefahrensituation für das Vereinigte Königreich stets präsenter. Anderer-

seits konnte die Regierung auf die historischen Leistungen der Sicherheitsbehörden verweisen. Das GCHQ als zentrale Institution für die britische Cybersicherheitspolitik genießt unter allen politischen Parteien einen ausgezeichneten Ruf. Auch überwachungsskeptische PolitikerInnen betonten die historischen Leistungen des Nachrichtendienstes. Historischer Bezugspunkt war dabei zumeist der Zweite Weltkrieg und die Erfolge, die durch die Entschlüsselung deutscher Kommunikation möglich wurden. Die vergangenen Herausforderungen wurden dabei auf eine Stufe mit der aktuellen Gefahrenlage gestellt und erforderten so auch im Cyberspace einen handlungsfähigen Nachrichtendienst. Dieses Vertrauen in die Institution, das von zahlreichen domestischen signifikanten Anderen geteilt wurde, ermöglichte es der britischen Regierung insgesamt eine deutlich offensivere und weitreichendere Beschützer-Rolle einzunehmen. International wurde die Ausrichtung des Nachrichtendienstes folglich nicht angepasst. Aus Sicht der Regierung ist es für die Sicherheit im Vereinigten Königreich zudem zentral, dass das GCHQ international als technisch versiert und auf Augenhöhe mit der NSA wahrgenommen wird. So wird aus Sicht der Regierung eine Kooperation mit dem GCHQ attraktiv und der Datenaustausch gesichert. Die Einbettung in den Kreis der 5-Eyes stabilisierte die expansive Beschützer-Rolle so auf internationaler Ebene.

Mit Blick auf die militärische Nutzung des Netzes betonten zwar beide Regierungen, die Übertragbarkeit etablierter völkerrechtlicher Vorgaben. In der Einschätzung, was legitim sein sollte, unterscheiden sie sich dennoch. Während die deutsche Regierung zur freiwilligen Selbstbeschränkung mit Blick auf die militärische Zielauswahl bereit ist, entwickelt die britische Regierung eine Bandbreite verschiedener Angriffsmöglichkeit, darunter auch solche mit potenziell schwerwiegenden kinetischen Effekten. In beiden Untersuchungsstaaten lag die Referenz (Schutz für wen?) der militärischen Beschützer-Rolle zunächst auf dem Schutz der Infrastruktur der Streitkräfte, um die sicherheitspolitische Handlungsfähigkeit zu wahren. In beiden Untersuchungsstaaten wurden aber unter Verweis auf die immer ausgefeilteren Angriffe und die wachsende Verwundbarkeit eigene Angriffskapazitäten aufgebaut. Die Bundesregierung betonte in diesem Kontext domestisch, dass Cyberangriffe geringere kinetische Effekte und Kollateralschäden verursachen und daher militärische Ziele relativ schonend erreicht werden könnten. Die historisch gewachsenen domestischen Begrenzungen der militärischen Beschützer-Rolle wurden von der Regierung nach Kontestationsprozessen der parlamentarischen Opposition bestätigt und auf die Cybersicherheitspolitik übertragen. So versicherte die Regierung, dass der Einsatz der CNO-Kräfte ein konstitutives Mandat des Bundestages erfordert. Cyberangriffe erreichen bislang aber kaum die Schwelle eines bewaffneten Konflikts, so dass es in Deutschland nach wie vor umstritten ist, ob bzw. wann die Bundeswehr auf Cyberangriffe reagieren darf. Die Bundesregierung hat die Beschützer-Rolle

in diesem Kontext im Gegensatz zur britischen Regierung nicht neu ausgerichtet, da aufgrund der domestischen Beschränkungen im Bereich des Militärs ein flexibler Einsatz unterhalb der Schwelle eines bewaffneten Angriffs unzulässig ist. Die Beschützer-Rolle blieb damit auf die historisch gewachsenen Aufgaben Landesverteidigung bzw. parlamentarisch mandatierte Einsätze beschränkt. Die Debatte um die Zuständigkeit für einen Hack-Back im Falle eines Cyberangriffs illustriert diese unsichere Gestaltung der Beschützer-Rolle.

Die britische Regierung sah in offensiven Cyberfähigkeiten dagegen schon früh ein wichtiges Werkzeug zur Abschreckung feindlicher Staaten. Nach den zunehmenden internationalen Spannungen mit Russland und insbesondere nach der Vergiftung von Sergei Skripal, wurde Russland zum Referenzpunkt der Rolle (Schutz vor wem?). Die Beschützer-Rolle der britischen Regierung wurde daher flexibel auf die internationale Konfrontation mit Russland zugeschnitten. Cyberangriffe sind aus dieser Warte ein sicherheitspolitisches Werkzeug unterhalb der Schwelle einer konventionellen Vergeltung. Sie ergänzten damit das Portfolio sicherheitspolitischer Handlungsmöglichkeiten. Domestisch musste die Regierung aber auch dem Parlament Kontrollrechte mit Bezug zu den neuen Fähigkeiten einräumen. Sie betraute daher das ISC mit der Überwachung der offensiven Cyberkapazitäten. Da die Trennung zwischen den drei Untersuchungsbereichen in Großbritannien nicht so ausgeprägt ist wie in Deutschland, wurde das GCHQ mit der Entwicklung dieser neuen Kapazitäten beauftragt.

*3. Da die Untersuchungsbereiche aufgrund ihrer Akteurskonstellationen und historischen Bezüge durch unterschiedliche Interaktionsprozesse geprägt sind, kommt es zu unterschiedlichen Konvergenzen von Interaktionsarenen.*

Mit der Kooperation zwischen GCHQ und den britischen Streitkräften wird deutlich, dass die klare Trennung der drei Sphären zwar konzeptionell und analytisch hilfreich ist, dass diese empirisch durch die Praxis der Cybersicherheitspolitiken aber mitunter unterlaufen wird. Dies kann als ein eigenständiger Befund gewertet werden, denn die Konvergenz verschiedener Untersuchungsbereiche ist nicht in beiden Untersuchungsstaaten erfolgt. Nur in Großbritannien ist mit dem GCHQ eine Institution entstanden, die Funktionen in unterschiedlichen Bereichen übernimmt und diese so verknüpft. Das GCHQ ist erstens maßgeblich am Aufbau offensiver Fähigkeiten für das Militär beteiligt und führt in diesem Kontext auch Operationen durch. Es ist zweitens mit der Signals Intelligence beauftragt und stellt drittens seine Expertise durch das NCSC auch Strafverfolgungsbehörden zur Verfügung. In Deutschland besteht dagegen nach wie vor eine stärkere Trennung zwischen den Handlungsfeldern, die durch innenpolitische Kontestationen stabilisiert wird.

Die Teilung ergibt sich aus den historisch geronnenen Beschützer-Rollen. Die Debatte um die Zuständigkeit für einen Hack-Back im Falle eines Cyberangriffs

stehen ebenso exemplarisch hierfür wie Diskussionen um das Trennungsgebot. Hier wird der Spielraum der Regierung einerseits durch die historisch gewachsenen Rollenbegrenzungen der Verfassung und durch die domestische Kontestation beschränkt. Zwar beraten die unterschiedlichen Institutionen im Nationalen Cyber-Abwehrzentrum über Reaktionen auf Cyberangriffe – ein Austausch findet also statt. Die Zuständigkeit für Vergeltungsmaßnahmen im Cyberspace ist aber nach wie vor nicht entschieden. Die Debatte, ob digitale Vergeltung durch den BND oder die Bundeswehr erfolgen, hält nach wie vor an. Beide Varianten würden gesetzliche Neuregelungen erfordern. Außerdem wurden in Deutschland auch Bedenken mit Blick auf das Völkerrecht formuliert, wonach militärische Cyberangriffe nur durch Kombattanten durchgeführt werden dürften. Eine enge Verzahnung im Sinne einer Arbeitsteilung zwischen Militär und Nachrichtendiensten ist in Deutschland daher schwieriger als in Großbritannien. Die britische Regierung konnte das GCHQ und die Streitkräfte gemeinsam mit dem Aufbau der militärischen Beschützer-Rolle betrauen, ohne folgenreiche Kontestationen auszulösen. Damit stellte die Regierung eine institutionelle Verknüpfung zwischen der nachrichtendienstlichen und militärischen Beschützer-Rolle her. Dies wurde wiederum durch die historischen Selbstbezüge ermöglicht, die auch auf die erfolgreiche Zusammenarbeit der Streitkräfte mit dem GCHQ verwiesen. Daher wurde es auch möglich, dass die offensiven Maßnahmen gegen den Islamischen Staat durch den Nachrichtendienst ausgeführt wurden. Im Gegensatz zu Deutschland, erkannte die britische Regierung hierin keine völkerrechtlichen Probleme.

*4. Es bestehen unterschiedliche Wechselwirkungen zwischen den Rollen Beschützer, Wohlstandsmaximierer und Garant liberaler Grundrechte.*

Die Beschützer-Rollen wurden in den Untersuchungsstaaten immer wieder durch Bezüge zu den Rollen Wohlstandsmaximierer und Garant liberaler Grundrechte beschränkt oder katalysiert. Im Folgenden werden einige dieser Prozesse kurz skizziert.

Sowohl in Deutschland als auch in Großbritannien wurde die Etablierung der Beschützer-Rollen im Bereich der Strafverfolgung zunächst durch die Rolle des Wohlstandsmaximierers katalysiert. Von der neuen Verwundbarkeit waren zunächst überwiegend Unternehmen betroffen und die volkswirtschaftliche Prosperität schien gefährdet. Dies ermöglichte den Regierungen ihre Beschützer-Rollen einzunehmen und Cyberkriminalität zu sanktionieren. Beschränkungen der Rolle wurden ebenfalls an der Rolle als Wohlstandsmaximierer ausgerichtet. So galt es durch die Regelungen nicht zu tief in die wirtschaftlichen Freiheiten einzugreifen.

Im Bereich der militärischen Beschützer-Rolle entfaltete sich ebenfalls eine katalytische Wirkung der Rolle als Garant liberaler Grundrechte. Diese führte in

beiden Untersuchungsstaaten dazu, dass das demokratische System nach 2016 selbst zur Referenz (Schutz für wen?) der Beschützer-Rolle wurde. Dies wurde durch den Verdacht ermöglicht, der US-Präsidentschaftswahlkampf bzw. das Brexit-Referendum seien durch Cyberangriffe von außen manipuliert worden. In der Folge wurde das demokratische System selbst zum Schutzgut, bemerkenswert ist, dass dies in beiden untersuchten Staaten im Kontext der militärischen Schutzfunktion debattiert wurde.

Katalytische oder begrenzende Wirkungen fanden aber nicht in beiden Untersuchungsstaaten gleichläufig statt. Auch hier ergeben sich Unterschiede, die durch die unterschiedlichen Interaktionen verstehbar werden. Im Bereich der Nachrichtendienste besteht in Großbritannien eine potenziell katalytische Beziehung zwischen der Rolle als Wohlstandsmaximierer und der Beschützer-Rolle. Sie äußert sich in der Zuschreibung, dass die Nachrichtendienste auch mit der Aufgabe betraut sind, das ökonomische Wohlergehen des Vereinigten Königreichs zu sichern. Eine Funktion, die auch in der Auseinandersetzung um nachrichtendienstliche Befugnisse für einen Ausbau sicherheitspolitischer Kompetenzen angeführt wird. Dieses Verhältnis wurde domestisch zwar kritisiert, bisher allerdings nicht aufgelöst. Im Gegensatz dazu beschränkt in Deutschland die Rolle als Wohlstandsmaximierer die Beschützer-Rolle in diesem Bereich, da die Bundesregierung hofft, durch das explizite Verbot von Wirtschaftsspionage, eine neue Norm zu unterstützen. Dies steht exemplarisch dafür, dass die Rollen nicht immer in gleicher Weise auf die Politiken wirken, sondern auch hier ergeben sich in der Interaktion Differenzen.

In beiden Untersuchungsstaaten hat die Rolle als Garant liberaler Grundrechte jedoch beschränkend auf die Beschützer-Rollen gewirkt. So haben die Exekutiven die Kontrollfunktionen der Parlamente und der Judikativen gestärkt. Dies gilt für den Bereich der Strafverfolgung, der juristisch kontrolliert wird. Aber auch für die Nachrichtendienste, wo sowohl in Deutschland als auch in Großbritannien neue Institutionen zur Kontrolle der Geheimdienste etabliert bzw. bestehende Institutionen gestärkt wurden. Außerdem sicherte die Regierung den Parlamenten bei militärischen Cyberoperationen die gleichen Kontrollbefugnisse wie beim Einsatz konventioneller Mittel zu.

Insgesamt wurde die Beschützer-Rolle in Deutschland deutlicher durch die Rolle als Garant liberaler Grundrechte beschränkt, als dies in Großbritannien der Fall war. Im Außenverhalten hat bspw. die anhaltende Kontestation der Beschützer-Rolle im Bereich der Strafverfolgung dazu geführt, dass die Bundesregierung einen europäischen Vorschlag zum Zugriff ausländischer Ermittlungsbehörden auf Daten in Deutschland ablehnte. Diese Haltung resultiert aus der Besorgnis, dass die Rolle als Garant liberaler Grundrechte durch Dritte nicht angemessen wahrgenommen werden könnte. Oft erfolgte die Beschränkung der Beschützer-Rolle in Kombination mit Verweisen auf das negative historische

Selbst oder aus den entsprechend historisch geronnenen Begrenzungen der Beschützer-Rolle. Dies zeigt sich bspw. bei der Regulation von Verschlüsselung und der restriktiven militärischen Nutzung des Netzes.

Insgesamt konnte die Untersuchung damit die bestehenden Befunde aus Sekuritisierungsstudien ausdifferenzieren und ein detaillierteres Bild der Cybersicherheitspolitiken zeichnen. Dies ist auch für das Verständnis potenzieller internationaler Kooperation hilfreich.

### 7.1.2 Implikationen für die internationale Cybersicherheitsordnung und das Netz

Die Darstellung, internationale Cybersicherheitsnormen seien nur zwischen Demokratien und Autokratien umstritten, konnte durch die Untersuchung differenziert werden. Die Regierungen der Untersuchungsstaaten weisen in ihren Politiken Unterschiede bei der Unterstützung internationaler Normen auf. Außerdem konnte die Analyse zeigen, dass auch die Cybersicherheitspolitiken der beiden Demokratien die IT-Sicherheit im globalen Netz unterminieren und potenziell geeignet sind, Unsicherheit zu verbreiten.

Konkret zeigt sich, dass Bestrebungen zur Regulation der militärischen Nutzung des Internets durch die britische Regierung von Beginn an grundsätzlich abgelehnt wurden. Die britische Regierung zeigte keine Bereitschaft, die Beschützer-Rolle im Cyberspace signifikant zu beschränken, sondern sieht in ihr eine logische Erweiterung des eigenen (Abschreckungs-)Potenzials. Die deutsche Bundesregierung dagegen setzte sich auch nach der Etablierung erster offensiver Kapazitäten im Jahr 2007 für eine Kultur der Zurückhaltung im Cyberspace ein. Die Position, die Bundeswehr arbeite nicht an Schadsoftware zeigt die Bereitschaft zur freiwilligen Selbstbeschränkung der Beschützer-Rolle. Sie wäre so mit einer weitgehenden Regulation militärischer Kapazitäten im Sinne eines Regimes zur Kontrolle von Cyberwaffen theoretisch vereinbar gewesen. Erst als sich die außenpolitische Gefahreneinschätzung änderte und signifikante Andere diese Haltung nicht teilten, gab auch die Bundesregierung diese Haltung auf. Beide Regierungen haben stets betont, dass die bestehenden völkerrechtlichen Regelungen auf den Cyberspace übertragbar seien. Während die deutsche Exekutive aber nach wie vor auf das explizite Verbot von Angriffen auf bestimmte Infrastrukturen hinarbeitet, ist eine solche Beschränkung der Beschützer-Rolle für die britische Regierung nicht akzeptabel, da sie in ihren Cyberfähigkeiten die Möglichkeit zur flexiblen Reaktion auf unterschiedliche Angriffsszenarien sieht. Das GCHQ hat im Zuge der parlamentarischen Kontrolle eingeräumt, auch die Fähigkeit zu folgenschweren Cyberangriffen aufzubauen. Dies legt zumindest die Vermutung nahe, dass es sich hierbei um Angriffe gegen kritische Infrastrukturen handeln könnte.

Der Aufbau einer verifizierbaren Kultur der Zurückhaltung wird zudem durch die verdeckten Operationen im Netz erschwert. Beide Regierungen nutzen das Netz zur Durchführung klandestiner Operationen. Die deutsche Bundesregierung hat im Kontext der militärischen Nutzung explizit darauf hingewiesen, dass zwar die durchführenden Kräfte als Kombattanten zu erkennen sein müssten, dass dies aber nicht für die technische Infrastruktur der Angriffe gelte. Auch wenn die gezielte Nutzung falscher Identitäten zur Schuldverschiebung aus Sicht der deutschen Regierung verboten ist, ist die Möglichkeit einer Fehlattribution in diesen Fällen dennoch gegeben. Die Sicht der britischen Regierung auf das Völkerrecht definiert ein noch weitreichenderes Handlungsrepertoire für staatliche Cyberoperationen. So erkennt die britische Exekutive in Cyberangriffen nicht zwingend eine Verletzung nationaler Souveränität. Erst wenn durch diese Aktivitäten eine nicht klar definierte Schwelle (bspw. die Manipulation von Wahlen) überschritten wird, stellt dies für die britische Exekutive eine Verletzung der Souveränität dar. Unterhalb dieser Schwelle sind Cyberangriffe damit legitim.

Verdeckte Operationen gegen Ziele im Ausland führen nicht nur die militärischen Cyberkräfte durch, sondern auch die Nachrichtendienste. Die britische Regierung hat mit dem Angriff auf Belgacom gezeigt, dass sie den Einsatz von Cyberkapazitäten auch gegen Verbündete nicht scheut. Sie sieht in der Überwachung Verbündeter Regierungen eine übliche nachrichtendienstliche Praxis. Die deutsche Regierung hat zwar die Überwachung europäischer Ziele beschränkt, sonst aber die Überwachungstätigkeiten des BND weitgehend legalisiert. Mit Blick auf das Eindringen in gegnerische Systeme ist auch das nicht unproblematisch, da die mit der Infiltrationen verbundenen Intentionen nicht ersichtlich sind und so zur Eskalation beitragen können. Die beiden Demokratien tragen so auch zur globalen Unsicherheit im Cyberspace bei. Was als unzulässige Operation im Netz gewertet wird, ist damit bereits zwischen diesen beiden Regierungen umstritten.

Die Cybersicherheitspolitiken der beiden Regierungen haben dabei auch Folgen für das globale Netz. Beide Regierungen nutzen Sicherheitslücken in allen drei Untersuchungsbereichen. Damit unterminieren sie potenziell die IT-Sicherheit im gesamten Internet, da Fehler nicht gemeldet und Lücken nicht geschlossen werden. Die unintendierten Konsequenzen, die durch die Geheimhaltung entstehen können, wurden durch WannaCry eindrücklich illustriert. Zur Bewertung, ob eine Sicherheitslücke gemeldet oder geheimgehalten wird, evaluieren die Staaten nur die Gefahren für die nationalen Infrastrukturen. Eine Schutzpflicht für das Netz als Ganzes, wie es immer wieder von VertreterInnen der Netzgemeinde gefordert wird, ist damit nicht anschlussfähig. Es lässt sich zwar argumentieren, dass die meisten Industrienationen von ähnlichen kommerziellen Soft- und Hardwareprodukten abhängig sind, sodass die Risikoeinschätzungen potenziell ähnlich ausfallen könnten. Dies ist aber keine Gewähr dafür,

dass Sicherheitsbehörden bei der Evaluation einer Schwachstelle tatsächlich zu ähnlichen Entscheidungen gelangen. Für die Wahrung der Beschützer-Rollen in allen Untersuchungsbereichen akzeptieren die beiden Staaten ein potenzielles Risiko für das Netz und die NutzerInnen. Werden Staaten so auch zu Einkäufern von Zero-Day-Exploits, unterstützen sie zudem einen potenziell problematischen Markt für Sicherheitslücken.

Im Bereich der Kriminalitätsbekämpfung hat bisher die weitreichendste internationale Kooperation stattgefunden. Mit der Convention on Cybercrime konnten Straftatbestände harmonisiert und die Zusammenarbeit verbessert werden. Mit Blick auf weitere Kooperationen im Bereich der Strafverfolgung zeigt der deutsche Fall aber, dass die nächsten Schritte – die gegenseitige Zugriffsgewährung auf Daten – problematisch werden, da rechtsstaatliche Bedenken im Wege stehen. Großbritannien hat ein solches Abkommen mit den USA zwar abgeschlossen, ist aber darauf bedacht, die souveräne Kontrolle über die Beschützer-Rolle zu wahren. Der Ausbau der Kooperation im Bereich der Strafverfolgung ist daher ebenfalls nicht sicher.

Eine gewisse Skepsis bleibt auch mit Blick auf eine Norm, die die Regierungen wiederholt betont haben. Beide Regierungen haben immer wieder darauf hingewiesen, dass Staaten eine Sorgfaltsverantwortung für den eigenen Cyberspace tragen. Sie haben daher darauf gedrängt, dass Staaten illegitime Cyberangriffe, die von ihren Territorien ausgehen, nicht dulden oder unterstützen dürften. Diese Forderung wurde insbesondere immer lauter formuliert, als die Angriffe durch Proxies zunahmen. Domestisch wurden aber auch in beiden Staaten Bedenken dazu geäußert, welche Maßnahmen die Normeinhaltung gewährleisten könnten. Befürchtet wurde in diesem Kontext, dass dies eine umfassende Kontrolle der Internetverkehrs nötig mache. Der Nachweis der Compliance könnte so im Widerspruch mit der Rolle als Garant liberaler Grundrechte stehen. Eine Norm der Staatenverantwortung könnte auch von Autokratien zur Rechtfertigung eigener Überwachungspraktiken genutzt werden und ggf. eine Fragmentierung des Netzes befördern, da Eingriffe in Inhalte oder Praktiken unter dem Vorwand der Normdurchsetzung erfolgen könnten.

## 7.2 Theoretische Reflexion: Fruchtbarkeit des Zwei-Ebenen-Rollenspiels und alternative Erklärungen

Die Studie hat zur Analyse der Cybersicherheitspolitiken ein neues rollentheoretisches Zwei-Ebenen-Spiel entworfen. In Abgrenzung zu realistischen Ansätzen, die das internationale Rollenspiel als vorrangig betrachten und liberalen Perspektiven, die die innerstaatlichen Prozesse des Interessenuploads in den Vordergrund stellen, wurde so ein theoretisches Konzept entwickelt, das keiner der Sphären

Vorrang einräumt, sondern diese gleichberechtigt betrachtet und deren Wechselwirkungen nachvollzieht.

Das rollentheoretische Zwei-Ebenen-Spiel wurde hier in Abgrenzung zum etablierten TLG von Putnam für Handlungskontexte angewendet, in denen es nicht um die Aushandlung eines Abkommens geht, sondern im Rahmen der Entwicklung von Cybersicherheitspolitiken. Es wurde zuvor meist in relativ kontextarmen Analysen genutzt. Hier wurde es dagegen für eine vergleichsweise lange diachrone Untersuchung angewendet. Die theoretische Weiterentwicklung hat sich in diesem Kontext als hilfreich beim Verständnis der Cybersicherheitspolitiken bewährt. Der Vorteil gegenüber der etablierten Analyse von domestischen Kontestationsprozessen aus rollentheoretischer Perspektive liegt in der Auflösung der strikten Trennung zwischen innen- und außenpolitischen Einflüssen. Das rollentheoretische Zwei-Ebenen-Spiel dynamisiert das Verhältnis der beiden Sphären über die Interaktion der Regierungen mit domestischen und internationalen signifikanten Anderen. Es ermöglicht so auch Befunde, wie bspw. das internationale Rollenspiel, dass auf das domestische zurückwirkt (Second Image reversed).

Dass etablierte Theorien der IB, die Befunde dieser Arbeit nicht besser erklären können als der gewählte theoretische Zugang, lässt sich an zwei Beispielen illustrieren: Erstens mit einem neorealistischen Blick auf die Politiken, der die systemischen Machtverteilungen zur Erklärung staatlichen Handelns heranzieht sowie zweitens aus der Perspektive eines liberalen Ansatzes, bei dem das domestische Rollenspiel im Fokus der Betrachtung steht.

