Standardization and Risk Governance

This multi-disciplinary book conceptualizes, maps, and analyses ongoing standardization processes of risk issues across various sectors, processes, and practices.

Standards are not only technical specifications and guidelines to support efficient risk governance, but also contain social, political, economic, and organizational aspects. This book presents a variety of standardization processes and applications of standards that may influence our judgements of risk, the organizing of risk governance, and, accordingly, our behaviour. Standardization and standards can impact risk governance in different ways. The most important lessons drawn from the present volume can be summarized in three areas: (1) how standardization might impact on power relations and interests; (2) how standardization may change flexibility in decision-making, communication, and cooperation; and (3) how standardization could (re)direct attention and risk perception.

The volume's aim is to present an analysis of standardization processes and how it affects our thinking about risk, how we organize risk governance, and how standardization may influence risk management. In so doing, it contributes to a more informed discourse regarding the use of standards and standardization in contemporary risk management.

Standardization and Risk Governance will be of great interest to students of risk, standardization, global governance, and critical security studies.

Odd Einar Olsen is Professor in Risk Management and Societal Safety at the University of Stavanger, Norway.

Kirsten Juhl is Associate Professor in Risk Management and Societal Safety at the University of Stavanger, Norway.

Preben H. Lindøe is Emeritus Professor in Risk Management and Societal Safety at the University of Stavanger, Norway.

Ole Andreas Engen is Professor in Risk Management and Societal Safety at the University of Stavanger, Norway.

Routledge New Security Studies
Series Editors: J. Peter Burgess,
École Normale Supérieur (ENS), Paris

The aim of this book series is to gather state-of-the-art theoretical reflection and empirical research into a core set of volumes that respond vigorously and dynamically to new challenges to security studies scholarship. Routledge New Security Studies is a continuation of the PRIO New Security Studies series.

Visual Security Studies
Sights and Spectacles of Insecurity and War
Edited by Juha A. Vuori and Rune Saugmann Andersen

Privacy and Identity in a Networked Society
Refining Privacy Impact Assessment
Stefan Strauß

Energy Security Logics in Europe
Threat, Risk or Emancipation?
Izabela Surwillo

Crypto-Politics
Encryption and Democratic Practices in the Digital Era
Linda Monsees

Negotiating Intractable Conflicts
Readiness Theory Revisited
Amira Schiff

Standardization and Risk Governance
A Multi-Disciplinary Approach
Edited by Odd Einar Olsen, Kirsten Juhl, Preben H. Lindøe, and Ole Andreas Engen

For more information about this series, please visit: www.routledge.com/Routledge-New-Security-Studies/book-series/RNSS

Standardization and Risk Governance

A Multi-Disciplinary Approach

Edited by Odd Einar Olsen, Kirsten Juhl, Preben H. Lindøe, and Ole Andreas Engen

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2020
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
52 Vanderbilt Avenue, New York, NY 10017

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
Names: Olsen, Odd Einar, 1954- editor. | Juhl, Kirsten, editor. | Lindøe, Preben Hempel, editor. | Engen, Ole Andreas, editor.
Title: Standardization and risk governance : a multi-disciplinary approach / edited by Odd Einar Olsen, Kirsten Juhl, Preben Lindøe and Ole Andreas Engen.
Description: Abingdon, Oxon ; New York, NY : Routledge, 2020. | Series: Routledge new security studies | Includes bibliographical references and index.
Identifiers: LCCN 2019029736 (print) | LCCN 2019029737 (ebook) | ISBN 9780367259730 (hardback) | ISBN 9780429290817 (ebook)
Subjects: LCSH: Risk management–Standards. | Risk assessment–Standards. | Standardization–Social aspects. Classification: LCC HD61 . S725 2020 (print) | LCC HD61 (ebook) | DDC 363.34/62–dc23
LC record available at https://lccn.loc.gov/2019029736
LC ebook record available at https://lccn.loc.gov/2019029737

ISBN: 978-0-367-25973-0 (hbk)
ISBN: 978-0-429-29081-7 (ebk)

Typeset in Times New Roman
by Wearset Ltd, Boldon, Tyne and Wear

Contents

Figures

Contributors

Marcus Abrahamsson is an Associate Professor in the Division of Risk Management and Societal Safety, Lund University, Sweden. His research focuses on risk and vulnerability assessment, preparedness, and capacity development in various contexts.

Michael S. Baram is Professor Emeritus, Boston University Law School, USA. He has dealt with risk regulation, environmental law, product liability law, occupational safety, and risk management issues in technological, chemicals, biotech, nuclear, and oil and gas industries.

Louise Bengtsson holds a PhD in International Relations from Stockholm University. Her work specializes in critical security studies as well as the politics of the EU and global health security.

Ole Andreas Engen is a Professor at the University of Stavanger, Norway. He holds a master's degree in Economics and a PhD in Sociology. His research focuses on the relationship between risk, regulation, technology, and policy.

Henrik Hassel is an Associate Professor in the Division of Risk Management and Societal Safety, Lund University, Sweden. His research concerns development and the evaluation of risk and vulnerability assessments in contexts such as critical infrastructures and municipalities.

Ian Higham is a PhD candidate in the Department of Political Science at Stockholm University, Sweden. His research focuses on early adopters of public policies for business and human rights.

Sindre Aske Høyland is a postdoctoral researcher at the University of Stavanger, Norway, focusing on theoretical and methodological developments within qualitative research, in the fields of societal safety and security and safe work practices.

Fredrik Johnsson is Lieutenant Colonel and Chief of Staff at the Swedish Explosive Ordnance Disposal and Demining Center (SWEDEC). He is also a doctoral student in the Division of Risk Management and Societal Safety, Lund University, Sweden.

Sissel H. Jore is an Associate Professor at the University of Stavanger, Norway. Her main research topics are critical terrorism studies, discourse analysis, and security risk management. She is currently the chair of the Security and Defence group in SRA International.

Lene Jørgensen is an Associate Professor in the Department of Business Administration, Western Norway University of Applied Sciences, Bergen, Norway. She teaches and conducts research within the fields of organization, management, and leadership.

Kirsten Juhl is a former Associate Professor in Risk Management and Societal Safety at the University of Stavanger, Norway. She retired in January 2019.

Preben H. Lindøe is an Emeritus Professor at the University of Stavanger, Norway, in the Division of Risk Regulation and Societal Safety. He has worked within applied research, Occupational Health and Safety, risk regulation, and safety management.

Peter Månsson is a postdoctoral researcher in the Division of Risk Management and Societal Safety, Lund University, Sweden. His research focuses on the challenges and opportunities for collecting and making sense of disaster risk information from multiple organizations.

Claudia Morsut is a postdoctoral researcher at the University of Stavanger, Norway. Her research focuses on EU risk and crisis management policy and governance, the EU Civil Protection Mechanism, and EU security policy.

Odd Einar Olsen is a Professor in Risk Management and Societal Safety at the University of Stavanger, Norway. His main research topics are crisis management in humanitarian disasters, the role of the media in crisis management, and dilemmas in risk governance.

Ruth Østgaard Skotnes is a Research Scientist at NORCE Norwegian Research Centre AS. She has a PhD in Social Science with a specialization in Risk Management and Societal Safety from the University of Stavanger, Norway.

Henrik Tehler is a Professor in the Division of Risk Management and Societal Safety, Lund University, Sweden. He is also the Director of Lund University Centre for Risk Assessment and Management (LUCRAM).

Grahame F. Thompson is Emeritus Professor of Political Economy at the Open University, UK. His most recent books are *Globalization Revisited* (Routledge, 2015) and *Corporate Governance in Contention* (edited with Ciaran Driver, Oxford University Press, 2018).

Sirpa Virta is Professor of Policing and Security Governance at Tampere University, Finland, and Adjunct Professor of Defence. She is a political scientist and has published articles in leading criminological journals and chapters in many edited books.

Preface

In this book, we present a variety of standardization processes and applications of standards that may influence our judgements of risk, the organizing of risk governance, and accordingly our behaviour. They include regulations of international and national cooperation in risk governance and crisis management, regulation of infrastructure and industrial sectors, and risk management in activities and duties within or among organizations.

The idea to analyse standards as a safety and security technology evolved slowly. Compared to the penetrating impact they have on the organization of society, standards and standardization have been unrecognized phenomena in the social sciences. Standardization has rarely been linked to risk governance in a systematic way before. But standards are everywhere and we often take them for granted. The contributors started by taking another look at their ongoing projects, trying to see the standards and standardization processes. It is when you start to look for standards that you really see them. The more you dig into them, the more you understand that standards are not only technical specifications and guidelines to support efficient risk governance. They also contain social, political, economic, and organizational aspects. A new world of knowledge about risk governance unfolded.

Acknowledgements

This project could never have been accomplished without NordForsk funding the Nordic Centre of Excellence for Security Technologies and Societal Values, which served as the home for the project. As an institution represented by the Scientific Advisory Board, Nordforsk could be tough when making demands and assessments, but it also represented a strange feeling of safety when we were able to meet the standards set by the Scientific Advisory Board. The professional and careful advice from Andrew Humphrys and Bethany Lund-Yates at Routledge helped us through the publishing process. The anonymous reviewers provided inspirational and valuable inputs, encouraging the contributors to improve their manuscripts before submission. Most importantly, grateful thanks to all the contributors, who had the stamina to follow the project to the end, but most of all to Kirsten Juhl. She did a tremendous job as a contributor and resource person before she retired.

Odd Einar Olsen
Kirsten Juhl
Preben Hempel Lindøe
Ole Andreas Engen

Abbreviations

AI	artificial intelligence
APA	Administrative Procedure Act
API	American Petroleum Institute
BAST	best available and safest technology
BSEE	Bureau of Safety and Environmental Enforcement
CBA	cost-benefit analysis
CECIS	Common Emergency Communication and Information System
CEN	European Committee for Standardization
CENELEC	Committee for Electrotechnical Standardization
COSO	Committee of Sponsoring Organizations of the Treadway Committee
CSEC	Cyber Security Education Consortium
CT	counterterrorism
CVE	countering violent extremism
DG	Directorate-General
DG CLIMA	Directorate-General for Climate Action
DG DEVCO	Directorate-General for International Cooperation and Development
DG ECHO	Directorate-General for European Civil Protection and Humanitarian Aid Operations
DG ENV	Directorate-General for Environment
DG HOME	Directorate-General for Migration and Home Affairs
DNV	Det Norske Veritas
DRM	disaster risk management
DRMKC	Disaster Risk Management Knowledge Centre
DRR	Disaster Risk Reduction
ECDC	European Centre for Disease Prevention and Control
ECHO	EU Humanitarian Aid and Civil Protection Department
EEC	European Economic Community
EERC	European Emergency Response Capacity
EFSA	European Food Safety Authority
EKF	Export Credit Agency
ELFA	English as a Lingua Franca in Academic Settings
EMA	European Medicine Agency
EMU	Economic and Monetary Union

ENISA	European Union Agency for Network and Information Security
EPR	electronic patient records
ERCC	Emergency Response Coordination Centre
ERM	enterprise risk management
ERNCIP	European Reference Network for Critical Infrastructure Protection
ESS	European Standardization System
ETF	exchange traded funds
ETSI	European Telecommunications Standards Institute
FFFP	aerial forest fire fighting module using planes
FHOS	field hospital
FOI	Swedish Defence Research Institution
FORTV	Swedish Fortifications Agency
GDP	gross domestic product
GDPR	General Data Protection Regulation
GICHD	Geneva International Centre for Humanitarian Demining
HCP	high capacity water pumping
HRO	high reliability organization
HRT	high reliability theory
HSCB	Human Socio-Cultural Behavior Modelling Program
HSE	health, safety, and environment
HUSAR	heavy urban search and rescue
IADC	International Association of Drilling Contractors
ICS	industrial control systems
ICS-CERT	Industrial Control Systems Emergency Response Team
IEC	International Electrotechnical Commission
IMoLIN	International Money Laundering Information Network
IPR	independent project review
IRGC	International Risk Governance Council
IRGC	International Risk Governance Center
ISO	International Organization for Standardization
ISS	information systems security
IT	information technology
LUCRAM	Lund University Centre for Risk Assessment and Management
MCDA	multi-criteria decision analysis
MIUN	Mid Sweden University
MMS	Minerals Management Service
MSB	Swedish Civil Contingencies Agency
NAP	National Action Plan
NCS	Norwegian Continental Shelves
NIST	National Institute of Standards and Technology
NORCE	Norwegian Research Centre
NOU	Norsk Offentlig Utredning
NPD	Norwegian Petroleum Directorate
OECD	Organisation for Economic Co-operation and Development
OMC	open method of coordination

OSCE	Organization for Security and Co-operation in Europe
PRIO	Peace Research Institute, Oslo
PSA-N	Petroleum Safety Authority Norway
RCBA	risk-cost-benefit analysis
RVA	risk and vulnerability assessments
SCADA	supervisory control and data acquisition
SDO	standards development organizations
SWEDEC	Swedish Explosive Ordnance Disposal and Demining Center
TFEU	Treaty on the Functioning of the European Union
TOC	technical operator company
TTAA	Technology Transfer and Advancement Act
UC	uncommon categorization
UN	United Nations
UNDRR	United Nations Office for Disaster Risk Reduction
UNHRC	UN Human Rights Council
UNISDR	United Nations International Strategy for Disaster Reduction
UNODC	United Nations on Drugs and Crime
VOICE	Vienna-Oxford International Corpus of English
WHO	World Health Organization
WP	water purification
WrELFA	Written Academic
YLD	years lived with disability

Part I

Introduction

1 The standardization of risk governance

Odd Einar Olsen

Introduction

Compared to the penetrating impact they have on our daily life, economic development, and the organization of society, standards and standardization have been greatly unrecognized phenomena in the social sciences (Timmermans and Epstein, 2010). Most contributions have been linked to economic issues, technologies, medicine, working life, and administration in some way or another. Relations between risk and standards have scarcely been analysed in a systematic way. In more general contributions on standardization and standards, while the links between risk and standards have been touched upon, they have not been the focus of analysis (Busch, 2011; Timmermans and Epstein 2010). Uncertainty and unpredictability concerning the future are vital elements in understanding and conceptualizing risk, whereas standardization constitutes tools providing certainty, predictability, and control. In that sense, standardization of risk governance seems like a good idea. But there is a lack of empirical studies extending our knowledge between risk and risk governance, on one hand, and standards and standardization, on the other. This anthology's contribution is to fill that gap.

Transboundary risks and the growing complexity, internationalization, and integration of economic and social life call for similar apprehensions of risk and compatible approaches to risk management. Cross-border and institutional cooperation call for compatible organization, plans and equipment, as well as clear communication. These factors both underpin the need for standardization and act as driving forces in developing standards. In this volume, the contributors attempt to standardize vital elements in risk governance, such as risk assessments, contingency planning, risk and crisis management, and even risks themselves. The production of standards impacts the way we think about risks and organize risk governance in general. But is it really possible to define risks in terms of standards? For 'pure' technical devices and systems, foods, or medical devices, etc., building on natural science, it makes sense. But when it comes to risks characterized by complexity and ambiguity, standardization could be a failure, leading to negative outcomes. Or, at least, standardization of such risks and risk governance is a challenge that is not yet solved.

The chapters in this book discuss standardization of risk and the risk of standardization from different viewpoints using different theoretical perspectives. Furthermore, our chosen perspectives reveal and expose how standardization of risk influences our understanding, perception, and organizing of risk governance. Our hope is that the anthology will contribute to a better-informed discourse and reflexive practice in the use of standards and standardization in contemporary risk management.

Risk in the real world and risk as concepts

According to a realist point of view, risk knowledge is related to a phenomenon or an activity, and research related to such risks aims to acquire knowledge about the specific activity or problem (Lypton, 2013). We have often learnt or intuitively felt such risks when we met them. Based on experience, we can judge them and try to avoid or control them by adapting to the situation. Conceptualizing risks implies that we introduce some theoretical assumptions and characteristics to the phenomenon moving risk from the real world into the academic world, and often from the practical world to the theoretical world. Defining and conceptualizing the phenomenon form the first step towards transforming the phenomenon to concepts and models. Consequently, standardizing concepts and models of risk and risk governance will be a further development of assumptions and characteristics into what already are theoretical constructions of risk.

Definitions of risk in this volume fall roughly into two categories. The most common definitions express the relations between probabilities and expected outcomes, including the uncertainty always embedded in risks. The other way of defining risk combines threats, values, and the vulnerability of the object or subject at stake, where probabilities are avoided (see Juhl, Chapter 2, and Jore, Chapter 9, in this volume). Most authors discuss standardization as elements in risk governance concepts and models. The SRA Glossary[1] defines risk governance as the application of governance principles to the identification, assessment, management, and communication of risk. Governance refers to the actions, processes, traditions, and institutions by which authority is exercised and decisions are taken and implemented. Risk governance includes the totality of actors, rules, conventions, processes, and mechanisms concerned with how relevant risk information is collected, analysed, and communicated, and management decisions are taken. Consequently, processes and outcomes of standardization elements in risk governance influence the way we try to manage risks. According to the SRA Glossary, risk management can be defined as activities to handle risk, such as prevention, mitigation, adaptation, or sharing. It often includes trade-offs between costs and benefits of risk reduction and the choice of a level of tolerable risk.

So far, there has been limited research on the role of standardization and the use of standards in risk governance. The possibility that such standardization might produce other risks due to inherent dilemmas and paradoxes has virtually not been tested. This multi-disciplinary book addresses some of these shortcomings

through conceptualizing, mapping, and analysing ongoing standardization processes and the use of standards across sectors and practices.

Standards and standardization

Brunsson and Jacobsson (2000) regard standards and standardization as major tools in organizing and regulating the global order. Standards contribute to coordination and cooperation between people, organizations, and countries. They are instruments of control, as well as guidelines for acceptable and ethical behaviour. Standardization is normally a product of institutional work (Slager, Gond, and Moon, 2012). The introduction and application of standards often follow a trajectory from being formally adopted guidelines to collectively accepted valid solutions to a problem (Haack, Schoeneborn, and Wickert, 2012). And they have comprehensive and penetrating consequences for society. Standards could be rules that classify objects or actors (e.g. measurement methods, such as the metric system or internet codes). Standards could define the design and quality of products, production processes, and trade (e.g. Quality Management: ISO 9001). Standards could be rules and guidelines defining the plans and documentation of organizations and institutions (e.g. requirements for jobs, education certificates). Standards could be rules and guidelines that describe organizational and institutional behaviour (e.g. internal and external procedures, cooperation, etc.). And standards and norms could define and guide governments and international cooperation, among other things because they reduce transaction costs.

In short, standards may include everything from generally accepted norms to legally binding agreements and definitions. The term 'standard', as used here, can be regarded as a subset of 'shared social norms' with implicit or explicit rules and expectations in a larger social community or society. Standards may exist as unwritten norms within a professional community or be explicitly defined directives and agreements (Brunsson and Jacobsson, 2000; Sandholtz, 2012). They can also be determined by technologies in use. The standards provide rules, guidelines, and characteristics for activities or their results, with the aim of maintaining a high degree of order, compatibility, transparency, and predictability in a given context.[2]

Consequently, standards and standardization can be highly political or used as political means. Standards can define requirements benefiting some actors and excluding others. And if something goes wrong, standards could serve as scapegoats. Blaming a standard for the failures may absolve organizations and individuals from guilt and punishment. Standards appear as power without responsibility, because we cannot punish a standard – or the anonymous experts who developed it. One implication of standards as politics is that working standards ought to be arbitrary and not associated with any defined actor of power. The more arbitrary, the more neutral and invisible they appear to be. One of our most widespread standards is established for measuring distances. A metre is defined as the distance light is moving in a vacuum during a time interval of 1/299,792,458 of a second: a meaningless thing in itself but, at the same time, a core measure for the functioning of society.

Standardization of risk governance

The bureaucratization of safety and security work has been going on for decades (Dekker, 2014). One example is the standardization of risk management, organized by the International Organization for Standardization (ISO) for almost 30 years.[3] Governments have overall responsibility for security and keeping citizens safe. They normally do this by managing risks through laws, regulations, and resource allocation. Public and private contingency organizations and risk management departments need to organize their missions, based on routines, guidelines, and rules, such as standards. All these arrangements need to have some references defining responsibilities and capacities. These processes have created new institutions and organizations working with safety/security-related education and training opportunities, coordination and division of labour, new methodologies and technologies.

Systematic approaches to risk management are elaborated in general frameworks like the ISO 31000 of 2009 and the International Risk Governance Council (IRGC) Risk Governance-framework.[4] A variety of risk management frameworks have been developed, based on system thinking (Rasmussen, 1997; Cassano-Piche, Vicente, and Jamieson, 2009). These framework prescriptions are not necessarily the solution to all risk governance challenges. The main elements in risk management are risk analysis and risk evaluation (assessment), treatment of risks, and risk communication (Aven and Renn, 2010). The risk assessment is the basis for the treatment of risks. In the ISO 31000 Risk Management standard of 2009, we can find lists of principles for effective management of risk, for instance, how risk management should be tailored within the organization's context. The standard also lists important components like the commitment and resources necessary for the implementation of risk management in the organization. Klinke and Renn (2012) stress that risk management systems are based on available resources and institutional means. In short, standards are seemingly ordinary tools present in most risk-related planning activities.

Risk analysis most often requires (scientific) expertise, both within the objects and processes analysed and in the techniques for analysing risks. But this is only the starting point. Although mathematical calculations or science-based judgements of risks may look convincing, there are rarely scientific answers that can give an exhaustive conclusion on the risk or the most appropriate risk management systems. This is where standards can help out and guide risk management, contingency planning, and responses in accidents and disasters. The 'risk landscape' has changed, and risks appearing within different sectors/domains have become interconnected. Risk issues, assigned to and managed by individual risk owners, no longer seem to be the state of the art. Theories of risks, risk management and communication, contingency planning, and response in emergencies and disasters have shifted the attention from 'simple' risk issues towards issues with high complexity and unresolved uncertainty (Renn, 2014). As a consequence, new ideas about the complex interplay between different risk factors and actors are required in risk management and governance.

Driving forces for standardizing risk governance

The growing interest in and the need to standardize risks and risk management have developed for different reasons.

First, risk is about the future, and nobody knows exactly what the future will bring. Impressive calculations and logical arguments may disguise this fact but never remove it. And standards may bring about some feeling of certainty in an uncertain world.

Second, a calculated risk must be judged as acceptable or not acceptable by someone, which implies that non-scientific arguments based on one's own experiences, interests, and feelings will come into play. There is a functional distinction between risk analysis, which is a matter of evidence, and value-oriented risk evaluation, which is normally a management responsibility. In practical life, they can be intertwined processes (Aven and Renn, 2010). Whereas risk analysis and risk assessment are a profession for so-called risk experts, managing risk is for managements that may have a different understanding and approach to the risks at stake (see Jørgensen and Lindøe, Chapter 11, in this volume). Risk experts and managements need some common ground to establish a fruitful dialogue, where agreed standards may help out and build bridges between different stakeholders and perspectives.

Third, risk is very often a consequence of many factors and processes that come together in ways that were not anticipated. Even the understanding of what a risk may be is contested. This is reflected, for example, in the many definitions of risk that flourish in the risk literature. Since Ulrich Beck launched his famous book about the risk society in German in 1986, the understanding of risks as complex cross-border phenomena has grown tremendously (Beck, 1992). International organizations provide new analyses on future transboundary risks on a regular basis. Concepts like the IRGC's and the Organisation for Economic Co-operation and Development's (OECD) emerging risks (OECD, 2003; Renn, 2014; Florin and Bürkler, 2017), global shocks (OECD, 2011), global risks (annual reports from the World Economic Forum), the World Bank and urban risks (Dickson *et al.,* 2012), and disaster risk reduction (UNISDR, 2004, 2005, 2015) have changed the way we regard serious threats. What they all have in common is that the globalization of economic and infrastructure systems, production, and consumption, together with the character of new threats, contributes to the internationalization of threats and risks. Such risks cannot be handled at a national level alone.

Fourth, as long as the new threats do not acknowledge any national borders, meeting them calls for international cooperation. Improving security and safety has always been a key issue in most societies. As a consequence, ways of organizing safety and security in society have developed in different ways and have been institutionalized over decades and centuries. Different national systems are therefore not compatible, and attempts in the European Union (EU) to integrate national emergency response systems in a common EU Civil Protection Mechanism

appear extremely difficult without standards for capacities and operations (see Morsut, Chapter 3 in this volume).

Fifth, the need for standardization has opened up and accelerated a new market for consultants in safety and security, whose predominant competence is not necessarily within specific sectors or substantial topics. Standardization of risk management and governance, and even of risks themselves, has therefore appeared as a growing business among standardization bureaus, consultants, and agencies responsible for risk management. The prices charged for a few pages describing the recommended standards indicate that it is a good business.

Consequently, the need for universally accepted and agreed procedures and measures for risk judgements, risk management, and risk governance is easy to understand. If things go wrong, it may rapidly become a political issue that could destroy the reputation and the future of both individuals and organizations. Third-party certification is one way of protecting oneself and the organization. Engaging an independent expert who certifies to recognized standards could be a tempting way to reduce uncertainty and misunderstandings, to improve communication between different actors in risk governance, and to safeguard one's own decisions. But it could also create an exaggerated feeling of security (see Jore, Chapter 9, in this volume). Furthermore, defining standards is highly political. Global (private) regulators, writing and thereby defining standards, have put themselves in a very powerful position (Büthe and Mattli, 2011).

The invisible standardization of risk

The digitalization of working processes, administration, public and private services, and even our private lives, has reinforced a development in which machines are replacing people, and artificial intelligence is replacing human reasoning. This development has been predicted for decades, but it was only in the 2010s that this development has materialized in an accelerating digitalization of almost all sectors in modern societies. ICT systems are integrated into the ability of different sectors to uphold their services (see Skotnes, Chapter 10, in this volume), and these systems can contribute to creating a sense of confidence that technologies aimed at improving performance and welfare will not endanger data privacy, confidentiality, integrity, or availability.

However, nobody seems to have a full overview of the speed, direction, or consequences of this technological revolution. In almost all chapters, although it has not been the main focus, the authors deal with problems and challenges that in some way or another are relevant to digitalization.

Artificial intelligence (AI) is currently not as intelligent as it appears to be. A machine will be able to beat the world champion in chess but will never understand that it has won the match. AI is based on machine learning, which basically is the capacity to automatically discover, systemize, and act on pattern recognitions at a speed that humans can never dream of. Making decisions, based only on patterns generated in the past, is an efficient but also a risky way of exercising risk governance. Furthermore, machine learning and

AI are based on algorithms. An algorithm is simply explained as a set of rules that precisely defines a sequence of operations, including input of data and calculations based on input data. The calculations stop when a satisfactory answer (or solution) is found. These tools may become extremely powerful when they are used on Big Data. Big Data are ways to analyse, systematically extract information from, or otherwise deal with, data sets that are too large or too complex to be dealt with by traditional data processing applications (used by humans).

Digitalization will represent and is already representing increasing challenges for risk governance. By nature, risk and disaster management are characterized by many factors playing together in unexpected ways and by high degrees of uncertainty; they often also require fast decision-making processes. Consequently, it is likely that digitalization and artificial intelligence will be an increasingly important part of risk governance in the future. Applied in risk governance, AI and digitalization constitute an invisible standardization of operations, judgements, and decisions.

More and more standards are inscribed in ICT infrastructures, also including tools and systems for risk governance. Such standards will guide work in ways that a paper-based standard cannot because they can quickly provide simple answers to tricky problems, while at the same time being faceless, invisible, and convincing. But AI reacts according to the standard, either set by a human or developed by the machine, and not necessarily according to reality and the action needed to secure good risk governance.

For many purposes within risk governance, AI could be an efficient tool for better decisions, for example,

- when it comes to improving information used in human analysis of risk and risk governance;
- reducing people's exposure to dangerous working environments and situations;
- overseeing the condition of technical installations, aspects of risk-related coordination, logistics, and standard operating procedures;
- 'performing risk communication' (Turkle, 2011).

Some see no limits.[5] KMPG's visions include nothing less than the integration of information from the past, present, and future, covering all thinkable risks, workflows in the organization, and, finally, risk and control indicators and actions.

In the financial sector, an estimated 85 per cent of stock trading in 2018 was done automatically by the use of algorithms and AI. Thompson (see Chapter 12, in this volume) examines several features of the financial system that involve issues of standardization, paying special attention to the specific standardization of algorithmic trading. This involves recognizing that standardization can be a consequence of the informal adoption of a codified social norm rather than a formal process of overt construction and implementation.

'Algorithms by themselves are neither good nor bad; they are useful, and they may be employed for disputable businesses – but that's none of their business' (Krasmann, 2018, p. 10). But behind the impressive speed of recognizing patterns and automatic decision-making, there are humans. People design the algorithms that structure the decisions the machine will make for us. Humans have to set some criteria for input of data, how the calculations are made and what a satisfactory answer or solution is and, furthermore, for how these processes should constantly add to the machine learning. Consequently, knowledge and values possessed by the programmers may reflect the direction and outcome of digitalization. When Amazon introduced automatic evaluation of job applicants, women were systematically losing in the competition with men. The reason was traced back to an algorithm downplaying women's capabilities.

In risk governance, a commonly used example of an ethical dilemma is what a driverless car should do if it has to choose between hitting a child or two elderly people. In a digital world, this must be decided upon in advance. But how is it possible to decide on that in an open process? Disguising it in an algorithm may solve the problem. An even more questionable case is the *Human Socio-Cultural Behavior Modeling Program (HSCB)*, organized by the Pentagon, of 2008. HSCB included the Social Radar project, aiming to identify so-called sentiment-target constellations and changes in population attitudes by using AI and Big Data. The information in turn was used to attack unknown persons by drones, based on anticipated behaviour identified by AI (Cohn *et al.,* 2016). Similar projects, aiming to identify suspect and dangerous persons automatically as part of border control, have been developed, for instance, in the EU Horizon research programme. Algorithms could also be design failures. In March 2019, all new Boeing 737 MAX aircraft were grounded after two serious crashes that took 348 lives. A failure in the autopilot system forced the planes down.

In risk governance and disaster management, programmes aiming to assist in planning, monitoring, and response are being constantly developed to handle information but also to identify and prioritize action points. A *digital divide*, between actors who have access to advanced digital tools and those who have not, could create unforeseen challenges in the cooperation between different actors. When digital tools and AI are introduced, working and communications routines tend to change. In situations following natural disasters or in conflict zones, digitalization has created barriers between international relief organizations and national authorities. Almost classic examples are how national authorities are excluded from information and organizational cooperation with international relief organizations because they have limited access to advanced digital tools. Sustainable risk governance 'is an important instrument to assign the adequate trade-offs between efficiency, effectiveness, resilience, and fairness of decisions' (Kelnberger, 2018, p. 235). But will extended use of digital solutions and Big Data reduce the importance of such trade-offs in risk governance?

How the invisible standardization of risk governance through digitalization and AI will impact on risk governance in the future is difficult to estimate. The development is still in its early stages.

The risk of standardization

We can turn over the coin labelled 'standardization of risk' and look for the 'risk of standardization'. Although the standardizing of risk assessments and risk management may create more efficient risk governance, the process of standardization could appear to be a risk in itself. The risk of standardization refers to the probability that deliberately installed measures to counter risks may produce not only intended desirable consequences but also unintended and undesirable consequences. The different contributions in this book show that standardization of risk may create new risks, new dilemmas, and paradoxes.

Standards appears in different shapes and often in disguise. Standards define our lives and routines and contribute to the development of a common 'language' for production, consumption, and communication. But standards could also shrink the space for alternative perspectives and solutions. In risk governance, characterized by ambiguity and uncertainty, means of standardization could therefore present new risks. Failure to manage risk causes accidents and disasters, which have hallmarks that make them great media events. Disasters carry some dramatic objective features; they may have some symbolic aspects, calling for leadership and fortitude, and they carry aspects that could trigger political change (Boin, Stern, and Sundelius, 2016). Few things may develop to become more politicized than the management of risks, disasters, accidents, and even incidents, if it is revealed that responsible leaders failed in judging and managing the risks. Consequently, leaders will immediately be exposed if a serious incident occurs. Success or failure to handle unknown as well as known risks may thus determine the professional future of political leaders and top managers in organizations. Implicit and explicit standards may develop as sources of failure. Elegant and comprehensive contingency plans, which seemingly cover all alternatives and standards for an appropriate understanding of risks and responses, could seduce operating responders to be more occupied by following the plan than adapting to what happens on the ground. Furthermore, this can give rise to the paradox of effective coordination. When the initial structuring of information, command flows, and communication in a crisis is perceived as successful, the emerging coordination structure achieves legitimacy. 'This, in turn, firmly establishes the initial structuring. In no time, there is only one way to manage' (ibid., p. 73).

Applying acknowledged standards may function as a good excuse if something goes wrong but not if they have misled responsible actors to apply wrong strategies and prioritize inappropriate measures. In Chapter 16, by Olsen, unintended consequences of standardization in risk governance are discussed in more detail.

The structure of the book

The book is organized into four Parts, reflecting the main themes discussed. The two chapters in Part I 'Introduction' set the scene of the book. In Chapter 1, the background for the anthology is presented and the problems for discussion

introduced. Digitalization as a driving force in the standardization of risk governance is afforded special attention, due to its relevance to many of the issues discussed in the other chapters. Chapter 2 explores the core concepts around which the discussions of the following chapters pivot: standardization and risk.

In Part II, 'Standardization of risk in business activity', standardization management is discussed in Chapters 3–7. Standards could be useful tools to establish a common language between risk experts, risk managers, and governments. And they could prepare the ground for accepted and agreed procedures and measures in a complex and uncertain world. Attempts to standardize risk management appear at all institutional levels, in different sectors, and for different purposes. The chapters in Part II reflect these diversities. The establishment of standards in the EU has become a necessity to ensure the EU member states adhere to the same legal frameworks. Morsut (Chapter 3) discusses efforts to standardize risk and disaster risk management within the European Union Civil Protection Mechanism. Tehler *et al*. (Chapter 4) discuss whether an increased level of standardization leads to more effective risk and disaster management, where different actors need to cooperate. Johnsson (Chapter 5) discusses how removing explosive remnants from military activities involves different risks that are currently managed in isolation and by different stakeholders. The analysis shows that a high degree of standardization takes place at the expense of comparability with other societal risks. Bengtsson (Chapter 6) explores the tensions between different ways of approaching risk in infectious disease control. This chapter contrasts the pre-emptive governance model of infectious disease control with a pilot project at the European Centre for Disease Prevention and Control (ECDC), trying to rank health risks according to actual likelihood and vulnerabilities incurred. Høyland (Chapter 7) explores whether increased standardization reduces flexibility and thereby may increase risks in surgical operations.

In Part III, 'Impact of standardization processes', standardization processes appear in different ways and have different outcomes. Virta (Chapter 8) discusses pre-crime as a special frame and approach of contemporary criminal justice systems. This chapter deals with the relationship between standardization of security, pre-crime, and decision-making. In Chapter 9, Jore discusses the consequences of standardizing the management of a dynamic, strategic risk, such as the risk of terrorism in light of the security risk analysis standards published by the Norwegian authorities. Skotnes (Chapter 10) highlights how sense-making and translation processes could impact the use of standards, as well as the role these processes can play in the standardization of cybersecurity for critical infrastructures. Jørgensen and Lindøe (Chapter 11) explore why and how the risk matrix has become a widespread and appealing tool for risk assessment and risk communication in different contexts. Patterns of use affect the relationship between project management and risk management and may trigger tensions when narrowly scoped projects meet cautious risk management.

In Part IV, 'Standardization of risk in business activity', Thompson (Chapter 12) examines several features of the financial system that involve issues of standardization, with a special focus of standardization in the context of algorithmic

trading. Higham (Chapter 13) takes a critical look at risk logics in the United Nations Guiding Principles on Business and Human Rights. He discusses how two totally different risk logics (economic and human rights risks) are hard to manage in the same system. In Chapter 14, Lindøe and Baram explore how and why standards play an important role within safety regulation and enterprises risk management (ERM) and how, using standards, conflicting interests and dilemmas may arise. Engen (Chapter 15) discusses how national and international industrial capital interests challenge national requirements of risk regulations and how the development and maintenance of national standards intends to develop and maintain Norwegian industry's competitiveness, nationally and internationally.

Finally, in Chapter 16, by Olsen, general findings are summarized, by exploring pros and cons. In addition, some dilemmas emerging when using standards in risk governance are highlighted.

This contribution is a first step towards increased interest in opportunities and threats arising from the standardization of risk governance. As demonstrated in the different chapters, standardization is taking place in almost all aspects of risk governance. This is a development that probably will accelerate, not least because of the ongoing digitalization in risk governance and society as a whole. An interesting field for future research will therefore be a more thorough investigation into the driving forces and impact of the digitalization of risk governance and emergency management.

Notes

1 See https://sra.org/sites/default/files/pdf/SRA%20Glossary%20-%20FINAL.pdf.
2 The International Organization for Standardization (ISO) defines a standard as a document established by consensus and approved by a recognized body for common and repeated use.
3 See https://ieeetv.ieee.org/mobile/video/26-years-of-risk-management-standardisation-kevin-knight-closing-ceremony-sections-congress-2017
4 IRGC is both the International Risk Governance Center and the International Risk Governance Council. Since 2016, the IRGC has consisted of two distinct and independent entities that collaborate and support each other: The International Risk Governance Center (IRGC@EPFL) is a transdisciplinary centre at the Ecole polytechnique fédérale de Lausanne. The International Risk Governance Council Foundation, established in 2003 at the initiative of the Swiss government, the IRGC Foundation is based at EPFL in Lausanne, Switzerland, with network partners in Europe, the US and Asia. The IRGC Framework of 2005 provides guidance for early identification and handling of risks, involving multiple stakeholders. It recommends an inclusive approach to frame, assess, evaluate, manage, and communicate important risk issues, often marked by complexity, uncertainty, and ambiguity. An updated version can be found at https://infoscience.epfl.ch/record/233739?ln=en
5 See www.compact.nl/en/articles/digitalization.

References

Aven, T. and Renn, O. (2010). *Risk management and governance: Concepts, guidelines and applications*. Vol. 16. Heidelberg: Springer Science & Business Media.

Beck, U. (1992). *Risk society: Towards a new modernity*. London: Sage.

Boin, A., Stern, E., and Sundelius, B. (2016). *The politics of crisis management: Public leadership under pressure*. Cambridge: Cambridge University Press.

Brunsson, N. and Jacobsson, B. (2000). *A world of standards*. Oxford: Oxford University Press.

Busch, L. (2011). *Standards: Recipes for reality*. Cambridge, MA: MIT Press.

Büthe, T. and Mattli, W. (2011). *The new global rulers: The privatization of regulation in the world economy*. Princeton, NJ: Princeton University Press.

Cassano-Piche, A. L., Vicente, K. J., and Jamieson, G. A. (2009). A test of Rasmussen's risk management framework in the food safety domain: BSE in the UK. *Theoretical Issues in Ergonomics Science*, 10(4), pp. 283–304.

Cohn, J. V., Schatz, S., Freeman, H., and Combs, D. J. Y. (2016). *Modelling sociocultural influences on decision making: Understanding conflict, enabling stability*. Boca Raton, FL: CRC Press.

Dekker, S. W. A. (2014). The bureaucratization of safety. *Safety Science*, 70, pp. 348–357.

Dickson, E., Baker, J. L., Hoornweg, D., and Tiwari, A. (2012). *Urban risk assessments: An approach for understanding disaster and climate risk in cities*. Washington, DC: The World Bank.

Florin, M.-V. and Bürkler, M. T. (2017). *Introduction to the IRGC Risk Governance Framework*. Lausanne: International Risk Governance Center.

Haack, P., Schoeneborn, D., and Wickert, C. (2012). Talking the talk, moral entrapment, creeping commitment? Exploring narrative dynamics in corporate responsibility standardization. *Organization Studies*, 33(5–6), pp. 815–845.

Kelnberger, M. (2018). The smart city concept: A review concerning sustainable risk management. In P. A. Wilderer, O. Renn, M. Grambow, M. Molls, and K. Mainzer (eds), *Sustainable risk management*. Cham: Springer International Publishing, pp. 235–249.

Klinke, A. and Renn, O. (2012). Adaptive and integrative governance on risk and uncertainty. *Journal of Risk Research*, 15(3), pp. 273–292.

Krasmann, S. (2018). The secret of algorithms: On transparency, truth and power. Paper presented at the International Workshop on Data, Security and Values at the Peace Research Institute, Oslo (PRIO), 10–11 December 2018.

Lypton, D. (2013). *Risk.* 2nd edn. London: Routledge.

OECD (2003). *Emerging risks in the 21st century: An agenda for action*. Paris: Organisation for Economic Co-operation and Development.

OECD (2011). *OECD reviews of risk management policies–future global shocks: Improving risk governance*. Paris: Organisation for Economic Co-operation and Development.

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science*, 27(2–3), pp. 183–213.

Renn, O. (2014). Emerging risks: Methodology, classification and policy implications. *Journal of Risk Analysis and Crisis Response*, 4(3), pp. 114–132.

Sandholtz, K. W. (2012). Making standards stick: A theory of coupled vs. decoupled compliance. *Organization Studies*, 33(5–6), pp. 655–679.

Slager, R., Gond, J-P., and Moon, J. (2012). Standardization as institutional work: The regulatory power of a responsible investment standard. *Organization Studies*, 33(5–6), pp. 763–790.

Timmermans, S. and Epstein, S. (2010). A world of standards but not a standard world: Toward a sociology of standards and standardization. *Annual Review of Sociology*, 36, pp. 69–89.

Turkle, S. (2011). *Life on the screen*. New York: Simon & Schuster.

UNISDR (United Nations International Strategy for Disaster Reduction) (2004). *Living with risk: A global review of disaster reduction initiatives*. Vol. 1. Geneva: United Nations Publications.

UNISDR (United Nations International Strategy for Disaster Reduction) (2005). *Hyogo Framework for Action, 2005–2015: Building the resilience of nations and communities to disasters*. Extract from the final report of the World Conference on Disaster Reduction (A/CONF. 206/6). Vol. 380. Geneva: The United Nations International Strategy for Disaster Reduction.

UNISDR (United Nations International Strategy for Disaster Reduction) (2015). *Sendai Framework for Disaster Risk Reduction, 2015–2030*. Geneva: United Nations.

2 Standardization of risk versus the risk of standardization

A conceptual analysis

Kirsten Juhl

Introduction

Neither risk analysis, as the basis for risk management strategies, nor standardizations are performed purely as theoretical exercises predominantly of interest to a narrow circle of specialists. Rather, the results of such exercises have a very wide variety of stakeholders and end users. From a societal safety perspective, the primary stakeholder is *society as such*, which – among other things – is constituted by its members. These are predominantly ordinary – not specialized – language users. As Max Boholm *et al*. point out, specialist definitions that are too narrowly technical and stray too far from everyday use of the same terms are open to misunderstanding and miscommunication and may produce obfuscation rather than clarification (Boholm, Möller, and Hansson, 2016, pp. 320–321). Furthermore, specialized definitions may have ramifications for the distribution of power in society, in that they may (intentionally or unintentionally) benefit certain stakeholders at the expense of others. Hence, a pertinent *a priori* question for any risk analyst or standardizer, as well as for examiners of risk analyses and standards, ought to be: In whose interest is the risk analysis, respectively standardization, carried out? Who is it supposed to serve, and who does it actually serve? What also needs to be kept in mind right from the start of any risk analysis or standardization exercise is whether attempts to resolve one problem might create other and maybe more difficult issues, which subsequently must be resolved.

The term ‘standardization of risk’ is not only a contradiction in terms but, in a strictly literal sense, meaningless. Neither standardization nor risk are autonomous concepts. Both require human subjects to define their content. Neither can be understood except in relation to something else, and the ‘something else’ of standardization cannot be risk with a zero article, i.e. *risk as such*. There is no end to what someone somewhere may consider to be a risk to someone or something, be it distinct individuals, specific groups in society, or society as a whole. There is no such thing as *a standard risk*, against which all imaginable risks can be measured. In addition, there is an abundance of specialized risk conceptualizations that are not mutually compatible, either because they originate from diametrically opposed epistemological positions or because they – though

belonging within the same epistemological paradigm – emphasize different aspects of the concept at the expense of others.

Standards and standardizations of all sorts – formal or informal, technical or social, processual or procedural, etc. – are likewise abundant (Brunsson *et al.,* 2000; Busch, 2011). Even when limiting the term 'standards' to the products of standards organizations, the forest of formal standards seems to expand unbridled on a daily basis. As of December 2016, the European Committee for Standardization (CEN) had already published 14,739 European Standards, including 1,135 new ones issued in 2016 alone. A search for the word 'risk' in these standards produced 519 results, 'safety', 2015 results and 'security', 151 results.[1] By October 2017, the International Organization for Standardization (ISO) had published 21,840 International Standards, 4,439 pertaining to risk in various constellations.[2] An internet search for the word 'risk' produced 39,600 results, 'safety', 126,000 results and 'security', 52,800 results.[3] Standardization certainly seems to be the order of the day.

There are very many players on the field, in terms of both producing standards and defining what constitutes the essence of risk and what counts as risks in practice. Each has their own pragmatics of what these terms mean, pragmatics they may like to make applicable to all other actors and to fields other than their own. These pragmatics may very well be perfectly suitable for their purpose within the context in which they were developed and yet not be adequately transferable to other contexts. However, as said above, not to recognize that one's specialized definitions revolve around meanings in terms of pragmatics hampers communication and understanding, both within and across disciplines and in society at large. More than 20 years ago, Stan Kaplan formulated the problem this way: 'Theorem 1: 50% of the problems in the world results from people using the same words with different meanings. Theorem 2: the other 50% comes from people using different words with the same meaning' (1997, p. 408).

Modern societies define as risks many issues that are similar or comparable across societies or transgress national borders. They may therefore benefit from one another's experiences with these issues or from coordinating their management practices. Even though many such international risks may still potentially be manageable at a national level or through limited cross-border cooperation, many are increasingly global in character, caused, for instance, by climate change, multi-resistant bacteria, epidemic or pandemic viruses, reduced biodiversity, intricate digital interdependencies, international terrorism, and cybercrime – to name just a few. These issues cannot be resolved on a national basis or through limited international cooperation. Nor can they be resolved through simple precautions or scientific means alone. As in many other fields of societal concern, issues that are commonly considered risks in more than one society are becoming increasingly internationalized or globalized. This automatically directs the attention and emphasis more towards similarities than dissimilarities or differences in local conditions. Thus, by their own impetus, approaches to such risks will become increasingly standardized, even if no standards are deliberately formulated and even if there may be reason to safeguard local practices.

Without having yet defined the concept of risk, there are undoubtedly issues which some societies, due to national specifics, consider societal risks and which other societies do not (or need not) have the slightest concerns about. What might result from mudslides, rockslides, and huge mountain chunks that come loose is, for instance, a concern in Norway but, for good reason, not in Denmark.[4] Furthermore, different societies also have different cultural attitudes towards the same sort of risks and may rank them differently in terms of how important they are. Such attitudes are not fixed but have changed over time and will continue to change, both within societies and between societies, due to contact, cooperation, and what Timur Kuran and Cass R. Sunstein have termed *availability cascades*: 'a self-reinforcing process of collective belief formation by which an expressed perception triggers a chain reaction that gives the perception increasing plausibility through its rising availability in public discourse' (1999, p. 683). 'Such cascades may develop into international availability cascades and create an equalization of attitudes and policies towards risks' (cf.ibid., p. 745, note 215) – that is, cause a standardization of risk perceptions and risk policies that disregards local or national contexts and circumstances.

Hence, it seems more important than ever to overcome differences in pragmatics – if not in order to reconcile them, which may not be possible – then at least in order to create a certain mutual respect and understanding that pragmatics different from one's own may have something valuable to offer to the resolution of what we may consider common societal risk. Rather than adopting a specific pragmatic meaning of the core concepts of this volume, the present chapter discusses these concepts based on their lexical (semantic) meanings, in order to see how far this might take us to towards such an aim. After all, the semantic meaning of the words we use is the starting point of all pragmatic meanings. Taking ordinary word meanings into account will also greatly improve the ability to communicate with, and take seriously, the risk concerns of non-specialists, which in turn may exempt us from the allegedly widening gap between so-called experts and lay persons. In this context it is also fair to remember that we are all mostly non-specialists; even specialists are non-specialists in every other field than their own.

Whose semantics?

To communicate in a satisfactory manner across native language barriers about issues of common interest or global character, we need a lingua franca. For historical, geo-political (and maybe linguistic?) reasons, English has become today's most widespread lingua franca, completely dominating international relations, business, the sciences, and the internet. As of 2012, there were thus four times as many non-native English speakers (about 1,500 million) as native English speakers (about 375 million).[5] This figure can be expected to steadily increase.

Non-native English speakers using English as a lingua franca have recently been termed ELF speakers to indicate that ELF is a vehicular language in its own right, not to be judged primarily in terms of Standard English. There are

several formally recognized and standardized 'Englishes' besides British English and American English. In contrast to many a native speaker of 'Englishes', ELF speakers are always at the very least bilingual and sometimes also plurilingual. Research based on two huge corpora linguistics[6] on spoken ELF shows that ELF speakers, in their attempts to communicate with other ELF speakers, draw as much on their respective lingua-cultural backgrounds as on their knowledge of the English language, and that in order to safeguard the communication in question, they make an effort to grasp the intended meaning of the other's language use (Siedlhofer, 2011; Mauranen, 2012).

The present volume originated in a Nordic research project between six research institutions in the four Nordic countries, Denmark, Finland, Norway, and Sweden. Hence, in order to make a valid conceptualization using semantics as a starting point, it seems relevant to consider not only the semantics – that is, the literal (denotations) and associated meanings (connotations) – of the Standard English terms used but also of the equivalent terms in the Nordic languages. This also applies when these terms can be directly translated into Standard English, as is the case with 'standardization', 'standard', 'risk',[7] and many other terms we use, but which is not the case concerning other terms, such as 'safety' and 'security',[8] commonly considered the antonyms of 'risk'. It is not inconceivable that the societal conceptualization of these latter terms in the respective Nordic countries may also influence the understanding of the former terms and maybe change their connotations in ways that pull them in slightly different directions from how identical terms are conceptualized in other native languages.

The native languages of the Nordic countries comprise several Norse or North Germanic languages, the closely related Scandinavian languages, Danish, Norwegian, and Swedish, as well as Icelandic and Faroese. Together they constitute a sub-family of Indo-European languages. The native Nordic languages do, however, also include Finnish and Sami, which both belong to the altogether different Uralic language family. In Norway, the official languages are two different forms of Norwegian, as well as Sami, which is spoken across the Northern hemisphere by people in Norway, Sweden, and Finland. Finland likewise has two official languages, Finnish and Swedish. The de facto, but not formally, official language in Sweden is Swedish, but the country also has a large minority, whose native language is Finnish. Danish is the official language of Denmark and the Faroe Islands, and Icelandic is the official language of Iceland, where, however, Danish is still a mandatory foreign language at school. At least Danes, Norwegians, and Swedes are able to communicate with each other in their respective languages without using a lingua franca. In addition, the historical and cultural ties between the Nordic countries go far back in time and have been shaped through varying periods of friendship and enmity, and, up until recently, people speaking different varieties of these official languages constituted the largest groups of immigrants into one another's countries.

However, the terms 'standardization', 'standard', and 'risk' do not originate in any of the native languages of the Nordic countries but are loanwords from

different Indo-European language sub-families and adopted into virtually all European languages. Using semantics as a starting point for conceptualizing these terms in relation to one another thus makes sense. Since, unfortunately, I am not personally familiar with either Finnish or Sami, my exploration will be restricted to the Scandinavian languages, in combination with English and German, which are both West Germanic languages.[9]

Standardization

'Standardization' is a verbal noun with three semantic meanings:

1 Setting a standard for something.
2 Evaluating something by comparing it to a set standard.
3 Making something comply with an already set standard.

In all meanings, standardization is always performed by a human actor (person or persons) – even when the 'set standard' in the second and third meanings of standardization has become so well established that its origins are lost in history and it, hence, appears to have emerged by itself or always to have existed.

In modern language, the noun 'standard' means a guideline, a rule, a set of rules, or a norm – from Latin *norma*: literally the name of a tool for measuring angles, figuratively used to denote a guideline, rule, or regulation.[10] *Setting a standard* is thus exactly the same as *establishing a norm*. Standards are prescriptions of what is the better, if not the best, way to relate to something of concern – which is likewise a matter of normativity. Ideally, standardization in the first meaning of the term would aim at establishing the best possible standard for whatever is at stake. However, both intentionally produced standards and 'best practices' (recommended standards) are adopted schemes that can be low as well as high and which, in order to come into existence, need not be very good or even very useful. 'Best practices' are not best in any absolute sense of the word but only relative to which other practices, if any, exist at the point in time when the 'best practice' in question is established.