Mit Blick auf den Neorealismus stellen sich fragen zu dessen Erklärungskraft auch dann, wenn man nur den Bereich der Streitkräfte betrachtet und sich damit auf den Kernbereich realistischen Erklärungsanspruchs beschränkt. Auch wenn im Neorealismus das Verhältnis zwischen Macht on- und offline nach wie vor umstritten ist (s. Kapitel 1), gibt es Befunde, die eine neorealistische Erklärung vor substanzielle Herausforderungen stellen. Geht man davon aus, dass es der Cyberspace potenziell unterlegenen Akteuren ermöglicht, konventionelle Defizite teilweise zu kompensieren und damit asymmetrische Konstellationen etwas anzugleichen, eine Einschätzung die beide Regierung teilen, dann stellt sich die Frage, warum Deutschland, das sich im konventionellen Bereich durch freiwillige Selbstbeschränkung auszeichnet und über keine eigene nukleare Abschreckung verfügt, die Option offensiver Cyberkapazitäten nicht stärker nutzt, sondern im Gegenteil auch hier zurückhaltender agiert als das Vereinigte Königreich. Die deutsche Regierung lässt damit bewusst eine Chance zur Kompensation konventioneller Unterlegenheit aus. Großbritannien hat dagegen öffentlich deutlich gemacht, dass das GCHQ auch Angriffsfähigkeiten mit erheblichen kinetischen Potenzialen aufbaut, obwohl die eigene Abschreckungsfähigkeit konventionell verfügbar ist. Der relative Gewinn durch den Aufbau der Fähigkeiten ist daher für das Vereinigte Königreich deutlich geringer als er für die konventionell schwächere

Bundesrepublik wäre. Dieser Befund macht es zweifelhaft, dass eine realistische Erklärung für die empirischen Ergebnisse dieser Studie besser geeignet ist, da die domestischen Einflüsse in einer strukturell realistischen Untersuchung keinen Raum finden.

Die Annahme, das internationale System präge allein durch den anarchischen Anpassungsdruck die Außenpolitiken, greift daher zu kurz. Sie wird mit Blick auf die deutsche Bundesregierung durch die freiwillige Selbstbeschränkung konterkariert. Diese Zurückhaltung findet sich aber nicht nur im militärischen, sondern auch im Bereich der nachrichtendienstlichen Nutzung des Netzes. Auch hier begrenzt die Exekutive die Maßnahmen gegen europäische Ziele bzw. setzt für sie besonders hohe Hürden. Aus realistischer Perspektive, in der die Verbündeten von heute die Gegner von morgen sein können (Waltz, 2000, S. 10), ist dies kein plausibles Vorgehen. Aber auch im Vereinigten Königreich sind die domestischen Einflüsse für das Verständnis der Cybersicherheitspolitiken bedeutsam. Die positiven historischen Erfahrungen mit den Nachrichtendiensten und die negativen Erfahrungen als Opfer terroristischer Anschläge begünstigen, zusammen mit der internationalen Gefahrenlage und der besonderen Beziehung zu den USA, eine offensivere und weniger restriktive Cybersicherheitspolitik. Die frühe Entwicklung der britischen Beschützer-Rolle im Bereich der Strafverfolgung, ist ohne die historischen Erfahrungen mit domestischem Terrorismus dagegen gar nicht zu verstehen (sie entzieht sich zugegebenermaßen aber auch realistischen Erklärungsansprüchen). Die innenpolitischen Faktoren abzuschneiden, verdeckt daher einen substanziellen Teil der Interaktionen, die für das Verständnis der Politiken bedeutsam sind.

Aus liberaler Perspektive ergeben sich andere Fragen. Prinzipiell zielt die liberale Annahme darauf, dass durch den Wechsel der RollenträgerInnen andere gesellschaftliche Interessen auf die Regierung übertragen werden. Es bleibt hier aber einerseits zweifelhaft, ob die Cybersicherheitspolitiken in den Untersuchungsstaaten die Salienz aufweisen, die Wahlentscheidung der BürgerInnen zu beeinflussen. Ob also überhaupt gezielt neue Interessen transferiert werden. In beiden Fällen sprechen Indizien gegen diese Annahme. Einerseits stand die britische Regierung nach den Snowden-Enthüllungen domestisch wie international aufgrund ihrer ausgreifenden Überwachungstätigkeiten in der Kritik. Diese führte bei der Wahl 2015 aber nicht zu einer Stärkung des überwachungsskeptischen Koalitionspartners (den Liberal Democrats), sondern zu einem Sieg und einer Alleinregierung für die Tories. In Deutschland spricht der Niedergang der Piraten Partei und die Abwahl der FDP während bzw. nach den Snowden-Enthüllungen ebenfalls dafür, dass die Cybersicherheitspolitiken bzw. Kritik an diesen, nicht wahlentscheidend waren.

Die Wechsel der RollenträgerInnen durch Wahl bzw. Abwahl haben im gesamten Untersuchungszeitraum die Cybersicherheitspolitiken nur geringfügig beein-

flusst (bspw. in Großbritannien mit Blick auf die militärische Cybersicherheit 2010). Die Erwartung, (physische) Sicherheit zu gewährleisten, hat VertreterInnen unterschiedlicher Parteien dazu veranlasst, den Ausbau der Beschützer-Rollen mitzutragen. Auch wenn bei Regierungswechseln die Cybersicherheitspolitiken der Vorgängerregierung als zu umfassend kritisiert wurden, wurde der weitere Aufbau der Beschützer-Rolle nach dem Machtwechsel oftmals fortgesetzt. Dies zeigt sich bspw. nach dem Wahlerfolg der Labour Party 1997, die noch vor der Wahl die Haltung der Tories zur Kryptographie abgelehnt hatte, nach der Wahl aber eine ähnliche Politik verfolgte. In Deutschland zeigt sich ein ähnliches Phänomen zum Zeitpunkt der Snowden-Enthüllungen. Noch vor dem Regierungswechsel war die oppositionelle SPD in ihrer Kritik an der Regierung aus CDU/CSU und FDP deutlicher als nach dem Eintritt in die Regierung. Die Parteien definieren die Beschützer-Rollen zwar etwas unterschiedlich und liberale bzw. linke Parteien sind öfter gewillt, diese Rolle unter Abwägung mit der Rolle als Garant liberaler Grundrechte zu beschränken. Allerdings hat dies in keinem Fall zu einem Rückbau der Kompetenzen geführt. So hat die antizipierte soziale Erwartungshaltung, dass die Regierung für den Schutz der BürgerInnen verantwortlich ist und auch die Sorge davor, im Ernstfall für ein Versagen verantwortlich gemacht zu werden, auch eigentlich skeptische Parteien für Erweiterungen der Beschützer-Rolle stimmen lassen (bspw. die Liberal Democrats für DRIPA 2014). Liberale Ansätze zur Erklärung der Politiken scheitern ferner daran, dass Veränderungen nicht zu den Hochzeiten innergesellschaftlichen Interessenuploads (Wahlen) stattfinden, sondern sich langsam auch über unterschiedliche Regierungskonstellationen hinweg vollziehen. Vielmehr zeigt sich, dass die Beschützer-Rolle durch verschiedene Parteien zwar unterschiedlich definiert wird, kommt es dann zum Machtwechsel, sind die Politiken aber zumeist ähnlich. Das spricht dafür, dass die mit der Rolle verbundenen antizipierten sozialen Erwartungen und die Konsequenzen von deren Nichterfüllung im Ernstfall auch skeptischere Parteien zu Anpassungen veranlassen.

Für liberale Erklärungsansätze ist zudem problematisch, dass sie Rückwirkungen der internationalen Ebene auf die domestischen Entwicklungen (second image reversed) nicht nachvollziehen. Ein Defizit, das auch rollentheoretische Arbeiten betrifft. Dass diese Effekte für das Verständnis der Cybersicherheitspolitiken aber wichtig sind, zeigt die empirische Analyse. In der Bundesrepublik wurde der Ausbau der Beschützer-Rolle im Bereich der Nachrichtendienste durch die Abhängigkeit von den USA beeinflusst. Das außenpolitische Scheitern der Verhandlungen und die ablehnende Haltung der USA und des Vereinigten Königreichs, begünstigten, dass sich die domestische Aufklärung auf die Untersuchung der eigenen Beschützer-Rolle fokussierte. Die antizipierten Folgen eines Bruchs mit den Verbündeten moderierten diese domestische Aufarbeitung. In Großbritannien ging es in diesem Bereich auch darum, die Kooperation mit

der NSA nicht zu gefährden. Die domestischen Kontestationen forderten unter anderem deshalb keine einschneidenden Begrenzungen für die technischen Fähigkeiten des Nachrichtendienstes. Im militärischen Bereich waren es, neben der Gefahrenlage, Erwägungen zur Verbesserung der Kooperationsfähigkeit mit den NATO-Partnern, die in Deutschland den Aufbau des Kdo CIR erleichterten. In Großbritannien wurde der Ausbau durch die zunehmende Konfrontation mit Russland ermöglicht. Die unterschiedlichen Kryptopolitiken werden ebenfalls erst dann besser verständlich, wenn auch die internationale Ebene mitgedacht wird. Während in Deutschland eine zu ausgreifende US-Politik abgelehnt wurde, wurde dies von der britischen Regierung nicht so kritisch gesehen. Hierdurch wurde in Großbritannien zumindest ein freiwilliges System nach amerikanischem Vorbild installiert, während Deutschland eine weniger restriktive Politik verfolgte.

In beiden Untersuchungsstaaten und in unterschiedlichen Bereichen der Cybersicherheitspolitik zeigt das rollentheoretische Modell so, dass sowohl außen- als auch innenpolitische Entwicklungen die Politiken beeinflussen. Die empirische Analyse hat verdeutlicht, dass das rollentheoretische Zwei-Ebenen-Spiel dabei hilft, die unterschiedlichen Dynamiken und Interaktionen zwischen den Sphären zu analysieren und die Politikentwicklung besser zu verstehen. Das Zwei-Ebenen-Rollenspiel illustriert dabei erstens, dass das internationale Rollenspiel nicht im realistischen Sinne gleich auf beide Staaten wirkt und dass ein Fokus auf eine Ebene wichtige Interaktionen ausblendet. Zweitens wird deutlich, dass sich die beiden Ebenen wechselseitig beeinflussen und in dynamischem Interaktionsverhältnis stehen. Die Fruchtbarkeit dieses Ansatzes zeigt sich daher auch in unterschiedlichen Wechselwirkungen zwischen domestischer und innenpolitischer Sphäre, die die unterschiedlichen Cybersicherheitspolitiken in den beiden Untersuchungsstaaten besser verständlich machen.

## 7.3 Limitationen, Desiderate und Ausblick

Grundsätzlich lassen sich zwei Limitationen der vorliegenden Studie identifizieren. Die erste folgt aus dem Design der Studie, das durch sein verstehendes Vorgehen und die begrenzte Fallzahl mit Blick auf die Übertragbarkeit der Befunde notwendigerweise begrenzt bleibt. Die zweite ergibt sich aus dem empirischen Forschungsgegenstand, der sich durch ein beträchtliches Maß staatlicher Geheimhaltung auszeichnet. Die Befunde sind daher in doppelter Hinsicht kritisch zu reflektieren.

Die Untersuchung ist mit dem Ziel gestartet, zu analysieren, wie sich die Cybersicherheitspolitiken in den beiden Untersuchungsstaaten entwickelt haben. Für die beiden Regierungen konnte gezeigt werden, dass sie ihre Beschützer-Rollen innerhalb des Untersuchungszeitraumes ausgebaut haben. In beiden Staa-

ten haben sich – in unterschiedlichem Maße – kontestierende oder katalytische Effekte mit den Rollen als Garant liberaler Grundrechte bzw. Wohlstandsmaximierer ergeben. Die Untersuchung ist in ihrer verstehenden theoretisch-methodischen Herangehensweise aber nicht darauf angelegt, generalisierbare Erkenntnisse über Cybersicherheitspolitiken zu gewinnen. Sie zielt darauf, die beiden untersuchten Fälle besser zu verstehen und einen möglichst plausiblen Interaktionsverlauf nachzuzeichnen. Die Befunde der Untersuchung sprechen dafür, dass sich auch westliche Demokratien, die sich durch Mitgliedschaften in ähnlichen Organisationen und durch ähnliche kulturelle Prägungen auszeichnen, substanziell in ihren Cybersicherheitspolitiken unterscheiden. Aufschlussreich wären daher weitere Studien, mit mehr Fällen auch aus anderen geografischen und kulturellen Kontexten. Nur auf diesem Weg ließe sich ein umfassenderes Bild, auch mit Blick auf die internationale Cybersicherheitsordnung, zeichnen.

Insgesamt ist zu hoffen, dass die theoriegeleitete Forschung auch in Zukunft verstärkt vergleichend arbeiten wird, um das Verständnis für unterschiedliche Einflüsse auf Cybersicherheitspolitiken zu verbessern. Ein Blick auf innen- wie außenpolitische Einflüsse hilft dabei, ein differenziertes Bild der Politiken zu zeichnen. Jedes Gemeinwesen nimmt, durch seine historischen Erfahrungen und die Einbettung in unterschiedliche soziale Handlungskontexte, einen eigenen Weg in die sicherheitspolitische Erschließung des Netzes. Diese Wege besser zu verstehen, wird dabei helfen, auszuloten, welche internationalen Verhaltensstandards an die Rollen der Regierungen anschlussfähig sind. Auch zwischen Demokratien bestehen, wie diese Untersuchung gezeigt hat, beträchtliche Unterschiede in den Cybersicherheitspolitiken.

In diesem Kontext ist aber darauf hinzuweisen, dass eine Übertragbarkeit des Analysekonzepts insbesondere jenseits demokratischer Systeme schwierig ist bzw. substanzieller empirischer Nacharbeit bedarf. In autokratischen Regimen ist die Rolle als Garant liberaler Grundrechte wenn überhaupt nur begrenzt anwendbar. Ein einfacher Transfer des Analysekonzeptes ist damit kaum möglich. Vielmehr müssten für autokratische Systeme zunächst die prägenden Rollen der Cybersicherheitspolitik aus den entsprechenden Dokumenten herausdestilliert werden. Es muss ferner bezweifelt werden, dass das innenpolitische Rollenspiel in Autokratien ähnlichen Regeln folgt wie in Demokratien. Die signifikanten Anderen sind vermutlich andere (bspw. das Militär, Herrscherdynastien, Parteien, etc.) und auch die Interaktionen folgen anderen Mustern. All das müsste empirisch nachvollzogen werden. Eine Erweiterung der analysierten Fälle – auch über demokratische Staaten hinaus – wäre aber dennoch wünschenswert, um ein besseres Verständnis für die unterschiedlichen Interaktionen und für die internationale Cybersicherheitsordnung zu gewinnen. Insbesondere mit Blick auf die Erweiterung der untersuchten Fälle und Integration von Autokratien ergeben sich aber besondere Schwierigkeiten beim Zugang zum empirischen Analysematerial.

Die Cybersicherheitspolitik gehört zu den besonders sensiblen Bereichen der Sicherheitspolitik und ist daher ein potenziell schwieriger Forschungsgegenstand. Es bleibt daher stets fraglich, ob denn tatsächlich die Politiken in Gänze analysiert werden können. Diese Einschränkung gilt weniger für den Bereich der Strafverfolgung, der durch die entsprechenden gesetzlichen Regelungen relativ explizit geregelt ist. Sie betrifft aber besonders die Arbeit der Nachrichtendienste sowie der Streitkräfte. Zwei Argumente lassen sich kritischen Stimmen entgegnen, die in diesem Kontext ggf. sogar für einen Forschungsverzicht plädieren, da keine abschließenden und belastbaren Erkenntnisse gewonnen werden könnten. Erstens lässt sich dem Argument grundsätzlich mit Blick auf die hier vertretene wissenschaftstheoretische Position begegnen. Wendet man das Argument zum Forschungsverzicht nämlich radikal um, zeigt sich, dass ein Verzicht aus Furcht davor, keine finalen Erkenntnisse zu generieren fehl geht, da unhintergehbares Wissen ohnehin nicht erreichbar ist. Wissen bleibt aus pragmatistischer Perspektive stets veränderbar und muss sich in Interaktion bewähren. Die Untersuchung von Cybersicherheitspolitiken unterscheidet sich hier nicht von anderen wissenschaftlichen Studien. Das bedeutet daher nicht, dass die Analyse von Cybersicherheitspolitiken aufgrund der (potenziell höheren) Fallibilität unterbleiben sollte.

Zweitens lässt sich der Kritik im Kontext dieser Studie empirisch begegnen. Da es sich bei den beiden hier untersuchten Staaten um Demokratien handelt, sind Daten zumindest teilweise zugänglich. Die Regierungen unterliegen auch in sensiblen Sicherheitspolitiken parlamentarischer und juristischer Kontrolle. Auch wenn diese Kontrollen nicht alle Praktiken öffentlich machen, besteht so doch die Möglichkeit, Einblick in die praktische Politikgestaltung zu erlangen. Dies wird in demokratischen Systemen durch die Arbeit einer freien Presse und der damit einhergehenden Publikation geheimer Dokumente weiter begünstigt. Die Snowden-Enthüllungen und die damit verbundene erzwungene Öffentlichkeit, waren für diese Studie – wie für viele andere – die einzige Gelegenheit, die Entwicklung der Politiken im Bereich der Nachrichtendienste zu analysieren. Sie zeigen auch, dass es mitunter einer/eines Mitwisserin/Mitwissers bedarf, um verdeckte Praktiken öffentlich zu machen. Eine Analyse der Cybersicherheitspolitiken ist daher in Demokratien potenziell einfacher, da die Regierungen verschiedenen Kontrollen unterworfen sind und es so einfacher möglich ist, Interaktionen zu rekonstruieren. Es ist aber nicht auszuschließen, dass weitere Veröffentlichungen oder das zukünftige Öffnen staatlicher Archive die Informationslage signifikant verändern und die Befunde der Arbeit infrage stellen werden.

Ein Forschungsverzicht ist aber auch mit Blick auf Autokratien nicht angeraten, denn das dritte Argument richtet sich allgemeiner gegen KritikerInnen. Auch wenn Untersuchungen nicht das ganze Ausmaß staatlicher Cybersicherheitspolitiken aufdecken können, tragen sie doch wesentlich zum Erkenntnisgewinn in diesem Bereich bei. Regierungen müssen ihre Positionen zumindest grundsätz-

lich rechtfertigen und nicht alle Maßnahmen im Netz können geheimgehalten werden. Dies liegt einerseits an WhistleblowerInnen, an nichtstaatlichen Akteuren im Netz, die Infrastrukturen betreiben und Attributionen durchführen und andererseits daran, dass sich folgenschwere Cyberangriffe nicht geheimhalten lassen und dass auch nachrichtendienstliche Operationen entdeckt und mitunter veröffentlicht werden. All dies lässt sich analysieren. Regierungen handeln in diesen Kontexten sowohl international als auch domestisch. Dieses Handeln konstituiert – in Interaktion mit den signifikanten Anderen – soziale Realität. Es ist diese soziale Realität, die einer wissenschaftlichen Analyse offensteht. Die zugänglichen Praktiken berühren dabei so zentrale Werte, dass auch ein begrenzter Erkenntnisgewinn gesellschaftlich und wissenschaftlich wertvoll ist. Dass die informationstechnische Verwundbarkeit in absehbarer Zukunft eher zu- als abnehmen wird, spricht ebenfalls dafür, sich dem Thema zuzuwenden. Untersuchungen können dabei helfen, die emergente internationale Cybersicherheitsordnung besser zu verstehen. Die Politiken zu verstehen, heißt dabei auch nachzuvollziehen, welche Abwägungen die Regierungen vornehmen, welche Konflikte zwischen Staaten auftreten und welche Dynamiken sich hieraus ergeben können. Auch wenn Untersuchungen zur Cybersicherheitspolitik durch künftige Enthüllungen infrage gestellt werden, so bilden sie doch zum Zeitpunkt der Erstellung soziale Wirklichkeit ab. Der rollentheoretische Zugang mit seinem Fokus auf den Praktiken sozialer Interaktion kann diese soziale Wirklichkeit rekonstruieren und analysieren.

# 8. Literatur- und Quellenverzeichnis


Abels, Heinz (2010). *Interaktion, Identität, Präsentation*. Wiesbaden: VS Verlag für Sozialwissenschaften. ISBN: 978-3-531-17357-3. DOI: 10.1007/978-3-531-92048-1.

Access Now (2019). *Open Letter to GCHQ*. URL: https://newamericadotorg.s3.amazonaws.com/documents/Coalition_Letter_to_GCHQ_on_Ghost_Proposal_-_May_22_2019.pdf.

Akdeniz, Yaman (1997). »UK Government Policy on Encryption«. In: *SSRN Electronic Journal*. ISSN: 1556-5068. DOI: 10.2139/ssrn.41701.

Amnesty International (2013). *UK must account for its actions to repress Guardian reporting on surveillance*. URL: https://www.amnesty.org.uk/press-releases/uk-must-account-its-actions-repress-guardian-reporting-surveillance.

Anderson, David (2015). *A Question of Trust*. URL: https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf.

— (2016). *Report of Bulk Powers Review*. URL: https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf.

Andress, Jason (2014). *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice*. 2. Aufl. Waltham, MA und Amsterdam: Syngress und Elsevier. ISBN: 978-0-12-800744-0.

Antonopoulos, Constantine (2015). »State responsibility in cyberspace«. In: *Research handbook on international law and cyberspace*. Hrsg. von Nikolaos K. Tsagourias und Russell Buchan. Research handbooks in international law. Cheltenham, UK und Northampton, MA, USA: Edward Elgar Publishing, S. 55–71. ISBN: 9781782547389.

Argomaniz, Javier (2015). »The European Union Policies on the Protection of Infrastructure from Terrorist Attacks: A Critical Assessment«. In: *Intelligence and National Security* 30.2-3, S. 259–280. ISSN: 0268-4527. DOI: 10.1080/02684527.2013.800333.

Arquilla, John (2012). *Cyberwar Is Already Upon Us*. URL: https://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/.

Arquilla, John und David Ronfeldt (1993). »Cyberwar is coming!« In: *Comparative Strategy* 12.2, S. 141–165. ISSN: 0149-5933. DOI: 10.1080/01495939308402915.

Article 19 (2019). *European Court of Human Rights: the use of government hacking »represents one of the greatest threats to fundamental rights in the digital age«*. URL: https://www.article19.org/resources/european-court-of-human-rights-the-use-of-government-hacking-represents-one-of-the-greatest-threats-to-fundamental-rights-in-the-digital-age/.

Augen Geradeaus! (2012). *Cyberwar: Bundeswehr meldet »Anfangsbefähigung zum Wirken«*. URL: https://augengeradeaus.net/2012/06/cyberwar-bundeswehr-meldet-anfangsbefahigung-zum-wirken/.

Augen Geradeaus! (2019). *Bundeswehr plädiert für digitalen Verteidigungsfall zur besseren Cyber-Abwehr*. URL: https://augengeradeaus.net/2019/06/bundeswehr-plaediert-fuer-digitalen-verteidigungsfall-zur-besseren-cyber-abwehr/.

Austin, Greg (2018). *Cybersecurity in China: The new wave*. SpringerBriefs in cybersecurity. Cham, Switzerland: Springer. ISBN: 978-3-319-68436-9.

Australian Government (2018). *Five country ministerial 2018*. URL: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/five-country-ministerial-2018.

Auswärtiges Amt (2013a). *Verwaltungsvereinbarung zum G10-Gesetz mit Frankreich außer Kraft*. URL: https://www.auswaertiges-amt.de/de/newsroom/130806-g10-frankreich/257000.

— (2013b). *Verwaltungsvereinbarungen zum G10-Gesetz mit USA und Großbritannien außer Kraft*. URL: https://www.auswaertiges-amt.de/de/newsroom/130802-g10gesetz/256984.

— (2014). *Rede von Außenminister Frank-Walter Steinmeier beim Transatlantischen Cyber-Dialog*. URL: https://www.auswaertiges-amt.de/de/newsroom/140627-bm-cyber-dialog/263286.