Used adjectively, 'standard' means what is normal or usual. In colloquial speech, the word is commonly used to refer to something that is mediocre, or something which most people possess, and which is neither very good nor very bad – that is, synonymous with 'average'. It is, for instance, 'all right' to own a 'standard' car, but most people are not particularly proud of it – after all, their neighbour also owns a 'standard' car. Likewise, most people do not deeply admire people living 'standard' lives, since they do so themselves; they admire people who live extraordinary lives – different or *deviating* in an attractive way from so-called ordinary lives.

The noun 'standard' is derived from the old French *estandart*, the *standart* or *standard*, that is, the spear banner that originally the Knights Templar, in mediaeval times, and later other mounted troops used to communicate in battle, in order to direct troops in the din of the battlefield, where other means of communication

would not work.[11] As the banner of each fighting unit had its own unique heraldry, the imperative, 'follow the standard', designed to keep one's troops together and prevent them from getting dispersed in all directions, was a standing order fairly easy to understand. The second etymological origin of the 'standard' is the old Frankish *standhard*, 'do not yield', again an order fairly easy to understand. These oversimplified orders were in force until collective retreat under the standard was signalled by the standard-bearer. The aim was to direct and stay in control of troop movements and thus increase the chance of victory by maintaining strict discipline. Troops were not to come up with their own strategies for how to better conduct the battle, and they were definitely not supposed to flee the banner,[12] even if the fortunes of war turned. Desertion has always been considered a serious offence, justifying a severe penalty. It is, however, important to remember that 'following the standard' in war was never in itself a guarantee of victory. The Saracens did not direct their troops by means of standards and did not fight in strict military formations like the Knights Templar and yet they overwhelmingly defeated the Knights at the conquest of Jerusalem in 1187. In later wars involving the use of 'standards', troops of all sides used standards. The 'standard' that won was the one that was able to communicate not only preconceived strategies and tactics but also instantaneous adjustments to these, necessitated by the kind of unforeseen situations that are bound to occur in any battle.

The meaning and logic behind the modern use of the term 'standard' have not changed much from its origins. The aim is still to achieve control of something – the 'battle', so to speak – by ensuring through simplified means of communication that everyone follows the command, with no one deviating from it. Some questions to ask when evaluating modern standards are thus: In whose service is the 'standard bearer'?, whose 'battle' is fought?, and is it worth fighting for? – in short, *cui bono*? And conversely, who stands to lose by the standard? Is the cause just or unjust? Is the standard based on a reasonable judgement of the situation? If so, are the implicated strategies and tactics sensible in comparison? Is the standard likely to bring 'victory'? What if the standard is considered likely to bring 'victory' and deemed to have a just cause but, at the same time, deemed ethically unacceptable, that is, the means are considered unjust? What unarticulated other standards might be layered within a given standard, might they not be double standards? Finally, how specific or general, rigid or flexible can a standard be? Can a standard allow for certain deviations, in order to meet unforeseen situations, without sacrificing its purpose and still warrant the term 'standard'? Is it at all possible to build dynamics into standards, or is that an antithetical proposition?

For the second and third meanings of standardization to make sense, a standard and the 'something' that is to be evaluated against the standard or brought into compliance with it must be quantitatively or qualitatively measurable by one and the same metric. Although it is possible to compare something to a standard, in terms of how similar or dissimilar it is, standardization and comparison are not synonyms. For standardization, commensurability, not just

comparability, is required. Standardization in these meanings of the term aims at conformity or uniformity with the set standard – regardless of how good or bad this might be. What is dissimilar from the set standard is considered not just difference but *deviation*, which it is the logic of standardization to eliminate or at least reduce as far as feasible. This logic of doing away with diversity and variability applies both when the potential deviations are 'below standard' and when they are 'above standard' – or the point of establishing the standard in the first place will be gone. Inherently, standards thus remove the incentives to do things differently, even if better, and it is hence by no means self-evident that a standard will change, even in light of the existence of 'above standard' deviations.

Standards, standardization, standardizers, and followers of standards

The pragmatics of the meaning of standards and standardization that immediately springs to mind in a risk governance context is the kind of standards that codify rules in written documents as a means of regularizing certain matters across various autonomous, but nonetheless interdependent, actors, without having the authority (or alternatively the desire to exercise the authority they have) to enforce these rules and/or sanction violations of them. This kind of standards results from a deliberately undertaken standardization of the matter in question (sense 1 above). Many of the chapters in the present volume examine precisely this kind of formal standards – usually referred to as *de jure* standards, even if they are not strictly 'by law'. Others take a broader perspective and examine more informal standards – for example, de facto standards, standards that have grown out of custom, convention, or general consent.

Brunsson and Jacobsson (2000a) restrict the term 'standardizers' to people or bodies who undertake deliberate standardization endeavours but have no formal authority to impose other kinds of rules, such as laws, regulations, or directives – despite admitting to the fact that public authorities also use standards as one of their instruments of governance. Among those who are included in their definition are thus supranational bodies, such as the United Nations (UN) or the Organisation for Economic Co-operation and Development (OECD). However, the kind of standards, with which Brunsson and Jacobsson (2000b) are mainly preoccupied, is the kind issued by national and international standards organizations: commercial actors operating in a market, whose sole occupation is to make standards. They are the ones referred to as standardizers, and those who follow their standards are called 'adopters'.

Although Brunsson and Jacobsson do discuss why 'adopters' adopt standards, the primary focus of the volume is, however, standardizers' production of standards and the generic properties of these standards. They distinguish between three types of standards: (1) standards for use of nomenclature, terminology and classification; (2) standards for how to act (e.g. procedures, routines, processes, etc.); and (3) standards for what one ought to possess (e.g. strategy

plans, preparedness plans, formal qualifications, skills, etc.). Busch, on the other hand, suggests a different typology of standards, consisting of four types, which pertain to things and humans alike: (1) *Olympic standards*, that is, standards that define a winner or a small group of winners; (2) *filters*, standards that identify criteria for passing requirements; (3) *ranks*, standards that define a hierarchical order; and (4) *divisions*, standards that classify things and humans (2011, pp. 42–52).

Although these typologies make various standards appear to be of different types, they are in essence all behavioural standards, laying down codes of conduct in given situations based on a specific mindset. Like other kinds of rule setting, standards are always normative, even when presented as being 'technical'. This pertains also to Brunsson and Jacobsson's type (1) and Busch's type (4).

Classification is akin to, but not synonymous with, standardization. As Geoffrey C. Bowker and Susan Leigh Star (1999) so pointedly demonstrate, how we classify both things and living beings, including humans, makes a difference and has consequences. To understand how such consequences can ultimately be very nasty, one need only think of the 1994 Rwanda genocide, which was in part made possible by the formal classification and mandated registration of the population into Hutu, Tutsi, and Twa and the way Belgian colonial politics built on this classification.

Brunsson and Jacobsson (2000b) and Busch (2011, pp. 23–27) attempt to establish a conceptual distinction between 'standards' and 'norms' that does not match the meaning of these terms in everyday language use. This may be due to their primary focus being on deliberately created standards, restricting the term 'norm' to each of their own narrow definitions of the kind of standards that are usually called 'social norms'. At the same time, they do point to the 'invisibility' and 'taken-for-grantedness' of many a *de jure* standard that has been around for a while and show the power they have to shape social life, how they may become institutionalized and internalized precisely as social norms, and how these phenomena in general blend into one another. Furthermore, the causality runs in both directions. Being normative as such, standards, to a very large extent, also build on existing social norms – or they would not stand a chance of being 'sold'.

Attaching the term 'adopter' to those who become followers of standards reflects a property claimed to characterize the standards that standardizers produce: they present their standards as an offer, a voluntary option that 'adopters' can choose to follow or ignore. This is a dubious claim. Standardizers may well be termed 'availability entrepreneurs', as Kuran and Sunstein coined the term (1999, p. 687). For standards to be options that one can choose between presupposes that alternatives exist, that is, no unified norm has yet been established. Possible standards are still 'in battle', competing to become *the* winning standard. If only one standard is on offer, the only alternative is to deviate, and that requires courage that few people or organizations have. We tend to take what is made available to us; we often do not have enough knowledge to challenge the wisdom of it, and we are concerned about our reputations; we look

over the hedge to our neighbours and we do what our neighbours do. We are fundamentally flock animals, no matter how little we like to admit it. Paradoxically, while modernity has managed to ideationally make standardization considered a great asset, it has also managed to ideationally do the same for individualism.

Martha Lampland and Susan Leigh Star (2009), as well as Busch (2011), demonstrate the very many ways in which the voluntariness of standards may indeed be rather involuntary. There are many mechanisms available for coercion and sanction, apart from legal ones, which can be used to ensure compliance with a given standard, for example, demands and reputational pressures, boycotts and various kinds of ostracism imposed by third parties. The very same mechanisms that work to ensure compliance with social norms also work with standards as soon as they have become sufficiently widespread. Brunsson furthermore demonstrates how the presumed voluntariness of standards serves as a way of evading responsibility on the part of the 'standardizer' and shifts the blame to the 'adopter' when things go wrong, and how this mechanism is further exacerbated by the lack of appeal and review bodies to whom one can address complaints (2000, pp. 24–26).

Of the books on standards and standardization referenced above, however, only Busch directly addresses 'standardizations of risk', when examining the two standard expert responses to risk: cost-benefit analysis (CBA) and risk analysis (Busch, 2011, pp. 278–286). CBA is based on the following set of assumptions: (1) only certain things count as costs and benefits; (2) these can be quantified; (3) the best way of quantifying them is through *economic* calculation; and (4) the best solution is the one implicating the greatest benefit for the lowest cost. CBA is thus strictly utilitarian. Risk analysis, on the other hand, is based on the assumptions that: (1) risks are identifiable; (2) they ought to be avoided; and (3) identified risks are manageable and in principle avoidable. When CBA and risk analysis are combined, one gets risk-cost-benefit analysis (RCBA), which 'is widely used and consists simply of converting the risks, cost, and benefit associated with a particular project to monetary terms and then aggregating each of them in order to determine whether the risks and costs outweigh the benefits' (Shrader-Frechette, 1991, p. 61). These standard responses are thus based on normative judgements that are not only oversimplified but also implicitly posited as being universal and therefore unproblematic. However, choosing money as *the* unit of measurement for standardizations, especially in the third sense of the term, is in fact normatively highly contested among non-specialists. When adopting RCBA as the standard method for risk analysis and management, one clearly runs the risk of underestimating risks that are not easily quantifiable in monetary terms, such as: risk of political collapse, risk of human rights violation, risk of loss of biodiversity, etc.

Risk: normativity and uncertainty

Authoritative Scandinavian dictionaries state the semantic meaning of 'risk' to be:

1 *Risk* is the possibility of *undesirable, adverse* outcome(s) of something happening.

The connotations of the term 'risk' being associated with negative outcomes seem to be the same in Standard English as in the Scandinavian languages and thus should present no problems. This association is, however, challenged by some specialist definitions that associate risk with both good and bad outcomes.

In order to clarify how this confusion may have arisen and to fully appreciate the meaning of the term 'risk', one might look at the term 'chance'.[13] The semantic meaning of 'chance' is either:

2a *Chance* is the possibility of *desirable, beneficial* outcome(s) of something happening.
2b *Chance* is *opportunity*.
2c *Chance* is the probability of a specified outcome (good or bad) of something happening.

The semantics of 'chance' in an exemplary way illustrate the difficulties involved in ELF communication. Since the connotations of the word 'opportunity' are decidedly positive – from Latin: *opportunitas*, a favourable condition or being of beneficial nature – 2a and 2b virtually mean the same thing. In meaning 2c, however, 'chance' is simply synonymous with 'probability'. The meaning dominating the use of the term in ordinary Scandinavian language use seems to differ somewhat between the Scandinavian countries, as well as in respect to Standard English-speaking countries.

For the sake of maintaining the clarity of the semantic meaning of the term 'risk', when 'chance' refers to the phenomenon of probability, I henceforth use the word 'probability', and when 'chance' refers to meanings 2a and 2b, I will use the word 'chance' as meaning 'opportunity'. We then get the following dichotomy:

1 *Risk* is the possibility of *undesirable, adverse* outcome(s) of something happening.
2 *Chance* (*opportunity*) is the possibility of *desirable, beneficial* outcome(s) of something happening.

The difference between the two thus lies exclusively in the *normative judgement* of the possible outcomes, which is the one major characteristic of both risk and opportunity. The other major characteristic is *uncertainty*, which is revealed by virtue of the word 'possibility'. Both terms concern the uncertainty of what might happen in the future (the 'something happening') and of what it might entail (the 'outcomes'), which – unless one holds a deterministic worldview – by definition is unpredictable.

In continuation of the above, there are two other possible 'outcomes of something happening' to consider:

3 The possibility of *indifferent* outcome(s) of something happening.
4 The possibility of *immaterial* outcome(s) of something happening.

To my knowledge, none of these possibilities has a specific term attached to it, maybe because usually we are not overly concerned with outcomes that we do not consider of good, bad, or significant magnitude. All the same, both these ways of viewing possible outcomes exist and consist of normative judgements, just as much as *undesirability* (risk) and *desirability* (chance/opportunity) do.

The normativity of risk

In his book, *Misconceptions of Risk*, Terje Aven states: 'Restricting the concept of risk to negative outcomes only is problematic as it is often difficult to determine what is a negative outcome and what is a positive outcome' (2010, p. 95). He is of course right that (short-term) undesirable consequences may have derivative (long-term) consequences that may be judged desirable and vice versa. This is not resolved, however, by conflating desirability and undesirability, by subsuming these normative judgements as equal components of risk. Rather, it calls for more careful considerations of possible future consequences of whatever event is under consideration, before assigning it the normative judgement of being bad (pertaining to risk) or good (pertaining to opportunity).

This claim of the risk concept, allowing for both favourable and unfavourable outcomes, is repeated in two later articles analysing the conceptual compatibility of a wide variety of specialist definitions of risk. In an article co-authored with Ortwin Renn and Eugene A. Rosa, 11 different stipulative definitions of risk by risk analysis researchers are examined (Aven, Renn, and Rosa, 2011). Another article examines 9 overall categories of specialist definitions, exemplifying these with a total of 27 differently formulated definitions (Aven, 2012, p. 37). The 2011 article claims that, except for two of them, the quoted definitions make for such an allowance and it notes that this kind of risk is 'often referred to as speculative risk in contrast to pure risk where the outcomes are purely unfavourable' (Aven, Renn, and Rosa, 2011, p. 1075). However, in standard language use − British English as well as American English − words such as 'loss', 'disutility', 'severity', 'adverse', and 'values at stake', either unambiguously or predominantly, have negative connotations.[14] This applies to five of the definitions given in the 2011 article, whereas the rest altogether disregard the issue. The same observations can be made for the various definitions presented in the 2012 article: two-thirds of the definitions refer to negative events or outcomes as part of the definition, the other nine disregard the normative component of risk in the very definition. That is not to say that there is no such judgement made – it may be tacitly implied, that is, taken for granted, as in the case of the definition ascribed to John Adams.[15]

Most of the 'non-normative' definitions appear more like *operationalizations* of the risk concept – recipes for *approaching* the issue of how to assess concrete risks, that is, efforts to standardize the risk approach – than conceptions of risk as such. They do not seem to meet Aven's first premise that risk definitions should distinguish between risk as such and how risk is managed (Aven, 2012, p. 33). They are, furthermore, more or less competing *risk approach standards*, emphasizing different aspects of risk as the most important. What is judged to be

important is – at least partly – normative and can been seen as resulting from different perceptions of reality. Hence, it is not obvious how the various definitions meet Aven's second premise, that risk definitions should distinguish between risk as such and how risk is perceived (ibid., p. 34).

It may be that many scientists rather want to shun normative issues, considering them to be 'not their table' but something that should be left to 'decision-makers' to determine. Indeed, in regard to questions of what is good or bad, professional risk analysts – researchers and practitioners alike – obviously are no more experts than non-specialists. However, without making normative pre-judgements, we are left without a clue as to which kind of events and consequences it is at all relevant to consider the possibility and uncertainty of, in the first place. Nor do any of the 'non-normative' definitions in and of themselves provide good guidance as to how to compare and rank risks as a basis for risk management priorities, whether at an organizational or a societal level, let alone at an international or a global level. These issues remain normative questions as well, and the answers are likewise inescapably normative.

According to the authoritative dictionaries of the Scandinavian languages (see note 7), conflating risk and chance is considered incorrect and poor language use. The two terms are antonyms (and they remain antonyms, regardless of whether they are replaced with terms such as 'upside risk' and 'downside risk', as is typical in the petroleum industry). Semantically, risk is linked to potential danger, hazard, injury, harm, accident, or loss, while chance is linked to potential benefit, success, gain, achievement, or opportunity. There are good reasons to keep that distinction alive in our language use – so as not to obscure the normative foundations of defining, describing, classifying, and judging possible 'outcome(s) of something happening' and thus muddle democratic risk discourses.

It is worth remembering that, in contrast to the definitions of the meaning of 'risk' in the specialist literature, the meaning of words in everyday language is in fact the standard meaning of the concepts – developed over a very long time through the conventional use of the words by millions of people. Hence, it is worth taking note of linguistic analyses of 'risk' and related terms. Based on British English and American English corpus linguistics data, as well as dictionaries, thesauri, and other lexicological resources, the Swede Max Boholm has recently conducted several thorough lexico-syntactic analyses of the meaning of 'risk' and a vast number of related or associated concepts in actual everyday language use, in comparison with specialist definitions (Boholm, 2012, 2017; Boholm, Möller, and Hansson, 2016). He has, furthermore, looked at how risk definitions stated by 21 Swedish government agencies on their websites match how they otherwise use the word 'risk' (Boholm, 2018).

In his 2018 article, Boholm (ibid., p. 3) lists the following four meanings of risk (R), commonly found in everyday language:

R1 'The *possibility* of an unwanted event which may or may not occur' (frequent in dictionaries).
R2 'An *unwanted event* which may or may not occur.'

R3 'The *cause* of an unwanted event which may or may not occur.'
R4 'The *probability* of an unwanted event which may or may not occur.'

From Boholm's analyses, it is clear that the normative component cannot be left out of the risk concept and that this component in everyday language use does indeed pertain to negative, not positive, evaluations of future events or consequences. 'Risk', 'safety' and 'security' are polysemic words and relative rather than absolute conceptions. In everyday (American English) language, 'risk' is used both qualitatively and quantitatively, but non-quantitative, non-technical meanings dominate, and numerical expressions of risk are very unusual (Boholm, Möller, and Hansson, 2016, p. 324).

The 21 Swedish government agencies examined formulated their risk definition in 40 different ways, which Boholm classified into 14 different types (2018, pp. 6–7, Table 1). Most definitions are explicitly or implicitly expressed in quantitative terms, in line with the most common of the specialist definitions discussed above. All 14 types are externally inconsistent with everyday language use, in that none captures all four ordinary uses of 'risk' (R1–R4), although five of them capture one of the senses. Most agencies also display internal inconsistency, in that the senses of 'risk' in the surrounding text differ from the senses stipulated by the stated definitions. To avoid misunderstandings in communication, Boholm makes the following six recommendations to improve specialist definitions of risk: (1) acknowledge everyday language; (2) acknowledge the polysemy of risk; (3) consider carefully the choice of *definiendum* (what term is defined?); (4) acknowledge the reductive aspects of the definition and their consequences; (5) use the right level of precision, neither too general nor too narrow; and (6) once a term is defined, stick to it (ibid., pp. 13–14).

In documents that outline the Norwegian public policy of and approach to societal safety, risk is defined predominantly as either the function or the combination of the probability of possible undesirable events (the 'something happening') and their consequences, in terms of loss of important values.[16] Here, the normativity involved in the concept of risk is retained. However, by moving the issue of undesirability from the consequences to the 'something happening', one seems to presuppose that only undesirable events will result in undesirable consequences, ruling out the possibility that undesirable consequences may also eventuate from desirable events and vice versa. This, furthermore, obscures the fact that most events – unless they are very uncomplicated – will have more than one possible consequence and that these may very well consist in a mixture of what one considers desirable, undesirable, indifferent, or immaterial.

Both outcomes that one considers undesirable and outcomes that one considers desirable may be present in different proportions, requiring balancing one against the other. At the same time, it is also fully conceivable that dreaded consequences of an event will not be accompanied by welcome consequences and vice versa. For most people, it is, for instance, hard to envisage what could be

considered the desirable consequences – at least in a short-term perspective – of a potential nuclear war, a technological disaster, a powerful earthquake, or a major epidemic or pandemic. Yet, whereas most countries in the world consider nuclear war an acute risk because North Korea now possesses nuclear weapons, North Korea itself seems to see it as a guarantee of not being invaded by foreign powers and hence a guarantee of peace to their own country. Conversely, few people will perceive a big lottery win as a risk or would imagine that wealth in itself should have undesirable rather than desirable consequences.

The decision on what is to be regarded as undesirable in the meaning of being potentially dangerous, harmful, or considered a loss, requires a human actor – either an individual or a collective – making normative judgements, and depends on this actor's fundamental value appreciation. This will vary with which value system dominates the social and societal context to which the performing actor belongs, as well as the time and the space. It boils down to who provides the premises and who owns the power of definition in the given context. At the same time, it need not be at all obvious who that actor is, which agendas exist, or from whose point of view these agendas can be considered legitimate. Nor does the premise provider and the owner of the power of definition need to be the same.

This may best be understood by looking at the case of intentionally harmful acts, which, from the point of view of the targeted party, are definitely undesirable, but, from the point of view of the targeting party, will be desirable. Examples will be all sorts of crimes, including sabotage, cybercrime, espionage, and international terrorism, as well as violent or armed conflicts and wars. Third parties may have their own perceptions of who is right or wrong, that is, who is the targeted party and who is the targeting party – perceptions that may change over time. For example, Nelson Mandala and the ANC were considered terrorists by the apartheid regime in South Africa, whereas, in the eyes of many other national and international actors, they were freedom activists and resistance fighters. After 27 years in prison, Mandela was released in 1990, won the Nobel Peace Prize in 1993 and became president of South Africa in 1994 – but nonetheless remained on the US terrorism watch list until 2008.[17]

Nor do the parties involved necessarily have the same expectations regarding the ensuing consequences. For example, the 9/11 Al-Qaeda terrorist attack on the Twin Towers in New York did not become an eye-opener for the Western world along the lines that Bin Laden allegedly expected.[18] Instead, the Western world engaged in the 'War on Terror' in Afghanistan in 2001 and Iraq in 2003, which also did not lead to the desired outcomes.[19] Furthermore, it can be argued that it has led to a number of undesirable consequences for democratic practices in the West, such as reduced civil rights, increased surveillance, torture being in some cases seen as acceptable (e.g. Guantanamo Bay), and increased criminalization of intent (e.g. certain countering violent extremism (CVE) measures).

Even in less celebrated cases of risk management, there is always an inescapable normative element present, no matter how professionally well informed they are or how 'objectively' they are presented. This applies, for example, to

the determination of criteria for establishing acceptable risk levels or tolerance limits, even though the normative judgement in these cases concerns what is 'good enough' rather than what is 'good'. What is felt to be socially acceptable at any given point in time undoubtedly also comes into the equation. The term 'risk appetite' – referring to the total acceptable risk exposure for an entity, whether a company or a whole society – is also clearly a normative term, since it is based on feelings of insecurity and preferences.

The uncertainty of risk

In the pragmatics of some scientific sub-disciplines and certain industries, as well as in recent everyday speech, 'risk' and 'chance' are used interchangeably, which may be an underlying reason for the increasingly frequent claim that uncertainty is *the* main component of risk. Such a claim is made, for instance, by Aven in his book, *Misconceptions of Risk* (2010, p. 227). Likewise, in 2014, the Petroleum Safety Authority Norway (PSA-N) changed its risk definition from 'Risk means the combination of probability and consequences' to 'Risk means the consequences of the activity with associated uncertainty' in an attempt to draw more attention to the uncertainty involved in calculating or estimating probabilities (PSA-N, 2016). The change of definition does not imply, however, that what one in practice considers risks in the petroleum industry have changed, only that they are to be approached in a different way.

Let us – for the sake of argument – assume we have settled the difficult issue of normative judgements, so that no ethical controversies exist concerning what is good or bad, undesirable, acceptable, or tolerable, and that we all have the same risk appetite. Let us furthermore – for the sake of simplicity – presume that we are not dealing with a complex or a dynamic reality, where developments can be set in motion by a butterfly fluttering its wings in China. Let us presume instead that there is a straightforward linear causality running from isolated events to their consequences and from this perspective look at the uncertainty otherwise involved in risk.

The 'something happening' of our semantic risk definition we may then call the triggering event, whereas we can call the consequences, which are also 'something happening', the resulting event. Concerning the relation between the two, there is not only the uncertainty about whether what we have determined a triggering event will or will not occur but also – if it occurs – at what time it may occur. Furthermore, there is the uncertainty of whether – if it occurs – it will indeed result in the dreaded consequences and what the lapse of time between the two might be. The wider the time span we allow for, the greater the uncertainty about the actual causality between the two will become. In both cases, we will always need to operate with a time frame. Finally, there may be uncertainty as to where – if it occurs – it will manifest itself.

Behind the triggering event, however, there may be other events, triggering the triggering event, so to speak, just as the resulting event may trigger new events, as exemplified above. There may be a great deal of uncertainty concerning

the character of potential underlying mechanisms, be they physical, biological, chemical, socio-political, ideational, or ideological, and how they may interact to release the triggering event. The same applies to resulting events: what societal effects they might have and to what they will eventually lead – new risks or new opportunities involving new uncertainties. Thus, there is huge uncertainty attached to the possible production of chain events or cascading effects that may at some point topple a well-functioning society, even if the initial risk seemed pretty straightforward.

All these uncertainties may not be measurable or even estimable in an easy and pertinent way. For instance, some human reactions – whether physical or psychological, such as pain, fear, and panic – are not quantitatively or even qualitatively estimable, neither across individuals nor across collectives. How people have reacted in the past provides no clear indication of how they will react in the future. The context may have changed, and, besides, the people of the future will not be the same people as the people in the past. Intent, whether malicious or benign, is also difficult to estimate, let alone measure, before the fact and, even after the fact, is notoriously difficult to prove. This, for instance, is one reason why the prosecution in international criminal courts and tribunals tends to raise charges of crimes against humanity rather than charges of genocide.[20]

Finally, there is significant uncertainty attached to *the notion of possibility* itself. Very naturally, when there is a possibility of something, one would like to get an indication of just how possible this is. In specialist definitions of risk, possibility is thus often replaced with probability. However, probability and possibility are not direct synonyms:

- 'Possibility' refers to 'the state or condition of being able to exist or come into being'.
- 'Probability' refers to *a measure* of the likelihood that an event will occur.