— (2019). *Rede von Außenminister Heiko Maas anlässlich der Konferenz "2019. Capturing Technology. Rethinking Arms Control"*. URL: https://www.auswaertiges-amt.de/de/newsroom/maas-konferenz-2019-capturing-technology-rethinking-arms-control/2199790.

Axelrod, Robert und Robert O. Keohane (1985). »Achieving Cooperation under Anarchy: Strategies and Institutions«. In: *World Politics* 38.1, S. 226–254. DOI: 10.2307/2010357.

Bäcker, Matthias (2014). *Erhebung, Bevorratung und Übermittlung von Telekommunikationsdaten durch die Nachrichtendienste des Bundes: Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 22. Mai 2014*. URL: https://www.bundestag.de/resource/blob/280844/35ec929cf03c4f60bc70fc8ef404c5cc/MAT_A_SV-2-3-pdf-data.pdf.

Baert, Patrick (2009). »A Neopragmatist Agenda for Social research: Integrating Levinas, Gadamer and Mead«. In: *Pragmatism in international relations*. Hrsg. von Harry Bauer und Elisabetta Brighi. London: Routledge, S. 47–64. ISBN: 978-0415663786.

Bailer-Jones, Daniela und Cord Friebe (2009). *Thomas Kuhn*. NachGedacht. Paderborn: Mentis. ISBN: 3897855038.

Baldwin, John D. (1988). »Mead's Solution to the Problem of Agency«. In: *Sociological Inquiry* 58.2, S. 139–162. ISSN: 0038-0245. DOI: 10.1111/j.1475-682X.1988.tb01052.x.

Baribieri, Cristian, Jean-Pierre Danis und Carolina Polito (2018). *Non-proliferation Regime for Cyber Weapons. A Tentative Study*. URL: http://www.iai.it/sites/default/files/iai1803.pdf.

Barichella, Arnault (2018). *Cybersecurity in the Energy Sector: A Comparative Analysis between Europe and the United States*. URL: https://www.ifri.org/sites/default/files/atoms/files/barichella_cybersecurity_energy_sector_2018.pdf.

Barlow, John Perry (1996). *A Declaration of the Independence of Cyberspace*. URL: https://www.eff.org/de/cyberspace-independence.

Barnard-Wills, David und Debi Ashenden (2012). »Securing Virtual Space: Cyber War, Cyber Terror, and Risk«. In: *Space and Culture* 15.2, S. 110–123. ISSN: 1206-3312. DOI: 10.1177/1206331211430016.

Baumann, Max-Otto (2014). *Humanitäre Interventionen: Struktureller Wandel in der internationalen Politik durch Staateninteraktion*. Bd. 21. Internationale Beziehungen. Baden-Baden: Nomos. ISBN: 978-3-8487-1662-3.

Baumann, Peter (2006). *Erkenntnistheorie*. 2. durchgesehene Auflage. Stuttgart: Verlag J. B. Metzler.

Baumard, Philippe (2017). *Cybersecurity in France*. SpringerBriefs in cybersecurity. Cham, Switzerland: Springer. ISBN: 978-3-319-54308-6.

Bayerischer Rundfunk (2019). *BR Recherche: Bundesregierung skizziert Hackback-Pläne*. URL: https://www.br.de/nachrichten/deutschland-welt/internes-papier-bundesregierung-skizziert-hackback-plaene,RRqyr1j.

Beasley, Ryan K., Hrsg. (2013). *Foreign policy in comparative perspective: Domestic and international influences on state behavior*. 2nd ed. Thousand Oaks, California: CQ Press. ISBN: 978-1-60871-696-8.

Behörden Spiegel (2018). *ZITiS: Forschung und Entwicklung für Sicherheitsbehörden*. URL: https://www.behoerden-spiegel.de/2018/08/08/zitis-forschung-und-entwicklung-fuer-sicherheitsbehoerden/.

Bendiek, Annegret (2016). *Sorgfaltsverantwortung im Cyberraum: Leitlinien für eine deutsche Cyber-Außen- und Sicherheitspolitik*. URL: https://www.swp-berlin.org/fileadmin/contents/products/studien/2016S03_bdk.pdf.

Bendrath, Ralf, Johan Eriksson und Giampiero Giacomello (2007). »From 'cyberterrorism' to 'cyberwar', back and forth: How the United States securitized cyberspace«. In: *International relations and security in the digital age*. Hrsg. von Johan Eriksson und Giampiero Giacomello. Routledge advances in international relations and global politics. London und New York: Routledge, S. 57–82. ISBN: 978-0415599672.

Benkler, Yochai (2008). *Wealth of Networks: How Social Production Transforms Markets and Freedom*. Yale University Press. ISBN: 978-0-300-11056-2.

Bennett, Andrew und Jeffrey T. Checkel, Hrsg. (2017). *Process tracing: From metaphor to analytic tool*. 6th printing. Strategies for social inquiry. Cambridge: Cambridge University Press. ISBN: 978-1-107-68637-3.

Berghel, Hal (2017). »On the Problem of (Cyber) Attribution«. In: *Computer* March, S. 84–89. ISSN: 0018-9162.

Betz, David und Tim Stevens (2011). *Cyberspace and the state: Toward a strategy for cyber-power*. Bd. 424. Adelphi. London, U.K.: IISS, The International Institute for Strategic Studies. ISBN: 978-0415525305.

Beucher, Klaus und Andrea Schmoll (1999). »Kryptotechnologie und Exportbeschränkungen«. In: *Computer und Recht*, S. 529–535.

Big Brother Watch (2015). *Written evidence submitted by Big Brother Watch*. URL: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25185.html.

— (2016). *Equipment Interference*. URL: https://www.bigbrotherwatch.org.uk/wp-content/uploads/2016/03/Equipment-Interference.pdf.

Bijker, Wiebe E. (1995). *Of bicycles, bakelites, and bulbs: Toward a theory of sociotechnical change*. Cambridge, Mass. [u.a.]: MIT Press. ISBN: 0-262-02376-8.

Bird, Alexander (2000). *Thomas Kuhn*. Philosophy now. Princeton N.J: Princeton University Press. ISBN: 978-0-691-05710-1.

Bloomfield, Alan (2016). »Norm antipreneurs and theorising resistance to normative change«. In: *Review of International Studies* 42.02, S. 310–333. DOI: 10.1017/S026021051500025X.

Blumer, Herbert (1986 [1969]). *Symbolic interactionism: Perspective and method*. Berkeley: University of California Press. ISBN: 0-520-05676-0.

Bochmann, Cathleen (2018). *Staaten in der evolutionären Sackgasse? Neue perspektiven der staatszerfallsforschung*. Bd. 10. Staatlichkeit und Governance in Transformation. Baden-Baden: Nomos. ISBN: 978-3-8487-4953-9.

Booz Allen Hamilton (2011). *Cyber Power Index*. URL: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf.

Bradshaw, Samantha und Laura DeNardis (2016). »The politicization of the Internets Domain Name System: Implications for Internet security, universality, and freedom«. In: *New Media & Society*. ISSN: 1461-4448. DOI: 10.1177/1461444816662932.

Bradshaw, Samantha, Laura DeNardis u. a. (2016). *The Emergence of Contention in Global Internet Governance*. URL: https://www.cigionline.org/sites/default/files/documents/GCIG%20Volume%202.pdf#page=50.

Brantly, Aaron F. (2018). *The Cyber Deterrence Problem*. URL: https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2002%20The%20Cyber%20Deterrence%20Problem.pdf.

Braun, Torsten (2010). »Geschichte und Entwicklung des Internets«. In: *Informatik-Spektrum* 33.2, S. 201–207. ISSN: 0170-6012. DOI: 10.1007/s00287-010-0423-9.

Brem, Stefan (2015). »Critical Infrastructure Protection from a National Perspective«. In: *European Journal of Risk Regulation* 6.02, S. 191–199. DOI: 10.1017/S1867299X00004499.

Breuning, Marijke (2017). »Role Theory in Foreign Policy«. In: *Oxford Research Encyclopedia of Politics*. DOI: 10.1093/acrefore/9780190228637.013.334. URL: http://politics.oxfordre.com/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-334.

Brodowski, Dominik und Felix C. Freiling (2011). *Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft*. Bd. Nr. 4. Schriftenreihe Forschungsforum Öffentliche Sicherheit. Berlin: Freie Univ. ISBN: 978-3-929619-66-9.

Brugger, Agnieszka (2015). *Statt von der Leyens Cyberkrieg mehr internationales Engagement für Frieden und Sicherheit*. URL: https://www.agnieszka-brugger.de/hauptmenue/presse/presse/datum/2015/07/10/statt-von-der-leyens-cyberkrieg-mehr-internationales-engagement-fuer-frieden-und-sicherheit/.

Brummer, Klaus und Cameron G. Thies (2015). »The Contested Selection of National Role Conceptions«. In: *Foreign Policy Analysis* 11.3, S. 273–293. ISSN: 17438586. DOI: 10.1111/fpa.12045.

Brunst, Phillip (2012). »Staatliche (Anti-)Krypto-Strategien: Kryptographie zwischen Bürgerrecht und Bedrohung der nationalen Sicherheit«. In: 5, S. 333–338.

Buchan, Russell (2016). »The International Legal Regulation of State-Sponsored Cyber Espionage«. In: *International cyber norms*. Hrsg. von Anna-Maria Osula und Henry Rõigas. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, S. 65–86. ISBN: 978-9949-9544-7-6.

— (2019). *Cyber Espionage and International Law*. London: Bloomsbury Publishing PLC und Hart. ISBN: 978-1782257349.

Bueger, Christian und Frank Gadinger (2015). »The Play of International Practice«. In: *International Studies Quarterly* 59.3, S. 449–460. ISSN: 00208833. DOI: 10.1111/isqu.12202.

Bueno de Mesquita, Bruce u. a. (1999). »An Institutional Explanation of the Democratic Peace«. In: *American Political Science Review* 93.4, S. 791–807. DOI: 10.2307/2586113.

Bundesamt für Verfassungsschutz (2015). *Verfassungsschutzbericht 2014*. URL: https://www.verfassungsschutz.de/embed/vsbericht-2014.pdf.

Bundesbeauftragte für den Datenschutz (2017). *Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze BT-Drs. 18/11272 und der Formulierungshilfe mit Änderungsantrag zur Einführung einer Quellen-Telekommunikationsüberwachung und einer Online-Durchsuchung in der Strafprozessordnung,*

*A-Drs. 18(6)334*. URL: https://freiheitsrechte.org/home/wp-content/uploads/2017/05/186346_Stellungnahme_BfDI_zu_18-11272_und_186334.pdf.

Bundesgerichtshof (2006a). *BGH 1 BGs 184/2006*. URL: https://www.hrr-strafrecht.de/hrr/1/06/1-bgs-184-2006.php.

— (2006b). *BGH 3 BGs 31/06*. URL: https://www.hrr-strafrecht.de/hrr/3/06/3-bgs-31-06.php.

— (2007). *BGH StB 18/06*. URL: https://www.hrr-strafrecht.de/hrr/3/06/stb-18-06.php.

Bundesgesetzblatt (1986). *Z 5702 A vom 23. Mai 1986*. URL: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl186s0721.pdf.

— (1995). *Verordnung über die technische Umsetzung von Überwachungsmaßnahmen des Fernmeldeverkehrs in Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind*. URL: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl195s0722.pdf.

— (2002). *Verordnungüber die technische und organisatorische Umsetzungvon Maßnahmen zur Überwachung der Telekommunikation*. URL: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl105s3136.pdf.

— (2003). *Fünfunddreißigstes Strafrechtsänderungsgesetz zur Umsetzung des Rahmenbeschlusses des Rates der Europäischen Union vom 28. Mai 2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln (35. StrÄndG)*. URL: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl103s2838.pdf.

— (2007). *Einundvierzigstes Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄndG)*. URL: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl107s1786.pdf.

— (2008a). *Gesetz zu dem Übereinkommen des Europarats vom 23. November 2001 über Computerkriminalität*. URL: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl208s1242.pdf.

— (2008b). *Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt*. URL: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl108s3083.pdf.

— (2016a). *Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes*. URL: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl116s3346.pdf.

— (2016b). *Gesetz zur weiteren Fortentwicklung der parlamentarischen Kontrolle der Nachrichtendienste des Bundes*. URL: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl116s2746.pdf.

— (2017a). *Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens*. URL: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s3202.pdf.

— (2017b). *Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes*. URL: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s1354.pdf.

Bundesministerium der Verteidigung (2006). *Weißbuch 2006 zur Sicherheitspolitik Deutschlands und zur Zukunft der Bundeswehr*. URL: http://archives.livreblancdefenseetsecurite.gouv.fr/2008/IMG/pdf/weissbuch_2006.pdf.

— (2011). *Verteidigungspolitische Richtlinien: Nationale Interessen wahren – Internationale Verantwortung übernehmen – Sicherheit gemeinsam gestalten*. URL: https://www.bmvg.de/resource/blob/13568/28163bcaed9f30b27f7e3756d812c280/g-03-download-die-verteidigungspolitische-richtlinien-2011-data.pdf.

Bundesministerium der Verteidigung (2015a). *Keynote der Verteidigungsministerin auf dem Kolloquium des Cyber-Workshop*. URL: https://www.bmvg.de/de/themen/weissbuch/perspektiven/keynote-von-ministerin-von-der-leyen-beim-cyber-workshop-11028.

— (2015b). *Projekt von herausragender Bedeutung*. URL: https://www.bmvg.de/de/aktuelles/projekt-von-herausragender-bedeutung-11458.

— (2016). *Abschlussbericht Aufbaustab Cyber- und Informationsraum*. URL: http://docs.dpaq.de/11361-abschlussbericht_aufbaustab_cir.pdf.

— (2020). *Der Organisationsbereich Cyber- und Informationsraum*. URL: https://www.bmvg.de/de/themen/cybersicherheit/cyber-verteidigung/cyber-abwehr.

Bundesministerium des Innern (2005). *Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI)*. URL: https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/05-12-09/05-12-09-anlage-nr-16.pdf?__blob=publicationFile&v=2.

— (2011). *Cyber-Sicherheitsstrategie für Deutschland*. URL: https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile.

— (2014a). URL: https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2014/06/bund-wechselt-netzbetreiber.html.

— (2014b). *Schriftliche Fragen des Abgeordneten Andrej Hunko vom 24. Juli 2014: (Monat August 2014, Arbeits-Nr. 8/1,2)*. URL: https://andrej-hunko.de/start/download/dokumente/489-schriftliche-fragen-zur-eigenentwicklung-einer-trojaner-software-durch-das-bka/file.

Bundesregierung (1994). *Stärkung der inneren Sicherheit als gesamtgesellschaftliche Aufgabe - Rede von Bundesminister Kanther in Essen*.

— (1996). *Sicherheit für die Bürger auf dem Weg in die Informationsgesellschaft - Rede von Bundesminister Kanther in Stuttgart*.

— (2001). *Berichtder Bundesregierung zu den Auswirkungen der Nutzung kryptografischer Verfahren auf die Arbeit der Strafverfolgungs- und Sicherheitsbehörden*. URL: https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/2002-06-06/anlage-15.pdf?__blob=publicationFile&v=2.

— (2013a). *Initiative für besseren Schutz der Privatsphäre*. URL: https://archiv.bundesregierung.de/archiv-de/dokumente/initiative-fuer-besseren-schutz-der-privatsphaere-389998.

— (2013b). *NSA-Aufklärung: Deutschland ist ein Land der Freiheit*. URL: https://archiv.bundesregierung.de/archiv-de/deutschland-ist-ein-land-der-freiheit-421338.

— (2015a). *Fernmeldeaufklärung des Bundesnachrichtendienstes*. URL: https://www.bundesregierung.de/breg-de/aktuelles/fernmeldeaufklaerung-des-bundesnachrichtendienstes-754538.

— (2015b). *Sommerpressekonferenz von Bundeskanzlerin Merkel*. URL: https://www.bundesregierung.de/breg-de/aktuelles/pressekonferenzen/sommerpressekonferenz-von-bundeskanzlerin-merkel-848300.

— (2019a). *Agentur für Innovation in der Cybersicherheit*. URL: https://www.bundesregierung.de/breg-de/themen/digital-made-in-de/agentur-fuer-innovation-in-der-cybersicherheit-1546892.

— (2019b). *E-Evidence (grenzüberschreitende Gewinnung elektronischer Beweismittel in Strafverfahren)*. URL: https://cdn.netzpolitik.org/wp-upload/2019/07/Hintergrundpapier-e-Evidence-cl.pdf.pdf.

Bundesverfassungsgericht (2008). *Urteil vom 27. Februar 2008 - 1 BvR 370/07*. URL: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html.

— (2009). *Beschluss vom 18. Mai 2009 - 2 BvR 2233/07*. URL: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2009/05/rk20090518_2bvr223307.html.
— (2014). *Beschluss vom 04. Dezember 2014 - 2 BvE 3/14*. URL: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2014/12/es20141204_2bve000314.html.
— (2016a). *Beschluss des Zweiten Senats vom 13. Oktober 2016 - 2 BvE 2/15 -*. URL: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/10/es20161013_2bve000215.html.
— (2016b). *Urteil des Ersten Senats vom 20. April 2016 - 1 BvR 966/09 - 1 BvR 1140/09 -*. URL: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html.
— (2020). *Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 -*. URL: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2020/05/rs20200519_1bvr283517.html.
Bundeswehr (2020). *Kommando Cyber- und Informationsraum*. URL: https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-cyber-und-informationsraum.
Burns, William J. und Jared Cohen (2017). *The Rules of the Brave New Cyberworld*. URL: http://foreignpolicy.com/2017/02/16/the-rules-of-the-brave-new-cyberworld/.
Buzan, Barry, Ole Waever und Jaap de Wilde (1998). *Security: A new framework for analysis*. Boulder, Colorado: Lynne Rienner Publishers. ISBN: 1-55587-784-2.
Cabinet Office (1999). *Encryption and Law Enforcement*. URL: https://webarchive.nationalarchives.gov.uk/20000816090738/http://www.cabinet-office.gov.uk:80/innovation/1999/encryption/report.pdf.
— (2008). *The National Security Strategy of the United KingdomSecurity in an interdependent world*. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228539/7291.pdf.
— (2009). *Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space*. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf.
— (2011). *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.
Cairncross, Frances (2001). *The death of distance: How the communications revolution is changing our lives*. Boston: Harvard Business School Press. ISBN: 978-1578514380.
Cantir, Cristian und Juliet Kaarbo (2012). »Contested Roles and Domestic Politics: Reflections on Role Theory in Foreign Policy Analysis and IR Theory«. In: *Foreign Policy Analysis* 8.1, S. 5–24. ISSN: 17438586. DOI: 10.1111/j.1743-8594.2011.00156.x.
— Hrsg. (2016a). *Domestic role contestation, foreign policy, and international relations*. Bd. 6. Role theory and international relations. New York: Routledge, Taylor & Francis Group. ISBN: 978-1138653818.
— (2016b). »Unpacking Ego in Role Theory: Vertical and Horizontal Role Contestation and Foreign Policy«. In: *Domestic role contestation, foreign policy, and international relations*. Hrsg. von Cristian Cantir und Juliet Kaarbo. Role theory and international relations. New York: Routledge, Taylor & Francis Group, S. 1–22. ISBN: 978-1138653818.
Carlsnaes, Walter (2013). »Foreign Policy«. In: *Handbook of international relations*. Hrsg. von Walter Carlsnaes, Thomas Risse-Kappen und Beth A. Simmons. London und Thousand Oaks, CA: SAGE Publications, S. 298–325. ISBN: 978-1-84920-150-6.

Carr, Madeline (2016). *US Power and the Internet in International Relations: The Irony of the Information Age*. London: Palgrave Macmillan UK. ISBN: 978-1-349-71539-8. DOI: 10.1057/9781137550248.

CCC (2008). *§ 202c StGB gefährdet den IT-Standort Deutschland*. URL: https://www.ccc.de/de/updates/2008/stellungnahme202c.

— (2011). *Analyse einer Regierungs-Malware*. URL: https://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf.

— (2017). *Risiken für die innere Sicherheit beim Einsatz von Schadsoftware in der Strafverfolgung*. URL: https://www.ccc.de/system/uploads/227/original/Stellungnahme_CCC-Staatstrojaner.pdf.

CDU/CSU, S. P.D. (2013). *Deutschlands Zukunft gestalten. Koalitionsvertrag zwischen CDU, CSU und SPD*. URL: https://www.cdu.de/sites/default/files/media/dokumente/koalitionsvertrag.pdf.

Chertoff, Michael (2017). »A public policy perspective of the Dark Web«. In: *Journal of Cyber Policy*, S. 1–13. ISSN: 2373-8871. DOI: 10.1080/23738871.2017.1298643.

Choucri, Nazli (2012). *Cyberpolitics in international relations*. Cambridge, Mass.: MIT Press. ISBN: 9780262517690.

Chowdhurry, Mridul (2008). *The Role of the Internet in Burma's Saffron Revolution*. URL: http://cyber.harvard.edu/sites/cyber.harvard.edu/files/Chowdhury_Role_of_the_Internet_in_Burmas_Saffron_Revolution.pdf_0.pdf.

Christou, George (2017). *The EU's Approach to Cybersecurity: Challenges and Opportunities*. URL: http://repository.essex.ac.uk/19872/1/EU-Japan_9_Cyber_Security_Christou_EU.pdf.

DE-CIX (2018). *Internetknoten-Betreiber DE-CIX reicht Klage beim Bundesverfassungsgericht ein*. URL: https://www.de-cix.net/de/about-de-cix/media-center/press-releases/internet-exchange-operator-de-cix-files-lawsuit-with-the-german-constitutional-court.

Clarke, Richard A. und Robert K. Knake (2010). *Cyber war: The Next Threat to National Security and What to Do About It*. New York: Ecco. ISBN: 978-0061962233.

Cochran, Molly (2002). »Deweyan Pragmatism and Post-Positivist Social Science in IR«. In: *Millennium - Journal of International Studies* 31.3, S. 525–548. ISSN: 0305-8298. DOI: 10.1177/03058298020310030801.

Cohen-Almagor, Raphael (2011). »Internet History«. In: *International Journal of Technoethics* 2.2, S. 45–64. DOI: 10.4018/jte.2011040104.

Collier, David (2011). »Understanding Process Tracing«. In: *PS: Political Science & Politics* 44.04, S. 823–830. DOI: 10.1017/S1049096511001429.

Committee to protect Journalists (2013). *CPJ alarmed by Cameron's threat against UK press*. URL: https://cpj.org/2013/10/cpj-alarmed-by-camerons-threat-against-uk-press.php.

Cornish, Paul (2013). »United Kingom«. In: *Strategic cultures in Europe*. Hrsg. von Heiko Biehl, Bastian Giegerich und Alexandra Jonas. Schriftenreihe des Zentrums für Militärgeschichte und Sozialwissenschaften der Bundeswehr. Wiesbaden: Springer VS, S. 371–386. ISBN: 978-3-658-01167-3.

Côté, Adam (2016). »Agents without agency: Assessing the role of the audience in securitization theory«. In: *Security Dialogue* 47.6, S. 541–558. ISSN: 0967-0106. DOI: 10.1177/0967010616672150.

Council of Europe (1981). *Recommendation No. R (81) 12*. URL: https://rm.coe.int/09000016804cae97.

— (2001a). *Convention on Cybercrime*. URL: https://www.coe.int/de/web/conventions/full-list/-/conventions/rms/090000168008157a.