The latter is the way in which 'probability' is used by risk analysts, regardless of whether they adhere to frequentist probability or Bayesian probability interpretations (Aven, 2012). In Danish, Norwegian, and Swedish, the common words for probability are, respectively, '*sandsynlighed*', '*sannsynlighet*', and '*sannolikhet*', which literally in English translate into 'what seems like or what is likened to the truth', 'what appears to be true'. This is a judgement that people can very well make without any reference to numerical values or indeed taking numerical values of probabilities into account. From Boholm's analyses, this way of using 'probability' also seems to be the way the word is used in everyday American English (Boholm, Möller, and Hansson, 2016).

Disregarding people's inexpert conceptions of probability causes uncertainty and uneasiness in the communication between specialists and non-specialists. It is mainly the responsibility of specialists to bridge this kind of miscommunication, and one does not build bridges by not being open about uncertain probability estimates. Even if numerically estimating probability is a relevant way of approaching concrete risks, measuring the probability of events that may or may

not occur in the future requires valid input data: either valid statistical data or valid priors. Advanced calculations on bad input may look good but are essentially misleading and hence (intentionally or unintentionally) manipulative. This becomes even worse if one tries to express the probabilities of a complex set of risk factors as one overall or aggregated probability. As is well known, a chain is no stronger than its weakest link. In such cases, it is more honest to acknowledge that no credible numerical probability estimate can be found and consequently revert to 'the possibility of *undesirable, adverse* outcome(s)' as the basis for initiating countermeasures.

Risk versus threat

According to Boholm, Möller, and Hansson, the terms 'risk', 'safety', and 'security' 'are all organized around potential (uncertain) adversity and share what we may call a threat-asset structure that is often made explicit in everyday discourse' (ibid., p. 330). Except for stating that, linguistically, threats like hazards are causes of risk to assets, the concept of threat is, however, not analysed in its own right as the other concepts are.

Risk and threat are not synonymous terms, even if they are frequently used interchangeably. The Scandinavian lexical meaning of the term 'threat' is thus:

- *Threat* is the *potential* of a person, an entity of persons, or a phenomenon to cause harm, damage or evil of some sort *due to its very nature or its mere existence*.[21]
- *Potential* is a currently unrealized ability.

Like risk, threat requires a human actor to define its content and rests on normative judgements to an even greater extent than 'risk' does. Extreme weather phenomena, explosives, toxins, bacteria, and viruses have no harmful intentions as such, they just are what they are. Even in the case where it is a person or an entity of persons that is considered to pose the threat, there is *a priori* no assumption of intent present: (1) the person or persons may inadvertently be a threat, for example careless drivers; or (2) the person or persons may not be a threat, except in the eyes of the entity feeling threatened, that is, the threat may be purely imaginary. Even in the case where a person or persons actively issues a threat, it does not necessarily involve an intention or a willingness to bring that threat to life; it may be a rumbling of empty barrels, an intimidation intended to lead to desired outcomes for the threatening party. Finally, even if the intent to carry through the threat can be adequately proved to exist, there still remains the question of whether or not the issuer of the threat possesses the capacity and/or the means to do so.

A priori, there is also no question of possibility involved in threat, even though 'possibility' and 'potential' are closely related concepts. In the first instance, the assessment of a threat, in addition to the above consideration, is not one of just how possible the threat is, but one of plausibility, that is, just how

credible the potential is. In contrast to risk, which is about which bad things might happen in the future, threats are about a potential that already exists in the present; it is only their realization that is a question concerning the future. There is thus quite a distance between threats and risk. Although it can be very tempting – since it seems much easier to deal with risks than with threats – threats cannot automatically be converted to or configured as risks and dealt with by means of risk analysis or risk management. Making threats into risks will require several analytical steps before one can reframe the definition of risk into a definition combining risks and threats:

- *Risk* is the possibility of *undesirable, adverse* outcome(s) of *a threat becoming realized.*

What if nothing happens?

One more issue needs to be contemplated before we can complete the considerations on risk:

- The possibility of the *undesirable, adverse* outcome of 'nothing happening'.

Now, this is a formally illogical proposition, since 'nothing happening' is a non-event and causality, is the relationship between something that happens or exists and what causes it. Still, it is a pertinent question in relation to risk, since risk management is all about preventing bad things from happening and reducing the consequences of them when they nonetheless do happen. Trying to counter what one has determined a risk is also an event, just as *not* trying to counter what one has determined a risk is a non-event. In the latter case, unless other factors come into play, the risk may remain not only unchanged but may worsen. An example would be climate change. In considering risk management options, one must hence ponder both the following alternatives:

1 The possibility of *undesirable, adverse* outcomes of implementing specific risk countermeasures.
2 The possibility of *undesirable, adverse* outcomes of *not* implementing specific risk countermeasures.

As eliminating the uncertainty involved in risk is virtually impossible, in principle, there are only two ways of 'eliminating' risk: by removing the source of risk altogether or by changing one's normative attitudes towards the outcomes from being undesirable into being desirable, indifferent, or immaterial outcomes. Concerning the first, there are plenty of examples of risks that have disappeared because the source no longer exists. For example, in the Western world, nobody is any longer at risk of being run down by horse-drawn vehicles, and city streets are not at risk of being covered in horse manure, as was a major concern in the late nineteenth century.[22] Concerning changing our attitudes, in many parts of

the Western world, the practising of homosexuality has gone from being posited as endangering the very fabric of society and hence criminalized to something that is not threatening society at all and hence no longer is a crime.

Risks of standardization

The *risk concept*, that is *risk as such*, is already standardized through ordinary language use. This standard risk concept is, furthermore, widely shared among everyday language users across several language and hence provides a basis for meaningful cross-cultural communication. Attempts to standardize the risk concept in more scientific terms usually selectively emphasize one component of the everyday standard meaning of risk at the expense of other components. Rather frequently, numerical 'probability', which is not at the core of the everyday meaning of risk, replaces 'possibility' and is made the salient component, with or without reference to the uncertainty involved in probability estimates. Rather than being standardized risk concepts, these specialist definitions can be seen as competing *risk approach standards* (standardization 1). As standardization attempts, they have not been successful, in that there has been a failure to reach a general agreement on the issue. Consequently, one encounters difficulties in making various actors comply with the various risk approaches and in evaluating concrete risks in comparison to one another (standardizations 2 and 3).

The normative judgement component is frequently left out of specialist definitions, maybe because it is not standardisable, or maybe because scientists have no primacy in making normative judgements. Normative judgement is, however, an inescapable component of risk. There is thus clearly a need to focus much more on the normativity of risk than is common, not only as regards what are to count as undesirable outcomes of specific risks but also regarding just how undesirable these outcomes are – in an absolute sense, relative to one another, and in relation to the outcomes of other risks. The issue of normativity should be highlighted to a greater extent than it is, as it underlies the question of whether it is possible to reduce concrete risks through standardization and whether there are issues with standardization that may increase concrete risks rather than reduce them.

There are undoubtedly aspects of risk that it is possible – and that it may also be highly relevant – to standardize, in order to know which risks to be concerned about and how to deal with them. There are, for instance, clearly benefits in implementing some degree of standardization in risk analysis and risk management, both for communication purposes and in order to make risks comparable from one area to another. However, since concrete risks themselves are always complex and not as such 'standardizable', standards for risk analysis will necessarily involve a considerable degree of simplification. Consequently, there is a risk of oversimplifying the risk analysis, thereby missing critical aspects and either underestimating or overestimating the seriousness of actual outcomes. This in turn may lead to either taking inadequate mitigating actions or spending

too many resources (both human and financial) on managing risks that might be less serious than dreaded – if and when they occur. In this context, there is a particular risk resulting from confusing uncertainty with risk as such and introducing the concept of 'upside risk'. When this idea is combined with an evaluation of economic impact, it is very tempting to think that the law of averages will partly or completely mitigate the risk, the consequence of that being that appropriate mitigating actions are *not* taken.

Standardizations of risk analysis and risk management based on probabilities entail a risk of leading to complacency, the illusion that one is in control when one is in fact far from it. As discussed above, not everything is measurable – not even reliably estimable. One should take care not to invent artificial metrics for what is not measurable or for what ought to be left unmeasured. Furthermore, not everything that is measurable is commensurable, and again it may not be pertinent to standardize everything that is commensurable. The choice of what unit of measurement to use in evaluative comparisons or to ensure compliance is crucial to the outcome. It is not just a matter of hypothetical practicality but also a matter of normativity – in terms of the norms underlying the choice of measurement unit and of affecting which norms might come to dominate future society.

Finally, when risk analysis and risk management are standardized in an entity such as a society, which again consists of many smaller entities such as municipalities, there is a risk of underestimating more global risks that impact *all* the smaller entities. One such example is the climate change risk. Each local municipality can prepare for severe local flooding or avalanches but must also to some degree take into account that this risk is global and that the state may not have the resources to give each municipality the support and financial compensation that they are accustomed to. Conversely, other risks may well affect society as such but still have no direct impact on each and every one of the smaller entities. In this case, implementing everywhere a standard based on worst case scenarios may hence be shooting far above the target – and become costly, without rendering a proportional dividend.

Conclusion

With so much inherent normativity and uncertainty involved in risk, as demonstrated above, risk is more than anything characterized by diversity and variability, whereas standardization implies abstracting from diversity and variability. Hence, one needs to very carefully consider what is the purpose of one's standardization in relation to which risk issues and whether it is at all pertinent.

In making such deliberation, since 'standardization' has three semantic meanings, one will need to distinguish between at least the following three overall *risks of standardization*:

1 The possibility of *undesirable, adverse* outcomes of *setting a standard.*
2 The possibility of *undesirable, adverse* outcomes of *evaluating something by comparing it to a set standard.*

3 The possibility of *undesirable, adverse* outcomes of *making something comply with an already set standard.*

But also take into consideration:

4 The possibility of *undesirable, adverse* outcome(s) of *not standardizing* (in all three senses).

Risks are of many kinds, some of which are not commensurable or even comparable to one another in any meaningful way. Standardization of certain aspects pertaining to specific risk issues may sometimes be appropriate, sometimes inappropriate. The diversity and variability of concrete risks may be a decisive factor in dealing with them; the ability to rapidly adapt to changes in concrete risk situations certainly is. Standards pertaining to risk issues must thus be able to distinguish between different kinds of risk and allow for the dynamics inherent to any kind of risk. Hence, more diversification – not more standardization – may be what is required. Furthermore, normative judgements are at the core of both standardization and risk – in fact, without them there would be neither standards nor risks. This aspect is all too often disregarded and – if at all contemplated – either taken for granted without further ado or treated as if the underlying norms were undoubtedly universal, that is, everywhere exactly the same. In an era where risks are becoming increasingly international or global, we need to acknowledge that there is a huge variation in normative judgements, depending on where in the societal stratigraphy and where in the world one is placed, and that it is necessary to be consciously aware of this if we are to successfully meet our common challenges.

Notes

1 See www.cen.eu/Pages/default.aspx, accessed 4 April 2017. As of 23 January 2018, however, the website no longer provides this sort of information in an easily accessible way.
2 See www.iso.org/standards.html, accessed 30 September 2017. When accessed on 4 April 2017, the number was 21,578, which means that in 180 days the number of standards issued by ISO had increased by 262. When accessed on 23 January 2018, the number was 22,009, which means that since the end of September 2017 (115 days) the number of standards issued by ISO had increased by another 431 standards.
3 See www.iso.org/standards.html, accessed 4 April 2017.
4 Despite the fact that every year portions of land are lost to both the North Sea and the Baltic Sea, and that, for instance, a French tourist was killed by a major landslide at the chalk cliffs of Møn in 1994. (www.ystrom.dk/naturviden/Moen/detunikke3LM.htm).
5 See www.statista.com/statistics/266808/the-most-spoken-languages-worldwide/ accessed 6 April 2017.
6 VOICE (the Vienna-Oxford International Corpus of English) in Austria, (www.univie.ac.at/voice/index.php), and ELFA (English as a Lingua Franca in Academic

Settings) in Finland (www.helsinki.fi/elfa). Recently a corpus on written academic ELF has also been compiled: WrELFA (Written Academic ELF) (www.helsinki.fi/englanti/elfa/wrelfa.html).

7 Danish and Norwegian *bokmål/nynorsk* (the two different forms of the Norwegian language): '*standardisering*', 'standard', '*risiko*'; Swedish: '*standardisering*', 'standard', 'risk'; and Finnish: '*standardointi*', '*standardi*', '*riski*'.

8 In Danish, Norwegian *bokmål* and Swedish: '*sikkerhed*', '*sikkerhet*', '*säkerhet*', and in German: '*Sicherheit*' all translate as both 'safety' and 'security' in English. In Norwegian *nynorsk*, the word is '*tryggleik*', which in Norwegian *bokmål* is '*trygghet*', Danish: '*tryghed*', Swedish: '*trygghet*' that likewise translate as both 'safety' and 'security', but which in German translate as '*Sicherheit*'. This is not the place to discuss in depth potential differences in the connotations of these words, only to indicate how this might complicate cross-language communication. Note that below, words that are identical in Norwegian *bokmål* and *nynorsk* will just be referred to as Norwegian.

9 I have predominantly used the following authoritative dictionaries: For Danish: *Ordbog over det danske Sprog* (http://ordnet.dk/ods); for Norwegian: *Språkrådets Bokmålsordbok* og *Nynorskordbok* (http://ordbok.uib.no/) supplemented with *Store norske leksikon* (https://snl.no/leksikon); for Swedish: *Svenska Akademiens Ordbok* (www.saob.se/om/); for British English: *The Oxford English Dictionary* (www.oxforddictionaries.com/oed); for American English: *The Merriam-Webster Dictionary* (online) (www.merriam-webster.com/); and for German: *Deutsches Wörterbuch von Jacob Grimm und Wilhelm Grimm* (http://woerterbuchnetz.de/DWB/).

10 Jensen and Goldschmidt. *Latinsk-dansk ordbog*. 4th ed. (Gyldendal: Nordisk forlag, 1955).

11 Roman centuries, cohorts, and legions also had what are often referred to as the Roman standards. Each unit thus had its own *signum*, a heraldic symbol on a tall pole, which could be a banner but was more often an image such as, for instance, the Roman eagle. Their purpose was not only and not primarily practical communication in battle.

12 The English word 'desertion' – in Danish: '*faneflugt*', Norwegian: '*faneflukt*', Swedish: '*fanflykt*' and German: '*Fahneflucht*' – literally means 'fleeing the banner'.

13 Danish: '*chance*', Norwegian: '*sjanse*', Swedish: '*chans*'.

14 *The Oxford English Dictionary* (www.oxforddictionaries.com/oed); *The Merriam-Webster Dictionary* (online) (www.merriam-webster.com/).

15 The actual quote is: ' "Risk" is defined, by most of those who seek to measure it, as the product of the probability and utility of some *future* event' (Adams, 1995, p. 30). Adams does not in any place state a definition of his own. However, the text of the book very clearly refers to risk as concerning exclusively detrimental, adversary outcomes of future events – 'the definition of common parlance' (ibid., p. 8).

16 For instance, Norwegian Official Reports, NOU 2000:24, 'Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet' [A vulnerable society: Challenges to safety and emergency preparedness in society; my trans.], available at: www.regjeringen.no/no/dokumenter/nou-2000-24/id143248/, and NOU 2006:6, 'Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner' [When safety is most important: Protection of the nation's critical infrastructures and critical societal functions; my trans.], available at: www.regjeringen.no/no/dokumenter/nou-2006-6/id157408/

17 'Mandela off U.S. terrorism watch list', *CNN*, 2 July 2008, available at: http://edition.cnn.com/2008/WORLD/africa/07/01/mandela.watch/

18 Tom Grant, 'Bin Laden's grand miscalculation', *Foreign Policy Research Institute* (FPRI), 13 October 2001, available at: www.fpri.org/article/2001/10/bin-ladens-grand-miscalculation/

19 Steve Chapman, 'Making enemies, one war at a time', *Chicago Tribune*, 5 November 2014, available at: www.chicagotribune.com/news/opinion/chapman/ct-steve-chapman-u-s-war-without-a-clue-perspec-1106-20141105-column.html

20 For instance, in the case of Radovan Karadžić, the prosecution indicted Karadžić on two counts of genocide, one concerning Srebrenica, the other concerning a number of places in municipalities throughout Bosnia and Herzegovina. In order to secure a conviction, this number was reduced twice in successive amended indictments, available at: www.icty.org/case/karadzic/4#ind. Even so, they did not succeed on the second count, available at: www.icty.org/en/press/tribunal-convicts-radovan-karadzic-for-crimes-in-bosnia-and-herzegovina

21 Danish and Norwegian *bokmål/nynorsk*: '*trussel*', Swedish: 'hot'.

22 See www.historic-uk.com/HistoryUK/HistoryofBritain/Great-Horse-Manure-Crisis-of-1894/

References

Adams, J. (1995). *Risk*. London: Routledge.

Aven, T. (2010). *Misconceptions of risk*. Chichester: John Wiley & Sons Ltd.

Aven, T. (2012). The risk concept: Historical and recent development trends. *Reliability Engineering & System Safety*, 99, pp. 33–44.

Aven, T., Renn, O. and Rosa, E. A. (2011). On the ontological status of the concept of risk. *Safety Science*, 49(8–9), pp. 1074–1079.

Boholm, M. (2012). The semantic distinction between 'risk' and 'danger': A linguistic analysis. *Risk Analysis*, 32(2), pp. 281–293.

Boholm, M. (2017). The semantic field of risk. *Safety Science*, 92, pp. 205–216.

Boholm, M. (2018). How do Swedish Government agencies define risk? *Journal of Risk Research*. doi.org/10.1080/13669877.2017.1422782.

Boholm, M., Möller, N. and Hansson, S. O. (2016). The concepts of risk, safety, and security: Applications in everyday language. *Risk Analysis*, 36(2), pp. 320–338.

Bowker, G. C. and Star, S. L. (1999). *Sorting things out: Classification and its consequences*. Cambridge, MA: MIT Press.

Brunsson, N. (2000). Regulating by standards. In N. Brunsson and B. Jacobsson (eds) *A world of standards*. Oxford: Oxford University Press, pp. 19–39.

Brunsson, N. and Jacobsson, B. (2000a). The contemporary expansion of standardization. In N. Brunsson, and B. Jacobsson (eds) *A world of standards*. Oxford: Oxford University Press, pp. 1–17.

Brunsson N. and Jacobsson, B. eds. (2000b). *A world of standards*. Oxford: Oxford University Press.

Busch, L. (2011). *Standards: Recipes for reality*. Cambridge, MA: MIT Press.

Jensen, J. T. and Goldschmidt, M. J. (1955). *Latinsk-dansk ordbog*. 4th ed. Gyldendal: Nordisk forlag.

Kaplan, S. (1997). The words of risk analysis. *Risk Analysis*, 17(4), pp. 407–417.

Kuran, T. and Sunstein, C. R. (1999). Availability cascades and risk regulation. *Stanford Law Review*, 51(April), pp. 683–768.

Lampland, M. and Star, S. L. (2009). *Standards and their stories. How quantifying, classifying, and formalizing practices shape everyday life*. Ithaca, NY: Cornell University Press.

Mauranen, A. (2012). *Exploring ELF: Academic English shaped by non-native speakers*. Cambridge: Cambridge University Press.

PSA-N (2016). *Risikobegrepet i petroleumsvirksomheten* [The risk concept in the petroleum industry]. Available at: www.ptil.no/getfile.php/1337784/PDF/RISIKORAPPORT%20 2016%20nett.pdf. See also www.ptil.no/risk-and-risk-management/new-definition-of-the-risk-concept-article11908-897.html

Seidlhofer, B. (2011). *Understanding English as a lingua franca*. Oxford: Oxford University Press.

Shrader-Frechette, K. S. (1991). *Risk and rationality: Philosophical foundations for populist reforms.* Berkeley, CA: University of California Press.

Part II

Standardization of risk management

3 Towards a standardization of EU disaster risk management?

Claudia Morsut

Introduction

This chapter aims to give an account of the EU disaster risk management policy and the initiatives that the EU has put in place within this policy. These initiatives contain, in different degrees, forms of standardization that this chapter will outline by pointing out which challenges the EU meets in a policy, which differs widely among states, since it is heavily influenced by national contexts. The chapter is mainly based on a review of key official EU documents on disaster risk management, which track the EU's efforts to establish its comprehensive disaster risk management framework.

According to EU jargon, the EU disaster risk management policy encompasses disaster prevention, preparedness, response, and reduction of risks, to help member states to better prevent, prepare for, and respond to disasters (ECHO, 2019a; JRC, 2019).[1] The EU promotes this policy to establish and to develop a comprehensive EU disaster risk management framework for member states and associate countries. However, this sounds like an impossible task to fulfil, due to two main challenges.

First, disaster risk management remains mainly a state's policy, shaped by historical, political, and socio-economic contexts. Risk has been increasingly studied in terms of socio-political phenomena since the seminal work by Beck on the risk society (Beck, 1992). Thus, risk and risk management are firmly anchored and influenced by factors such as culture (which includes the values, beliefs, and norms of a given society) and policy (which refers to political systems, decision-making, and modes of governance). Scholars, such as Wildavsky and Dake (1990), Renn (2008), and Luhmann (2005), have shown that risk is not only approachable through pure technical assessments but that social, cultural, and political dimensions also need to be taken into consideration.

Second, the impact of natural hazards depends mainly on the level of vulnerability of a territory and its population and the national/local organizational and interventional capacities. States have formulated their own risk assessments, developed their own risk management guidelines and standards, and put in place their own national civil protection systems. In addition, the management of the consequences of these natural hazards has always been at the national/local

level. States mobilize their resources and capacities to help their population, through their own civil protection systems, trained to cope with emergencies, crises, and disasters. If assistance from other countries becomes a necessity, states usually receive help from their neighbours, according to bilateral agreements.

Governing risk according to these elements becomes even more complicated when we consider the EU level. Here, risk prevention and mitigation, including identification, assessment, planning, communication, and consultation, involve several actors, different levels of governance, and numerous cultural and political approaches: EU institutions, states, and their national risk management systems, research communities, citizens, NGOs, and the private sector are all part of the EU framework.

Despite these challenges, the EU has increasingly taken several initiatives at the legislative and operative levels to promote and maintain cooperation among the member states and associated countries on ways to better cope with natural and man-made risks, hazards, crises, and disasters. In this sense, the EU represents a natural 'protection policy space' (Rhinard, Ekengren, and Boin, 2006, p. 513), where states can mobilize civilian (and military) means to manage together man-made and natural risks and their consequences. Cascading effects and transboundary crises have offered the EU the opportunity to highlight the need to seek shared solutions for governing risks that are common to several member states and challenge national capacities. Indeed, risks and consequences related to natural hazards are increasingly not confined by national borders, and they call for disaster risk governance and management that go beyond the nation state. Natural hazards often provoke crises and/or disasters that have cascading effects and a transboundary character, challenging the states' capacities to adequately respond (Boin and Ekengren, 2009). A good example is volcanic outbursts (e.g. the 2010 eruptions of Eyjafjallajökull in Iceland). In addition, a country's response to a crisis or a disaster can lead to negative consequences for another country, as can happen with floods of rivers crossing several states (e.g. the 2016 European floods).

Standardization at the EU level

The largest and most compelling project of standardization in the world is taking place within the EU. Since the birth of the European Economic Community (EEC) in the late 1950s, standardization has been achieved in most areas of public concern affecting the member states and the lives of millions of EU citizens. Nowadays, the EU can be regarded as the standard setter in a growing number of areas (Levi-Faur, 2011). In addition to the most thoroughly standardized domain, the Single Market, the EU has set standards inside a wide variety of policies, such as the protection of the environment and of human health, food safety, the postal sector, and agriculture. Since the late 1990s, higher education, research, the European currency system, as well as asylum policies, have been subject to standardization, mainly through the adoption of Regulations in line

with Treaty-mandated powers. Most recently, the EU intervened with the General Data Protection Regulation (GDPR), which establishes stricter rules for the processing of personal data relating to individuals in the EU (European Union, 2016). With the growth of the EU's tasks and the increasing complexity of the EU's system, the establishment of standards has become a necessity to ensure the EU's member states all adhere to the same concepts, legal frameworks, rules, and norms. Standardization may be seen as one of the means to keep the EU going, since its essence is to increasingly integrate the member states in certain domains of common interest. However, this is not an easy undertaking, since the EU – despite its efforts towards supranationalism – largely remains an intergovernmental organization of sovereign states, which have maintained standards (and standards bodies) of their own.

In general, standardization is mainly meant to improve efficiency, quality, and safety, by making products and services competitive and compatible, and has given rise to several regulatory regimes, such as the oil and gas regulatory regime or the aviation regulatory regime. These regimes comprise both the authorities in charge of setting standards and making various parties follow the standards and the parties that have adhered to a set of standards and agreed to follow them (Black, 2001). The EU is no exception and has established its own regulatory regime, based on voluntary cooperation and a consensus-building process that involves many actors: EU institutions (mainly the European Commission and the European standardization organizations),[2] national authorities, their standards agencies, and stakeholders (industrial bodies; trade unions; health, environment, and education associations; consumers' associations; SMEs; and so on). The Single Market is regarded as one of the most successful achievements of the EU. For decades, the European Commission has worked to establish standards for products, production processes, services, and market-based competition for the member states, mainly in three areas: transport, buildings, and energy. In the Single Market, standards have ensured interoperability and safety, reduced costs, facilitated companies' integration in trade and, in general, enhanced the competitiveness of EU industry. The standards in the Single Market are established within the European Standardization System (ESS),[3] through regulatory instruments. The Single Market's standards contain technical specifications to enhance uniformity, which I refer to as hard standardization. In addition, the EU pursues what I refer to as soft standardization: In this case, the EU aims to increase mutual understanding, remove political and cultural barriers, ease communication, foster a common European language on policy, and disseminate knowledge and expertise beneficial to all the member states. The EU promotes soft standardization, by recurring to particular forms of governance, such as policy convergence, the open method of coordination (OMC), agencies, and networks.

The EU's room for manoeuvre between hard and soft standardization is rather small, since it is determined by several factors, such as the Treaties' mandate, the policy area, the willingness of member states to cooperate, and the degree of urgency of the matter. In particular, EU primary and secondary law

offer different options, with regard to pursuing standardization. The various EU Treaties, signed by the member states, represent the EU primary law. They contain the EU's rules and goals, the relationship between the EU institutions and the member states, and the description of the various decision-making processes. Articles 2–6 of the Treaty on the Functioning of the European Union (TFEU) establish three kinds of EU competences: exclusive, shared, and supportive. In the first case, only the EU can adopt legal acts, as in the case of the competition rules within the Single Market. In the second case, the member states can act only if the EU has chosen not to. Transport and energy policies are an example. In the third case, the EU cannot adopt legally binding legislative acts that require the member states to harmonize their laws and regulations. In the EU's jargon, harmonization means that national laws and regulations are aligned with the EU law by means of EU regulations and directives. In other words, member states must include the entire EU legal system in their national legal system, by accepting the *acquis communautaire*. This is an ongoing process that starts when a state receives membership and continues after entry, since member states cannot maintain or introduce, in their national law system, provisions diverging from those laid down by the EU. Harmonization is quite a controversial term, especially since it has been used rather loosely, almost as a synonym of standardization (Andenas and Baasch Andersen, 2011; van den Brink, 2017). However, harmonization increases compatibility, by setting limits on how much they can vary and can use standards to reach this goal. Often standardization, on the other hand, means a more rigid and narrow set of rules (see Juhl, Chapter 2, and Olsen, Chapter 1, in this volume). Civil protection is one of the policies falling under the supportive competences (Article 2E, TFEU), where the EU can intervene, by coordinating or supplementing the actions of the member states. Disaster risk management is one of the areas covered by civil protection (European Union, 2019).

Regulations, directives, decisions, recommendations, opinions, and communications are known as secondary law. These legislative acts contain binding and non-binding provisions. Regulations are the highest level of binding acts; they do not need to be transposed in the national legislations of the member states, but they have legal effects from when they come into force. Directives usually contain common and obligatory goals to be achieved through essential requirements for all the member states, which are left free to find their own national ways to fulfil them. Directives are flexible, to the extent that the national authorities have the choice of the form and method of implementing the directive. If a state or a group of states does not adopt the directive within two years, the European Commission can start the so-called infringement procedure. Decisions are binding for the member state or the group of member states or companies they are addressed to. They do not need to be transposed in the national law system. Recommendations contain no obligation but mainly suggestions. Opinions and communications are also non-binding and mainly contain views issued by any of the EU institutions, including the Committee of the Regions and the European Economic and Social Committee (European Union, 2018a, 2018b).

In addition, the EU needs to take into account certain principles. The principle of proportionality means that EU action should not go beyond what is necessary to achieve the objective. Proportionality is about matching EU policy intervention to the size and nature of the identified problem. Furthermore, coherence with other related policy instruments is another principle that the EU seeks to achieve in order to exploit synergies and to avoid undermining the effectiveness of existing instruments.

Standardizing EU disaster risk management

The International Standards Organization (ISO) standard ISO 31000:2018 defines risk management as 'coordinated activities to direct and control an organization [or any other user of the standard] with regard to risk'. Several EU policies include risk management: health, agriculture, food safety, environment, industry, finance, transport, energy, and nuclear safety are a few examples (see Bengtsson, Chapter 6, in this volume, for an example of EU-initiated standardization of risk in the health sector). The EU follows a three-pillar approach in dealing with risks: risk assessment, risk management, and risk communication. Risk assessment mainly identifies the characteristics of a hazard, its probable consequences, and the potential losses. Risk management focuses on the policy options to face risk. Risk communication is transversal, since dialogue and communication with those dealing with risk and those affected by risks' consequences are of paramount importance for correct risk assessment and management. The EU has introduced risk management requirements that are not sector-related, to which all organizations must adhere (horizontal compliance). For example, occupational health and safety standards are applied independently from the sector. At the same time, the EU regulates specific sectors through its legislative acts.[4]

The United Nations Office for Disaster Risk Reduction (UNDRR, formerly known as UNISDR – the United Nations International Strategy for Disaster Reduction) defines disaster risk management as: 'The systematic process of using administrative directives, organizations, and operational skills and capacities to implement strategies, policies and improved coping capacities in order to lessen the adverse impacts of hazards and the possibility of disaster' (UNISDR, 2016, n.p.). Based on these two definitions, standardization means mainly achieving common national risk assessments, planning and mapping, and minimum prevention standards, all of which need to include a shared understanding of risks from natural hazards, within the EU disaster risk management framework. To reach this, the EU needs to consider several actors, policies, and initiatives, in both its vertical (UN–EU–states–regions–local governments) and horizontal relationships (natural disaster risks and policies, see Knill, 2001). As for the vertical relationships, the EU has anchored its disaster risk management inside the broad and global UN frameworks, first following the Hyogo Framework for Action (2005–2015) (United Nations, 2005) and then the Sendai Framework for Disaster Risk Reduction (2015–2030) (United Nations, 2015). Disaster Risk Reduction (DRR) is the strategy promoted by the UN to reduce

damage caused by natural (and technological) hazards, through long-term activities, encompassing mitigation, preparedness, sustainable development, and crisis management (UNISDR, 2018). To some extent, the EU has been involved in DRR for several years, and many of its policies (cohesion policy; health; environment; climate change adaptation; agriculture, food and nutrition security; water; flood risk management; major industrial accident prevention; nuclear safety) include elements of DRR, such as disaster prevention and preparedness, guidelines on risk assessment, guidelines for the assessment of risk management capabilities at national level, and so on. In the European Commission, some Directorate-Generals (DGs) deal with DRR on a daily basis: (DG ECHO European Civil Protection and Humanitarian Aid Operations; DG HOME Migration and Home Affairs; DG CLIMA Climate Action; DG DEVCO International Cooperation and Development; DG ENV Environment, etc.). In its relationship with the UN, the EU has taken the role of mediating between the overarching UN framework and what the EU member states already have in place, with regard to disaster risk management, also considering the differences between them (Eberlein and Grande, 2005). Here, the principle of subsidiarity plays a crucial role in finding a balance between member states' existing disaster risk management and the EU initiatives. As for the horizontal relationship, the EU has for some time followed a sectoral approach in disaster risk management. This sectoral approach has recently evolved into a more holistic approach for all natural (and man-made) risks throughout all phases of the disaster management cycle (prevention, preparedness, response, recovery).

The primary law, that is the Treaties, did not foresee natural disaster risk management as an EU policy area until the 2009 Treaty on the Functioning of the European Union (TFEU). In its Article 92, the 1957 Treaty of Rome mentions that aid to a state affected by a natural disaster has to be compatible with the Common Market (reiterated in Article 87 of the 2002 Treaty of Nice). The 1992 Maastricht Treaty (Article 103a) briefly refers to the vote system inside the Council in the case of a member state needing financial support after a natural disaster (as does Article 100 of the 2002 Treaty of Nice). The 2009 TFEU introduced substantial novelties. Article 196 of the TFEU describes the EU's role within civil protection. Here, disaster risk management is not explicitly mentioned as a concept in its own right, but nevertheless the article contains some of its components, such as risk prevention, preparedness, and cooperation:

1 The Union shall encourage cooperation between Member States in order to improve the effectiveness of systems for preventing and protecting against natural or man-made disasters. Union action shall aim to:
   a support and complement Member States' action at national, regional and local level in risk prevention, in preparing their civil-protection personnel and in responding to natural or man-made disasters within the Union;
   b promote swift, effective operational cooperation within the Union between national civil protection services;
   c promote consistency in international civil-protection work.

2 The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall establish the measures necessary to help achieve the objectives referred to in paragraph 1, excluding any harmonisation of the laws and regulations of the Member States.

The EU's activities in disaster risk management are thus enshrined in points a–c of paragraph 1 of Article 196. In risk prevention and in the crisis management circle, the EU is expected to support and complement the member states at all levels of governance and to promote effectiveness and consistency in civil protection. Paragraph 2 spells out that measures undertaken by the EU *cannot* entail any harmonization of member states' laws and regulations. In other words, the responsibility remains within the sole authority of the member states, and the EU cannot legislate, for example, on specific requirements on how to standardize procedures or allocation of resources. At the legislative level, the EU can intervene only with decisions, since directives and regulations replace national legislation. Following the same path as the Single Market is hence not an option here. Thus, the EU has sought to fulfil the goals of the article through soft standardization. This accomplishment has been facilitated by the introduction of the ordinary legislative procedure, after the TFEU came into force. This entails the Council deciding by a qualified majority (and not by unanimity as before), in a co-decision with the European Parliament, upon a proposal from the Commission.

In the following part of this chapter, I deepen the content of Article 196 by linking it to concrete initiatives taken by the EU and by describing soft standardization. First, I define the content of Article 196 as an example of *policy convergence*. Policy convergence stems from comparative public policy and studies on how similar policies across countries are developed. Knill (2005, p. 768) defines policy convergence as 'any increase in the similarity between one or more characteristics of a certain policy (e.g. policy objectives, policy instruments, policy settings) across a given set of political jurisdictions (supranational institutions, states, regions, local authorities) over a given period of time'. This similarity concerns three dimensions: structures, processes, and performances. Structures are represented by administrative organizations and rules; processes refer to policy-making, and performances refer to policy outcomes (Albrecht and Arts, 2005). In the EU context, the EU has pursued policy convergence since the beginning in a growing number of policy areas. Policy convergence remains an interesting but controversial concept, mainly since it is challenging to track down in the empirical research whether the EU is the initiator of policy convergence (Tercovich, 2018), whether the EU is the mediator (Holzinger and Knill, 2005) or whether member states are influenced by international actors other than the EU (Albrecht and Arts, 2005), and whether policy convergence is a bottom-up or bottom-down process or a mixture of the two. In the case of disaster risk management, the EU intervenes in an area which is common to all the member states and seeks to find ways to develop this area according to the three dimensions of policy convergence: structures, processes, and performances.

These dimensions, in different degrees, are present in the activities promoted by the EU according to Article 196.

In the case of risk prevention (Article 196, paragraph 1, point a), the only example of standardization within the ESS is represented by the CEN's Eurocodes 7 and 8 (Eurocodes, 2018). Eurocode 7 concerns geotechnical design in buildings, how to assess geotechnical data, and what is requested in the phase of execution of structures. Eurocode 8 deals with the design of structures for earthquake resistance in seismic-prone areas. Here, the Eurocode foresees the requirements and rules to assess seismic risk and specifies how to increase structural resistance. All the national standard agencies have given these Eurocodes a national status (Ranke, 2015). The 2007/60/EC Flood Directive (European Commission, 2007) represents another example of hard standardization – but outside the ESS and prior to the TFEU. This directive imposes an obligation on the member states to achieve quantitative and qualitative good standards in flood risk management and represents the legal framework for the assessment and management of flood risks through a mapping system, subject to existing standards. The aim is to reduce adverse consequences for human health, the environment, cultural heritage, and economic activities impacted by floods. Flood risk is considered an area in which member states have succeeded in finding common standards (European Union, 2019).

To push forward its initiatives in risk prevention, the EU has mainly followed the open method of coordination (OMC), which was officially launched by the Lisbon European Council in 2000, but both the Maastricht Treaty (1993) and the Amsterdam Treaty (1997) applied it to the Economic and Monetary Union (EMU) national policies and the EU Employment Strategy, respectively. The main features of the OMC are: 'common guidelines to be translated into national policy, combined with periodic monitoring, evaluation and peer review organized as mutual learning processes and accompanied by indicators and benchmarks as means of comparing best practice' (Council, 2000, p. 12). The main characteristics of the OMC are:

- the European Council establishes and defines common objectives and goals;
- the European Commission prepares guidelines to achieve them, by introducing quantitative and qualitative indicators and benchmarks;
- the member states translate the guidelines into their national policies;
- the European Commission evaluates the achievements, according to a mutual learning process and a soft law procedure (Council, 2000; Borras and Jacobsson, 2004; Eberlein and Dieter, 2004).

No sanctions are foreseen for those member states unwilling to participate, and participation is very much influenced by national interests to be part of a process regarding a certain policy. This is, however, an inclusive method, which seeks to involve not only member states but also several levels of governance (private actors, agencies, NGOs, local governments) in shaping arenas of cooperation and networking (Jacobsson and Schmid, 2003). The OMC is based on the

following principles: voluntarism, subsidiarity, flexibility, participation, policy integration, and multi-level integration (ibid.). The OMC has been employed mainly in the employment, innovation, and education policies but has not been exempt from criticism. For example, Gornitzka (2005) argues that, due to the lack of sanctions and constraints, the OMC does not offer real incentives to the different actors to be part of the process. On the other hand, as Radaelli (2003) points out, the OMC has resulted in establishing directives and regulations, thus binding rules.

The common objectives and goals in risk prevention are contained in the communication establishing the Community approach on the prevention of natural and man-made disasters, launched by the European Commission in 2009 (European Commission, 2009), to implement the Hyogo Framework for Action 2005–2015 at the European level. This approach has three main objectives: (1) the development of knowledge-based disaster prevention policies at all levels of government, through guidelines and inventories; (2) the establishment of links between actors and policies in the disaster management cycle, through exercises and dissemination of lessons learnt; and (3) the reinforcement of existing instruments at the EU level, through funding and existing legislation. The Council gave the Commission the mandate to pursue these objectives (Council, 2009), which have become the basis for all the subsequent initiatives promoted by the Commission in risk prevention. In the communication, the Commission recognized that the main challenge in risk prevention is the lack of common guidelines that would greatly help to compare the risks among the member states; thus, it prepared guidelines for the member states to make risk measurable and comparable. The Guidelines for National Risk Assessments and Mapping (European Commission, 2010) are meant to improve consistency and compatibility in risk assessments among the member states and, consequently, to facilitate cooperation, by forming a common EU terminology for national risk assessment. Higham (Chapter 13, in this volume) discusses a similar case of introducing international standards to analyse complex risks (the UN Guiding Principles on Business and Human Rights). Actually, the guidelines contain examples of international standards established by ISO and by the UNDRR, such as for disaster risk reduction (United Nations, 2005; OECD, 2009). After introducing key concepts, such as a 'multi-hazard and multi-risk approach' and 'knowledge-based disaster prevention' (European Commission, 2010, pp. 6–7), these guidelines move on to discuss the risk assessment process, by looking at the various ways in which risk can be conceptualized, and the basic methodology of a risk assessment. They propose a risk matrix according to two variables, impact and likelihood, in order to identify, analyse, and evaluate risks. Such a risk matrix is nothing new, since it has been used in the international standards for risk management and had already been reproduced in some national security strategies that served as international role models, such as in the Netherlands (Bossong and Hegemann, 2016). Jørgensen and Lindøe (Chapter 11, in this volume) discuss how and why the risk matrix has become a widespread tool and why it is appealing for risk assessment.

Recognizing that the member states are at different levels of advancement in their risk assessment efforts, the European Commission proposed that the states would follow a four-step process, according to (1) scenario building; (2) extent of quantitative analysis; (3) number of risks and risk scenarios considered; and (4) the temporal horizon. These steps were supposed to offer between 50 and 100 national risk scenarios, ranging from medium to serious (and probable) risk. Since the European Commission considered these guidelines as the first phase in establishing common risk management by 2014, it invited the participating states in the EU Civil Protection Mechanism[5] to translate the guidelines into their national policies, by elaborating their national risk assessments, based on the guidelines, and submitting them to the European Commission by the end of 2011. The OMC does not foresee sanctions if a state does not comply with the European Commission's requests in due time, as it is based on voluntary participation. Thus, the process was slower than expected by the European Commission. By Spring 2014, only 17 member states and one non-member, Norway, had delivered their own national risk assessments following the guidelines (European Commission, 2014b). Some of these states, such as Denmark, Germany, the UK, the Netherlands, and Sweden, were countries with well-developed national risk assessments, so one could doubt the causal influence of the guidelines on the elaboration of their national risk assessments (Bossong and Hegemann, 2016). Article 6 of Decision 1313/2013/EU on the EU Civil Protection Mechanism (European Parliament and Council, 2013) introduced the obligation for participating states to submit their national risk assessment every three years to the Commission, starting from December 2015. This time, the participating states delivered their national risk assessments according to the deadline. However, the national risk assessments varied from being very detailed and complete to not totally finalized (European Commission, 2017). Nonetheless, for the European Commission, the overview of national risk assessments was very useful to better understand the different risk management governance structures and risk management methods in place at national or sub-national levels (ibid.).

Another initiative following the OMC was taken by the Council in Spring 2011. The Council entrusted the European Commission to prepare an overview of natural and man-made disaster risks, based on the national risk assessments provided by the states. According to the Council, the overview should focus mainly on shared risks, with cross-border impact and/or of large scale, that require transboundary cooperation in the case of a crisis or disaster (Council, 2011). The Commission realized two overviews, one based on 18 national risk assessments (European Commission, 2014b) and one including all the participating states' risk assessments (European Commission, 2017a), after the introduction of the obligation contained in Article 6 of the 2013 decision. In both, floods and severe weather (such as storms, snowfall, and heavy precipitation) were considered the main natural risks provoking natural disasters. The second overview was more focused on the cross-border dimensions and the cascading effects of disasters than the previous one, since the Commission had received all the national risk assessments and could proceed with a comprehensive picture of risks.

The accomplishments obtained through the guidelines and the overviews were evaluated positively by the European Commission. The Commission obtained a 'cross-sectoral overview of the major natural and man-made risks that the European Union may face in the future' and was now able 'to identify, on the basis of the overview, risks or types of risks that are shared by Member States or regions in different Member States' (European Commission, 2010, p. 4). On the other hand, the 2010 guidelines contain certain wording that is typical of a standardization process, such as the objective to 'improve coherence and consistency among the risk assessments undertaken in the Member States … and to make these risk assessments more comparable between Member States' (ibid., p. 6), and to establish a 'common terminology and a shared understanding of concepts' (ibid., p. 7). These objectives were only partially achieved, and challenges persisted in the variety of processes and methodologies from country to country. For instance, the UK considered all the possible emergencies, while Denmark chose those which had a certain magnitude, geographical extent ,and/or were not manageable at the local level. Hungary, Portugal, Malta, and Cyprus explicitly considered climate change as a multiplier of risks, while the UK did not. Germany produced annual risk analysis reports, while other countries had different deadlines. The Netherlands was very inclusive in involving a high number of national stakeholders in framing risks, while Malta was very selective (European Commission, 2017a). As for the methodology, Denmark used quantitative data, while Austria employed qualitative and historic data, and Sweden applied a mix of the two (ibid.). In addition, the countries' different governance influenced the way the national risk assessments were formulated (Bossong and Hegemann, 2016).

Although the European Commission was aware of these terminological, institutional, legal, and cultural challenges (European Commission, 2010, p. 33) and Article 6 of the 2013 decision introduced an obligation to deliver national risk assessments, no initiative was taken to really cope with these challenges. The European Commission continued to provide information about risk prevention through Staff Working Documents, which are a low-level type of communication between the European Commission and the member states. This can be interpreted as a sign of the impossibility of overcoming the challenges mentioned above and of making risk assessment part of a standardization process.

An important aspect of the OMC is inclusiveness. Several times in the guidelines, the European Commission called for the involvement of 'public authorities, research and businesses, non-governmental organizations and the wider general public' (European Commission, 2010, p. 12) to reach a common and shared understanding of risks and to formulate 'objective and impartial' risk assessments (ibid., p. 13).

Civil protection is another important component of Article 196. The EU describes civil protection as 'governmental aid delivered in preparation for or immediate aftermath of a disaster in Europe and worldwide' (European Commission, 2019) by the participating states to the EU Civil Protection Mechanism. The mechanism was established in 2001 (Council, 2001), with the goal 'to strengthen cooperation between Participating States in the field of civil protection,

with a view to improving prevention, preparedness and response to disasters' (European Commission, 2019). The mechanism is a very peculiar framework: it can be described as a *sui generis* agency, which is placed under the EU Humanitarian Aid and Civil Protection Department (ECHO). Just as several EU agencies, such as the European Medicine Agency (EMA) or the European Food Safety Authority (EFSA), the mechanism has scientific and technical tasks within a defined area of expertise, such as civil protection. Like these agencies, the mechanism has a functional, administrative, and financial capacity and an internal hierarchy responding to the European Commission (Levi-Faur, 2011, p. 813). The mechanism, however, does not fulfil quasi-regulatory or regulatory tasks (Randall, 2006) as other European agencies do. In addition, its tasks cannot be described in terms of 'deciding on individual cases, preparing individual cases for the Commission, issuing guidelines on national application of EU law, preparing new/changing EU legislation and involvement in national agencies' handling of individual cases' (Egeberg and Trondal, 2011, p. 879). The mechanism seeks to foster a common understanding of civil protection procedures, capabilities, and responses to crises through centralized coordination from Brussels. Its components have been defined and redefined through Council and Commission decisions (Morsut, 2014) and non-binding legislative acts that have contributed to expanding the mechanism's tasks from those strictly related to response to crises to a wider range of tasks, following the crisis management circle (Gestri, 2012): the *Emergency Response Coordination Centre* (ERCC) with its *Common Emergency Communication and Information System* (CECIS); the *European Emergency Response Capacity* (EERC); and the *Union Civil Protection Mechanism Training Programme*. The mechanism has received about 300 requests for assistance, since 2001. It has intervened in some of the most devastating disasters the world has faced in recent years, such as the earthquake in Haiti (2010), the tsunami in Japan (2011), typhoon Haiyan that hit the Philippines (2013), the Ebola outbreak (2014), the conflict in Ukraine (2014), the earthquake in Nepal (2015), the refugee crisis, and floods and forest fires in Europe (European Union, 2018c).

Any country in the world can activate the mechanism, by sending a request to the ERCC. The ERCC was officially established by the 2013 decision (European Parliament and Council, 2013), followed by the 2014 European Commission decision, with the aim to 'ensure more effective, efficient and coherent disaster management in the years to come' (European Commission, 2014a, p. 17). This aim mirrors the wording of Article 196. In addition, effectiveness, efficiency, and coherence are important aspects of standardization. The ERCC is the coordination hub of the mechanism, monitoring hazards worldwide and operating 24/7. The response to a crisis is channelled by the ERCC, which sends national and EU experts, national and EU civil protection teams, and national modules, depending on the request of the affected country (ECHO, 2019b). All these assets belong to the participating states, which put at the EU's disposal their capacities inside the EERC, also called the voluntary pool. Elements of standardization are present in the modules, such as:

- HUSAR – Heavy Urban Search and Rescue
- WP – Water Purification
- HCP – High Capacity Water Pumping
- FHOS – Field Hospital
- FFFP – Aerial Forest Fire Fighting module using Planes.

The European Commission defines the quality requirements of these modules, based on established international standards (European Parliament and Council, 2013). In this way, the European Commission fosters better planning – since having one institution with the overview of the modules avoids duplication – and coordination – since these capabilities are channelled through the ERCC. Another component that enhances a common understanding of civil protection is the Training Programme, consisting of training courses, simulation exercises, and exchange of experts among participating states (ECHO, 2018). The exchange of practices, knowledge, lessons learned, the simulation of complex crisis on the ground, and the attendance of courses all stimulate the fostering of a common European civil protection language. After the Interim Evaluation of the Mechanism in 2017, the Commission put forward a proposal to amend the 2013 legislation (European Commission, 2017b) in two complementary issues: (1) establishment of the EU's civil protection's own capabilities (so-called RescEU), by renting or leasing them from the participating states; and (2) reinforcement of the EERC, through coverage of 75 per cent of the costs during the response phase, which should incentivize the participating states in pre-committing their capabilities. This proposal was approved in March 2019 (European Parliament and Council, 2019).

Knowledge, best practices, and information dissemination among the participating states are reinforced by two EU networks: the Disaster Risk Management Knowledge Centre (DRMKC, 2019) and the European Civil Protection Knowledge Network. These networks then represent another form of soft standardization, can be described as non-hierarchical decision-making arenas (Jordan and Schout, 2006), and are more informal than the agencies, as participation is voluntary (Ahrne and Brunsson, 2011, p. 6; Levi-Faur, 2011). Both these networks aim to strengthen the efficiency of comprehensive EU disaster risk management, to build a common culture in risk management and civil protection.

Conclusion

A common approach to disaster risk management with, for instance, manageable and unified types of risk, a common understanding of civil protection, and standardized modules is a process that still is far from conclusion, but progress has been made since the launch of the common approach in 2009 and the establishment of the mechanism in 2001. The EU ambition to establish a comprehensive EU disaster risk management meets distinct limits established by the Treaties, by the complexity of the matter, and by the national contexts. As for the first case, the EU cannot set up requirements and rules for the member states on how

to govern disaster risk management following the same path as the Single Market. As for the second and third cases, the EU cannot underestimate the fact that risks are complex and multifaceted, with a socio-political component derived from national peculiarities.

The EU has chosen a process of negotiation and deliberation with its member states, mainly through the OMC. This process has led to certain results, such as an overview of national risk assessment from all the mechanism's participating states. If the EU continues on this path, constantly negotiating and deliberating on definitions, resources, and capabilities, it should ultimately increase the quality of the analyses on risks and disasters and of responses through the mechanism. The advantage of the EU over its member states is its ability to administer an amount of information and data that the member states do not have at their disposal if they do not participate in the EU initiatives. However, where the EU seems least successful is in the terminology about risks, risk management, and civil protection. A shared terminology is the first step for more standardized forms of risk management. For instance, a univocal understanding of risk assessment might pave the way to forms of standardization, which, as of today, are missing.

This chapter concludes by envisaging three main challenges within the EU disaster risk management policy. First, the EU should be aware that, within the initiatives undertaken, the possibility of simplification, and thus of missing crucial dimensions of risks, is always present. Second, as a consequence of simplification, the EU should avoid regarding different social, political, and cultural contexts as compatible. Third, the transferability of knowledge, best practices, and information from the EU to its member states requires that the EU has access to a vast amount of knowledge about local, regional, and national situations and is able to manage this knowledge for the benefit of all the member states. In this sense, the Disaster Risk Management Knowledge Centre (DRMKC, 2019) and the European Civil Protection Knowledge Network are two promising initiatives. This last challenge is where the EU has succeeded the most, by sharing knowledge and by seeking to frame a common and mutual understanding on disaster risk management, which needs to be consistent and accessible to the member states.