— (2001b). *Explanatory Report to the Convention on Cybercrime*. URL: https://rm.coe.int/16800cce5b.
— (2019). *Unterschriften und Ratifikationsstand des Vertrags 185: Übereinkommen über Computerkriminalität*. URL: https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=zhlD26Xq.
Council of the European Union (2014). *7th EU-Brazil Summit Brussels, 24 February 2014 Joint Statement*. URL: https://www.consilium.europa.eu/media/23829/141145.pdf.
Council on Foreign Relations (2020). *Cyber Operations Tracker*. URL: https://www.cfr.org/interactive/cyber-operations.
Craig, Anthony J.S. und Brandon Valeriano (2018). »Realism and Cyber Conflict: Security in the Digital Age«. In: *Realism in Practice*. Hrsg. von Davide Orsi, J. R. Avgustini und Max Nurnus. Bristol: E-International Relations, S. 85–101. ISBN: 978-1-910814-37-6.
Davidson, Donald (2001). *Subjective, intersubjective, objective*. Oxford und New York: Oxford University Press. ISBN: 0-19-823752-9.
— (2004). *Problems of rationality*. Oxford: Clarendon Press. ISBN: 0-19-823755-3.
Defence and Security Media Advisory Committee (2020). *The DSMA Notice System*. URL: https://dsma.uk/standing-notices/.
Deibert, Ronald (2013). *Black code: Inside the battle for cyberspace*. Toronto: McClelland & Stewart. ISBN: 978-0771025334.
Deibert, Ronald, John Palfrey und Rafal Rohozinski, Hrsg. (2012). *Access contested: Security, identity, and resistance in Asian cyberspace*. Bd. 2012: 1. The information revolution & global politics. Cambridge, Mass.: MIT Press. ISBN: 978-1-55250-507-6.
Deibert, Ronald, John G. Palfrey u. a. (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace*. Information revolution and global politics. Cambridge, Mass.: MIT Press. ISBN: 978-0-262-51435-4.
Deibert, Ronald J. (2012). »The Growing Dark Side of Cyberspace (…and What To Do About It)«. In: *Penn State Journal of Law & International Affairs* 1.2, S. 260–274.
Della Porta, Donatella und Michael Keating (2008). »How many approaches in the social sciences? An epistemological introduction«. In: *Approaches and methodologies in the social sciences*. Hrsg. von Donatella Della Porta und Michael Keating. Cambridge, N.Y.: Cambridge University Press, S. 19–39. ISBN: 978-0-511-42920-0.
Demchak, Chris C. und Peter Dombrowski (2011). »Rise of a Cybered Westphalian Age«. In: *Strategic Studies Quarterly* 5.1, S. 32–61.
DeNardis, Laura (2013). *The global war for internet governance*. New Haven [u.a.]: Yale Univ. Press. ISBN: 0300181353.
Department of Trade and Industry (1997). *Paper on regulatory intent concerning use of encryption on public networks*. URL: https://webarchive.nationalarchives.gov.uk/20000819120238/http://www.dti.gov.uk:80/cii/encrypt/.
Der Bundesbeauftragte für den Datenschutz und die Informationssicherheit (1999). *Eckpunkte der deutschen Kryptopolitik - ein Schritt in die richtige Richtung*. URL: https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/58DSK-EckpunkteDerDeutschenKryptopolitik-EinSchrittInDieRichtigeRichtung.pdf?__blob=publicationFile&v=1.
Deutscher Anwaltverein (2017a). *Stellungnahme Nr.: 33/2017*. URL: https://anwaltverein.de/de/newsroom/sn-33-17-neustrukturierung-des-bundeskriminalamtgesetzes?scope=modal&target=modal_reader_24&page_n27=92&file=files/anwaltverein.de/downloads/newsroom/stellungnahmen/2017/DAV-SN_33-17.pdf.

Deutscher Anwaltverein (2017b). *Stellungnahme Nr.: 44/2017*. URL: https://anwaltverein.de/de/newsroom/sn-44-17-einfuehrung-der-online-durchsuchung-und-quellen-tkue?file=files/anwaltverein.de/downloads/newsroom/stellungnahmen/2017/DAV-SN_44-17_%C3%84nderungsantrag.pdf.

Deutscher Bundestag (1974). *Drucksache 7/2067*. URL: http://dipbt.bundestag.de/doc/btd/07/020/0702067.pdf.

— (1983a). *Drucksache 10/318*. URL: http://dipbt.bundestag.de/doc/btd/10/003/1000318.pdf.

— (1983b). *Plenarprotokoll 10/25 vom 29. September 1983*. URL: http://dipbt.bundestag.de/dip21/btp/10/10025.pdf.

— (1986a). *Drucksache 10/119*. URL: http://dipbt.bundestag.de/doc/btd/10/001/1000119.pdf.

— (1986b). *Drucksache 10/5058*. URL: http://dipbt.bundestag.de/doc/btd/10/050/1005058.pdf.

— (1986c). *Plenarprotokoll 10/201 vom 27. Februar 1986*. URL: http://dipbt.bundestag.de/dip21/btp/10/10201.pdf.

— (1996). *Drucksache 13/4105*. URL: http://dipbt.bundestag.de/doc/btd/13/041/1304105.pdf.

— (1997a). *Drucksache 13/8859*. URL: http://dipbt.bundestag.de/doc/btd/13/088/1308859.pdf.

— (1997b). *Plenarprotokoll 13/170 vom 18. April 1997*. URL: http://dipbt.bundestag.de/dip21/btp/13/13170.pdf.

— (1998a). *Drucksache 13/11002*. URL: https://dipbt.bundestag.de/doc/btd/13/110/1311002.pdf.

— (1998b). *Drucksache 13/11004*. URL: http://dip21.bundestag.de/dip21/btd/13/110/1311004.pdf.

— (1999). *Drucksache 14/1149*. URL: http://dipbt.bundestag.de/doc/btd/14/011/1401149.pdf.

— (2001). *Drucksache 14/6321*. URL: https://dipbt.bundestag.de/doc/btd/14/063/1406321.pdf.

— (2006). *Drucksache 16/3973*. URL: http://dipbt.bundestag.de/dip21/btd/16/039/1603973.pdf.

— (2007a). *Drucksache 16/5449*. URL: http://dip21.bundestag.de/dip21/btd/16/054/1605449.pdf.

— (2007b). *Plenarprotokoll 16/100 vom 24. Mai 2007*. URL: http://dipbt.bundestag.de/dip21/btp/16/16100.pdf.

— (2008). *Plenarprotokoll 16/186 vom 12. November 2008*. URL: https://dip21.bundestag.de/dip21/btp/16/16186.pdf.

— (2010a). *Drucksache 17/3388*. URL: http://dipbt.bundestag.de/dip21/btd/17/033/1703388.pdf.

— (2010b). *Plenarporotokoll Plenarprotokoll 17/71 vom 11. November 2010*. URL: http://dipbt.bundestag.de/dip21/btp/17/17071.pdf.

— (2010c). *Plenarprotokoll 17/74 vom 24. November 2010*. URL: http://dipbt.bundestag.de/dip21/btp/17/17074.pdf.

— (2011a). *Drucksache 17/6971*. URL: http://dipbt.bundestag.de/doc/btd/17/069/1706971.pdf.

— (2011b). *Drucksache 17/7760*. URL: https://dipbt.bundestag.de/doc/btd/17/077/1707760.pdf.

— (2011c). *Wissenschaftliche Dienste: Ausarbeitung WD 2 – 3000 – 037/11*. URL: https://www.bundestag.de/resource/blob/414822/04afe986fd8aba8fe0c534d95c389309/WD-2-037-11-pdf-data.pdf.

— (2012). *Drucksache 17/11598*. URL: http://dipbt.bundestag.de/doc/btd/17/115/1711598.pdf.

— (2013a). *Drucksache 17/14560*. URL: https://dipbt.bundestag.de/doc/btd/17/145/1714560.pdf.

— (2013b). *Drucksache 17/14677*. URL: http://dipbt.bundestag.de/dip21/btd/17/146/1714677.pdf.

— (2013c). *Drucksache 17/14739*. URL: https://dip21.bundestag.de/dip21/btd/17/147/1714739.pdf.

— (2013d). *Drucksache 18/159*. URL: https://dipbt.bundestag.de/dip21/btd/18/001/1800159.pdf.

— (2013e). *Drucksache 18/168*. URL: https://dip21.bundestag.de/dip21/btd/18/001/1800168.pdf.

— (2013f). *Drucksache 18/182*. URL: http://dipbt.bundestag.de/doc/btd/18/001/1800182.pdf.

— (2013g). *Drucksache18/56*. URL: http://dipbt.bundestag.de/doc/btd/18/000/1800056.pdf.

— (2013h). *Drucksache18/65*. URL: http://dipbt.bundestag.de/doc/btd/18/000/1800065.pdf.

— (2013i). *Plenarprotokoll 18/2 vom 18. November 2013*. URL: http://dip21.bundestag.de/dip21/btp/18/18002.pdf.
— (2014a). *Drucksache18/843*. URL: http://dip21.bundestag.de/dip21/btd/18/008/1800843.pdf.
— (2014b). *Plenarprotokoll 18/10 vom 29. Januar 2014*. URL: http://dipbt.bundestag.de/dip21/btp/18/18010.pdf.
— (2014c). *Plenarprotokoll 18/16 vom 19. Februar 2014*. URL: https://dipbt.bundestag.de/doc/btp/18/18016.pdf.
— (2014d). *Plenarprotokoll 18/7 vom 15. Januar 2014*. URL: https://dip21.bundestag.de/dip21/btp/18/18007.pdf.
— (2015a). *Drucksache 18/3963*. URL: https://dip21.bundestag.de/dip21/btd/18/039/1803963.pdf.
— (2015b). *Drucksache 18/4286*. URL: https://dip21.bundestag.de/dip21/btd/18/042/1804286.pdf.
— (2015c). *Drucksache 18/5144*. URL: http://dipbt.bundestag.de/dip21/btd/18/051/1805144.pdf.
— (2015d). *Drucksache 18/6989*. URL: https://dipbt.bundestag.de/doc/btd/18/069/1806989.pdf.
— (2015e). *Plenarprotokoll 18/102 vom 6. Mai 2015*. URL: https://dip21.bundestag.de/dip21/btp/18/18102.pdf.
— (2015f). *Plenarprotokoll 18/106 vom 21. Mai 2015*. URL: http://dipbt.bundestag.de/doc/btp/18/18106.pdf.
— (2015g). *Plenarprotokoll 18/108 vom 10. Juni 2015*. URL: https://dip21.bundestag.de/dip21/btp/18/18108.pdf.
— (2015h). *Wissenschaftliche Dienste: WD 2 - 3000 - 038/15*. URL: https://www.bundestag.de/blob/406028/de1946480e133cf38bbee41d8d3d6898/wd-2-038-15-pdf-data.pdf.
— (2016a). *Die Rolle der Bundeswehr im Cyberraum Verfassungs-, völker- und sonstige nationale und internationale rechtliche Fragen sowie ethische Aspekte im Zusammenhang mit Cyberwarfare und die hieraus erwachsenden Herausforderungen und Aufgaben für die Bundeswehr*. URL: https://www.bundestag.de/resource/blob/417878/d8a5369a9df83e438814791a2881c5ef/Protokoll-Cyber-data.pdf.
— (2016b). *Drucksache 18/9142*. URL: http://dip21.bundestag.de/dip21/btd/18/091/1809142.pdf.
— (2016c). *Drucksache 18/9142*. URL: http://dip21.bundestag.de/dip21/btd/18/091/1809142.pdf.
— (2016d). *Drucksache 18/9311*. URL: http://dipbt.bundestag.de/dip21/btd/18/093/1809311.pdf.
— (2016e). *Plenarprotokoll 18/184 vom 8. Juli 2016*. URL: https://dipbt.bundestag.de/dip21/btp/18/18184.pdf.
— (2016f). *Plenarprotokoll 18/197 vom 21. Oktober 2016*. URL: http://dipbt.bundestag.de/dip21/btp/18/18197.pdf.
— (2017a). *NSA-Untersuchungsausschuss: US-Unternehmen verweigern Auskunft*. URL: https://www.bundestag.de/presse/pressemitteilungen#url=L3ByZXNzZS9wcmVzc2VtaXRoZWlsdW5nZW4vMjAx Ny9wbS0xNzAxMTkxLXBtLW5zYS0tNDg5MTcy&mod=mod454504.
— (2017b). *Drucksache 18/10900*. URL: https://dip21.bundestag.de/dip21/btd/18/109/1810900.pdf.
— (2017c). *Drucksache 18/12850*. URL: https://dip21.bundestag.de/dip21/btd/18/128/1812850.pdf.
— (2017d). *Plenarprotokoll 18/240*. URL: http://dipbt.bundestag.de/dip21/btp/18/18240.pdf.
— (2018a). *Drucksache 19/1419*. URL: http://dip21.bundestag.de/dip21/btd/19/014/1901419.pdf.
— (2018b). *Drucksache 19/1435*. URL: http://dip21.bundestag.de/dip21/btd/19/014/1901435.pdf.
— (2018c). *Drucksache 19/3420*. URL: http://dip21.bundestag.de/dip21/btd/19/034/1903420.pdf.

Deutscher Bundestag (2018d). *Drucksache 19/6246*. URL: http://dip21.bundestag.de/dip21/btd/19/062/1906246.pdf.

— (2018e). *Drucksache19/5472*. URL: https://dip21.bundestag.de/dip21/btd/19/054/1905472.pdf.

— (2018f). *Verfassungsmäßigkeit von sog. „Hackbacks" im Ausland - WD 3-3000 -159/18*. URL: https://www.bundestag.de/resource/blob/560900/bafobfb8f00a6814e125c8fce5e89009/wd-3-159-18-pdf-data.pdf.

— (2019). *Drucksache 19/8270*. URL: http://dip21.bundestag.de/dip21/btd/19/082/1908270.pdf.

Deutschlandfunk (2019a). *„Aktive Cyber-Abwehr" für Deutschland: Der geheime Krieg im Netz*. URL: https://www.deutschlandfunk.de/aktive-cyber-abwehr-fuer-deutschland-der-geheime-krieg-im.724.de.html?dram:article_id=461140.

— (2019b). *Kundus-Affäre: Rücktritt wegen misslungener Informationspolitik*. URL: https://www.deutschlandfunk.de/kundus-affaere-ruecktritt-wegen-misslungener.871.de.html?dram:article_id=464342.

Dewey, John (1938). *Logic: The Theory of Inquiry*. New York: Henry Holt and Company.

Diamond, Larry (2010). »Liberation Technology«. In: *Journal of Democracy* 21.3, S. 69–83. DOI: 10.1353/jod.0.0190.

Diersch, Verena und Martin Schmetz (2017). »Vom Cyberfrieden«. In: *Politische Theorie und Digitalisierung*. Hrsg. von Daniel Jacob und Thorsten Thiel. Baden-Baden: Nomos, S. 297–312. ISBN: 978-3-8487-3733-8.

Diffie, Whitfield und Martin Hellman (1976). »New directions in cryptography«. In: *IEEE Transactions on Information Theory* 22.6, S. 644–654. DOI: 10.1109/TIT.1976.1055638.

Digitalcourage (2017). *Allein vor Ort gegen die Hacking-Behörde ZITiS*. URL: https://digitalcourage.de/blog/2017/allein-vor-ort-gegen-die-hacking-behoerde-zitis.

DTI (1991). *Information Technology Security Evaluation Criteria (ITSEC)*. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf?__blob=publicationFile.

Dunn Cavelty, Myriam (2008). *Cyber-security and threat politics: US efforts to secure the information age*. CSS studies in security and international relations. London: Routledge. ISBN: 978-0415569880.

— (2012). »The Militarisation of Cyberspace: Why Less May Be Better«. In: *2012 4th International Conference on Cyber Conflict*. Hrsg. von Christian Czosseck, Rain Ottis und Katharina Ziolkowski. Piscataway, NJ: IEEE, S. 141–153. ISBN: 978-9949-9040-9-9.

— (2013). »Der Cyber-Krieg, der (so) nicht kommt. Erzählte Katastrophen als (Nicht)Wissenspraxis«. In: *Aufbruch ins Unversicherbare*. Hrsg. von Leon Hempel, Marie Bartels und Thomas Markwart. Sozialtheorie. Bielefeld [Germany]: Transcript, S. 209–234. ISBN: 978-3837617726.

— (2018). »Cybersecurity Research Meets Science and Technology Studies«. In: *Politics and Governance* 6.2, S. 22–30. DOI: 10.17645/pag.v6i2.1385.

Dunn Cavelty, Myriam und Kristian Søby Kristensen (2008). *Securing 'the homeland': Critical infrastructure, risk and (in)security*. CSS studies in security and international relations. London und New York: Routledge. ISBN: 978-0415441094.

EDRi (2006). *Consultation launched by UK government on the controversial RIPA act*. URL: https://edri.org/edrigramnumber4-13ukripa/.

EFF (2015). *Written evidence submitted by Electronic Frontier Foundation*. URL: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25107.html.

— (2017). *Five Eyes Unlimited: What A Global Anti-Encryption Regime Could Look Like*. URL: https://www.eff.org/deeplinks/2017/06/five-eyes-unlimited.
— (2019). *A Race to the Bottom of Privacy Protection: The US-UK Deal Would Trample Cross Border Privacy Safeguards*. URL: https://www.eff.org/deeplinks/2019/10/race-bottom-privacy-protection-us-uk-deal-would-trample-cross-border-privacy.
Eggenschwiler, Jacqueline und Jantje Silomon (2018). »Challenges and opportunities in cyber weapon norm construction«. In: *Computer Fraud & Security* 2018.12, S. 11–18. ISSN: 13613723. DOI: 10.1016/S1361-3723(18)30120-9.
Egloff, Florian und Andreas Wenger (2019). *Public Attribution of Cyber Incidents*. URL: https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/340841/CSSAnalyse244-EN.pdf?sequence=2&isAllowed=y.
Ehney, Ryan und Jack D. Shorter (2016). »Deep web, dark web, invisible web and the post ISIS world«. In: *Issues in Information Systems* 17.4, S. 36–41.
Ellul, Jacques (1964). *The technological society*. New York, NY: Knopf.
English PEN (2018). *Press Release: UK mass surveillance ruled unlawful in landmark judgment*. URL: https://www.englishpen.org/campaigns/press-release-uk-mass-surveillance-ruled-unlawful-in-landmark-judgment/.
Erskine, Toni und Madeline Carr (2016). »Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace«. In: *International cyber norms*. Hrsg. von Anna-Maria Osula und Henry Rõigas. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, S. 87–110. ISBN: 978-9949-9544-7-6.
EU (2005). *Rahmenbeschluss 2005/222/JI des Rates*. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32005F0222&from=EN.
— (2013). *Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates*. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32013L0040&from=de.
Europäischer Gerichtshof (2014). *The Court of Justice declares the Data Retention Directive to beinvalid*. URL: https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf.
European Court of Human Rights (2018). URL: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwipz5WI2IDoAhUlsaQKHSocDcYQFjAAegQIARAC&url=https%3A%2F%2Fhudoc.echr.coe.int%2Fapp%2Fconversion%2Fpdf%2F%3Flibrary%3DECHR%26id%3D003-6187848-8026299%26filename%3DBig%2520Brother%2520Watch%2520and%2520Others%2520v.%2520the%2520United%2520Kingdom%2520%2520-%2520complaints%2520about%2520surveillance%2520regimes.pdf&usg=AOvVaw37TCIQTFnTGnyVCCJZaO4c.
Eurostat (2018a). *Internet access of households, 2017*. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals#Internet_access.
— (2018b). *Internet-Zugang von Unternehmen*. URL: http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_ci_in_en2&lang=de.
Fafinski, Stefan (2006). »Computer Misuse: Denial-of-Service Attacks«. In: *The Journal of Criminal Law* 70.6, S. 474–478. ISSN: 0022-0183. DOI: 10.1350/jcla.2006.70.6.474.
Farwell, James P. und Rafal Rohozinski (2011). »Stuxnet and the Future of Cyber War«. In: *Survival* 53.1, S. 23–40. ISSN: 0039-6338. DOI: 10.1080/00396338.2011.555586.
FIfF (1997). *Verschlüsselungsgesetze stellen Grundrechte auf den Kopf*. URL: https://www.fiff.de/archiv/1997/verschlusselungsgesetze-stellen-grundrechte-auf-den-kopf.
— (2015). *Pressemitteilung Cybersicherheits-Strategie der Bundeswehr*. URL: http://www.fiff.de/presse/pressemitteilungen/pm_bw-cybersicheits-strategie.

Financial Times (2013). *UK becomes first state to admit to offensive cyber attack capability*. URL: https://www.ft.com/content/9ac6ede6-28fd-11e3-ab62-00144feab7de.

— (2014). *The web is a terrorist's command-and-control network of choice*. URL: https://www.ft.com/content/c89b6c58-6342-11e4-8a63-00144feabdc0.

Finnemore, Martha (1993). »International organizations as teachers of norms: The United Nations Educational, Scientific, and Cutural Organization and science policy«. In: *International Organization* 47.4, S. 565–597. DOI: 10.1017/S0020818300028101.

— (1996). *National interests in international society*. Cornell Studies in Political Economy. Ithaca und London: Cornell University Press. ISBN: 978-0-8014-8323-3.

— (2016). »Constructing norms for Global Cybersecurity«. In: *The American Journal of International Law* 110.3, S. 425–479.

Fischerkeller, Michael P. und Richard J. Harknett (2017). »Deterrence is Not a Credible Strategy for Cyberspace«. In: *Orbis* 61.3, S. 381–393. ISSN: 00304387. DOI: 10.1016/j.orbis.2017.05.003.

Floyd, Rita (2015). »Extraordinary or ordinary emergency measures: What, and who, defines the 'success' of securitization?« In: *Cambridge Review of International Affairs* 29.2, S. 677–694. ISSN: 0955-7571. DOI: 10.1080/09557571.2015.1077651.

Foreign & Commonwealth Office (2010). *Explanatory Memorandum on the Council of Europe Convention on Cybercrime*. URL: https://webarchive.nationalarchives.gov.uk/20100707164210/http://www.fco.gov.uk/en/about-us/publications-and-documents/treaty-command-papers-ems/explanatory-memoranda/explanatory-memoranda-2010/050Cybercrime.

— (2011). *Speech by James Brokenshire, Parliamentary Under-Secretary for Crime and Security, delivered at the 10th anniversary of the Budapest Convention*. URL: https://webarchive.nationalarchives.gov.uk/20130102174313/http://ukcoe.fco.gov.uk/resources/en/22792210/pdf-brokenshire.

— (2013a). *Building a new international consensus on the future of cyberspace*. URL: https://www.gov.uk/government/speeches/building-a-new-international-consensus-on-the-future-of-cyberspace.

— (2013b). *Foreign Secretary responds to Intelligence and Security Committee statement on GCHQ*. URL: https://www.gov.uk/government/news/foreign-secretary-responds-to-intelligence-and-security-committee-statement-on-gchq.

— (2017). *Response to General Assembly resolution 71/28 "Developments in the field of information and telecommunications in the context of international security" United Kingdom of Great Britain and Northern Ireland*.

— (2019). *NATO Parliamentary Assembly, October 2019: Foreign Secretary's speech*. URL: https://www.gov.uk/government/speeches/foreign-secretary-speech-to-the-nato-parliamentary-assembly-12-october-2019.

Franke, Ulrich, Hrsg. (2013). *Rekonstruktive Methoden der Weltpolitikforschung: Anwendungsbeispiele und Entwicklungstendenzen*. Forschungsstand Politikwissenschaft. Baden-Baden: Nomos. ISBN: 978-3-8329-7845-7.

Franke, Ulrich und Ulrich Roos (2017). »Rekonstruktive Ansätze in den Internationalen Beziehungen und der Weltpolitikforschung: Objektive Hermeneutik und Grounded Theory«. In: *Handbuch Internationale Beziehungen*. Hrsg. von Frank Sauer und Carlo Masala. Wiesbaden: Springer Fachmedien Wiesbaden, S. 619–640. ISBN: 978-3-531-19917-7.

Freiberg, Michael (2015). »Grenzen und Möglichkeiten der öffentlich-privaten Zusammenarbeit zum Schutz Kritischer IT-Infrastrukturen am Beispiel des Umsetzungsplan KRITIS«. In: *Cyber-Sicherheit*. Hrsg. von Hans-Jürgen Lange und Astrid Bötticher. Studien zur Inneren Sicherheit. Wiesbaden [Germany]: Springer VS, S. 103–120. ISBN: 978-3-658-02797-1.

Frenkler, Ulf u. a. (1997). *Deutsche, amerikanische und japanische Außenpolitikstrategien 1985-1995: Eine vergleichende Untersuchung zu Zivilisierungsprozessen in der Triade*. URL: https://www.uni-trier.de/fileadmin/fb3/POL/Projekte/civil.pdf.

Frey, Carl Benedikt und Michael A. Osborne (2017). »The future of employment: How susceptible are jobs to computerisation?« In: *Technological Forecasting and Social Change* 114, S. 254–280. ISSN: 00401625. DOI: 10.1016/j.techfore.2016.08.019.

Friss, Simone Molin (2015). »'Beyond anything we have ever seen': Beheading videos and the visibility of violence in the war against ISIS«. In: *International Affairs* 91.4, S. 725–746. DOI: 10.1111/1468-2346.12341.

Gartzke, Erik (2013). »The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth«. In: *International Security* 38.2, S. 41–73. ISSN: 01622889. DOI: 10.1162/ISEC{\textunderscore}a{\textunderscore}00136.

Gartzke, Erik und Jon R. Lindsay (2015). »Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace«. In: *Security Studies* 24.2, S. 316–348. ISSN: 0963-6412. DOI: 10.1080/09636412.2015.1038188.

Gaskarth, Jamie (2014). »Strategizing Britain's role in the world«. In: *International Affairs* 90.3, S. 559–581. DOI: 10.1111/1468-2346.12127.

— (2016). »Intervention, Domestic Contestation, and Britain's National Role Conceptions«. In: *Domestic role contestation, foreign policy, and international relations*. Hrsg. von Cristian Cantir und Juliet Kaarbo. Role theory and international relations. New York: Routledge, Taylor & Francis Group, S. 105–121. ISBN: 978-1138653818.

Gaycken, Sandro (2011). *Cyberwar: Das Internet als Kriegsschauplatz*. Changes. München: Open Source Press. ISBN: 978-3941841239.

GCHQ (2013). *Director GCHQ gives keynote speech at the Defence and Security Dinner*. URL: https://webarchive.nationalarchives.gov.uk/20140306085921/http://www.gchq.gov.uk/press_and_media/news_and_features/Pages/Directors-speech-at-LCCI.aspx.

— (2014). *IA14: Director GCHQ's closing remarks*. URL: https://webarchive.nationalarchives.gov.uk/20141203182616/http://www.gchq.gov.uk/press_and_media/speeches/Pages/IA14-directors-closing-remarks.aspx.

— (2018a). *Director GCHQ speaks at Billington Cyber Security Summit*. URL: https://www.gchq.gov.uk/news/director-gchq-speaks-billington-cyber-security-summit.

— (2018b). *GCHQ and the NCSC publish the UK Equities Process*. URL: https://www.gchq.gov.uk/news/dealing-vulnerabilities.

— (2018c). *Speech at CyberUK18 - as-delivered version - Director GCHQ 12 April 2018*. URL: https://www.gchq.gov.uk/speech/director-cyber-uk-speech-2018.

— (2018d). *The Equities Process*. URL: https://www.gchq.gov.uk/information/equities-process.

Generalbundesanwalt (2017). *Untersuchungen wegen der möglichen massenhaften Erhebung von Telekommunikationsdaten durch britische und US-amerikanische Nachrichtendienste abgeschlossen*. URL: https://www.generalbundesanwalt.de/de/showpress.php?newsid=732.

Gesellschaft für Freiheitsrechte (2018). *GFF erhebt Verfassungbeschwerde gegen massenhaften Einsatz von „Staatstrojanern"*. URL: https://freiheitsrechte.org/trojaner/.

Gesellschaft für Informatik (2015). *Verteidigungsanstrengungen der Bundesregierung gegen Cyberangriffe aus dem Internet unzureichend - Wirkungsvolle Maßnahmen gegen Angriffe und Angriffskriege im Internet gefordert*. URL: https://gi.de/meldung/verteidigungsanstrengungen-der-bundesregierung-gegen-cyberangriffe-aus-dem-internet-unzureichend-wirkungsvolle-massnahmen-gegen-angriffe-und-angriffskriege-im-internet-gefordert.

Ghani, Ashraf und Clare Lockhart (2008). *Fixing failed states*. Oxford: Oxford University Press. ISBN: 978-0-19-534269-7.

Giddens, Anthony (1984). *The constitution of society: Outline of the Theory of Structuration*. Cambridge: Polity Press. ISBN: 0-7456-0006-9.

Gilmore, Jonathan (2015). »Still a 'Force for Good'? Good International Citizenship in British Foreign and Security Policy«. In: *The British Journal of Politics and International Relations* 17.1, S. 106–129. DOI: 10.1111/1467-856X.12032.

Glaser, Charles L. und Chairn Kaufmann (1998). »What Is the Offense-Defense Balance and How Can We Measure It?« In: *International Security* 22.4, S. 44–82. ISSN: 01622889.

Gohdes, Anita R. (2018). »Studying the Internet and Violent conflict«. In: *Conflict Management and Peace Science* 35.1, S. 89–106. DOI: 10.1177/0738894217733878. eprint: https://doi.org/10.1177/0738894217733878. URL: https://doi.org/10.1177/0738894217733878.

Goines, Timothy M. (2017). »Overcoming the Cyber Weapons Paradox«. In: *Strategic Studies Quarterly* 11.4, S. 86–111.

Golem.de (2014). *Ellalink: Seekabel wird zwischen Europa und Lateinamerika gebaut*. URL: https://www.golem.de/news/ellalink-seekabel-wird-zwischen-europa-und-lateinamerika-gebaut-1901-138589.html.

Gorr, David und Wolf J. Schünemann (2013). »Creating a secure cyberspace – Securitization in Internet governance discourses and dispositives in Germany and Russia«. In: *International Review of Information Ethics* 20, S. 39–51.

Gould, Harry D. und Nicholas Onuf (2009). »Pragmatism, Legal Realism and Constructivism«. In: *Pragmatism in international relations*. Hrsg. von Harry Bauer und Elisabetta Brighi. London: Routledge, S. 26–44. ISBN: 978-0415663786.

Gourevitch, Peter (1978). »The Second Image Reversed: The International Sources of Domestic Politics«. In: *International Organization* 32.4, S. 881–912.

Government of Canada (2017). *Five Country Ministerial 2017: Joint Communiqué*. URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/fv-cntry-mnstrl-2017/fv-cntry-mnstrl-2017-en.pdf.

Graulich, Kurt (2015). *Nachrichtendienstliche Fernmeldeaufklärung mit Selektoren in einer transnationalen Kooperation: Prüfung und Bewertung von NSA-Selektoren nach Maßgabe des Beweisbeschlusses BND-26*. URL: https://www.bundestag.de/resource/blob/393598/b5d50731152a09ae36b42be50f283898/mat_a_sv-11-2-data.pdf.

Green, James A., Hrsg. (2015). *Cyber warfare: A multidisciplinary analysis*. Routledge studies in conflict, security and technology. London: Routledge. ISBN: 978-1-315-76156-5.

Guitton, Clement (2013). »Cyber insecurity as a national threat: Overreaction from Germany, France and the UK?« In: *European Security* 22.1, S. 21–35. ISSN: 0966-2839. DOI: 10.1080/09662839.2012.749864.

— (2017). *Inside the enemy's computer: Identifying cyber-attackers*. New York: Oxford University Press. ISBN: 9780190699994.

Guzzini, Stefano (2000). »A Reconstruction of Constructivism in International Relations«. In: *European Journal of International Relations* 6.2, S. 147–182. ISSN: 1354-0661. DOI: 10.1177/1354066100006002001.

Habermas, Jürgen (1982). *Theorie des kommunikativen Handelns: Band I Handlungsrationalität und gesellschaftliche Rationalisierung*. Zweite Auflage. Frankfurt am Main: Suhrkamp. ISBN: 3-518-07591-8.

Hafner, Katie und Matthew Lyon (1996). *Where wizards stay up late: The origins of the Internet*. New York: Touchstone. ISBN: 0-684-87216-1.

Hammond, Brian (2013). »Failure to Reach Consensus at WCIT Prompts Calls for Renewed Effort to Support Multistakeholder Approach«. In: *Telecommunications Reports* 79.1, S. 48–51.

Handelsblatt (2015). *Ex-Richter Graulich als Sonderermittler berufen*. URL: https://www.handelsblatt.com/politik/deutschland/nsa-ausschuss-ex-richter-graulich-als-sonderermittler-berufen/12001902.html.

Harknett, Richard J. und Joseph S. Nye (2017). »Is Deterrence Possible in Cyberspace?« In: *International Security* 42.2, S. 196–199. ISSN: 01622889. DOI: 10.1162/ISEC{\textunderscore}c{\textunderscore}00290.

Harnisch, Sebastian (2012a). »Conceptualizing in the Minefield: Role Theory and Foreign Policy Learning«. In: *Foreign Policy Analysis* 8.1, S. 47–69. ISSN: 17438586. DOI: 10.1111/j.1743-8594.2011.00155.x.

— (2012b). »Role theory: Operationalization of key concepts«. In: *Role theory in international relations*. Hrsg. von Sebastian Harnisch, Cornelia Frank und Hanns Maull. Routledge advances in international relations and global politics. London: Routledge, Taylor & Francis Group, S. 7–15. ISBN: 978-0415830218.

— (2013). »German Foreign Policy: Gulliver's Travails in the 21st Century«. In: *Foreign policy in comparative perspective*. Hrsg. von Ryan K. Beasley. Thousand Oaks, California: CQ Press, S. 71–93. ISBN: 978-1-60871-696-8.

— (2014). *Full-spectrum role-taking: A two-level role theoretical model*. URL: http://www.uni-heidelberg.de/md/politik/harnisch/person/vortraege/harnisch_2014_-_isa_conference_paper_full_spectrum_role_taking_draft_24_03.pdf.

— (2016). »Role theory and the study of Chinese foreign policy«. In: *China's international roles*. Hrsg. von Sebastian Harnisch, Sebastian Bersick und Jörn-Carsten Gottwald. Role theory and international relations. New York: Routledge, S. 3–21. ISBN: 978-1-138-90381-4.

— (2018). *Role Theory in International Relations*. DOI: 10.1093/obo/9780199743292-0226. URL: http://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0226.xml?rskey.

— (2020). »Internationale Führung und ihre Kontestation. Zur Dynamik der außenpolitischen Rolle der Bundesrepublik in Europa«. In: *Zivilmacht Bundesrepublik?* Hrsg. von Klaus Brummer und Friedrich Kießling. Edition Themengruppe Außen- und Sicherheitspolitik. Baden-Baden: Nomos, S. 109–131. ISBN: 978-3-7489-0487-8.

Harnisch, Sebastian und Hanns Maull (2001). *Germany as a civilian power? The foreign policy of the Berlin Republic*. Issues in German politics. Manchester und New York: Manchester University Press. ISBN: 978-0719060410.

Hathaway, Melissa (2017). *Getting beyond Norms. When Violating the Agreement Becomes Customary Practice*. URL: https://www.cigionline.org/sites/default/files/documents/Paper%20no.127.pdf.

Häußling, Roger (2014). *Techniksoziologie*. 1. Aufl. Bd. 4184. UTB. Baden-Baden: Nomos. ISBN: 978-3-8252-4184-1.

Hegel, Georg Wilhelm Friedrich (1989 [1807]). *Phänomenologie des Geistes*. 2. Auflage. Bd. 603. Suhrkamp-Taschenbuch Wissenschaft. Frankfurt am Main: Suhrkamp.

heise.de (1997). *Kanther fordert Key Escrow*. URL: https://www.heise.de/tp/features/Kanther-fordert-Key-Escrow-3411134.html.

— (2001a). *Ein großer Schritt in Richtung europäischer Überwachungsstaat*. URL: https://www.heise.de/tp/features/Ein-grosser-Schritt-in-Richtung-europaeischer-Ueberwachungsstaat-3448504.html.

heise.de (2001b). *Fette Bugs im Cybercrime-Abkommen*. URL: https://www.heise.de/tp/features/Fette-Bugs-im-Cybercrime-Abkommen-3448055.html.

— (2006). *Mit Datennetzen zur Bundeswehr aus autonomen selbstorganisierenden Einheiten*. URL: https://www.heise.de/newsticker/meldung/Mit-Datennetzen-zur-Bundeswehr-aus-autonomen-selbstorganisierenden-Einheiten-124762.html.

— (2014). *NSA-Skandal: Wie der GCHQ Belgacom hackte*. URL: https://www.heise.de/newsticker/meldung/NSA-Skandal-Wie-der-GCHQ-Belgacom-hackte-2489400.html.

— (2017a). *Bitkom: Datenschutz bei Whatsapp & Co. nicht leichtfertig aushebeln*. URL: https://www.heise.de/newsticker/meldung/Bitkom-Datenschutz-bei-Whatsapp-Co-nicht-leichtfertig-aushebeln-3742668.html.

— (2017b). *Bundestag gibt Staatstrojaner für die alltägliche Strafverfolgung frei*. URL: https://www.heise.de/newsticker/meldung/Bundestag-gibt-Staatstrojaner-fuer-die-alltaegliche-Strafverfolgung-frei-3753530.html.

— (2018a). *Schlagabtausch zu ZITiS: IT-Sicherheitslücken schließen oder ausnutzen?* URL: https://www.heise.de/newsticker/meldung/Schlagabtausch-zu-ZITiS-IT-Sicherheitsluecken-schliessen-oder-ausnutzen-3976587.html.

— (2018b). *TLS-Standardisierung: Behörden und Banken wollen Verschlüsselung aushöhlen*. URL: https://www.heise.de/newsticker/meldung/TLS-Standardisierung-Behoerden-und-Banken-wollen-Verschluesselung-aushoehlen-3999118.html.

— (2019). *E-Evidence: Bundesregierung sieht Grundrechteschutz gefährdet*. URL: https://www.heise.de/newsticker/meldung/E-Evidence-Bundesregierung-sieht-Grundrechteschutz-gefaehrdet-4465328.html.

Hellmann, Gunther (2010). »Pragmatismus«. In: *Handbuch der internationalen Politik*. Hrsg. von Carlo Masala, Frank Sauer und Andreas Wilhelm. Wiesbaden: VS, Verl. für Sozialwiss., S. 148–181. ISBN: 3531921487.

Henriksen, Anders (2019). »The end of the road for the UN GGE process: The future regulation of cyberspace«. In: *Journal of Cybersecurity* 5.1, S. 1–9. DOI: 10.1093/cybsec/tyy009.

Herborth, Benjamin (2017). »Rekonstruktive Forschungslogik in den Internationalen Beziehungen«. In: *Handbuch Internationale Beziehungen*. Hrsg. von Frank Sauer und Carlo Masala. Wiesbaden: Springer Fachmedien Wiesbaden, S. 619–640. ISBN: 978-3-531-19917-7.

Herzog, Stephen (2011). »Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses«. In: *Journal of Strategic Security* 4.2, S. 49–60. DOI: 10.5038/1944-0472.4.2.3.

Hickson, Nigel (1997). »Encryption policy. A UK perspective«. In: *Computers & Security* 16, S. 583–589. ISSN: 01674048.

High Court of Justice (2019). *[2019] EWHC 2057 (Admin)*. URL: https://www.judiciary.uk/wp-content/uploads/2019/07/Liberty-judgment-Final.pdf.

Hill, Richard (2016). »Internet governance, multi-stakeholder models, and the IANA transition: Shining example or dark side?« In: *Journal of Cyber Policy* 1.2, S. 176–197. ISSN: 2373-8871. DOI: 10.1080/23738871.2016.1227866.

Hoffmann-Riem, Wolfgang (2014). *Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 22. Mai 2014*. URL: https://www.bundestag.de/resource/blob/280846/04f34c512c86876b06f7c162e673f2db/MAT_A_SV-2-1neu-pdf-data.pdf.

Hollis, Martin (1994). *The philosophy of social science: An introduction*. Cambridge [England] und New York, NY, USA: Cambridge University Press. ISBN: 0521447801.

Hollis, Martin und Steve Smith (1990). *Explaining and understanding international relations*. Oxford und New York: Clarendon Press und Oxford University Press. ISBN: 9780198275893.

Holsti, Kalevi J. (1970). »National Role Conceptions in the Study of Foreign Policy«. In: *International Studies Quarterly* 14.3, S. 233–309. ISSN: 00208833. DOI: 10.2307/3013584.

Home Office (2004). *The Computer Misuse Act 1990*. URL: https://webarchive.nationalarchives.gov.uk/20041123045128/http://www.homeoffice.gov.uk/crime/internetcrime/compmisuse.html.

— (2006). *Investigation of Protected Electronic Information - A public consultation*. URL: https://webarchive.nationalarchives.gov.uk/20060715162121/http://www.homeoffice.gov.uk/documents/cons-2006-ripa-part3/ripa-part3.pdf?view=Binary.

— (2007). *Investigatory Powers: The Regulation of Investigatory Powers (Investigation of Protected Electronic Information: Code of Practice) Order 2007*. URL: http://www.legislation.gov.uk/uksi/2007/2200/pdfs/uksi_20072200_en.pdf.

— (2015a). *Acquisition and Disclosure of Communications Data*. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015.pdf.

— (2015b). *Equipment Interference: Code of Practice*. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/401863/Draft_Equipment_Interference_Code_of_Practice.pdf.

— (2015c). *Regulation of Investigatory Powers Act Government Response: Interception of Communications and Equipment Interference Codes of Practice Public Consultation*. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473692/Interception_and_EI_codes_consultation_government_response.pdf.

— (2018a). *Equipment Interference - Code of Practice*. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf.

— (2018b). *GCHQ's planned use of the Investigatory Powers Act 2016 Bulk Equipment Interference Regime*. URL: http://data.parliament.uk/DepositedPapers/Files/DEP2018-1198/Security_Minister_to_Dominic_Grieve-Investigatory_Powers_Act_2016.pdf.

— (2018c). *Investigatory Powers Tribunal appeals route introduced*. URL: https://www.gov.uk/government/news/investigatory-powers-tribunal-appeals-route-introduced.

House of Commons (1990a). *Hansard for 4 May 1990*. URL: https://hansard.parliament.uk/commons/1990-05-04/debates/6b3d12e1-0ac4-4024-915d-2354a743621a/CommonsChamber.

— (1990b). *Hansard for 9 February 1990*. URL: https://api.parliament.uk/historic-hansard/sittings/1990/feb/09#commons.

— (1997). *Hansard for 12 February 1997*. URL: https://hansard.parliament.uk/Commons/1997-02-12/debates/733e34c5-183c-4222-9731-5d23c4415749/PoliceBillLords.

— (1999a). *Hansard for 14 December 1999*. URL: https://hansard.parliament.uk/Commons/1999-12-14/debates/2115925f-ac5b-4ebd-9364-2a8b93643a5a/CommonsChamber.

— (1999b). *Hansard for 29 November 1999*. URL: https://hansard.parliament.uk/Commons/1999-11-29/debates/297ab4e3-624f-45c5-9b94-8c459451c248/ElectronicCommunicationsBill.

— (1999c). *Trade and Industry - Seventh Report*. URL: https://publications.parliament.uk/pa/cm199899/cmselect/cmtrdind/187/18708.htm.

— (2000a). *Hansard for 10 July 2000*. URL: https://hansard.parliament.uk/Commons/2000-07-10/debates/7abd01aa-4cbc-4e74-99c3-13ae78ebd8ab/CommonsChamber.

House of Commons (2000b). *Hansard for 26 July 2000*. URL: https://hansard.parliament.uk/Commons/2000-07-26/debates/02d133e1-f824-4a39-8e1b-7d295414ebad/RegulationOfInvestigatoryPowersBill.
— (2000c). *Hansard for 26 June 2000*. URL: https://hansard.parliament.uk/Commons/2000-06-26/debates/41556d76-c075-45af-9b8c-fee0a6ec95bf/RegulationOfInvestigatoryPowersBill.
— (2000d). *Hansard for 6 March 2000*. URL: https://hansard.parliament.uk/Commons/2000-03-06/debates/ea7faab1-565e-4fd7-88e6-c908ee07b2c6/RegulationOfInvestigatoryPowersBill.
— (2011a). *Hansard for 3 February 2011*. URL: https://hansard.parliament.uk/Commons/2011-02-03/debates/11020321000003/ProposedDirective(InformationSystems).
— (2011b). *UK Government opt-in decisions in the Area of Freedom, Security and Justice*. URL: http://www.parliament.uk/briefing-papers/sn06087.pdf.
— (2013a). *Defence and Cyber-Security - Sixth Report of Session 2012-13*. URL: https://publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/106.pdf.
— (2013b). *Defence and Cyber-Security: Government Response to the Committee's Sixth Report of Session 2012-13*. URL: https://publications.parliament.uk/pa/cm201213/cmselect/cmdfence/719/719.pdf.
— (2013c). *Hansard for 10 June 2013*. URL: https://publications.parliament.uk/pa/cm201314/cmhansrd/chan14.pdf.
— (2013d). *Hansard for 28 October 2013*. URL: https://publications.parliament.uk/pa/cm201314/cmhansrd/chan64.pdf.
— (2013e). *Hansard for 31 October 2013*. URL: https://publications.parliament.uk/pa/cm201314/cmhansrd/chan67.pdf.
— (2014a). *Hansard for 4 March 2014*. URL: https://publications.parliament.uk/pa/cm201314/cmhansrd/chan130.pdf.
— (2014b). *Intervention: Why, When and How? Fourteenth Report of Session 2013-14*. URL: https://publications.parliament.uk/pa/cm201314/cmselect/cmdfence/952/952.pdf.
— (2015a). *Flexible response? An SDSR checklist of potential threats and vulnerabilities - First Report of Session 2015-16*. URL: https://publications.parliament.uk/pa/cm201516/cmselect/cmdfence/493/493.pdf.
— (2015b). *Hansard for 14 January 2015*. URL: https://publications.parliament.uk/pa/cm201415/cmhansrd/cm150114/debindx/150114-x.htm.
— (2015c). *Hansard for 19 October 2015*. URL: https://publications.parliament.uk/pa/cm201516/cmhansrd/cm151019/debtext/151019-0001.htm.
— (2015d). *Hansard for 25 June 2015*. URL: https://publications.parliament.uk/pa/cm201516/cmhansrd/chan16.pdf.
— (2015e). *Hansard for 4 November 2015*. URL: https://publications.parliament.uk/pa/cm201516/cmhansrd/cm151104/debindx/151104-x.htm.
— (2016a). *Hansard for 15 March 2016*. URL: https://publications.parliament.uk/pa/cm201516/cmhansrd/chan133.pdf.
— (2016b). *Hansard for 6 June 2016*. URL: https://hansard.parliament.uk/Commons/2016-06-06/debates/160606130000001/InvestigatoryPowersBill.
— (2016c). *Hansard for 7 January 2016: Delegated Legislation Committee. Draft Equipment Interference (Code of Practice) Order 2015*. URL: https://hansard.parliament.uk/Commons/2016-01-07/debates/2237e393-18e0-4724-8779-d90dcb1992ec/DraftRegulationOfInvestigatoryPowers(InterceptionOfCommunicationsCodeOfPractice)Order2015DraftEquipmentInterference(CodeOfPractice)Order2015.

— (2016d). *Investigatory Powers Bill: technology issues: Third Report of Session 2015–16*. URL: https://publications.parliament.uk/pa/cm201516/cmselect/cmsctech/573/573.pdf.
— (2016e). *Russia: Implications for UK defence and security - First Report of Session 2016–17*. URL: https://publications.parliament.uk/pa/cm201617/cmselect/cmdfence/107/107.pdf.
— (2018a). *Hansard for 12 March 2018*. URL: https://hansard.parliament.uk/pdf/Commons/2018-03-12.
— (2018b). *Hansard for 3 December 2018*. URL: https://hansard.parliament.uk/Commons/2018-12-03/debates/695775DE-5C86-4A56-81E9-88F1CFB9A8DA/Crime(OverseasProductionOrders)Bill(Lords).
— (2018c). *Hansard for 5 September 2018*. URL: https://hansard.parliament.uk/commons/2018-09-05.
— (2019). *Hansard for 3 July 2019*. URL: https://hansard.parliament.uk/pdf/Commons/2019-07-03.
House of Lords (1988). *HL 21 Apr 1988*. URL: https://swarb.co.uk/regina-v-gold-and-schifreen-hl-21-apr-1988/.
— (1990). *Hansard for 15 May 1990*. URL: https://hansard.parliament.uk/Lords/1990-05-15/debates/20879c49-6b5e-4420-835a-5163e08fdb20/LordsChamber.
— (1997). *Hansard for 20 January 1997*. URL: https://hansard.parliament.uk/Lords/1997-01-20/debates/44bc420f-56d2-4376-8663-bc82626d9430/PoliceBillHl.
— (2000). *Hansard for 6 April 2000*. URL: https://hansard.parliament.uk/Lords/2000-04-06/debates/b6d131c4-e09d-445c-880e-7dd05fcc90a5/LordsChamber.
— (2002a). *Computer Misuse (Amendment) Bill*. URL: https://publications.parliament.uk/pa/ld200102/ldbills/079/2002079.pdf.
— (2002b). *Hansard for 20 June 2002*. URL: https://hansard.parliament.uk/Lords/2002-06-20/debates/ef0c2fb5-7bdb-494e-a90e-5ab36ec6e84e/ComputerMisuse(Amendment)BillHl?.
House of Lords und House of Commons (2008). *A Bill of Rights for the UK? Twenty–ninth Report of Session 2007–08*. URL: https://publications.parliament.uk/pa/jt200708/jtselect/jtrights/165/165i.pdf.
— (2016). *Legislative Scrutiny: Investigatory Powers Bill: First Report of Session 2016-17*. URL: https://publications.parliament.uk/pa/jt201617/jtselect/jtrights/104/104.pdf.
Housen-Couriel, Deborah (2013). *The "Dubai Clash" at WCIT-12: Freedom of Information, Access Rights, and Cyber Security*. URL: http://www.inss.org.il/uploadImages/systemFiles/06%20The%20Dubai%20Clash.pdf.
Howard, Philip N. und Muzammil M. Hussain (2011). »The Role of Digital Media«. In: *Journal of Democracy* 22.3, S. 35–48. DOI: 10.1353/jod.2011.0041.
Howard, Tiffiany (2016). *Failed states and the origins of violence: A comparative analysis of state failure as a root cause of terrorism and political violence*. London: Routledge. ISBN: 978-1-4724-1780-0.
Hoyningen-Huene, Paul (1989). *Die Wissenschaftsphilosophie Thomas S. Kuhns: Rekonstruktion und Grundlagenprobleme*. Bd. 27. Wissenschaftstheorie Wissenschaft und Philosophie. Wiesbaden: Vieweg+Teubner Verlag und Imprint. ISBN: 978-3-663-07954-5.
Hudson, Valerie M. (2014). *Foreign policy analysis: Classic and contemporary theory*. Second edition. Lanham: Rowman & Littlefield. ISBN: 978-1-4422-2005-8.
Human Rights Watch (2017). *Joint Letter to Five Eyes Intelligence Agencies Regarding Encryption*. URL: https://www.hrw.org/sites/default/files/supporting_resources/five_eyes_coalition_letter.pdf.