Notes

1 This chapter will follow the EU terminology for disaster risk management according to the official policy documents. For instance, the EU defines prevention as reducing the impact of natural and man-made disasters and making societies, critical infrastructures, and ecosystems more resilient.
2 The European Committee for Standardization (CEN) provides standards for most goods, systems and services; the European Committee for Electrotechnical Standardization (CENELEC) provides standards in the electro-technical field; the European Telecommunications Standards Institute (ETSI) provides standards in the field of electronic communications and ICT.
3 The ESS consists of three European Standardization Organizations (ESOs) – CEN, CENELEC and ETSI – and European stakeholders working inside the Single Market.

4 For instance, Regulation 178/2002 (European Union, 2002) represents the main regulatory source for the risk management functions required in food safety, while the REACH Regulation 1907/2006 (European Union, 2006) establishes a clear procedure for the registration, evaluation, authorization, and restriction of chemicals that can damage health. Regulation 765/2008 (European Union, 2008) describes the requirements for market surveillance authorities in performing risk identification in products.
5 The EU Civil Protection Mechanism is discussed later in the chapter. As of today, the Mechanism covers all the member states, in addition to Norway, Iceland, Liechtenstein, Serbia, Turkey and the Republic of North Macedonia for a total of 34 participating states. In 2011, there were 32 participating states (28 member states and the non-EU countries Norway, Iceland, Liechtenstein and the Republic of North Macedonia).

References

Ahrne, G. and Brunsson, N. (2011). Organization outside organizations: The significance of partial organization. *Organization*, 18, pp. 83–104.

Albrecht, J. and Arts, B. (2005). Climate policy convergence in Europe: An assessment based on national communications to the UNFCCC. *Journal of European Public Policy*, 12(5), pp. 885–902.

Andenas, M. and Baasch Andersen, C. (eds) (2011). *Theory and practice of harmonisation*. Cheltenham: Edward Elgar Publishing Ltd.

Beck, U. (1992). *The risk society: Toward a new modernity*. London: Sage.

Black, J. (2001). Decentring regulation: understanding the role of regulation and self-regulation in a 'post-regulatory' world. *Current Legal Problems*, 54, pp. 103–147.

Boin, A. and Ekengren, M. (2009). Preparing for the world risk society: Towards a new security paradigm for the European Union. *Journal of Contingencies and Crisis Management*, 17(4), pp. 285–294.

Borras, S. and Jacobsson, K. (2004). The open method of coordination and new governance patterns in the EU. *Journal of European Public Policy*, 11(2), pp. 185–208.

Bossong, R. and Hegemann, H. (2016). EU internal security governance and national risk assessments: Towards a common technocratic model? *European Politics and Society*, 17(2), pp. 226–241.

Council (2000). *Presidency conclusions*. Lisbon European Council, 23 and 24 March 2000. Available at: www.europarl.europa.eu/summits/lis1_en.htm (accessed 3 September 2019).

Council (2001). *Council Decision 2001/792/EC of 23 October 2001 establishing a Community mechanism to facilitate reinforced cooperation in civil protection assistance interventions.* Brussels: EC.

Council (2009). *Council conclusions on a community framework on disaster prevention within the EU*, 2979th Justice and Home Affairs Council meeting. Brussels, 30.11.2009.

Council (2011). *Council conclusions on further developing risk assessment for disaster management within the European Union*, 3081st Justice and Home Affairs Council meeting. Brussels, 11.4.2011.

DRMKC (2019). *Disaster Risk Management Knowledge Centre*. [online] Available at: https://drmkc.jrc.ec.europa.eu/ (accessed 25 March 2019).

Eberlein, B. and Dieter, K. (2004). New governance in the European Union: A theoretical perspective. *Journal of Common Market Studies*, 42(1), pp. 121–142.

Eberlein, B. and Grande, E. (2005). Beyond delegation: Transnational regulatory regimes and the EU regulatory state. *Journal of European Public Policy*, 12(1), pp. 89–112.

ECHO (2018). EU conducts its biggest exercise Civil Protection Mechanism exercise. [online]. Available at: http://ec.europa.eu/echo/news/eu-conducts-its-biggest-civil-protection-mechanism-exercise_en (accessed 16 October 2018).

ECHO (2019a). *ECHO factsheet. European disaster risk management*. [online]. Available at: https://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/disaster_risk_management_en.pdf (accessed 17 June 2019).

ECHO (2019b). *ECHO factsheet. Emergency Response Coordination Centre (ERRC)*. [online]. Available at: https://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en (accessed 17 June 2019).

Egeberg, M. and Trondal, J. (2011). EU-level agencies: New executive centre formation or vehicles for national control? *Journal of European Public Policy*, 18(6), pp. 868–887.

Eurocodes (2018). About the UN Eurocodes. [online]. Available at: https://eurocodes.jrc.ec.europa.eu/showpage.php?id=1 (accessed 1 October 2018).

European Commission (2007). Directive 2007/60/EC of the European Parliament and of the Council of 23 October 2007 on the assessment and management of flood risks. Brussels: EU.

European Commission (2009). COM(2009) 82 final. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *A Community approach on the prevention of natural and man-made disasters*. Brussels: EU.

European Commission (2010). COM(2010) 1626 final. Risk assessment and mapping guideline for disaster management. Commission staff working paper. Brussels.

European Commission (2014a). COM(2014) 537 final. Report from the Commission to the European Parliament and the Council. *Annual Report on the European Union's Humanitarian Aid and Civil Protection Policies and their Implementation in 2013*. Brussels: EC.

European Commission (2014b). SWD(2014b) 134 final. Overview of natural and man-made risks in the EU. Commission staff working document. Brussels: EC.

European Commission (2017a). SWD(2017) 176 final. Overview of natural and man-made disaster risks the European Union may face. Commission staff working document. Brussels: EC.

European Commission (2017b). COM(2017) 773 final. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions. Strengthening EU disaster management: rescEU solidarity with responsibility. Brussels: EC.

European Commission (2019). Civil protection. [online]. Available at: https://ec.europa.eu/echo/what/civil-protection_en (accessed 17 June 2019).

European Parliament and Council (2013). Decision 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union civil protection mechanism. *Official Journal of the European Union*, L (347), 20.12.2013.

European Parliament and Council (2019). Decision (EU) 2019/420 of the European Parliament and of the Council of 13 March 2019 amending Decision No 1313/2013/EU on a Union civil protection mechanism. Available at: eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019D0420 (accessed 3 September 2019).

European Union (2002). Regulation 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety. *Official Journal of the European Communities.* Available at: eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002R0178 (accessed 3 September 2019).

European Union (2006). Regulation 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the registration, evaluation, authorisation and restriction of chemicals (REACH), establishing a European Chemicals Agency. Available at: eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:396:0001:0849:EN:PDF (accessed 3 September 2019).

European Union (2008). Regulation 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products. Available at: publications.europa.eu/en/publication-detail/-/publication/fdd70f57-7032-4121… (accessed 3 September 2019).

European Union (2016). Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at: eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (accessed 3 September 2019).

European Union (2018a). Regulations, directives and other acts. [online]. Available at: https://europa.eu/european-union/eu-law/legal-acts_en (accessed 1 October 2018).

European Union (2018b). Types of EU law. [online]. Available at: https://ec.europa.eu/info/law/law-making-process/types-eu-law_en (accessed 1 October 2018).

European Union (2018c). EU Civil Protection Mechanism. [online]. Available at: http://ec.europa.eu/echo/what/civil-protection/mechanism_en (accessed 1 October 2018).

European Union (2019). Environment: Overview of progress. [online]. Available at: http://ec.europa.eu/environment/water/flood_risk/overview.htm (accessed 25 March 2019).

Gestri, M. (2012). EU Disaster Response Law: Principles and instruments. In A. de Guttry, M. Gestri, and G. Venturini, eds. *International Disaster Response Law*. Berlin: Springer, pp. 105–128.

Gornitzka, A. (2005). Coordinating policies for a 'Europe of knowledge': Emerging practices of the "Open Method of Coordination" in education and research. Working Paper No. 16: 1–40, Centre for European Studies, University of Oslo.

Holzinger, K. and Knill, C. (2005). Causes and conditions of cross-national policy convergence. *Journal of European Public Policy*, 12(5), pp. 775–796.

ISO (2018). *31000:2018 Risk management – Guidelines*. Geneva: ISO.

Jacobsson, K. and Schmid, H. (2003). The European employment strategy at the crossroads: Contribution to the evaluation. In D. Foden and L. Magnusson, eds. *Five years' experience of the Luxembourg Employment Strategy*. Brussels: ETUI.

Jordan, A. and Schout, A. (2006). *The coordination of the European Union: Exploring the capacities of networked governance*. Oxford: Oxford University Press.

JRC (2019). Disaster risk management. [online]. Available at: https://ec.europa.eu/jrc/en/research-topic/disaster-risk-management (accessed 17 June 2019).

Knill, C. (2001). *The Europeanization of national administrations. Patterns of institutional change and persistence*. Cambridge: Cambridge University Press.

Knill, C. (2005). Introduction: Cross-national policy convergence: concepts, approaches and explanatory factors. *Journal of European Public Policy*, 2(5), pp. 764–774.

Levi-Faur, D. (2011). Regulatory networks and regulatory agencification: Towards a Single European Regulatory Space. *Journal of European Public Policy*, 18(6), pp. 810–829.

Luhmann, N. (2005). *Risk: A sociological theory*. New York: Aldine De Gruyter.

Morsut, C. (2014). The EU's Community Mechanism for Civil Protection: Analysing its development. *Journal of Contingencies and Crisis Management*, 22(3), pp. 143–149.

OECD (2009). *Innovation in country risk management*. Paris: Organisation for Economic Co-operation and Development.

Radaelli, M. C. (2003). The open method of coordination: A new governance architecture for the European Union? *Swedish Institute for European Policy Studies*, 3(1), pp. 1–65.

Randall, E. (2006). Not that soft or informal: A response to Eberlein and Grande's account of regulatory governance in the EU with special reference to the European Food Safety Authority (EFSA). *Journal of European Public Policy*, 13(3), pp. 402–419.

Ranke, U. (2015). *Natural disaster risk management*. Cham: Springer.

Renn, O. (2008). *Risk governance: Coping with uncertainty in a complex world*. London: Earthscan.

Rhinard, M., Ekengren, M. and Boin, A. (2006). The European Union's Emerging Protection Space: Next steps for research and practice. *European Integration*, 28(5), pp. 511–527.

Tercovich, G. (2018). A quest for legitimacy: The evolution of the EU in the humanitarian aid and crisis management field. In C. Morsut and D. Irrera, eds. *Security beyond the state. The EU in an age of transformation*. Leverkusen, Germany: Barbara Budrich Publishers, pp. 77–94.

UNISDR (United Nations International Strategy for Disaster Risk Reduction) (2016). Disaster risk reduction terminology. [online] Available at: www.unisdr.org/files/26462_8.annex2andacronyms.pdf (accessed 27 March 2019).

UNISDR (United Nations International Strategy for Disaster Risk Reduction) (2018). *United Nations Office for Disaster Risk Reduction* [online] Available at: www.unisdr.org/ (accessed 15 March 2019).

United Nations (2005). *Hyogo Framework for Action 2005–2015: Building the Resilience of Nations and Communities to Disasters*. Geneva: UNISDR.

United Nations (2015). *Sendai Framework for Disaster Risk Reduction 2015–2030*. Geneva: UNISDR.

Van den Brink, T. (2017). The impact of EU legislation on national legal systems: Towards a new approach to EU–member state relations. *Cambridge Yearbook of European Legal Studies*, 19, pp. 211–235.

Wildavsky, A. and Dake, K. (1990). Theories of risk perception: Who fears what and why? *Daedalus*, 119, pp. 41–60.

4 Standardization of disaster risk management

Challenges and opportunities

Henrik Tehler, Marcus Abrahamsson, Henrik Hassel and Peter Månsson

Introduction

The aim of the present chapter is to explore the role that standardization might play in situations where several actors, possibly with diverging interests, manage risk. Will an increased level of standardization lead to more effective risk management, by facilitating collaboration, or will it lead to less effectiveness, by hampering creativity and adaptation to risks?

Losses due to disasters are continuously increasing, and there seems to be a general agreement that more efforts need to be directed towards reducing the risk of future losses (UN, 2015). So-called 'all-hazards' and 'whole-of-society' approaches are crucial in this respect. They imply the involvement of many different actors, both public and private, and the consideration of a broad range of hazards that threaten what is considered valuable (OECD/G20, 2012; von Lubitz, Beakley, and Patricelli, 2008). Different countries use different terms to denote the processes implemented to achieve this: for example, 'country risk management' (OECD, 2009, 2011) or 'disaster risk management' (UNISDR, 2009; Lin and Abrahamsson, 2015). Although the terminology might differ, the key idea from a risk management perspective is the same: no single actor can manage the task by themselves, and no one is 'in charge' of all other actors. Cooperation is therefore the key to success.

When risk is managed in this type of multi-actor networks, the joint effort might suffer from various types of problems or challenges. Sometimes they are called 'deficits' (IRGC, 2017) or 'barriers' (Kramer, 2005) or are even referred to as 'fragmentation of processes' (Cedergren and Tehler, 2014; Rivera, Tehler, and Wamsler, 2015). No matter which term is used, they all indicate situations in which the overall collaboration and the management of risk are negatively affected in some way. One strategy commonly used to facilitate collaboration, regardless of whether the focus of the collaboration effort is risk-related or not, is standardization.

The chapter is organized as follows. First, we provide a brief description of disaster risk management (DRM) and why DRM is a suitable context to explore collaborative risk management. Additionally, we describe the Swedish system for DRM, which will be the basis from which most of the empirical data that we rely on originates. Second, we discuss what standardization of risk and effective risk management might mean in the present context. Then follow several

sections, each one addressing different themes relevant to the overall question. Finally, we end the chapter by offering some conclusions. The chapter is based on several empirical studies conducted during the past five years.

Effective disaster risk management?

Following a shift in attitudes concerning how to cope with natural hazards, the interest in DRM has increased during the past decades (UNISDR, 2009). Instead of focusing only on responding to disasters and providing relief to affected societies, increased attention is paid to how one can prevent and prepare for disasters *before* they happen, thus managing the *risk* of disasters rather than only their *consequences*. Although disasters due to natural hazards (e.g. hurricanes, floods, and earthquakes) affect millions of people every year, resulting in more than 50,000 fatalities on average (CRED, 2015), DRM is nowadays also focused on so-called man-made risks (OECD/G20, 2012). It is commonly defined as 'the systematic process of using administrative directives, organizations, and operational skills and capacities to implement strategies, policies and improved coping capacities in order to lessen the adverse impacts of hazards and the possibility of disaster' (UNISDR, 2009).

At the same time as the focus on risk management has increased, it has also become clear that the various hazards threatening our societies are interconnected, thus influencing each other. For example, critical infrastructures, such as electricity distribution systems and transport systems, are increasingly dependent on each other. Should one of these systems fail, it can quickly affect others, spreading the consequences of the initial failure over vast geographic areas and to other systems (Rinaldi, Peerenboom, and Kelly, 2001). Therefore, it is questionable whether traditional approaches to risk management, which often were designed based on single risks addressed one at a time (Hoyt and Liebenberg, 2011), are useful in an increasingly interconnected world.

The interconnectedness of hazards and risks affects both private companies, seeking to maximize shareholder value, and governments, trying to ensure the functioning of society and the safety and security of their citizens. In the corporate world,

> a paradigm shift has occurred regarding the way to view risk management. Instead of looking at risk management from a silo-based perspective, the trend is to take a holistic view of it. This holistic approach toward managing an organization's risk is commonly referred to as enterprise risk management (ERM).
>
> (Gordon, Loeb, and Tseng, 2009)[1]

A similar shift in perspective has taken place in governmental efforts to manage disaster risk, and nowadays many countries have implemented so-called 'all-hazards' and 'whole-of-society' approaches (OECD, 2009), which are similar to the ERM, with respect to the ambition to encourage a more holistic risk management approach.

Such holistic risk management approaches are examples of standards, in the sense that they establish a norm for something (see Juhl, Chapter 2, in this volume).

For example, the COSO framework is an important standard for ERM established by five private sector organizations (www.coso.org), and the EU guidelines for risk assessment (European Commission, 2010), which subsequently resulted in the first overview of natural and man-made risks in the EU (European Commission, 2014), constitute a standard for an important aspect of DRM. In addition, there are standards for risk management, emergency management capability assessment, business continuity, etc., issued by ISO (ISO, 2009, 2016), that are more or less commonly used in DRM. Moreover, there are also standards relevant to DRM in specific sectors such as the information technology sector (see Skotnes, Chapter 10, in this volume, for a more in-depth discussion of standardization in ICT systems). There are differences regarding which aspects the standards focus on and in terms of the level of detail. Therefore, they can sometimes coexist and be applied simultaneously.

A common view is that the implementation of standards for risk management, such as the ones described above, will lead to an increased ability to protect human lives, economic and environmental values, etc.; see, for example, OECD (2014) and European Commission (2015). However, there are very few empirical studies investigating whether such assumptions are true (Hoyt and Liebenberg, 2011; Rivera, Wamsler, and Tehler, 2017). To be effective means that an activity such as DRM produces the desired effect. The desired effect of DRM is 'to lessen the adverse impacts of hazards and the possibility of disaster' (UNISDR, 2009). Thus, if increased use of standards to support DRM work leads to a reduction of the consequences of disasters and/or to disasters being less frequent than otherwise, then it leads to more effective DRM. However, as noted by Rivera, Wamsler, and Tehler (2017), to evaluate whether specific ways of conducting risk management actually lead to such improvements is very difficult.

Notwithstanding these difficulties, the question of whether an increased level of standardization leads to more effective DRM is important, not least because of the considerable resources that are spent on DRM and the potentially huge losses that DRM aims at preventing or reducing. The following sections deal with that question and seek to clarify what 'an increased level of standardization' might mean in a DRM context. Moreover, we also discuss what evidence there is to support claims that increasing the level of standardization leads to more or less efficient DRM. The discussion is to a considerable extent based on studies conducted within the Swedish DRM system[2] during the past five years. The next section is devoted to describing that system.

The Swedish disaster risk management system

The word 'disaster' ('*katastrof*' in Swedish) is seldom used in the relevant Swedish legislation controlling much of the structure and activities aimed at avoiding or mitigating the effects of events threatening the life and health of the population, the functionality of society, or any other of the goals stipulated in the national security strategy (see Government Offices of Sweden, 2017). Instead, terms like 'crisis' ('*kris*') and 'extraordinary event' ('*extraordinär händelse*') are more often used. Notwithstanding these semantic differences, we

chose to use the term 'disaster risk management' here when focusing on activities aimed at reducing the occurrence and/or consequences of extraordinary events, crises, or disasters. Moreover, since our interest is disaster *risk* management, we chose to focus less on the ability to *respond to* various disasters but, instead, more on activities aimed at *preparing for* or *mitigating* such events.

According to Swedish legislation (SFS, 2006:544, SFS 2015:1052), all municipalities, county administrative boards (henceforth abbreviated to county boards), county councils,[3] and a number of selected national authorities have to carry out risk and vulnerability assessments (RVAs). Constituting the primary tool for identifying and analysing various events that might lead to disasters, the assessments have several purposes. They are, for example, supposed to be used as a basis for reducing the risks faced by the actor conducting the analysis (e.g. a local municipality or a county board), but they are also supposed to inform other actors and ultimately contribute to an overview of risks and vulnerabilities in Sweden (Abrahamsson and Tehler, 2013). The second of these objectives entails that results from RVAs that are carried out by individual entities (e.g. municipalities, county boards) will be used as input to a situational picture of the risks in the country as a whole. In this sense, municipal RVAs are collected and function as a basis for RVAs carried out by the county boards, which in turn will be collected and function as a basis for RVAs at the national level. The Swedish Civil Contingencies Agency (MSB) is supposed to enact a national picture of the risks and vulnerabilities that exist in Sweden. Conversely, MSB and county boards should provide feedback on the analyses they collect, as well as convey the results of their own analyses downwards in the system. This process is illustrated in Figure 4.1.

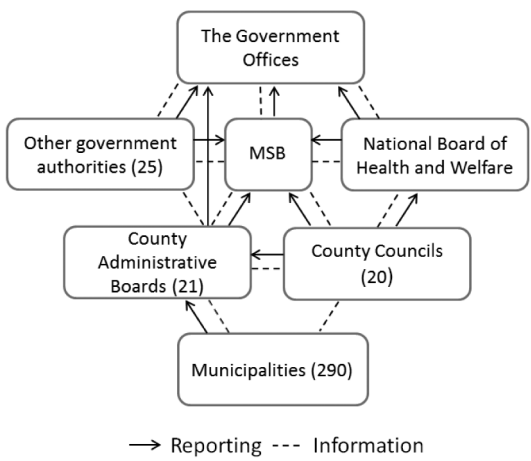

Figure 4.1 Illustration of the flow of risk information and RVA reports in Sweden.

Source: Adapted from MSB (2011).

Note

Numbers in brackets represent numbers of units of different types of stakeholders involved.

One could argue that the Swedish disaster risk management system is broader than is indicated in Figure 4.1. No private companies are, for example, included in Figure 4.1, and they can assume very important roles related to disaster risk management. Nevertheless, our focus, in our discussion of the standardization of disaster risk management, and in the empirical data we rely on, is on the public actors in Sweden. More comprehensive descriptions of the system are available in Abrahamsson and Tehler (2013) and Becker and Bynander (2017). In the next section, we question what an increased level of standardization might mean in the present context, and then we focus on the ability of the system to identify and analyse disaster risks.

What does standardization of disaster risk management mean?

Increasing the standardization of disaster risk management might mean many different things. As a point of departure for our discussion, we need to establish what a DRM system *does* in order to achieve its purpose. In line with previous research, we call it the *functions* of the DRM system (see Cedergren and Tehler, 2014; Rivera, Tehler, and Wamsler, 2015). A common model, which is in line with the ISO standard on risk management (ISO 31000), is that, in order to reduce the occurrence or consequences of events that might harm what is considered valuable, a DRM system needs to *identify* risks, *analyse* them, *make decisions* on risk-reducing measures, and *implement* as well as *monitor* the results of those decisions. There are other aspects of DRM that are important for achieving the long-term goals, such as learning from previous events. Nevertheless, here we restrict our attention to the basic risk management functions: identify -> analyse -> decide -> and implement.

One important reason for standardization being an interesting topic in the present DRM context is that the functions referred to above need to permeate the whole DRM system (i.e. they need to cross administrative and functional boundaries). However, as noted above, risk management has often been implemented in a silo fashion, with one actor focusing on one or a limited number of types of risks. An implicit assumption in such arrangements has been that it is possible to split up the responsibility for risk management into pieces that can be managed independently of each other but still result in a desirable overall outcome. The assumption might have been true when there was less interaction between hazards and the different functional sectors of a society (e.g. electricity distribution and transport), but it is becoming less and less valid.

It is becoming increasingly clear that DRM is a *collective* effort. An important question is whether an increased level of standardization in terms of DRM might help various actors to *collectively* identify risks, analyse them, etc. To that end, we might also use the functions of risk management when clarifying what standardization might mean in the present context. For example, we might standardize *how* we identify risk, *how* we analyse risk, *how* we describe risk, *how* we evaluate and make decisions, and implement measures.

Here, we focus on *how risk is described*, and we discuss standardization with respect to such descriptions. Thus, to standardize in the present context means to establish a norm for how risk should be described. There are many different aspects of such a norm; here, we focus on a few important ones, basing our discussion on five studies focusing on the Swedish DRM system. Although each study has its specific focus, much of the material is still relevant here.

Study 1

In 2015, we published a study (Månsson *et al.,* 2015) focusing on *uncommon categorization* (UC), that is, disparities within the Swedish DRM system with respect to how similar terms and information are interpreted, coded, and categorized by different actors (Kramer, 2005). We concluded that UC 'is a widespread phenomenon in the Swedish disaster risk management system. It is prevalent at all administrative levels, and in all aspects analyzed' (Månsson *et al.,* 2015). The study was based on interviews with professionals working in the Swedish DRM system and on analyses of risk and vulnerability assessments produced within the system. We studied, for example, how risk was described in the documents and found significant variations. Some documents did not contain any estimations of the likelihood or potential consequences of risk scenarios. Others contained risk descriptions using risk matrices of the type described in Jørgensen and Lindøe (Chapter 13, in this volume), and yet others employed frequencies/probabilities in combination with detailed descriptions of consequences. There are several more studies arriving at similar conclusions regarding how information concerning risks and vulnerabilities is described. See, for example, Abrahamsson and Tehler (2013), Tehler, Brehmer, and Jensen (2012), Lin and Abrahamsson (2015), and Rivera, Tehler, and Wamsler (2015).

An interesting question related to the focus of the present chapter is whether the considerable extent of UC in the Swedish DRM system causes the system to be more inefficient than it otherwise would be. Expressed differently: would an increased level of standardization, with respect to how risk is described in the Swedish DRM system, lead to less-adverse impacts of hazards and/or a reduced likelihood of disasters?

Neither our 2015 study nor the other studies referred to above could answer such questions, the reason being that it was a descriptive study, relying on interviews and documents produced in the Swedish DRM system. Although we investigated the development of UC in terms of its extent and character between the years of 2010 and 2014, we had no way of studying its impact on the effectiveness of DRM. Nonetheless, we did interview people working with risk and vulnerability assessments and asked their opinions regarding what was effective and what was not. However, opinions and perceptions are easily biased when questions such as the one above are asked. Moreover, the answers that we received concerning the effect of standardization were ambiguous. Some interviewees warned about the effect of standardizing too much, as it could lead to a loss of ownership and motivation and thus reduce the quality of assessments,

while others claimed that standardization was necessary in order to facilitate the integration of several sources of information in multi-actor risk assessment processes (Månsson *et al.,* 2015).

Thus, the studies we have referred to so far would not be of much use if asked to provide advice on whether to increase or decrease the level of standardization in practice. It was also clear that answering such questions, by studying the direct relationship between levels of standardization and the occurrence of and outcome of disastrous events in Sweden (and elsewhere), would be challenging; see, for example, Rivera, Wamsler, and Tehler (2017). For example, assuming that we were able to find a sufficient number of municipalities or other actors that could participate in such a study, it would be very difficult to control for all confounding variables that might influence the outcome, for example, changes in term of exposure to risk.