Intelligence and Security Committee (2013a). *Statement on GCHQ's Alleged Interception of Communicationsunder the US PRISM Programme*. URL: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20130717_ISC_statement_GCHQ.pdf.

— (2013b). *Uncorrected Transcript of Evidence*. URL: https://docs.google.com/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDoyYjM3NWU1NDQ5NTg0OTQ0.

— (2014a). *Annual Report 2013-2014*. URL: http://isc.independent.gov.uk/files/2013-2014_ISC_AR.pdf.

— (2014b). *Privacy and Security Inquiry: Public Evidence Session 1*. URL: http://isc.independent.gov.uk/public-evidence/14october2014/20141014_ISC_Uncorrected_Transcript_P%2BS_Session1.pdf.

— (2014c). *Privacy and Security Inquiry: Public Evidence Session 2*. URL: http://isc.independent.gov.uk/public-evidence/15october2014/20141015_ISC_Uncorrected_Transcript_P%2BS_Session2.pdf.

— (2014d). *Privacy and Security Inquiry: Public Evidence Session 3*. URL: http://isc.independent.gov.uk/public-evidence/15october2014-1/20141015_ISC_Uncorrected_Transcript_P%2BS_Session3.pdf.

— (2014e). *Report on the intelligence relating to the murder of Fusilier Lee Rigby*. URL: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20141125_ISC_Woolwich_Report%28website%29.pdf.

— (2015). *Privacy and Security: A modern and transparent legal framework*. URL: isc.independent.gov.uk/files/20150312_ISC_P+S+Rpt(web).pdf.

— (2017). *Annual Report 2016-2017*. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727949/ISC-Annual-Report-2016-17.pdf.

International Centre for Security Analysis (2017). *Written evidence by the International Centre for Security Analysis, King's College London, to the Parliamentary Joint Committee on the National Security Strategy's Inquiry on Cyber Security: UK National Security in a Digital World*. URL: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/national-security-strategy-committee/cyber-security-uk-national-security-in-a-digital-world/written/47199.pdf.

Investigatory Powers Tribunal (2014). *Case Nos: IPT/13/77/H, IPT/13/92/CH, IPT/13/168-173/H, IPT/13/194/CH, IPT/13/204/CH*. URL: https://www.ipt-uk.com/docs/IPT_13_168-173_H.pdf.

— (2015a). *[2015] UKIPTrib 13_132-H*. URL: https://www.ipt-uk.com/docs/ABDEL%20HAKIM%20BELHADJ%20Final.zip.

— (2015b). *[2015] UKIPTrib 13_77-H_2*. URL: https://www.ipt-uk.com/docs/Final_Liberty_Ors_Open_Determination_Amended.pdf.

— (2015c). *Case Nos: IPT/13/77/H, IPT/13/92/CH, IPT/13/168-173/H, IPT/13/194/CH, IPT/13/204/CH*. URL: https://www.ipt-uk.com/docs/Liberty-Order6Feb15.pdf.

— (2015d). *Witness Statement of Eric King*. URL: https://privacyinternational.org/sites/default/files/2018-03/2015.10.05%20Witness_Statement_Of_Eric_King.pdf.

— (2016). *[2016] UKIPTrib 14_85-CH*. URL: https://www.ipt-uk.com/docs/Privacy_Greennet_and_Sec_of_State.pdf.

IOCCO (2014). *2013 Annual Report of the Interception of Communications Commissioner*. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/302597/InterceptionCommunicationsCommissionerPrint.pdf.

Jackson, Patrick Thaddeus (2011). *The conduct of inquiry in international relations: Philosophy of science and its implications for the study of world politics*. The new international relations. London und New York: Routledge. ISBN: 0-203-84332-0.

Jahn, Detlef (2015). »Fälle, Fallstricke und die komparative Methode in der vergleichenden Politikwissenschaft«. In: *Vergleichen in der Politikwissenschaft*. Hrsg. von Sabine Kropp und Michael Minkenberg. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 55–75. ISBN: 978-3-531-13876-3.

James, William (1922). *Pragmatism: A New Name for Some Old Ways of Thinking*. New York und London: Longmans, Green and Co. ISBN: 0915145057.

Jones, Evan (2017). »"Sellout" Ministries and Jingoes: China's Bureaucratic Institutions and the Evolution of Contested National Role Conceptions in the South China Sea«. In: *Foreign Policy Analysis* 13.2, S. 361–379. ISSN: 17438586. DOI: 10.1093/fpa/orw059.

Jönsson, Christer (1984). *Superpower: Comparing American and Soviet foreign policy*. London: Frances Pinter. ISBN: 0861873777.

Jünemann, Annette und Anja Zorob, Hrsg. (2012). *Arabisches Erwachen: Zur Vielfalt von Protest und Revolte im Nahen Osten und Nordafrika*. 2012. Aufl. Politik und Gesellschaft des Nahen Ostens. Wiesbaden: VS Verlag für Sozialwissenschaften. ISBN: 978-3-531-19273-4.

Junk, Julian und Christopher Daase (2013). »Germany«. In: *Strategic cultures in Europe*. Hrsg. von Heiko Biehl, Bastian Giegerich und Alexandra Jonas. Schriftenreihe des Zentrums für Militärgeschichte und Sozialwissenschaften der Bundeswehr. Wiesbaden: Springer VS, S. 139–152. ISBN: 978-3-658-01167-3.

JUSTICE (2000). *Regulation of Investigatory Powers Act 2000*. URL: https://justice.org.uk/regulation-investigatory-powers-act-2000/.

Justizministerium (2018). *Letter to the EU Commission*. URL: https://cdn.netzpolitik.org/wp-upload/2018/11/2018-11-20_Justizminister-Brief_E-Evidence1.pdf.

Kaarbo, Juliet (2015). »A Foreign Policy Analysis Perspective on the Domestic Politics Turn in IR Theory«. In: *International Studies Review*, S. 1–28. DOI: 10.1111/misr.12213.

Kalathil, Shanthi und Taylor C. Boas (2003). *Open networks, closed regimes: The impact of the internet on authoritarian rule*. Washington: Carnegie Endowment for International Peace. ISBN: 0-87003-194-5.

Kant, Immanuel (1965 [1795]). »Zum ewigen Frieden. Ein philosophischer Entwurf (1795)«. In: *Immanuel Kant*. Hrsg. von Otto Heinrich von der Gablentz. Klassiker der Politik. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 104–150. ISBN: 978-3-663-19698-3.

Karatzogianni, Athina (2015). *Firebrand Waves of Digital Activism 1994–2014*. London: Palgrave Macmillan UK. ISBN: 978-1-349-56096-7. DOI: 10.1057/9781137317933.

Kaunert, Christian, Sarah Léonard und Alex MacKenzie (2012). »The social construction of an EU interest in counter-terrorism: US influence and internal struggles in the cases of PNR and SWIFT«. In: *European Security* 21.4, S. 474–496. ISSN: 0966-2839. DOI: 10.1080/09662839.2012.688812.

Keane, Conor und Steve Wood (2016). »Bureaucratic Politics, Role Conflict, and the Internal Dynamics of US Provincial Reconstruction Teams in Afghanistan«. In: *Armed Forces & Society* 42.1, S. 99–118. ISSN: 0095-327X. DOI: 10.1177/0095327X15572113.

Kehl, Danielle, Andi Wilson und Kevin Bankston (2015). *Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s*. URL: https://static.newamerica.org/attachments/3407-doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/Crypto%20Wars_ReDo.7cb491837ac541709797bdf868d37f52.pdf.

Keller, Reiner (2013). »Zur Praxis der Wissenssoziologischen Diskursanalyse«. In: *Methodologie und Praxis der Wissenssoziologischen Diskursanalyse*. Hrsg. von Reiner Keller und Inga Truschkat. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 27–68. ISBN: 978-3-531-17874-5.

Kello, Lucas (2013). »The Meaning of the Cyber Revolution: Perils to Theory and Statecraft«. In: *International Security* 38.2, S. 7–40. ISSN: 01622889. DOI: 10.1162/ISEC{\textunderscore}a{\textunderscore}00138.

King, Gary, Robert O. Keohane und Sidney Verba (1994). *Designing social inquiry*. Princeton, N.J., Chichester: Princeton University Press. ISBN: 0-691-03471-0.

Kink, Markus und Janine Ziegler, Hrsg. (2013). *Staatsansichten - Staatsvisionen: Ein politik- und kulturwissenschaftlicher Querschnitt*. Bd. Band 8. Studien zur visuellen Politik. Berlin: Lit. ISBN: 978-3-643-11613-0.

Kleinrock, Leonard (2010). »An Early History of the Internet«. In: *IEEE Communications Magazine* August, S. 26–36.

Kneuer, Marianne (2015). »Mehr demokratische Qualität durch das Internet?« In: *Journal of Self-Regulation and Regulation* 1, S. 47–63. DOI: 10.11588/josar.2015.0.23481.

Kuhn, Thomas S. (1996). *The structure of scientific revolutions*. 3rd edition. Chicago und London: University of Chicago Press. ISBN: 0-226-45807-5.

Kurz, Constanze und Frank Rieger (2018). *Cyberwar – Die Gefahr aus dem Netz: Wer uns bedroht und wie wir uns wehren können*. München: C. Bertelsmann. ISBN: 978-3570103517.

Lake, David A. (1992). »Powerful Pacifists: Democratic States and War«. In: *American Political Science Review* 86.1, S. 24–37. DOI: 10.2307/1964013.

— (2013). »Theory is dead, long live theory: The end of the Great Debates and the rise of eclecticism in International Relations«. In: *European Journal of International Relations* 19.3, S. 567–587. ISSN: 1354-0661. DOI: 10.1177/1354066113494330.

Lawson, Sean T. u. a. (2016). »The Cyber-Doom Effect: The Impact of Fear Appeals in the US Cyber Security Debate«. In: *2016 8th International Conference on Cyber Conflict*. Hrsg. von Nikolaos Pissanidis, Henry Rõigas und Matthijs Veenendaal. Tallinn, Estonia: NATO CCD COE Publications, S. 65–80. ISBN: 978-9949-9544-9-0.

Lazanski, Dominique (2013). »Splitting up the internet«. In: *Index on Censorship* 42.1, S. 57–60. ISSN: 0306-4220. DOI: 10.1177/0306422013481535.

Leibfried, Stephan und Michael Zürn, Hrsg. (2006). *Transformationen des Staates?* Frankfurt am Main: Suhrkamp.

Léonard, Sarah und Christian Kaunert (2011). »Reconceptualizing the audience in securitization theory«. In: *Securitization theory*. Hrsg. von Thierry Balzacq. PRIO new security studies. Milton Park, Abingdon, Oxon und New York: Routledge, S. 57–76. ISBN: 0415556279.

Levy, Ian und Crispin Robinson (2018). *Principles for a More Informed Exceptional Access Debate*. URL: https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate.

Lewis, James A. und Götz Neuneck (2013). *The Cyber Index: International Security Trends and Realities*. URL: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf.

Liberty (2013). *A Breach of Trust on the Grandest Scale*. URL: https://www.libertyhumanrights.org.uk/news/blog/breach-trust-grandest-scale.

— (2016a). *Liberty's briefing on Part 6 of the Investigatory Powers Bill for Committee Stage in the House of Commons*. URL: https://www.libertyhumanrights.org.uk/sites/default/files/Liberty%27s%20Briefing%20on%20Part%206%20of%20the%20Investigatory%20Powers%20Bill%20for%20Committee%20Stage%20in%20the%20House%20of%20Commons.pdf.

— (2016b). *Liberty's briefing on the Investigatory Powers Bill for Report Stage in the House of Commons*. URL: https://www.libertyhumanrights.org.uk/sites/default/files/campaigns/resources/Liberty%27s%20Briefing%20on%20the%20Investigatory%20Powers%20Bill%20for%20Report%20Stage%20in%20the%20House%20of%20Commons.pdf.

— (2019). *Court judgment allows the government to continue spying on us*. URL: https://www.libertyhumanrights.org.uk/news/press-releases-and-statements/court-judgment-allows-government-continue-spying-us.

Libicki, Martin C. (2017). »The Convergence of Information Warfare«. In: *Strategic Studies Quarterly* Spring, S. 49–65.

— (2018). »Expectations of Cyber Deterrence«. In: *Strategic Studies Quarterly* 12.4, S. 44–57.

Lindsay, Jon R. (2013). »Stuxnet and the Limits of Cyber Warfare«. In: *Security Studies* 22.3, S. 365–404. ISSN: 0963-6412. DOI: 10.1080/09636412.2013.816122.

— (2015). »Tipping the scales: The attribution problem and the feasibility of deterrence against cyberattack«. In: *Journal of Cybersecurity*, S. 53–67. DOI: 10.1093/cybsec/tyv003.

Lindsay, Jon R. und Erik Gartzke (2018). In: *Coercion*. Hrsg. von Kelly M. Greenhill und Peter Krause. New York, NY: Oxford University Press, S. 179–203. ISBN: 9780190846343.

Liu, Ian Yuying (2017). »The due diligence doctrine under Tallinn Manual 2.0«. In: *Computer Law & Security Review* 33.3, S. 390–395. ISSN: 02673649. DOI: 10.1016/j.clsr.2017.03.023.

MacKenzie, Donald A. und Judy Wajcman (1999). »Introductory Essay: The social shaping of technology«. In: *The social shaping of technology*. Hrsg. von Donald A. MacKenzie und Judy Wajcman. Buckingham [England] und Philadelphia: Open University Press, S. 3–27. ISBN: 978-0-335-19913-6.

Madsen, Wayne u. a. (1998). »Cryptography and Liberty: An International Survey of Encryption Policy«. In: *The John Marshall Journal of Information Technology and Privacy Law* 16.3, S. 475–527.

Mai, Manfred (2011). *Technik, Wissenschaft und Politik: Studien zur Techniksoziologie und Technikgovernance*. 1. Aufl. Wiesbaden: VS - Verl. ISBN: 3531179039.

Malici, Akan (2006). »Reagan and Gorbachev: Altercasting at the End of the Cold War«. In: *Beliefs and leadership in world politics*. Hrsg. von Mark Schafer und Stephen G. Walker. Advances in foreign policy analysis. New York, NY: Palgrave Macmillan, S. 127–149. ISBN: 978-1-4039-7182-1.

Mansfield-Devine, Steve (2016). »DDoS goes mainstream: How headline-grabbing attacks could make this threat an organisation's biggest nightmare«. In: *Network Security* 2016.11, S. 7–13. DOI: 10.1016/S1353-4858(16)30104-0.

Margolis, Joseph (2006). »Introduction: Pragmatism, Retrospective, Pragmatism, Retrospective, and Prospective«. In: *A companion to pragmatism*. Hrsg. von John R. Shook und Joseph Margolis. Blackwell companions to philosophy. Malden, Mass.: Blackwell Publishing, S. 1–10. ISBN: 978-1-4051-1621-3.

Mastanduno, Michael, David A. Lake und G. John Ikenberry (1989). »Toward a Realist Theory of State Action«. In: *International Studies Quarterly* 33.4, S. 457–474. ISSN: 00208833.

Maull, Hanns W. (2007). »Deutschland als Zivilmacht«. In: *Handbuch zur deutschen Außenpolitik*. Hrsg. von Siegmar Schmidt, Gunther Hellmann und Reinhard Wolf. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 73–84. ISBN: 978-3-531-13652-3.

— (1990/91). »Germany and Japan: The New Civilian Powers«. In: *Foreign Affairs* 69.5, S. 91–106.

Maurer, Tim (2011). *Cyber norm emergence at the United Nations: An Analysis of the UN's Activities Regarding Cyber-security*. URL: https://www.belfercenter.org/sites/default/files/legacy/files/maurer-cyber-norm-dp-2011-11-final.pdf.

— (2018). *Cyber Mercenaries: The state, hackers, and power*. Cambridge: Cambridge University Press. ISBN: 978-1107566866.

Maurer, Tim (2019). »A Dose of Realism: The Contestation and Politics of Cyber Norms«. In: *Hague Journal on the Rule of Law* 54.3, S. 1–23. DOI: 10.1007/s40803-019-00129-8.

Maurer, Tim u. a. (2014). *Technological Sovereignty: Missing the Point?* URL: http://www.gppi.net/fileadmin/user_upload/media/pub/2014/Maurer-et-al_2014_Tech-Sovereignty-Europe.pdf.

May, Timothy C. (1988). *The Crypto Anarchist Manifesto*. URL: https://koeln.ccc.de/archiv/drt/crypto-anarchy.html.

Mayer, Maximilian Benedikt (2017). *The Unbearable Lightness of International Relations: Technological Innovations, Creative Destruction and Assemblages*. URL: http://hss.ulb.uni-bonn.de/2017/4652/4652.pdf.

McAfee und CSIS (2018). *Economic Impact of Cybercrime*. URL: https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email.

McCarthy, Daniel R. (2015). *Power, information technology, and international relations theory: The power and politics of US foreign policy and the internet*. Palgrave studies in international relations. New York, NY: Palgrave Macmillan. ISBN: 978-1-137-30689-0.

McCourt, David M. (2012). »The roles states play: A Meadian interactionist approach«. In: *Journal of International Relations and Development* 15.3, S. 370–392. DOI: 10.1057/jird.2011.26.

— (2014). *Britain and world power since 1945: Constructing a nation's role in international politics*. Configurations : critical studies of world politics. Ann Arbor: University of Michigan Press. ISBN: 978-0-472-05221-9.

McKune, Sarah und Ahmed Shazeda (2018). »Authoritarian Practices in the Digital Age: The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda«. In: *International Journal of Communication* 12, S. 3835–3855.

Mead, George Herbert (1979). *Mind, self, and society: From the standpoint of a social behaviorist*. 20th print. Bd. Vol. 1, Print. 20. Works of George Herbert Mead. Chicago: University of Chicago Press. ISBN: 0-226-51668-7.

Mearsheimer, John J. (1990). »Back to the Future: Instability in Europe after the Cold War«. In: *International Security* 15.1, S. 5. ISSN: 01622889. DOI: 10.2307/2538981.

Ministry of Defence (2013). *Cyber Primer*. URL: https://webarchive.nationalarchives.gov.uk/20141221145837/https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/360973/20140716_DCDC_Cyber_Primer_Internet_Secured.pdf.

— (2015). *Speech: Building a British military fit for future challenges rather than past conflicts*. URL: https://www.gov.uk/government/speeches/building-a-british-military-fit-for-future-challenges-rather-than-past-conflicts.

— (2016a). *Cyber Primer - Second Edition*. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf.

— (2016b). *Defence Secretary's speech at the second RUSI Cyber Symposium*. URL: https://www.gov.uk/government/speeches/defence-secretarys-speech-at-the-second-rusi-cyber-symposium.

— (2019). *Defence Secretary Ben Wallace addresses the NATO Parliamentary Assembly 2019*. URL: https://www.gov.uk/government/speeches/defence-secretary-ben-wallace-addresses-the-nato-parliamentary-assembly-2019.

Misak, Cheryl J. (2006). »Scientific Realism, Anti-Realism, and Empiricism«. In: *A companion to pragmatism*. Hrsg. von John R. Shook und Joseph Margolis. Blackwell companions to philosophy. Malden, Mass.: Blackwell Publishing, S. 398–409. ISBN: 978-1-4051-1621-3.

Mitzen, Jennifer (2006). »Ontological Security in World Politics: State Identity and the Security Dilemma«. In: *European Journal of International Relations* 12.3, S. 341–370. ISSN: 1354-0661. DOI: 10.1177/1354066106067346.

Moore, Daniel und Thomas Rid (2016). »Cryptopolitik and the Darknet«. In: *Survival* 58.1, S. 7–38. ISSN: 0039-6338. DOI: 10.1080/00396338.2016.1142085.

Moravcsik, Andrew (1993). »Preferences and Power in the European Community: A Liberal Intergovernmentalist Approach«. In: *Journal of Common Market Studies* 31.4, S. 473–524.

— (1997). »Taking Preferences Seriously: A Liberal Theory of International Politics«. In: *International Organization* 51.4, S. 513–553.

Morozov, Evgeny (2011). *The net delusion: The dark side of Internet freedom*. New York: Public Affairs. ISBN: 978-1-61039-106-1.

Mueller, Milton (2017). *Will the Internet Fragment?* Cambridge, U.K.: Polity Press. ISBN: 978-1509501229.

Mueller, Milton und Farzaneh Badiei (2017). »Governing Internet Territory: ICANN, Sovereignty Claims, Property Rights and Country Code Top-level Domains«. In: *The Columbia Science & Technology Law Review* 18.Spring, S. 435–491.

Mueller, Milton L. (2010). *Networks and States: The Global Politics of Internet Governance*. The MIT Press. ISBN: 9780262014595. DOI: 10.7551/mitpress/9780262014595.001.0001.

Murray, Andrew (2016). *Information technology law: The law and society*. Third edition. Oxford: Oxford University Press. ISBN: 978-0198732464.

Naked Security (2019). *Five Eyes nations demand access to encrypted messaging*. URL: https://nakedsecurity.sophos.com/2019/08/01/five-eyes-nations-demand-access-to-encrypted-messaging/.

National Audit Office (2018). *Investigation: WannaCry cyber attack and the NHS*. URL: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

NATO (2016). *Warsaw Summit Communiqué*. URL: https://www.nato.int/cps/ic/natohq/official_texts_133169.htm.

Naughton, John (2016). »The evolution of the Internet: From military experiment to General Purpose Technology«. In: *Journal of Cyber Policy* 1.1, S. 5–28. ISSN: 2373-8871. DOI: 10.1080/23738871.2016.1157619.

Netzpolitik.org (2013). *Schengen-Routing, DE-CIX und die Bedenken der Balkanisierung des Internets*. URL: https://netzpolitik.org/2013/schengen-routing-de-cix-und-die-bedenken-der-balkanisierung-des-internets/.

— (2014a). *Arbeitserleichterung für die NSA: Deutscher Bundestag bezieht Internet von US-Anbieter Verizon (12 Updates)*. URL: https://netzpolitik.org/2014/arbeitserleichterung-fuer-die-nsa-deutscher-bundestag-bezieht-internet-von-us-anbieter-verizon/.

— (2014b). *Merkels Acht-Punkte-Programm ein Jahr nach Snowden: Was ist passiert?* URL: https://netzpolitik.org/2014/merkels-acht-punkte-programm-ein-jahr-nach-snowden-was-ist-passiert/#spendenleiste.