Therefore, we decided to measure the relationship between the level of standardization, in terms of how risk is described, and some intermediate variables that presumably have an influence on the occurrence and consequences of adverse events. We chose to focus on how different degrees and types of standardization influenced how useful the risk descriptions were perceived to be. By focusing on perceived usefulness, we avoided the difficulties in measuring the relationship between risk descriptions and outcomes, in terms of level of consequences. Although highly useful risk assessments are no guarantee for a favourable outcome, it is nevertheless a reasonable starting point, given how most models of risk management (e.g. the ISO model) are structured. In such models, risk descriptions (e.g. in the form of a risk assessment) are used as a basis for decisions regarding whether one should invest in risk-reducing measures – and which ones in that case. Supporting decision-making is therefore one of the most important purposes of risk assessments.

In trying to determine what makes a risk assessment useful in the present context, we wanted to have control over potentially confounding variables. Therefore, we used experiments to study the usefulness of different ways of presenting risk assessments. The participants in the experiments, both students and professionals, were shown different risk assessments and asked questions regarding them. Although the questions differed somewhat in the experiments, they all aimed at capturing some aspects of what usefulness might mean in the present context. The following sections describe some of the experimental studies that are relevant for the discussion on standardization of risk.

How to describe and communicate risk

Selecting how to describe and communicate risk is not easy. But the choice might be easier if the purpose of describing and communicating risk is made clear. More specifically, there seems to be a difference, depending on whether one aims at describing and communicating risk to the public or if the target audience are experts. Much of the research in risk communication has focused on how experts should communicate with the public (see e.g. Fischhoff, 1995) and

less on how experts should communicate with decision-makers or other experts (Thompson and Bloom, 2000; Bier, 2001).

The focus of the present chapter is on risk management in DRM systems and not on communication to the public. Even if one restricts attention to professional communication of risk, for example, expert-to-expert or expert-to-decision-maker, there are many different suggestions on how to describe and communicate risk. Some of them focus on specific conditions such as augmented stress during emergency response (Yu, Lejarraga, and Gonzalez, 2012), while others focus on specific contexts, such as the energy sector (Colli *et al.,* 2009; Colli, Serbanescu, and Ale, 2009).

Communication of risk within DRM systems is the focus of interest here. But, as described at the beginning of the chapter, modern DRM usually implements 'all-hazards' and 'whole-of-society' approaches, and therefore the risk problems often become general in nature. From a standardization perspective, one can distinguish two important aspects that influence how one should communicate risk in such a context. First, it is a question of whether one should establish a common standard for how to describe and communicate risk in a DRM system at all. Second, if a common standard is desired, what should it look like? Our initial experiments were aimed at contributing to answering the second question, and the later experiments (described in the next section) were designed to focus on the first.

Study 2

In 2015, we published a study intended to contribute to answering the second question (Lin *et al.,* 2015). We focused on what makes descriptions of risk be perceived as useful as a basis for making decisions. We defined perceived usefulness as 'the degree to which a person believes that a specific risk description would enhance the basis for decision-making' (ibid.). The perceived usefulness was thus not directly related to a decision per se but, rather, to the process of constructing the basis for a decision. An implicit assumption was that the perceived usefulness of a risk description is related to its actual usefulness as determined by the extent to which the actual decisions made are successful.

The study was a collaboration with the county board of Scania (the southernmost region in Sweden). Thirty-three local municipal risk and vulnerability assessments (RVA documents) produced in the region in 2012 were analysed in terms of six variables: (1) whether the documents contained scenario descriptions; (2) whether the documents contained information on how the scenarios were selected; (3) how the uncertainty regarding the occurrence of the scenarios was described; (4) whether the documents contained background information regarding the likelihood assessments; (5) how the consequences of the scenarios were described; and (6) whether the documents contained background information regarding the consequence assessments. The documents were then ranked by professionals based on their perceived usefulness for decision-making.

An analysis was then conducted to identify correlations between the overall ranking of the usefulness of the documents and each of the variables. The idea was thus to identify what it is that makes a risk description useful. We concluded that the way the likelihood and consequences of scenarios are described influences the perceived usefulness. More precisely, documents involving quantitative expressions, for example, describing how many houses would be flooded in a specific scenario, were perceived to be more useful than those lacking such descriptions. In addition, including background information in the estimates of likelihood in a risk description positively influences its perceived usefulness.

Thus, the results from the study suggested that, if one should standardize the way risk is communicated in DRM systems, it is probably a good idea to select a way that allows quantitative descriptions[4] of how likely various events are judged to be and the consequences of them. Moreover, a standard of communication that also facilitates the communication of background information (to the judgements) is desirable. This advice assumes that by standardizing one aims to reduce long-term losses, and it also assumes that there is a correlation between the reduction of long-term losses and the perceived usefulness of the risk descriptions. Admittedly, the advice is rather vague (e.g. it is not clear what 'probably a good idea …' means), and there are some strong assumptions with limited evidence to back up the premise associated with them. Nevertheless, we believed the study was a step in the right direction, that is to use empirical data to support design propositions of the type 'If you want to achieve X in context Y, then you should do something like Z'. X would, in our case, correspond to a reduction of long-term losses, Y would be the DRM context, and Z would be a description of how to standardize the way risks are described in that context. Developing such design propositions is common in other fields (see e.g. Romme, 2003; Denyer, Tranfield, and Van Aken, 2008; Kuechler and Vaishnavi, 2008) but not in the area of disaster risk management.

Study 3

Building on our first experimental study ('Study 2' above), we designed a second one, aimed at providing stronger evidence regarding how important different ways of presenting risk were in order to make the descriptions useful in a DRM system. In the second experimental study, we created a number of hypothetical risk descriptions that differed with respect to how risk was described. The benefit of using hypothetical risk descriptions compared to using real ones (as in Study 2) was that it increased the internal validity of the study, making it easier to isolate the effect of changing the way risk was described. We ran a series of experiments, in which both students and professionals participated. The results from the experiments were in line with the findings of the first study: the participants rated risk descriptions that contained quantitative judgements of the likelihood and consequences of various scenarios as more useful than those that only contained qualitative ones (Lin *et al.,* 2017). Thus, our two studies suggested that using quantitative descriptions of uncertainty and consequences is beneficial to the usefulness of a risk description.

However, one should be careful when interpreting this advice. First of all, the 'quantitative descriptions' we used in our experiments were rather simple. They consisted of statements of the type 'If scenario X occurs, 200 houses will be flooded' and 'Scenario X is judged to occur once every 50 years'. Thus, it is not certain that more complex quantitative ways of describing risk, for example FN-curves or individual risk profiles (see e.g. Johansen and Rausand, 2014) will be perceived as equally useful. Presumably, the subjects' prior knowledge of risk assessment methodologies will play a more decisive role when judging the usefulness of such descriptions than it did in our experiment (ibid.).

Nevertheless, the results from both the field studies and the experiments referred to here are conclusive enough to suggest that *simple* quantitative descriptions of risk (likelihood and consequences of scenarios), in combination with supporting background information, are, in general, perceived as more useful as a basis for decision-making than descriptions lacking quantitative components.

The problem of combining risk information

The experiments involving real risk and vulnerability assessments (Lin *et al.,* 2015) and hypothetical risk descriptions (Lin *et al.,* 2017) gave us an increased understanding of how a person using a *single* risk assessment might perceive their usefulness. But our interviews with professionals (Månsson *et al.,* 2015) revealed that the main benefit of introducing more standardization, with respect to how risk is described, might come from the fact that it then might be easier to *combine several* risk assessments. Although it might not be the main traditional role of a risk assessment (which is to support decision-making), one important role in a multi-stakeholder, all-hazards DRM system is to support *other* risk assessments. For example, in order to produce the national risk assessment in Sweden, the Swedish Civil Contingencies Agency uses risk assessments produced by other national and regional authorities. They use those documents to obtain information about, for example, various scenarios and their estimated consequences. Thus, a modern DRM system is more like several supply chains of risk information, rather than a group of isolated actors that only produce or use information. This also means that the ability to combine risk information from various sources becomes more important and, as noted by some of the interviewees referred to above, standardization might facilitate the work.

Study 4

To test this, we designed a series of experiments, in which we used the same type of procedures that we employed in Study 3; that is, we created hypothetical descriptions of risk and tested how useful they were perceived to be. However, this time we were interested in investigating the extent to which several risk descriptions were useful *in combination*. We designed an experiment that allowed us to study the perceived usefulness of pairs of risk descriptions. If

increasing the standardization in terms of how risk is described made it easier to combine risk information from different sources (different risk assessments), then the participants in the experiments would perceive combinations of two risk assessments where risk is described *in the same way* (hereafter termed pure combinations) as more useful than a combination of two risk assessments using *different ways of describing risk* (hereafter termed mixed combinations). The procedure we used in the experiments is illustrated in Figure 4.2. There, the two risk descriptions shown to the participants are illustrated (A and B), together with the three types of risk descriptions employed in the experiments.

A participant could, for example, be shown one qualitative risk description (A-1), in combination with a quantitative one (B-3). This is an example of a *mixed* combination. An example of a *pure* combination is when the participants were shown one qualitative ranking description (A-2), in combination with another qualitative ranking description (B-2).

Our initial experiments involved 27 students from the Faculty of Engineering at Lund University (for details regarding the experiment, see Månsson and Tehler, 2016). The students, henceforth referred to as 'LTH students', were shown hypothetical flood risk assessments for two local municipalities. They were asked to assume the role of an official at a regional county administrative board. In that role, they were asked to compare the assessments provided by the two local municipalities, with respect to the likelihood and consequences of the flood scenarios, and assess the overall, regional risk, on this basis. To this end, they were asked a number of questions. The two most important ones for the discussion here asked the participants to indicate (on a 7-level Likert-type scale) the extent to which (1) 'It is easy to understand which of the municipalities faces the greatest risk'; and (2) 'The description of the scenario and adhering risk assessments are useful as a basis for decisions on risk-reducing measures in the area concerned (municipalities 1 and 2).'

The results from the experiments indicated that mixed combinations of risk descriptions were perceived as less useful than their pure counterparts, both with respect to the task of using them as a basis for decision-making and as a basis for judging where the risk was the greatest. The general pattern observed in the previous experiments, i.e. that quantitative descriptions were perceived more useful than qualitative, were also present in this experiment. Thus, the results can be seen as a support for standardization, in terms of how one describes risk

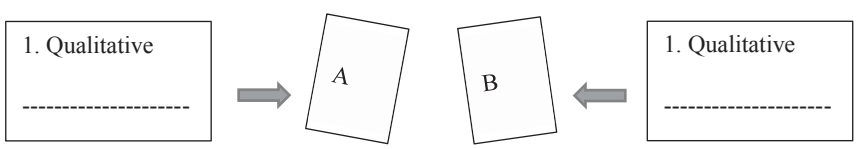

Figure 4.2 Illustration of the experiment. Two risk descriptions were shown to the participants (A and B). The descriptions were of three types, qualitative, qualitative ranking, or quantitative.

(to avoid the mixed situations from the experiments). Moreover, they also suggest that one should try to include quantitative descriptions of risk, where it is possible.

Study 5

Although the results from Study 4 were clear, we were concerned with the potential bias of using only engineering students as participants. In particular, we thought that the LTH students' mathematical training might skew the results in favour of pure quantitative descriptions. Numerical ability has previously been shown to influence people's judgements and decisions in risk contexts (Peters *et al.,* 2006; Reyna *et al.,* 2009), and the students in our initial experiments were probably not representative, in terms of numeracy, of the professionals working in the Swedish DRM system. Therefore, we wanted to find another group to involve in the study.

The risk management programme at Mid Sweden University (MIUN) approaches risk from a sociological perspective. Students from that programme were thus deemed to have a suitable profile to complement the engineering students. We ran exactly the same experiment as previously but, instead of LTH students, we used MIUN students. The results were surprisingly similar. More precisely, the relative rankings of the usefulness of the different combinations of risk descriptions were almost identical. Thus, similar to the LTH students, the MIUN students thought that the quantitative risk descriptions were more useful than their qualitative counterparts, albeit the differences were not as large as for the LTH students. However, the most important conclusion for the discussion here is that both student groups perceived the pure combinations of risk descriptions as more useful than the mixed ones.

The final aspect we wanted to investigate in our experiments was whether the inclusion of background information in the risk descriptions (see e.g. Aven, 2016) would alter the conclusions arrived at so far. Background information can be seen as a type of narrative evidence, explaining the assumptions and methods employed in generating the description of risk. Previous research had shown that narrative evidence is most influential when people find it difficult to understand quantitative probability estimates or in cases when stated likelihoods are very uncertain (Dieckmann, Slovic, and Peters, 2009; Dieckmann, Mauro, and Slovic, 2010; Betsch *et al.,* 2015). Therefore, we ran exactly the same experiment again for both groups of students (the participants were different), but we also included a short narrative, providing background information regarding the risk descriptions.

Thus, the present study involved two different experiments (with or without narrative evidence) with two different groups (LTH students and MIUN students). There were 127 participants, 53 with an engineering background and 74 with a sociological background (see Månsson, Abrahamsson, and Tehler, 2017, for details). As stated above, the results show that pure combinations of risk descriptions were perceived as more useful than their mixed counterparts. The

result applies when the risk descriptions are used both as a basis for decisions and for comparing risk levels. But mixing different types of risk descriptions was particularly negative when focusing on comparing risk levels. Moreover, we also found that the inclusion of background information enhanced the usefulness of almost all combinations of risk descriptions. Aside from clarifying ambiguous qualitative estimates (e.g. likely and severe), the background information can also compensate for the challenge of combining different types of risk descriptions (i.e. qualitative, semi-quantitative, and quantitative) and thus enhance the possibilities of aggregating information from multiple stakeholders with heterogeneous ways of presenting risks.

Seen in isolation, the results from the experiments provide support for a higher level of standardization of risk descriptions, that is, the way risk is communicated, in DRM systems than is currently implemented in the Swedish one. This conclusion is in line with the ambition expressed in recent reports by the European Commission (2010) and various EU member states, for example Sweden (MSB, 2016) and the Netherlands (Ministry of Security and Justice, 2014).

Discussion

The issue of whether or not to increase the level of standardization in this context is not as easy as it might appear when focusing on the results from the experiments referred to above. First of all, the experiments only tested one variable that might potentially influence how effective a DRM system is, that is, the perceived usefulness of risk descriptions. However, there were indications from the interviews that increasing standardization might lower the motivation of some actors to conduct risk assessments. The influence of increased standardization on the motivation to conduct risk assessments was not tested in the experiments and therefore we do not know the extent of the influence between the variables. It is possible that increasing the level of standardization will result in more useful risk descriptions but that the effect is counter-balanced by the fact that it decreases the motivation to conduct risk assessments. This might, in turn, make the resulting risk descriptions less rather than more useful.

Figure 4.3 illustrates the possible relationships between variables. The dashed arrows represent potential relationships that have not been investigated in the experiments.

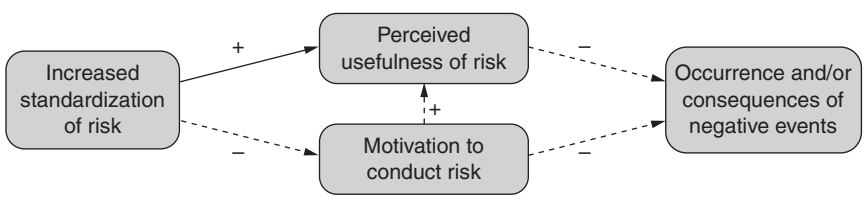

Figure 4.3 Possible relationships between variables.

In addition, the key issue from a practical perspective is the extent to which increased standardization will ultimately lead to a reduction in the occurrences and/or consequences of the events one is trying to prevent or mitigate the effect of. It was not investigated in the experiments, but it is an implicit assumption that increasing the perceived usefulness of risk descriptions would increase their value as a basis for decision-making, leading to more well-balanced decisions and ultimately to a reduction in the occurrence and/or the consequences of negative events. However, a similar relationship might be true for the motivation to conduct risk assessments and the occurrence and/or consequences of various events. For example, decreasing the motivation to conduct risk assessments might lead to an increased occurrence of negative events, due to the fact that people stop caring about risk issues and do not contribute to the risk management work (see dashed arrows in Figure 4.3).

Thus, turning the experimental evidence into concrete advice on how to act in practice is far from easy. One reason for this has been illustrated above. The experiment can only investigate the relationship between a limited number of variables, and practical problems might involve numerous important variables, influencing each other in complex ways. Thus, the reduction in scope and complexity, when investigating problems in real DRM systems using experiments, might make the results less relevant to the problems that motivated the experiments in the first place. Nevertheless, the opposite might be said about conducting field studies. Admittedly, the full complexity of the problem context might make a field study highly relevant, but it might also hinder the researcher's ability to draw conclusions regarding the effect of potential interventions, such as increased standardization. It might simply be impossible to know the reasons for an observed effect (or the absence of such effects). More specifically, it can be difficult to determine whether the effect (or absence of effect) was caused by the intervention in question or was due to other factors. Therefore, if the aim is to supply professionals with advice of the type, 'If you would like to achieve A in context B, then you should do something like C', it is probably a good idea to combine field studies with experiments, trying to leverage the benefits of both types of studies, while minimizing the drawbacks. However, as argued by Falk and Heckman (2009), 'The issue of realism, however, is not a distinctive feature of lab versus field data. The real issue is determining the best way to isolate the causal effect of interest.' Thus, the best way might sometimes be to use field studies and sometimes to use laboratory experiments.

Conclusion

The empirical basis for normative suggestions on how one should communicate risk in DRM systems is limited. Nevertheless, the experiments referred to in this chapter indicate that standardization in terms of using *simple* quantitative risk descriptions, and including background information, is preferred if one wants to increase the usefulness of the descriptions. More specifically, an increased standardization of the way risk is described in DRM systems would probably

facilitate comparisons (e.g. between local municipalities) and aggregation of risk information (e.g. from local municipalities to the regional level). But a prudent approach for implementing such advice is recommended. One should, for example, be aware that standardization could result in unintended side effects, and therefore any effort to increase standardization should be closely monitored to make sure that the positive effects outweigh the negative ones. Participatory and deliberative approaches, where the actors that are supposed to abide by standards have the chance to influence their contents, might also be a way to ensure that ownership and motivation are retained, while increasing the chance of combining multiple risk descriptions in support of societal safety.

Notes

1 Enterprise risk management (ERM) has also been called holistic risk management and integrated risk management.
2 Similar to Rivera, Wamsler, and Tehler (2017), we use the term 'DRM system' to denote 'the actual organisations, rules, regulations, technical systems, etc., used to implement DRM. Thus, the DRM system encompasses the stakeholders that perform related DRM activities.'
3 A county board is responsible for coordinating the development of the county in line with goals set by the government. This embraces a vast and varied number of policy areas, including disaster risk management. In each county there is also a county council, which principally is responsible for the public health care system.
4 Here 'quantitative' refers to an expression of the likelihood of various events, using probabilities or frequencies (e.g. once every 10 years); 'qualitative' refers to the use of statements such as 'Event X is unlikely' or 'The consequences of event X are estimated to be severe'.

References

Abrahamsson, M. and Tehler, H. (2013). Evaluating risk and vulnerability assessments: A study of the regional level in Sweden. *International Journal of Emergency Management*, 9, pp. 76–92.

Aven, T. (2016). On the difference between risk as seen from the perspectives of the analysts and management. *Journal of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering*, 2, 031002-031002-7.

Becker, P. and Bynander, F. (2017). The system for crisis management in Sweden: Collaborative, conformist, contradictory. In C. N. Madu and C.-H. Kuei, eds. *Handbook of disaster risk reduction and management.* Singapore: World Scientific Press & Imperial College Press.

Betsch, C., Haase, N., Renkewitz, F., and Schmid, P. (2015). The narrative bias revisited: What drives the biasing influence of narrative information on risk perceptions? *Judgement and Decision Making*, 10, pp. 241–264.

Bier, V. M. (2001). On the state of the art: Risk communication to decision-makers. *Reliability Engineering & System Safety*, 71, pp. 151–157.

Cedergren, A. and Tehler, H. (2014). Studying risk governance using a design perspective. *Safety Science*, 68, pp. 89–98.

Colli, A., Serbanescu, D., and Ale, B. J. M. (2009). Indicators to compare risk expressions, grouping, and relative ranking of risk for energy systems: Application with some accidental events from fossil fuels. *Safety Science*, 47, pp. 591–607.

Colli, A., Vetere Arellano, A. L., Kirchsteiger, C., and Ale, B. J. M. (2009). Risk characterisation indicators for risk comparison in the energy sector. *Safety Science*, 47, pp. 59–77.

CRED (2015). *The human cost of natural disasters 2015: A global perspective*. Brussels: Centre for Research on the Epidemiology of Disasters (CRED).

Denyer, D., Tranfield, D., and Van Aken, J. E. (2008). Developing design propositions through research synthesis. *Organization Studies*, 29, pp. 393–413.

Dieckmann, N. F., Mauro, R., and Slovic, P. (2010). The effects of presenting imprecise probabilities in intelligence forecasts. *Risk Analysis*, 30, pp. 987–1001.

Dieckmann, N. F., Slovic, P., and Peters, E. M. (2009). The use of narrative evidence and explicit likelihood by decisionmakers varying in numeracy. *Risk Analysis*, 29, pp. 1473–1488.

European Commission (2010). SEC(2010) 1626 final. Risk assessment and mapping guidelines for disaster management. Commission Staff Working Paper. Brussels: EC.

European Commission (2014). SWD(2014) 134 final. Overview of natural and man-made disaster risks in the EU. Commission Staff Working Paper. Brussels, 8.4.2014.

European Commission (2015). (2015/C 261/03). Risk management capability assessment guidelines. Commission notice. Brussels: EC.

Falk, A. and Heckman, J. J. (2009). Lab experiments are a major source of knowledge in the social sciences. *Science*, 326, pp. 535–538.

Fischhoff, B. (1995). Risk perception and communication unplugged: Twenty years of process. *Risk Analysis*, 15, pp. 137–145.

Gordon, L. A., Loeb, M. P., and Tseng, C.-Y. (2009). Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy*, 28, pp. 301–327.

Government Offices of Sweden (2017). *National security strategy*. Stockholm: Prime Minister's Office.

Hoyt, R. E. and Liebenberg, A. P. (2011). The value of enterprise risk management. *Journal of Risk and Insurance*, 78, pp. 795–822.

IRGC (2017). *An introduction to the IRGC Risk Governance Framework*, revised version. Lausanne: EPFL International Risk Governance Center.

ISO (2009). *ISO 31000:2009 Risk management: Principles and guidelines.* Geneva: ISO.

ISO (2016). *ISO 22325:2016(E) Security and resilience — Emergency management: Guidelines for capability assessment.* Geneva: ISO.

Johansen, I. L. and Rausand, M. (2014). Foundations and choice of risk metrics. *Safety Science*, 62, pp. 386–399.

Kramer, R. M. (2005). A failure to communicate: 9/11 and the tragedy of the informational commons. *International Public Management Journal*, 8, pp. 397–416.

Kuechler, B. and Vaishnavi, V. (2008). On theory development in design science research: Anatomy of a research project. *European Journal of Information Systems*, 17, pp. 489–504.

Lin, L. and Abrahamsson, M. (2015). Communicational challenges in disaster risk management: Risk information sharing and stakeholder collaboration through risk and vulnerability assessments in Sweden. *Risk Management*, 17, 165–178.

Lin, L., Nilsson, A., Sjolin, J., Abrahamsson, M., and Tehler, H. (2015). On the perceived usefulness of risk descriptions for decision-making in disaster risk management. *Reliability Engineering & System Safety*, 142, pp. 48–55.

Lin, L., Rivera, C., Abrahamsson, M., and Tehler, H. (2017). Communicating risk in disaster risk management systems: Experimental evidence of the perceived usefulness of risk descriptions. *Journal of Risk Research*, 20, pp. 1534–1553.

Månsson, P., Abrahamsson, M., Hassel, H., and Tehler, H. (2015). On common terms with shared risks: Studying the communication of risk between local, regional and national authorities in Sweden. *International Journal of Disaster Risk Reduction*, 13, pp. 441–453.

Månsson, P., Abrahamsson, M., and Tehler, H. (2017). Aggregated risk: An experimental study on combining different ways of presenting risk information. *Journal of Risk Research*, 22, pp. 497–512..

Månsson, P. and Tehler, H. (2016). How form affects function: On the possibility of aggregating risk information. Paper presented at 13th International Conference on Probabilistic Safety Assessment and Management (PSAM13), Seoul, Korea, 2016.

Ministry of Security and Justice (2014). *Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherlands*. Den Haag: Ministry of Security and Justice.

MSB (2011). *Vägledning för Risk- och sårbarhetsanalyser*. Stockholm: Swedish Civil Contingencies Agency (MSB).

MSB (2016). *Nationell risk- och förmågebedömning 2016*. Stockholm: Swedish Civil Contingencies Agency (MSB).

OECD (2009). *Innovation in country risk management*. Paris: Organisation for Economic Co-operation and Development.

OECD (2011). *Future global shocks: Improving risk governance*. Paris: Organisation for Economic Co-operation and Development.

OECD (2014). *Recommendation of the Council on the Governance of Critical Risks: Meeting of the OECD Council at ministerial level*. Paris: Organisation for Economic Co-operation and Development.

OECD/G20 (2012). *Disaster risk assessment and risk financing: A G20/OECD methodological framework*. Paris: G20 and Organisation for Economic Co-operation and Development.

Peters, E., Västfjäll, D., Slovic, P., Mertz, C. K., Mazzocco, K., and Dickert, S. (2006). Numeracy and decision making. *Psychological Science*, 17, pp. 407–413.

Reyna, V. F., Nelson, W. L., Han, P. K., and Dieckmann, N. F. (2009). How numeracy influences risk comprehension and medical decision making. *Psychological Bulletin*, 135, pp. 943–973.

Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, pp. 11–25.

Rivera, C., Tehler, H., and Wamsler, C. (2015). Fragmentation in disaster risk management systems: A barrier for integrated planning. *International Journal of Disaster Risk Reduction*, 14, pp. 445–456.

Rivera, C., Wamsler, C., and Tehler, H. (2017). Evaluating the performance of disaster risk management systems: Is it possible? In C. N. Madu and C.-H. Kuei, eds. *Handbook of disaster risk reduction and management.* Singapore: World Scientific Press & Imperial College Press.

Romme, A. G. L. (2003). Making a difference: Organization as design. *Organization Science*, 14, pp. 558–573.

SFS 2006:544. *Lag om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap*. Stockholm: Justitiedepartementet.