— (2015). *Geheime Cyber-Leitlinie: Verteidigungsministerium erlaubt Bundeswehr „Cyberwar" und offensive digitale Angriffe*. URL: https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/.

Netzpolitik.org (2016a). *Das neue BND-Gesetz: Alles, was der BND macht, wird einfach legalisiert. Und sogar noch ausgeweitet.* URL: https://netzpolitik.org/2016/das-neue-bnd-gesetz-alles-was-der-bnd-macht-wird-einfach-legalisiert-und-sogar-noch-ausgeweitet/.

— (2016b). *Fünf drastische Folgen des geplanten BND-Gesetzes*. URL: https://netzpolitik.org/2016/fuenf-drastische-folgen-des-geplanten-bnd-gesetzes/.

— (2017). *Staatstrojaner: Bundestag hat das krasseste Überwachungsgesetz der Legislaturperiode beschlossen (Updates)*. URL: https://netzpolitik.org/2017/staatstrojaner-bundestag-beschliesst-diese-woche-das-krasseste-ueberwachungsgesetz-der-legislaturperiode/#spendenleiste.

Niedersächsischer Landtag (2014). *Drucksache 17/1206*. URL: https://www.landtag-niedersachsen.de/ps/tools/download.php?file=/ltnds/live/cms/dms/psfile/docfile/96/17_1206530313d042815.pdf.

Nikkarila, Juha-Pekka und Mari Ristolainen (2017). »?RuNet 2020? - deploying traditional elements of combat power in cyberspace?« In: *2017 International Conference on Military Communications and Information Systems (ICMCIS)*. IEEE, S. 1–8. ISBN: 978-1-5386-3858-3. DOI: 10.1109/ICMCIS.2017.7956478.

Nissenbaum, Helen (2005). »Where Computer Security Meets National Security«. In: *Ethics and Information Technology* 7.2, S. 61–73. DOI: 10.1007/s10676-005-4582-3.

Nye, Joseph S. (2010). *Cyber Power*. URL: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf.

— (2016). »The regime complex for managing global cyber activities«. In: *The Turn to Infrastructure in Internet Governance*. Hrsg. von Francesca Musiani u. a. New York: Palgrave Macmillan US, S. 5–17. ISBN: 978-1-349-57846-7.

— (2017). »Deterrence and Dissuasion in Cyberspace«. In: *International Security* 41.3, S. 44–71. ISSN: 01622889. DOI: 10.1162/ISEC{\textunderscore}a{\textunderscore}00266.

OECD (1997). *Recommendation of the Council concerning Guidelines for Cryptography Policy*. URL: http://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm.

Ofcom (2009). *Online Protection*. URL: https://webarchive.nationalarchives.gov.uk/20090508191527/http://www.ofcom.org.uk/research/telecoms/reports/onlineprotection/summary/?lang=default.

Ogburn, William Fielding (1969). *Kultur und sozialer Wandel: Ausgewählte Schriften*. Bd. 56. Soziologische Texte. Neuwied.

Olsen, Matthew G., Bruce Schneier und Jonathan Zittrain (2016). *Don't Panic: Making Progress on the "Going Dark" Debate*. URL: https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

Open Rights Group (2016a). *GCHQ and Mass Surveillance Report*. URL: https://www.openrightsgroup.org/assets/files/pdfs/reports/gchq/05-Part_One-Chapter_Five-Offensive_capabilities.pdf.

— (2016b). *Special Rapporteur on the right to privacy condemns Investigatory Powers Bill*. URL: https://www.openrightsgroup.org/press/releases/2016/special-rapporteur-on-the-right-to-privacy-condemns-investigatory-powers-bill.

Oppermann, Kai (2012). »National Role Conceptions, Domestic Constraints and the New 'Normalcy' in German Foreign Policy: The Eurozone Crisis, Libya and Beyond«. In: *German Politics* 21.4, S. 502–519. ISSN: 0964-4008. DOI: 10.1080/09644008.2012.748268.

OSCE (2016a). *Decision No 1202: OSCE Confidence-Building Measures to reduce the risks of conflict stemming from the use of information and communication technologies*. URL: https://www.osce.org/pc/227281?download=true.

— (2016b). *OSCE participating States, in landmark decision, agree to expand list of measures to reduce risk of tensions arising from cyber activities*. URL: https://www.osce.org/cio/226656.

Ottis, Rain (2008). »Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective«. In: *Proceedings of the 7th European Conference on Information Warfare and Security*. Hrsg. von Dan Remenyi. Reading: Academic Publishing Limited, S. 163–168.

Paar, Christof und Jan Pelzl (2016). *Kryptografie verständlich*. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-662-49296-3. DOI: 10.1007/978-3-662-49297-0.

Papier, Hans-Jürgen (2014). *Gutachtliche Stellungnahme Beweisbeschluss SV-2 des ersten Untersuchungsausschusses des Deutschen Bundestages der 18. Wahlperiode*. URL: https://www.bundestag.de/resource/blob/280842/9f755b0c53866c7a95c38428e262ae98/MAT_A_SV-2-2-pdf-data.pdf.

— (2016). »Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten«. In: *Neue Zeitschrift für Verwaltungsrecht* 35.15, S. 1–15.

Parliamentary Office of Science and Technology (2006). *Data Encryption*. URL: http://researchbriefings.files.parliament.uk/documents/POST-PN-270/POST-PN-270.pdf.

Parsons, Talcott (1991). *The social system*. 2nd ed. Routledge sociology classics. London: Routledge. ISBN: 0-203-99295-4.

Peirce, Charles Sanders (1868). »Some Consequences of four Incapacities«. In: *The Journal of Speculative Philosophy* 2.3, S. 140–157.

— (1877). »Illustrations of the Logic of Science: The Fixation of Belief«. In: *Popular Science Monthly* November, S. 1–15.

— (1878). »Illustrations of the Logic of Science: How to make our ideas clear«. In: *Popular Science Monthly* January, S. 286–302.

Pelletier, Laura und Justin Massie (2017). »Role conflict: Canada's withdrawal from combat operations against ISIL«. In: *International Journal: Canada's Journal of Global Policy Analysis* 72.3, S. 298–317. ISSN: 0020-7020. DOI: 10.1177/0020702017723357.

Pouliot, Vincent (2017). »Practice tracing«. In: *Process tracing*. Hrsg. von Andrew Bennett und Jeffrey T. Checkel. Strategies for social inquiry. Cambridge: Cambridge University Press, S. 237–259. ISBN: 978-1-107-68637-3.

Privacy International (2015a). *UK government claims power for broad, suspicionless hacking of computers and phones*. URL: https://privacyinternational.org/press-release/1350/uk-government-claims-power-broad-suspicionless-hacking-computers-and-phones.

— (2015b). *Written evidence submitted by Privacy International*. URL: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25170.html.

— (2018). *Press release: Campaigners win vital battle against UK mass surveillance at European Court of Human Rights*. URL: https://privacyinternational.org/press-release/2265/press-release-campaigners-win-vital-battle-against-uk-mass-surveillance-european?PageSpeed=noscript.

— (2019). *Privacy International Wins Historic Victory at UK Supreme Court*. URL: https://privacyinternational.org/press-release/2897/privacy-international-wins-historic-victory-uk-supreme-court.

Putnam, Robert D. (1988). »Diplomacy and Domestic Politics: The Logic of Two-Level Games«. In: *International Organization* 42.3, S. 427–460.

Rammert, Werner (2016). *Technik - Handeln - Wissen: Zu einer pragmatistischen Technik- und Sozialtheorie*. Wiesbaden: Springer Fachmedien Wiesbaden. ISBN: 978-3-658-11772-6. DOI: 10.1007/978-3-658-11773-3.

Rathbun, Brian (2008). »A Rose by Any Other Name: Neoclassical Realism as the Logical and Necessary Extension of Structural Realism«. In: *Security Studies* 17.2, S. 294–321. ISSN: 0963-6412. DOI: 10.1080/09636410802098917.

Raustiala, Kal (2017). »An Internet Whole and Free: Why Washington Was Right to Give up Control«. In: *Foreign Affairs* 96.2, S. 140–147.

Reardon, Robert und Nazli Choucri (2012). *The Role of Cyberspace in International Relations: A View of the Literature*. URL: http://ecir.mit.edu/images/stories/Reardon%20and%20Choucri_ISA_2012.pdf.

Reporter ohne Grenzen (2018). *Verfassungsbeschwerde gegen das BND-Gesetz*. URL: https://www.reporter-ohne-grenzen.de/pressemitteilungen/meldung/verfassungsbeschwerde-gegen-das-bnd-gesetz/.

Reus-Smit, C. (2013). »Beyond metatheory?« In: *European Journal of International Relations* 19.3, S. 589–608. ISSN: 1354-0661. DOI: 10.1177/1354066113495479.

Reuters (2013). *U.N. anti-spying resolution weakened in bid to gain U.S., British support*. URL: https://www.reuters.com/article/us-usa-surveillance-un-idUSBRE9AK14220131121.

— (2016). *Massive cyber attack could trigger NATO response: Stoltenberg*. URL: https://www.reuters.com/article/us-cyber-nato/massive-cyber-attack-could-trigger-nato-response-stoltenberg-idUSKCN0Z12NE.

Rid, Thomas (2012). »Cyber War Will Not Take Place«. In: *Journal of Strategic Studies* 35.1, S. 5–32. ISSN: 0140-2390. DOI: 10.1080/01402390.2011.608939.

— (2013). *Cyber war will not take place*. Oxford und New York: Oxford University Press. ISBN: 978-0199330638.

— (2016). *Rise of the machines: The lost history of cybernetics*. Melbourne und London: Scribe. ISBN: 978-1925228854.

Rid, Thomas und Ben Buchanan (2014). »Attributing Cyber Attacks«. In: *Journal of Strategic Studies* 38.1-2, S. 4–37. ISSN: 0140-2390. DOI: 10.1080/01402390.2014.977382.

Rid, Thomas und Peter McBurney (2012). »Cyber-Weapons«. In: *The RUSI Journal* 157.1, S. 6–13. ISSN: 0307-1847. DOI: 10.1080/03071847.2012.664354.

Risse, Thomas (1999). »The socialization of international human rights norms into domestic practices: introduction«. In: *The power of human rights*. Hrsg. von Thomas Risse, Steven C. Ropp und Kathryn Sikkink. Cambridge studies in international relations. Cambridge: Cambridge University Press, S. 1–38. ISBN: 978-0-521-65882-9.

Risse, Thomas, Steven C. Ropp und Kathryn Sikkink, Hrsg. (1999). *The power of human rights: International norms and domestic change*. Bd. 66. Cambridge studies in international relations. Cambridge: Cambridge University Press. ISBN: 978-0-521-65882-9.

Rivest, Ron L., Adi Shamir und Leonard Adleman (1978). »A method for obtaining digital signatures and public-key cryptosystems«. In: *Communications of the ACM* 21.2, S. 120–126. DOI: 10.1145/359340.359342.

Roggan, Fredrik (2018). »Quellen-Telekommunikationsüberwachung und Online-Durchsuchung zur Strafverfolgung«. In: *Grundrechte-Report 2018*. Hrsg. von Till Müller-Heidelberg. Fischer Taschenbuch. Frankfurt am Main: FISCHER Taschenbuch, S. 38–41. ISBN: 978-3-596-70189-6.

Roos, Ulrich (2010). *Deutsche Außenpolitik*. Wiesbaden: VS Verlag für Sozialwissenschaften. ISBN: 978-3-531-17445-7. DOI: 10.1007/978-3-531-92355-0.

Ropohl, Günter (1999). *Technologische Aufklärung: Beiträge zur Technikphilosophie*. 1. Aufl., [Nachdr.] Bd. 971. Suhrkamp-Taschenbuch Wissenschaft. Frankfurt am Main: Suhrkamp. ISBN: 978-3518285718.

Rorty, Richard (1992). *Contingency, irony, and solidarity*. Cambridge: Cambridge University Press. ISBN: 0-521-36781-6.

— (2000). »Response to Brandom«. In: *Rorty and his critics*. Hrsg. von Robert Brandom. Philosophers and their critics. Malden und Oxford: Blackwell Publishers, S. 183–190. ISBN: 0-631-20982-4.

Rose, Gideon (1998). »Neoclassical Realism and Theories of Foreign Policy«. In: *World Politics* 51.1, S. 144–172.

Rovner, Joshua und Tyler Moore (2017). »Does the Internet Need a Hegemon?« In: *Journal of Global Security Studies* 2.3, S. 184–203. DOI: 10.1093/jogss/ogx008.

Sauter, Molly (2014). *The Coming Swarm: DDOS Actions, Hacktivism, and Civil Disobedience on the Internet*. New York: Bloomsbury Publishing. ISBN: 978-1-6289-2153-3.

Schälike, Julius (2010). *Spielräume und Spuren des Willens: Eine Theorie der Freiheit und der moralischen Verantwortung*. Perspektiven der analytischen Philosophie. Paderborn: Mentis. ISBN: 978-3897852211.

Schallbruch, Martin und Isabel Skierka (2018). *Cybersecurity in Germany*. Cham: Springer International Publishing. ISBN: 978-3-319-90013-1. DOI: 10.1007/978-3-319-90014-8.

Schelsky, Helmut (1965). »Der Mensch in der wissenschaftlichen Zivilisation«. In: *Auf der Suche nach Wirklichkeit*. Hrsg. von Helmut Schelsky. Düsseldorf und Köln: Eugen Diederichs, S. 439–480.

Schmitt, Michael und Liis Vihul (2017). *International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms*. URL: https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

Schneiders, Thorsten Gerald, Hrsg. (2013). *Der Arabische Frühling: Hintergründe und Analysen*. Wiesbaden: Springer VS. ISBN: 978-3-658-01174-1.

Schultz, Kenneth (2013). »Domestic Politics and International Relations«. In: *Handbook of international relations*. Hrsg. von Walter Carlsnaes, Thomas Risse-Kappen und Beth A. Simmons. London und Thousand Oaks, CA: SAGE Publications, S. 478–502. ISBN: 978-1-84920-150-6.

Schulze, Matthias (2016). »(Un)Sicherheit hinter dem Bildschirm: Die Versicherheitlichung des Internets«. In: *Innere Sicherheit nach 9/11*. Hrsg. von Susanne Fischer und Carlo Masala. Wiesbaden: Springer Fachmedien Wiesbaden, S. 165–185. ISBN: 978-3-658-02637-0.

— (2019). *Überschätzte Cyber-Abschreckung*. DOI: 10.18449/2019A39. URL: https://www.swp-berlin.org/fileadmin/contents/products/aktuell/2019A39_she.pdf.

Schulze, Tillmann (2006). *Bedingt abwehrbereit: Schutz kritischer Informations-Infrastrukturen in Deutschland und den USA*. 1. Aufl. Wiesbaden: VS Verlag für Sozialwissenschaften/GWV Fachverlage, Wiesbaden. ISBN: 978-3531148663.

Schulzke, Marcus (2018). »The Politics of Attributing Blame for Cyberattacks and the Costs of Uncertainty«. In: *Perspectives on Politics* 16.4, S. 954–968. DOI: 10.1017/S153759271800110X.

Schünemann, Wolf J., Sebastian Harnisch und Stefan Artmann (2018). »Cybersicherheit und Rollenwandel«. In: *Zeitschrift für Politikwissenschaft* 28.3, S. 263–287. DOI: 10.1007/s41358-018-0164-x.

Schünemann, Wolf J. und Stefan Steiger (2019). »Jenseits der Versicherheitlichung: Zu Stand und Aussichten der Cybersicherheitsforschung«. In: *Politik in der digitalen Gesellschaft*. Hrsg. von Jeanette Hofmann u. a. Bielefeld: Transcript, S. 247–268. ISBN: 978-3-8376-4864-5.

Schweitzer, Yoram, Gabi Siboni und Einav Yogev (2013). »Cyberspace and Terrorist Organizations«. In: *Cyberspace and national security*. Hrsg. von Gabi Siboni. Tel Aviv: Institute for National Security Studies, S. 17–26. ISBN: 978-965-7425-51-0.

Science and Technology Committee (2016). *Investigatory Powers Bill: technology issues*. URL: https://publications.parliament.uk/pa/cm201516/cmselect/cmsctech/573/573.pdf.

Segal, Adam (2016). *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age*. New York: PublicAffairs. ISBN: 978-1610394154.

— (2017). *The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?* URL: https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what.

Severson, Daniel (2017). *The Encryption Debate in Europe*. URL: http://www.hoover.org/sites/default/files/research/docs/severson_webreadypdf.pdf.

Shackelford, Scott J. u. a. (2017). »From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure and What to Do About It«. In: *Nebraska Law Review* 96.1, S. 320–338.

Sharp, Travis (2017). »Theorizing cyber coercion: The 2014 North Korean operation against Sony«. In: *Journal of Strategic Studies* 58.3, S. 1–29. ISSN: 0140-2390. DOI: 10.1080/01402390.2017.1307741.

Shaw, Tony und Tricia Jenkins (2017). »An Act of War? The Interview Affair, the Sony Hack, and the Hollywood–Washington Power Nexus Today«. In: *Journal of American Studies* 29, S. 1–27. DOI: 10.1017/S0021875817000512.

Sheldon, John B. (2014). »Geopolitics and Cyber Power: Why Geography Still Matters«. In: *American Foreign Policy Interests* 36.5, S. 286–293. ISSN: 1080-3920. DOI: 10.1080/10803920.2014.969174.

Shirky, Clay (2009). *Here comes everybody: The power of organizing without organizations*. London [u.a.]: Penguin Books. ISBN: 978-0-713-99989-1.

— (2011). »The Political Power of Social Media: Technology, the Public Sphere, and Political Change«. In: *Foreign Affairs* 90.1, S. 28–41.

Shlaim, Avi (1975). »Britain's Quest for a World Role«. In: *International Relations* 5.1, S. 838–856. ISSN: 0047-1178. DOI: 10.1177/004711787500500105.

Shook, John R. und Joseph Margolis, Hrsg. (2006). *A companion to pragmatism*. Bd. 32. Blackwell companions to philosophy. Malden, Mass.: Blackwell Publishing. ISBN: 978-1-4051-1621-3.

Siedler, Ragnhild Endresen (2016). »Hard Power in Cyberspace: CNA as a Political Means«. In: *2016 8th International Conference on Cyber Conflict*. Hrsg. von Nikolaos Pissanidis, Henry Rõigas und Matthijs Veenendaal. Tallinn, Estonia: NATO CCD COE Publications, S. 23–36. ISBN: 978-9949-9544-9-0.

Singer, Peter W. und Allan Friedman (2014). *Cybersecurity*. What everyone needs to know. New York und Oxford: Oxford University Press. ISBN: 978-0199918119.

Sky News (2018). *Britain to create 2,000 - strong cyber force to tackle Russia threat*. URL: https://news.sky.com/story/britain-to-create-2000-strong-cyber-force-to-tackle-russia-threat-11503653.

Sliwinski, Krzysztof Feliks (2014). »Moving beyond the European Union's Weakness as a Cyber-Security Agent«. In: *Contemporary Security Policy* 35.3, S. 468–486. ISSN: 1352-3260. DOI: 10.1080/13523260.2014.959261.

Snowden, Edward (2015). *Tweet from 4 November 2015*. URL: https://twitter.com/Snowden/status/661950808381128704.

Soesanto, Stefan und Fosca D'Incau (2017). *The UN GGE is dead: Time to fall forward*. URL: http://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance.

Soltan, Saleh, Prateek Mittal und H. Vincent Poor (2018). *BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid*. URL: https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-soltan.pdf.

Spannbrucker, Christian (2004). *Convention on Cybercrime (ETS 185) - Ein Vergleich mit dem deutschen Computerstrafrecht in materiell- und verfahrensrechtlicher Hinsicht*. URL: https://epub.uni-regensburg.de/10281/1/CCC.pdf.

Spiegel (2008). *Online-Durchsuchungen: Richter erfinden das Computer-Grundrecht*. URL: http://www.spiegel.de/politik/deutschland/online-durchsuchungen-richter-erfinden-das-computer-grundrecht-a-538238.html.

— (2013a). *Ausspähen unter Freunden - das geht gar nicht*. URL: https://www.spiegel.de/politik/deutschland/handy-spaehaffaere-um-merkel-regierung-ueberprueft-alle-nsa-erklaerungen-a-929843.html.

— (2013b). *Demonstrationen gegen Prism - Tausende fordern Stopp der Ausspähung*. URL: https://www.spiegel.de/politik/deutschland/10-000-menschen-protestieren-gegen-nsa-ueberwachung-a-913513.html.

— (2013c). *NSA-Protest in Berlin - Freiheit unterm Alu-Hut*. URL: https://www.spiegel.de/netzwelt/netzpolitik/freiheit-statt-angst-2013-demonstration-gegen-nsa-ueberwachung-a-920927.html.

— (2014a). *An den USA vorbei: Internet-Tiefseekabel soll Brasilien und Europa verbinden*. URL: https://www.spiegel.de/netzwelt/netzpolitik/internet-kabel-von-brasilien-nach-europa-geplant-a-955506.html.

— (2014b). *Belgacom Attack Britain's GCHQ Hacked Belgian Telecoms Firm*. URL: https://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html.

— (2014c). *Neue Spionageaffäre erschüttert BND*. URL: https://www.spiegel.de/politik/deutschland/ueberwachung-neue-spionageaffaere-erschuettert-bnd-a-1030191.html.

— (2015a). *Bewusste Täuschung*. URL: https://www.spiegel.de/spiegel/print/d-138273612.html.

— (2015b). *Geheime Bundeswehr-Strategie: Von der Leyen rüstet an der Cyberfront auf*. URL: https://www.spiegel.de/politik/deutschland/bundeswehr-ursula-von-der-leyen-ruestet-an-der-cyber-front-auf-a-1042985.html.

— (2015c). *Offenbar auch Rechner von Regierungsmitgliedern betroffen*. URL: https://www.spiegel.de/netzwelt/netzpolitik/cyberangriff-auf-bundestag-offenbar-auch-rechner-von-regierungsmitgliedern-betroffen-a-1034588.html.

— (2016). *Bundeswehr-Hacker knackten afghanisches Mobilfunknetz*. URL: https://www.spiegel.de/politik/ausland/cyber-einheit-bundeswehr-hackte-afghanisches-mobilfunknetz-a-1113560.html.

— (2018). *Auch Bundesregierung macht Russland verantwortlich für Cyberangriffe*. URL: https://www.spiegel.de/netzwelt/netzpolitik/apt28-bundesregierung-beschuldigt-offiziell-russland-der-cyberangriffe-a-1231744.html.

Steiger, Stefan (2017). »The Unshaken Role of GCHQ: The British Cybersecurity Discourse After the Snowden Revelations«. In: *Privacy, data protection and cybersecurity in Europe*. Hrsg. von Wolf J. Schünemann und Max-Otto Baumann. Cham, Switzerland: Springer, S. 79–95. ISBN: 978-3-319-53634-7.

Steiger, Stefan u. a. (2018). »Conceptualising conflicts in cyberspace«. In: *Journal of Cyber Policy* 3.1, S. 77–95. ISSN: 2373-8871. DOI: 10.1080/23738871.2018.1453526.

Stevens, Tim (2018). »Cyberweapons: Power and the governance of the invisible«. In: *International Politics* 55.3-4, S. 482–502. DOI: 10.1057/s41311-017-0088-y.

Stiennon, Richard (2015). *There Will Be Cyberwar: How the Move to Network-Centric Warfighting Set The Stage For Cyberwar*. Birmingham, MI: IT-Harvest Press. ISBN: 978-0985460785.

Stier, Sebastian (2017). *Internet und Regimetyp*. Wiesbaden: Springer Fachmedien Wiesbaden. ISBN: 978-3-658-17206-0. DOI: 10.1007/978-3-658-17207-7.

Stifel, Megan (2017). *Maintaining U.S. Leadership on Internet Governance*. URL: http://i.cfr.org/content/publications/attachments/CyberBrief_Stifel_Governance_OR.pdf.

Stone, John (2013). »Cyber War Will Take Place!« In: *Journal of Strategic Studies* 36.1, S. 101–108. ISSN: 0140-2390. DOI: 10.1080/01402390.2012.730485.

Strauss, Anselm L. und Juliet M. Corbin (1996). *Grounded theory: Grundlagen qualitativer Sozialforschung*. Weinheim: Beltz, PsychologieVerlagsUnion. ISBN: 978-3621272650.

— (1998). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. 2. ed. London: SAGE. ISBN: 9780803959392.

Süddeutsche Zeitung (2013). *Briten schöpfen deutsches Internet ab*. URL: https://www.sueddeutsche.de/politik/nachrichtendienst-gchq-briten-schoepfen-deutsches-internet-ab-1.1704670.

— (2014a). *Codewort Eikonal - der Albtraum der Bundesregierung*. URL: https://www.sueddeutsche.de/politik/geheimdienste-codewort-eikonal-der-albtraum-der-bundesregierung-1.2157432-0#seite-4.

— (2014b). *Regierung gibt neuen Bundestrojaner frei*. URL: https://www.sueddeutsche.de/digital/ueberwachung-regierung-gibt-neuen-bundestrojaner-frei-1.2875186.

— (2015). *Ahnungslos im BND*. URL: https://www.sueddeutsche.de/politik/nsa-ausschuss-ahnungslos-im-bnd-1.2488549-0.

— (2016a). *Abhörpraxis des BND: Nicht verfassungskonform*. URL: https://www.sueddeutsche.de/politik/geheimdienst-abhoerpraxis-des-bnd-nicht-verfassungskonform-1.2878299.

— (2016b). *BND und NSA kooperieren wieder in Bad Aibling*. URL: https://www.sueddeutsche.de/politik/abhoerskandal-bnd-und-nsa-kooperieren-wieder-in-bad-aibling-1.2810828.

— (2017). *Bundesbehörde diskutiert digitale Gegenschläge*. URL: https://www.sueddeutsche.de/digital/2.220/it-sicherheit-bundesbehoerde-diskutiert-ob-sie-zurueck-hacken-soll-1.3554124.

— (2018). *Deutsche Späh-Software gegen türkische Oppositionelle eingesetzt*. URL: https://www.sueddeutsche.de/digital/ueberwachung-deutsche-spaeh-software-gegen-tuerkische-oppositionelle-eingesetzt-1.3979824.

t-online.de (2019). *Interview mit Ursula von der Leyen - Digitalisierung muss Chefsache sein*. URL: https://www.t-online.de/nachrichten/deutschland/militaer-verteidigung/id_85916004/ursula-von-der-leyen-im-interview-digitalisierung-muss-chefsache-sein-.html.

Tabansky, Lior (2011). »Basic Concepts in Cyber Warfare«. In: *Military and Strategic Affairs* 3.1, S. 75–92.

Tabansky, Lior und Isaac Ben-Israel (2015). *Cybersecurity in Israel*. Springer briefs in cybersecurity. Cham [Switzerland]: Springer. ISBN: 978-3-319-18986-4.

Takano, Akiko (2018). »Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications«. In: *Laws* 7.4. DOI: 10.3390/laws7040036.

Taliaferro, Jeffrey W., Steven E. Lobell und Norrin M. Ripsman (2009). »Introduction: Neoclassical realism, the state, and foreign policy«. In: *Neoclassical realism, the state, and foreign*

*policy*. Hrsg. von Steven E. Lobell, Norrin M. Ripsman und Jeffrey W. Taliaferro. Cambridge: Cambridge University Press, S. 1–41. ISBN: 978-0-521-73192-8.

techUK (2015). *Written evidence submitted by techUK*. URL: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25160.html.

The Guardian (2007). *Russia accused of unleashing cyberwar to disable Estonia*. URL: https://www.theguardian.com/world/2007/may/17/topstories3.russia.

— (2011). *UK developing cyber-weapons programme to counter cyber war threat*. URL: https://www.theguardian.com/uk/2011/may/30/military-cyberwar-offensive.

— (2013a). *GCHQ taps fibre-optic cables for secret access to world's communications*. URL: https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

— (2013b). *NSA files: why the Guardian in London destroyed hard drives of leaked files*. URL: https://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london.

— (2013c). *NSA surveillance: Merkel's phone may have been monitored 'for over 10 years'*. URL: https://www.theguardian.com/world/2013/oct/26/nsa-surveillance-brazil-germany-un-resolution.

— (2014a). *David Miranda detention at Heathrow airport was lawful, high court rules*. URL: https://www.theguardian.com/world/2014/feb/19/david-miranda-detention-lawful-court-glenn-greenwald.

— (2014b). *Edward Snowden interview - the edited transcript*. URL: https://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript.

— (2014c). *Sun makes official complaint over police use of Ripa against journalists*. URL: https://www.theguardian.com/media/2014/oct/06/sun-official-complaint-ripa-journalists-met-police.

— (2015a). *David Davis: British 'intellectually lazy' about defending liberty*. URL: https://www.theguardian.com/politics/2015/nov/08/david-davis-liberty-draft-investigatory-powers-bill-holes.

— (2015b). *How has David Cameron caused a storm over encryption?* URL: https://www.theguardian.com/technology/2015/jan/15/david-cameron-encryption-anti-terror-laws.

— (2016). *Investigatory powers bill not up to the task*. URL: https://www.theguardian.com/law/2016/mar/14/investigatory-powers-bill-not-up-to-the-task.

— (2018). *British spies 'hacked into Belgian telecoms firm on ministers' orders'*. URL: https://www.theguardian.com/uk-news/2018/sep/21/british-spies-hacked-into-belgacom-on-ministers-orders-claims-report.

— (2019a). *PM accused of cover-up over report on Russian meddling in UK politics*. URL: https://www.theguardian.com/politics/2019/nov/04/no-10-blocks-russia-eu-referendum-report-until-after-election.

— (2019b). *UK government security decisions can be challenged in court, judges rule*. URL: https://www.theguardian.com/uk-news/2019/may/15/government-security-gchq-decisions-can-be-challenged-in-court-judges-rule.

— (2020). *UK to launch specialist cyber force able to target terror groups*. URL: https://www.theguardian.com/technology/2020/feb/27/uk-to-launch-specialist-cyber-force-able-to-target-terror-groups.

The Law Commission (1988). *Computer Misuse: Working Paper No. 110*. URL: https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2015/06/No.110-Computer-Misuse.pdf.

The Law Commission (1989). *Criminal Law - Computer Misuse: LAW COM. No. 186*. URL: https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2015/06/lc186.pdf.

The New York Times (2015). *Hackers Took Fingerprints of 5.6 Million U.S. Workers, Government Says*. URL: https://www.nytimes.com/2015/09/24/world/asia/hackers-took-fingerprints-of-5-6-million-us-workers-government-says.html.

— (2017). *Signs of Russian Meddling in Brexit Referendum*. URL: https://www.nytimes.com/2017/11/15/world/europe/russia-brexit-twitter-facebook.html.

The Stationery Office (1990). *Computer Misuse Act 1990*. URL: https://www.legislation.gov.uk/ukpga/1990/18/pdfs/ukpga_19900018_en.pdf.

— (1994). *Intelligence Services Act 1994*. URL: http://www.legislation.gov.uk/ukpga/1994/13/pdfs/ukpga_19940013_en.pdf.

— (1997). *Police Act 1997*. URL: http://www.legislation.gov.uk/ukpga/1997/50/pdfs/ukpga_19970050_en.pdf.

— (1998). *Human Rights Act 1998*. URL: http://www.legislation.gov.uk/ukpga/1998/42/pdfs/ukpga_19980042_en.pdf.

— (2000a). *Electronic Communications Act 2000*. URL: http://www.legislation.gov.uk/ukpga/2000/7/pdfs/ukpga_20000007_en.pdf.

— (2000b). *Regulation of Investigatory Powers Act 2000*. URL: http://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf.

— (2000c). *Terrorism Act 2000*. URL: https://www.legislation.gov.uk/ukpga/2000/11/pdfs/ukpga_20000011_en.pdf.

— (2006). *Police and JusticeAct 2006*. URL: http://www.legislation.gov.uk/ukpga/2006/48/pdfs/ukpga_20060048_en.pdf.

— (2014). *Data Retention and Investigatory Powers Act 2014*. URL: http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga_20140027_en.pdf.

— (2016). *Investigatory Powers Act 2016*. URL: http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf.

— (2019). *Crime (Overseas Production Orders) Act 2019*. URL: http://www.legislation.gov.uk/ukpga/2019/5/pdfs/ukpga_20190005_en.pdf.

The Supreme Court (2019). *[2019] UKSC22*. URL: https://www.supremecourt.uk/cases/docs/uksc-2018-0004-judgment.pdf.

The Telegraph (2014). *Facebook 'could have prevented Lee Rigby murder'*. URL: https://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11253518/Facebook-could-have-prevented-Lee-Rigby-murder.html.

— (2018). *Britain steps up cyber offensive with new £250m unit to take on Russia and terrorists*. URL: https://www.telegraph.co.uk/news/2018/09/21/britain-steps-cyber-offensive-new-250m-unit-take-russia-terrorists/.

The Times (2018a). *May vows revenge on Russia over Salisbury novichok poisonings*. URL: https://www.thetimes.co.uk/edition/news/may-vows-revenge-on-russia-over-salisbury-novichok-poisonings-93lk85sjr?utm_campaign=Echobox&utm_medium=Social&utm_source=Twitter#Echobox=1536215469.

— (2018b). *Novichok attack: GCHQ's reputation is its greatest weapon in secret battle*. URL: https://www.thetimes.co.uk/edition/news/gchq-s-reputation-is-its-greatest-weapon-in-secret-battle-0mcnj93wg.

The Washington Post (2017). *NSA officials worried about the day its potent hacking tool would get loose. Then it did.* URL: https://www.washingtonpost.com/business/technology/nsa-

officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html.

Thiele, Ulrich (2012). »Vom Sicherheitsstaat zum Rechtsstaat – und zurück«. In: *Sicherheit versus Freiheit*. Hrsg. von Rüdiger Voigt. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 101–123. ISBN: 978-3-531-18643-6.

Thies, Cameron (2010). »Role Theory and Foreign Policy«. In: *The international studies encyclopedia*. Hrsg. von Robert Allen Denemark. Malden, MA: Wiley-Blackwell, S. 6335–6356. ISBN: 978-1-4051-5238-9.

Thies, Cameron G. und Marijke Breuning (2012). »Integrating Foreign Policy Analysis and International Relations through Role Theory«. In: *Foreign Policy Analysis* 8.1, S. 1–4. ISSN: 17438586. DOI: 10.1111/j.1743-8594.2011.00169.x.

Trade and Industry Select Committee (1999). *Seventh Report - Session 1998-99*. URL: https://publications.parliament.uk/pa/cm199899/cmselect/cmtrdind/187/18702.htm.

Traylor, John Mylan (2016). »Shedding Light on the
Going Dark
Problem and the Encryption Debate«. In: *University of Michigan Journal of Law Reform* 50.2, S. 489–524.

Treasury (2018). *Budget 2018*. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752202/Budget_2018_red_web.pdf.

Turner, Ralph H. (1990). »Role Change«. In: *Annual Review of Sociology* 16, S. 87–110.

U.S. Department of Homeland Security (2016). *Five Country Ministerial and Quintet of Attorneys General Joint Communiqué*. URL: https://www.dhs.gov/news/2016/02/18/five-country-ministerial-and-quintet-attorneys-general-joint-communique.

UK Government (1999). *Interception of Communications in the United Kingdom: A Consultation Paper*. URL: https://webarchive.nationalarchives.gov.uk/20100408131425/http://www.homeoffice.gov.uk/documents/cons-1999-interception-comms2835.pdf.

— (2009). *The National Security Strategy of the United Kingdom: Update 2009 - Security for the Next Generation*. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/229001/7590.pdf.

— (2010). *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf.

— (2011). *Armed Forces Minister - Responding to Cyber War*. URL: https://www.gov.uk/government/news/armed-forces-minister-responding-to-cyber-war.

— (2013a). *New cyber reserve unit created*. URL: https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit.

— (2013b). *PM statement on European Council: October 2013*. URL: https://www.gov.uk/government/speeches/pm-statement-on-european-council-october-2013.

— (2013c). *PM's European Council press conference: October 2013*. URL: https://www.gov.uk/government/speeches/pms-european-council-press-conference-october-2013.

— (2014). *Security and Privacy in the Internet Age*. URL: https://www.gov.uk/government/speeches/security-and-privacy-in-the-internet-age.

— (2015a). *Chancellor's speech to GCHQ on cyber security*. URL: https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security.

— (2015b). *Factsheet –Bulk Equipment Interference*. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473753/Factsheet-Bulk_Equipment_Interference.pdf.

UK Government (2015c). *Factsheet –Bulk Interception*. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473751/Factsheet-Bulk_Interception.pdf.
— (2016a). *Chancellor speech: launching the National Cyber Security Strategy*. URL: https://www.gov.uk/government/speeches/chancellor-speech-launching-the-national-cyber-security-strategy.
— (2016b). *Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny*. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/504174/54575_Cm_9219_WEB.PDF.
— (2016c). *Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny*. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/504174/54575_Cm_9219_WEB.PDF.
— (2016d). *Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny*. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/504174/54575_Cm_9219_WEB.PDF.
— (2016e). *Investigatory Powers Bill: Obligations on Communications Service Providers (CSPs)*. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/530557/Obligations_on_CSPs_Factsheet.pdf.
— (2016f). *National Cyber Security Strategy 2016-2021*. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.
— (2017a). *Foreign Office Minister condemns North Korean actor for WannaCry attacks*. URL: https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks.
— (2017b). *PM speech at UNGA: preventing terrorist use of the internet*. URL: https://www.gov.uk/government/speeches/pm-speech-at-unga-preventing-terrorist-use-of-the-internet.
— (2018a). *Foreign Office Minister condemns criminal actors based in Iran for cyber-attacks against UK universities*. URL: https://www.gov.uk/government/news/foreign-office-minister-condemns-criminal-actors-based-in-iran-for-cyber-attacks-against-uk-universities.
— (2018b). *Speech - Cyber and International Law in the 21st Century*. URL: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.
— (2018c). *UK and allies reveal global scale of Chinese cyber campaign*. URL: https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign.
— (2018d). *UK exposes Russian cyber attacks*. URL: https://www.gov.uk/government/news/uk-exposes-russian-cyber-attacks.
— (2019a). *Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime*. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.
— (2019b). *Deterrence in the cyber age: Foreign Secretary's speech*. URL: https://www.gov.uk/government/speeches/deterrence-in-the-cyber-age-speech-by-the-foreign-secretary.
— (2019c). *Joint Meeting of FCM and Quintet of Attorneys-General*. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822818/Joint_Meeting_of_FCM_and_Quintet_of_Attorneys_FINAL.pdf.

— (2020). *UK condemns Russia's GRU over Georgia cyber-attacks*. URL: https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks.

Ulbert, Cornelia (2014). »Social constructivism«. In: *Theories of international relations*. Hrsg. von Siegfried Schieder und Manuela Spindler. London: Routledge, S. 248–268. ISBN: 978-0415741149.

UN (2013). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. URL: https://undocs.org/A/68/98.

United Nations (1990). *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*. URL: https://digitallibrary.un.org/record/1296532/files/a-conf-144-28-rev-1-e.pdf.

— (2004). *A/59/116 - Developments in the field of information and telecommunications in the context of international security Report of the Secretary-General*. URL: https://undocs.org/A/59/116.

— (2011). *Developments in the field of information and telecommunications in the context of international security: Report of the Secretary-General*. URL: http://undocs.org/A/66/152.

— (2013a). *A/68/156/Add.1*. URL: https://undocs.org/A/68/156/Add.1.

— (2013b). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. URL: https://undocs.org/A/68/98.

— (2013c). *Resolution 68/167*. URL: https://undocs.org/A/RES/68/167.

— (2016a). *Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, the Special Rapporteur on the situation of human rights defenders and the Special Rapporteur on the idependence of judges and lawyers*. URL: https://cdn.netzpolitik.org/wp-upload/2016/09/160829_Stellungnahme_UN-Sonderbeauftragte_zur_BND-Reform.pdf.

— (2016b). *Report of the Special Rapporteur on the right to privacy*. URL: https://undocs.org/en/A/HRC/31/64.

United Nations Human Rights Special Procedures (2018). *Encryption and Anonymity follow-up report*. URL: https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf.

Valeriano, Brandon und Ryan C. Maness (2014). »The dynamics of cyber conflict between rival antagonists, 2001–11«. In: *Journal of Peace Research* 51.3, S. 347–360. ISSN: 0022-3433. DOI: 10.1177/0022343313518940.

— (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford und New York: Oxford University Press. ISBN: 978-0190204792.

Vice (2014). *How Refusing to Hand Over Your Passwords Can Land You in Jail*. URL: https://www.vice.com/en_us/article/wnjgdq/how-refusing-to-hand-over-your-passwords-can-land-you-in-jail.

Voeller, John G., Hrsg. (2010). *Wiley handbook of science and technology for homeland security*. Hoboken, N.J.: Wiley. ISBN: 978-0-470-13851-9.

Votsis, Ioannis, Michela Tacca und Gerhard Schurz (2015). »Theory-Ladenness Special Issue: Introduction«. In: *Journal for General Philosophy of Science* 46.1, S. 83–86. DOI: 10.1007/s10838-015-9283-y.

Walker, Stephen G. (2011). »The Integration of Foreign Policy Analysis and International Relations«. In: *Rethinking foreign policy analysis*. Hrsg. von Stephen G. Walker, Akan Malici und Mark Schafer. New York, N.Y.: Routledge, S. 267–282. ISBN: 978-0-415-88698-7.

— (2017). »: Role Theory as an Empirical Theory of International Relations: From Metaphor to Formal Model«. In: *Oxford Research Encyclopedia of Politics*. DOI: 10.1093/acrefore/

9780190228637 . 013 . 286. URL: http : / / politics . oxfordre . com / view / 10 . 1093 / acrefore / 9780190228637.001.0001/acrefore-9780190228637-e-286.

Walter, Barbara F. (2017). »The New New Civil Wars«. In: *Annual Review of Political Science* 20.1, S. 469–486. DOI: 10.1146/annurev-polisci-060415-093921.

Waltz, Kenneth N. (2000). »Structural Realism after the Cold War«. In: *International Security* 25.1, S. 5–41. ISSN: 01622889. DOI: 10.1162/016228800560372.

Washington Post (2016). *The British want to come to America — with wiretap orders and search warrants*. URL: https://www.washingtonpost.com/world/national-security/the-british-want-to-come-to-america--with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9_story.html.

Wasik, Martin (2010). »The emergence of computer law«. In: *Handbook of Internet crime*. Hrsg. von Yvonne Jewkes und Majid Yar. Abingdon: Routledge, S. 395–412. ISBN: 978-1843925248.

Wehner, Leslie E. und Cameron G. Thies (2014). »Role Theory, Narratives, and Interpretation: The Domestic Contestation of Roles«. In: *International Studies Review* 16.3, S. 411–436. DOI: 10.1111/misr.12149.

Weidmann, Nils B. (2015). »Communication, technology, and political conflict: Introduction to the special issue«. In: *Journal of Peace Research* 52.3, S. 263–268. ISSN: 0022-3433. DOI: 10.1177/0022343314559081.

Welt (2013). *Friedrich erklärt Sicherheit zum „Supergrundrecht"*. URL: https://www.welt.de/politik/deutschland/article118110002/Friedrich-erklaert-Sicherheit-zum-Supergrundrecht.html.

— (2016). *Spähsoftware Bundestrojaner ist kaum brauchbar*. URL: https://www.welt.de/politik/deutschland/article154173376/Spaehsoftware-Bundestrojaner-ist-kaum-brauchbar.html.

— (2018). *Ministerium gibt neuen Bundestrojaner für den Einsatz frei*. URL: https://www.welt.de/politik/deutschland/article173121473/Verdeckte-Ueberwachung-Ministerium-gibt-neuen-Bundestrojaner-fuer-den-Einsatz-frei.html.

Wendt, Alexander (1999). *Social theory of international politics*. Bd. 67. Cambridge studies in international relations. Cambridge, U.K. und New York: Cambridge University Press. ISBN: 978-0521469609.

Weyer, Johannes (2008). *Techniksoziologie: Genese, Gestaltung und Steuerung sozio-technischer Systeme*. Grundlagentexte Soziologie. Weinheim: Juventa. ISBN: 978-3779914853.

White, Brian (2013). »British Foreign Policy: Continuity and Transformation«. In: *Foreign policy in comparative perspective*. Hrsg. von Ryan K. Beasley. Thousand Oaks, California: CQ Press, S. 27–52. ISBN: 978-1-60871-696-8.

White, Lynn (1962). *Medieval technology and social change*. London: Oxford University Press. ISBN: 978-0195002669.

White, Sarah P. (2018). *Understanding Cyberwarfare. Lessons from the Russia-Georgia War*. URL: https://mwi.usma.edu/wp-content/uploads/2018/03/Understanding-Cyberwarfare.pdf.

Whyte, Christopher (2018). »Dissecting the Digital World: A Review of the Construction and Constitution of Cyber Conflict Research«. In: *International Studies Review* 80.3. DOI: 10.1093/isr/viw013.

Wiener, Antje (2008). *The Invisible Constitution of Politics: Contested Norms and International Encounters*. Cambridge: Cambridge University Press. ISBN: 978-0-521-89596-5.

Wilholt, Torsten (2009). »Die Objektivität der Wissenschaften als soziales Phänomen«. In: *Analyse & Kritik* 2, S. 261–273.

Willett, Marcus (2019). »Assessing Cyber Power«. In: *Survival* 61.1, S. 85–90. ISSN: 0039-6338. DOI: 10.1080/00396338.2019.1569895.

Wired (2016). *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*. URL: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

Wissenschaftlicher Dienst des Bundestages (2007). *Verfassungsmäßigkeit von Online-Durchsuchungen - Ausarbeitung -*. URL: https://www.bundestag.de/resource/blob/423596/d5187cd3b1169df1834da5b9f662c9bb/wd-3-161-07-pdf-data.pdf.

World Bank (2019). *Individuals using the Internet (% of population)*. URL: https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2016&locations=DE-GB&start=1993.

Zajácz, Rita (2017). »Silk Road: The market beyond the reach of the state«. In: *The Information Society* 33.1, S. 23–34. ISSN: 0197-2243. DOI: 10.1080/01972243.2016.1248612.

ZDF (2018). *heute.de-Interview - Baum: Staatstrojaner gefährdet die Freiheit*. URL: https://www.zdf.de/nachrichten/heute/baum-der-staatstrojaner-gefaehrdet-die-freiheit-100.html.

— (2019). *Planspiele der Bundesregierung - Kommt der große Cyber-Gegenangriff?* URL: https://www.zdf.de/nachrichten/heute/bundessicherheitsrat-horst-seehofer-will-den-bundesnachrichtendienst-fuer-den-cyber-krieg-aufruesten-100.html#xtor=CS5-62.

Zeit (2009). *Verfassungsklage gegen neues BKA-Gesetz: Jeder ist verdächtig*. URL: https://www.zeit.de/2009/18/BKA-Gesetz.

— (2018). *Maaßen spricht von Attacke russischen Ursprungs*. URL: https://www.zeit.de/politik/2018-04/hackerangriff-bundesregierung-russland-verfassungsschutz-hans-georg-maassen.

— (2019). *Cybersicherheit: Gutachten warnt Bundesregierung vor Hackback*. URL: https://www.zeit.de/digital/2019-09/cybersicherheit-hackback-plaene-bundesgutachten-bundesregierung.

Zetter, Kim (2014). *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*. First edition. New York: Crown Publishers. ISBN: 978-0770436179.

# Politik in der digitalen Gesellschaft


Jeanette Hofmann, Norbert Kersting,
Claudia Ritzi, Wolf J. Schünemann (Hg.)

**Politik in der digitalen Gesellschaft**

**Zentrale Problemfelder und Forschungsperspektiven**

2019, 332 S., kart., 25 SW-Abbildungen
39,99 € (DE), 978-3-8376-4864-5
E-Book: kostenlos erhältlich als Open-Access-Publikation
PDF: ISBN 978-3-8394-4864-9


Kathrin Braun, Cordula Kropp (Hg.)

**In digitaler Gesellschaft**

**Neukonfigurationen zwischen Robotern, Algorithmen und Usern**

2021, 318 S., kart., 3 SW-Abbildungen, 22 Farbabbildungen
29,00 € (DE), 978-3-8376-5453-0
E-Book: kostenlos erhältlich als Open-Access-Publikation
PDF: ISBN 978-3-8394-5453-4
EPUB: ISBN 978-3-7328-5453-0