SFS 2015:1052. *Förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap*. Stockholm: Justitiedepartementet.

Tehler, H., Brehmer, B., and Jensen, E. (2012). Designing societal safety: A study of the Swedish crisis management system. Paper presented at PSAM 11 & ESREL 2012, Helsinki.

Thompson, K. M. and Bloom, D. L. (2000). Communication of risk assessment information to risk managers. *Journal of Risk Research*, 3, pp. 333–352.

UN (2015). *Sendai framework for disaster risk reduction 2015–2030*. New York: United Nations.

UNISDR (2009). *UNISDR terminology on disaster risk reduction*. Geneva: United Nations International Strategy for Disaster Reduction.

Von Lubitz, D. K. J. E., Beakley, J. E., and Patricelli, F. (2008). 'All hazards approach' to disaster management: The role of information and knowledge management, Boyd's OODA Loop, and network-centricity. *Disasters*, 32, pp. 561–585.

Yu, M., Lejarraga, T., and Gonzalez, C. (2012). Context-specific, scenario-based risk scales. *Risk Analysis*, 32, pp. 2166–2181.

5 Explosive remnants in Swedish society

Standardization to visualize a complex risk picture

Fredrik Johnsson

Introduction

In this chapter, the strengths and weaknesses of varying degrees of standardization, where different risk dimensions are combined in a common risk picture, are analysed. Explosive remnant remediation involves the simultaneous management of different risk dimensions and the coordination of multiple stakeholders. Does the implementation of an agency-wide approach also require standardization?

In Sweden, defence cuts have given rise to the release of former military areas of land no longer needed for military purposes. These areas are often contaminated with explosive remnants, such as unexploded ordnance on former shooting ranges and surplus ammunition dumped in lakes and rivers. Complete removal of such sources of contamination is not normally possible; there still will be a residual risk after remediation.

Several government agencies and other stakeholders are involved in and concerned with the risk management, but no single body has overall responsibility. Liability is sometimes difficult to establish. For example, who is responsible if an accident occurs after remediation and release to a new landowner? What was previously only an issue for the military has become a risk challenge for society in general.

Explosive remnants remediation attracts substantial costs that increase rapidly with increased levels of remediation. With limited resources available, their use should be based on the risk reduction that they can provide to society. The question, 'What is the acceptable residual risk from a societal perspective?' becomes the main criterion for decision-making.

Reducing the risk to acceptable levels requires a management model that takes into account all relevant risk dimensions (see also Jørgensen and Lindøe, Chapter 11, in this volume). The total risk picture needs to be communicated to decision-makers so they can prioritize the costly risk-reduction measures. A common risk picture requires standardization of how the different dimensions are visualized. What are the advantages and disadvantages of different levels of standardization?

The problem of explosive remnants in Swedish society

The technical problem

Many countries have to deal with daily problems related to the presence of explosive remnants in their society. Examples are:

- unexploded conventional and chemical ammunition around First World War battlefields in the Benelux countries;
- unexploded Second World War bombs in European cities, such as Berlin, London, Hamburg, and Dresden;
- remaining landmines (despite extensive mine action programmes) after the 1990s war in the Balkans;
- sea-dumped chemical ammunition in the Baltic Sea and Skagerrak (GICHD, 2014; Zalasiewicz and Zalasiewicz, 2015).

Sweden has been spared war on its own territory for more than 200 years. Therefore, it is easy to believe that it has been spared the problem of explosive remnants. However, the truth is that large areas are contaminated with explosive remnants. Two categories of contamination are predominant (SWEDEC, 2015; Johnsson and Vretblad, 2017):

1 Unexploded ordnance on former shooting ranges and training areas.
2 Surplus ammunition dumped in lakes, rivers and mines.

These are remnants of a time when the Swedish Armed Forces and the domestic defence industry were far more extensive than today. Defence cuts have gradually decreased the need for facilities, training areas, and large stocks of ammunition. Land and water areas, no longer needed for defence-related purposes, have been sold or transferred for new use within society (Johnsson, 2016). To ensure that explosive remnants do not pose a threat to people, activities, or economic values, remediation or restrictions are required.

During the last three to four decades, the Swedish Armed Forces have terminated, closed down, and sold over 300 geographical areas (SWEDEC, 2015). In addition, there are significant areas that had been terminated earlier, used by other agencies for research and testing, used temporarily (e.g. for a single exercise), and areas used by the defence industry. Live ammunition has not been used at all locations, but changing usage and low historical traceability make it difficult or even impossible to identify and categorize hazardous areas (Johnsson, 2016).

In the 1940s, sea dumping became a common method of disposing of surplus and obsolete ammunition. The method was used by both the Swedish Armed Forces and the defence industry until the late 1960s, when it was abandoned in favour of more environmentally friendly methods. In total, several thousand metric tons of ammunition were officially dumped at more than 100 different dump sites at sea and in lakes, rivers, and mines across the country. In addition

to these centralized decisions, undocumented local decisions about dumping were taken, with limited traceability. In most cases, the ammunition was dumped in its original packaging and is slowly decomposing in the bottom sediments (Andersson *et al.,* 1998; Sjöström, Karlsson, and Qvarfort, 2004).

A complex risk picture

The risk picture related to the problem of explosive remnants is multifaceted, and at least three dimensions need to be considered. First, there is an environmental risk that explosives and other toxic substances slowly leach from the ammunition into the surrounding soil and groundwater. Second, there is a safety risk that people or economic values will be damaged if a piece of ammunition explodes. Finally, there is a security risk that someone might improperly exploit heavily contaminated sites to gain access to explosives (SWEDEC, 2015; Johnsson, 2016; Johnsson and Vretblad, 2017).

There is a range of possible approaches for remediation, where the choices of technical equipment and working methods are influenced by: type of ammunition, status and condition, local conditions of the contaminated site, available resources, and, not least, level of ambition. No method will completely eliminate the problem, regardless of the approach; there will always be a residual risk after remediation. Furthermore, the costs increase rapidly with increased levels of remediation. Therefore, remediation measures must be balanced against the expected utility and against what constitutes an acceptable risk in relation to the new land or water usage (MacDonald *et al.,* 2004).

An overall picture, showing all the areas in Sweden contaminated with explosive remnants, does not exist. The existing information only covers part of the problem. The documentation is spread among various stakeholders, and no organization has access to all the documents. Moreover, significant parts of the history are not documented at all and are, at best, locked in the memory of an ageing generation (SWEDEC, 2015). Prioritizing between contaminated areas, to determine where the need for remediation measures is greatest, is therefore a challenging task.

To further complicate the situation, the problem is surrounded by several fundamental uncertainties because of the lack of scientific knowledge regarding the danger posed by explosive remnants. A similar uncertainty prevails about the long-term environmental impact of dumped ammunition. Consequently, several of the most fundamental parameters for assessing the risk are missing (Johnsson, 2016).

Liability: who is responsible?

The problem concerns several stakeholders, whose rationales for dealing with it are sometimes divergent. In this context, the Swedish Armed Forces can be regarded as the tenant of all military facilities in use, and the Swedish Fortifications Agency (FORTV) is the formal landlord. As the user, the Swedish Armed Forces are responsible for the contamination they cause, while the FORTV has

the responsibility for converting the land to its new usage when it is sold. Normally a third party, a commercial company, is contracted for remediation prior to release. The Swedish Civil Contingencies Agency (MSB) is the licensing and regulatory authority in the handling of explosives, which also includes ammunition clearance operations (SWEDEC, 2015).

Liability is sometimes difficult to establish. For example, who is responsible if an incident occurs after remediation and release to a new landowner? The Swedish Armed Forces, who used the land for military activities? The FORTV, that converted the land for its new usage? The commercial company that carried out the remediation? The MSB that issued permits to the remediation company? Or, has the new landowner also taken over responsibility for historical explosive remnants?

Acceptable risk: how safe is safe enough?

The question of whether or not remediation is required should be related to what constitutes an acceptable risk from a societal perspective. This risk analysis needs to include (at least) three risk dimensions: (1) environmental risk, that is, the risk of damage to the environment; (2) safety risk, that is, the risk of accidents; and (3) security risk, that is, the risk of explosives falling into the wrong hands. It also addresses the question of what residual risk, after remediation, is acceptable in relation to the new land and water usage.

From a Swedish perspective, there is a lack of both a model for how the aggregated risk should be analysed and an approach to what constitutes an acceptable risk from the explosive remnants in society. This should be the foundation for decision-making, prioritization, and management of this costly problem.

Lack of a national risk-based approach

Based on the identified knowledge gaps, related to the problem of explosive remnants in Swedish society, a substantial need for new knowledge can be identified. A fundamental inadequacy in today's handling (or non-handling) is related to the absence of a holistic risk-based approach at the societal level. The need for adapted risk management models can be identified for (at least) three different decision points during the release process, as illustrated in Figure 5.1.

Initially, at the national level, a risk assessment is required for prioritization of all contaminated sites in the country, regardless of whether the problem relates to unexploded ordnance, dumped ammunition, or a combination of the two. The purpose, regardless of the type of explosive contamination, is to rank all areas based on their aggregated risk, that is, the combination of environmental, safety and security risks. The result provides input for decision-making about which areas should be prioritized for remediation measures. The level of knowledge for this risk assessment is limited and consists of the incomplete and fragmented information currently available.

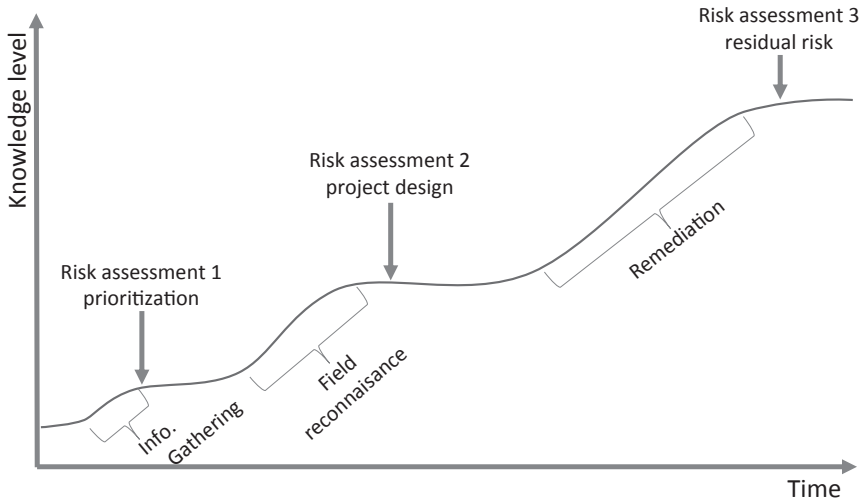

Figure 5.1 The need for risk assessments in different phases.

After initial prioritization and a decision to take remediation measures, an in-depth risk assessment of the individual site is required. This assessment refers to a specific site and is based on site-specific information. The knowledge level, prior to this assessment, is substantially improved through field reconnaissance and detailed mapping of local conditions. The aim is to design a remediation programme and generate input for decisions about the design of the remediation programme.

Finally, a third risk assessment is required after completion of the remediation programme. The purpose here is to determine the actual residual risk, to provide a basis for a decision as to whether or not the results can be considered acceptable from a societal perspective. This assessment is based on all the information collected during the remediation phase.

Given that complete elimination of the problem is not realistic, combined with the fact that it is not financially feasible to remediate every contamination, management needs to be risk-based. The overall risk picture has three dimensions, and remediation measures usually affect all three to varying degrees; thus, the total risk picture should be the basis for all decisions. Remediation measures should only be taken at places where the risk is assessed as unacceptable. In order to optimize the cost-benefit effect, sufficient measures should be taken until the risk is reduced to acceptable levels – no more and no less.

The most urgent need is for a national risk management model for the initial prioritization and ranking of all sites contaminated by explosive remnants in the whole country, that is, Risk Assessment 1, according to Figure 5.1. The model needs to combine environmental, safety, and security risk dimensions in a joint assessment. Furthermore, the model needs to be adapted to the limited information available, with a particular focus on uncertainty.

Approaches to the problem

A risk-informed approach

First, one can ask whether a risk-informed approach to the problem is right at all. One approach could be to remediate all areas that are released to society. This would lead to the remediation of large areas that are not contaminated, which would be very costly in relation to the utility gained. This approach was previously common in humanitarian mine-clearing projects but has now been abandoned in favour of the *land release* concept, simply to ensure that exclusive clearance resources are only used where the need is greatest (GICHD, 2008, 2011).

Another approach could be to just cope with problems as and when ammunition is encountered. Since the consequences of incidents involving ammunition/explosives usually become very serious, such an approach is difficult to justify in a modern society. However, this could be a way of dealing with remaining ammunition during a reactive phase after remediation measures have been taken (White, 2017).

The most rational approach is probably based on the overall risk of explosive remnants, that is, an aggregated risk picture – a combination of environmental, safety, and security risk dimensions. Since complete remediation can neither be achieved technically nor justified socio-economically, only areas with an unacceptable level of risk should be remedied until acceptable levels are achieved (Johnsson and Vretblad, 2017).

The risk management approach

A risk management approach is needed to deal with the different risks associated with explosive remnants. According to the International Organization for Standardization (ISO), risk management is the 'coordinated activities to direct and control an organization with regard to risk' (ISO, 2009). (See also Lindøe and Baram, Chapter 14, in this volume.)

Even at this general stage, an important limitation can be identified in the definition. The process refers to *an organization*; this means that there is a defined and distinct system to be managed (ibid.). In the current case, the system boundaries are unclear, with several stakeholders lacking a common management structure.

Risk management is part of the decision-making process and helps decision-makers to make rational risk decisions (ibid.). One person or entity within the organization is the risk owner, who is formally accountable and has the authority to manage the risk (ibid.). Another limitation can be identified here related to the problem under discussion. No single entity has overall responsibility for dealing with explosive remnants in Sweden. The stakeholders involved have no common command structure nor any mandate to exercise leadership over each other.

The objective of (most) risk management frameworks is to support rational decisions on how to manage risks that are considered unacceptable. These concepts are not normally designed to deal with problems where stakeholders have different rationales for managing the same risks, which is the case with explosive remnants.

Traditional management models are normally based on a hierarchical structure with linear command and control conditions. Furthermore, these models assume a common rationale among the stakeholders for dealing with certain risks. Applying a more traditional risk management model to this problem would entail significant shortcomings and sub-optimal solutions. The traditional approach is simply too narrow, and a model that also considers other, primarily 'soft' values must be found (see Tehler *et al.,* Chapter 4, in this volume).

The risk governance approach

An approach to risk management that better matches the complexity of the problem would be risk governance. This theoretical framework has been developed to manage (risk-related) problems involving multiple stakeholders, major uncertainties, unclear causality, and, not least, divergent rationales behind the required course of action (IRGC, 2005, 2012; Renn, 2008; Aven and Renn, 2010).

The risk governance framework comprises two main elements: deciding and understanding (Figure 5.2). The left half, deciding, refers to the management process, where decisions are made, translated into activities, and experiences are reported back to the stakeholders. The right half, understanding, focuses on generating knowledge, so that the complex reality can be understood. The knowledge generated and the understanding of the problem are the basis for the decisions taken and the activities carried out (Renn, 2008; IRGC, 2012).

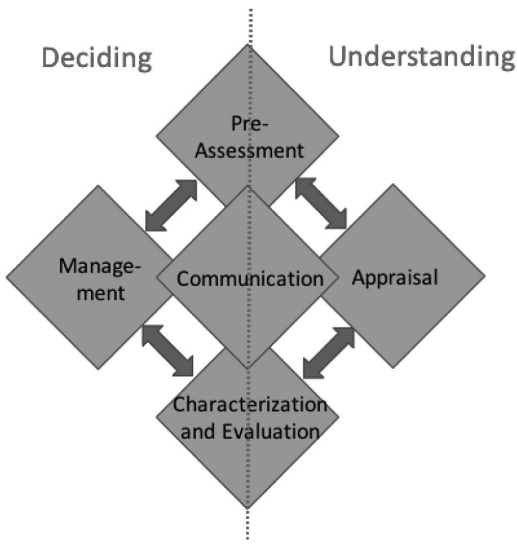

Figure 5.2 Schematic of main components of the risk governance framework.
Source: After IRGC (2012), p. 8.

According to the International Risk Governance Council (IRGC 2005, 2012), the whole process is based on four activities: (1) pre-assessment; (2) appraisal; (3) characterization and evaluation; and (4) management. The initial stage, pre-assessment, involves identification, definition, and framing of the problem. The aim is to identify, at an early stage, phenomena that can pose a risk. The second step, appraisal, is an analysis of all parameters influencing the risk. It is important to emphasize that this is a much broader analysis than a traditional risk analysis, since 'soft' aspects, such as perception and values, are also taken into account. In the third step, characterization and evaluation, the risk is summarized, and alternative courses of action designed. The risk is evaluated on the basis of tolerance and acceptance, which are the main criteria for deciding whether mitigation measures are required. The final step, management, is the organizational implementation of mitigation measures. Decisions are based on the knowledge generated in the previous steps and implemented in the business. Results and experiences are worked back into this iterative process and will improve the level of knowledge. Additionally, there is a fifth system element, communication. This has a central position, is linked to all the steps already described, and underlines the importance of a continuous dialogue with all stakeholders (ibid.).

The risk governance framework adds two new components to the risk field: (1) inclusion of the societal context; and (2) categorization of the risk-related knowledge. The societal context focuses on contextual aspects and includes the interplay of different actors, their perception of the risk, and their different concerns regarding the consequences. The societal context also includes policy-making and regulatory styles, as well as the socio-political impacts within the institutions that have a role in the risk process. The categorization of risk-related knowledge depends on the degree of difficulty of establishing the cause-effect relationship between the risk and consequences, and distinguishing between 'simple', 'complex', 'uncertain', and 'ambiguous' (IRGC, 2005).

Explosive remnants in Sweden from a risk governance perspective

There are great similarities between the risk governance framework and the circumstances surrounding the problem of explosive remnants in Sweden. The actors involved in dealing with the problem represent different aspects of the problem, such as unexploded ammunition or dumped ammunition, or only the environmental or safety aspects. Usually today, there is no coordination of the different sub-areas based on an overall risk picture.

The main actors are government agencies acting within their respective regulatory directives and associated budgets. This gives rise to divergent rationales as to why the problem should or should not be addressed. Some problems are common to several actors, and some issues are completely unmanaged.

The risk picture is complex, which imposes special requirements on a management model. Three fundamentally different risk dimensions need to be expressed collectively and presented as one common risk picture to decision-makers. At the

same time, the risk management process must be able to handle several different risk dimensions, expressed in completely different quantities and based on different parameters.

No acceptable level of risk from explosive remnants is defined in Swedish society. Perhaps one cannot expect a specific position on this issue. At the same time, this should not be the reason for the problem not being addressed. Rather, the problem must be dealt with without a defined level of acceptable risk.

The exposure to risk is also related to the future use of the land and waters after release. Indirectly, this also means that the limit of what can be considered acceptable varies with future use – a dynamic that further complicates the risk management.

The degree of uncertainty must be considered when choosing a model for dealing with the problem. Uncertainty can be found at several different levels, and the effect is often significant. However, lack of information should not lead to failure to deal with the problem. Major uncertainties are part of the particular nature of the problem and must be a prerequisite for the model chosen to solve it.

Although the risk governance framework corresponds, in many ways, very well to the nature of the current problem, the question remains: How should it be applied? An important development step is required to transform this theoretical framework into something that can be operationalized in practical management. The product should be a model for dealing with the specific problem of explosive remnants in Sweden. Such a model should constitute a common ground for all involved stakeholders – that is, a standardized approach.

When the risk governance framework is operationalized in a model, standardization is required at multiple levels:

- a common set of concepts;
- principles for risk analysis;
- limit values for an acceptable risk;
- common criteria for remedial measures, etc.

An initial step should be a common, standardized approach to aggregation of the three risk dimensions (environment, safety, and security) into a common risk picture.

Need for standardization?

Based on the description of the problem area, three main requirements for the generation of a common risk picture are defined as follows:

1 Combine the three risk dimensions (environment, safety, and security) in a joint risk assessment.
2 Aggregate and visualize the impact of uncertainties.
3 Define and visualize the acceptable risk level.

What does fulfilment of these requirements mean, from a standardization perspective?

Combine the three risk dimensions

The main purpose of combining three fundamentally different risk dimensions in a joint assessment is to present a comprehensive basis for decision-making.

Today, the different risk dimensions are handled separately, and there is a lack of dissemination and communication between the sub-areas. Decisions about remediation measures are often taken based on information that only represents a subset of the problem, leading to sub-optimal solutions and unnecessary expense. The stakeholder constellations vary for the different risk dimensions, all the way from the policy level down to the implementation level. No stakeholder has the overall risk picture, and knowledge about the other sub-areas is often limited.

Another complication is that the individual risk dimensions are assessed within different time perspectives. The risk of accidents and deliberate acts is normally estimated close to real time, while environmental risks need to be evaluated based on a time horizon of several hundred years or more.

In addition, the calculation of individual risk dimensions is based on different parameters and expressed in different quantities, units, and scales. Such conditions make it difficult to combine them into a joint risk picture.

Therefore, the fundamental question is: What degree of coordination and standardization between the risk dimensions is appropriate?

Four levels of standardization are discussed below. The first option is based on today's separate management; in addition, another three new options are defined, with different degrees of coordination and standardization, illustrated in Figure 5.3.

1 *Separated*: The risk dimensions are handled separately, without any overall risk picture being presented to the decision-makers. Each dimension is handled in isolation by a separate group of stakeholders, without transparency

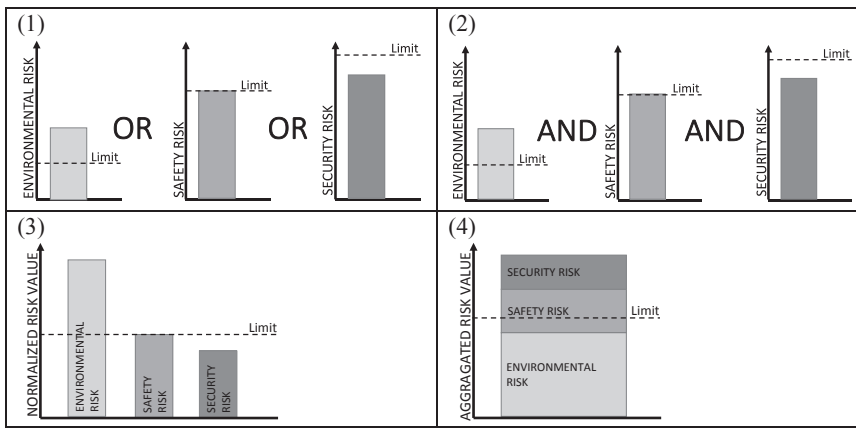

Figure 5.3 Different levels of coordination and standardization: (1) 'Separated', (2) 'Isolated', (3) 'Normalized', and (4) 'Aggregated'.

in the other sub-areas. Decisions are made within each sub-area and without considering the overall risk picture. Remediation measures are decided upon, based solely on data related to part of the total risk picture. Measures that address multiple risk dimensions are absent, and synergy effects are not assessed. Limit values for what constitutes an acceptable risk are defined for each risk category. See (1) in Figure 5.3.

2 *Isolated*: The three risk dimensions are still assessed individually and in isolation, according to current principles. However, for the decision-makers, the individual risk assessments are presented together. This gives a complete risk picture. On the other hand, the results are not coordinated, which means that individual dimensions are presented according to their own routines and procedures, and any comparison of them is difficult. The difference between this option and option (1) is that actors involved in risk-based decisions about remediation measures have access to all risk assessments. See (2) in Figure 5.3.

3 *Normalized*: The three risk dimensions are assessed separately, then the individual aspects are weighted and presented according to a common risk scale. Since the different sub-areas are expressed in the same unit, further development work is needed to standardize the risks. Existing risk assessment models are unique for each risk dimension and are based on various parameters and expressed according to divergent principles. In reality, it is about creating a tool for translation to a common scale. The traceability of the individual risk dimension remains, even though a new method is used to express the risk. See (3) in Figure 5.3.

4 *Aggregated*: The three risk dimensions are assessed jointly, expressed in the same unit and presented as one aggregated risk value. The different sub-areas are assessed based on a common standardized risk scale, including environmental, safety, and security dimensions. Existing risk assessment models must be further developed or completely replaced. When the three risk dimensions are combined into a common risk value, a standardized method of weighting the different sub-areas is also required. Only one limit for the 'total risk' exists, which requires a separate standardization decision. Decision-makers are then presented with a single risk value, which is related to an acceptable level of risk. See (4) in Figure 5.3.

The four options have different advantages and disadvantages. The following analysis refers to the main aspects of the risk management process.

One important aspect is to be able to use both the input data and risk analysis methods that are currently available. Both options (1) and (2) have the advantage of not requiring any adjustments of either existing analytical methods or any data in use today. Options (3) and (4) require relatively extensive adjustment, because standardization and normalization between risk categories are required, which is a complex task.

The risk needs to be put into a broader context, to be able to compare it with other societal risks, such as traffic accidents, other environmental hazards, or

terrorist threats. It is of note that, for other sources of risk, different categories of risks are assessed and described separately. For example, for a nuclear power plant, the risk of accidents is assessed and expressed separately; similarly, environmental aspects and threats of deliberate action are analysed separately, even though there are links between them. This means that comparability with other societal risks is good, as long as risks are expressed according to standard routines, that is, alternatives (1) and (2). Comparability is partly lost when subcategories are expressed according to a 'common' unit and scale, that is, alternatives (3) and (4).

The main advantage of aggregating the various risk categories is that it provides an overview of the overall risk from explosive remnants. Since only one limit value is required − the overall risk level − it is easy to rank and prioritize contaminated areas. Options (3) and (4) provide equivalent benefits and a clear picture of the overall risk. Option (2) certainly provides the overall risk picture but requires more of the receiver, in terms of interpretation and understanding. Option (1) is completely incapable of providing a basis for ranking locations.

Communicating risk to decision-makers is crucial. In principle, the fewer the parameters that need to be considered, the easier the communication of risk becomes. As soon as there are several measurement values, problems arise as to how they should be weighted against each other. Option (4) is superior in this regard, but the link to individual risks gets a little lost. Although option (3) has three risk values to communicate, all of them are comparable and based on a common limit value. Option (2) imposes greater demands on risk communication; all partial risks are reported, but they require separate handling. Option (1) does not give the opportunity to communicate an overall risk picture.

In summary, it can be concluded that a choice between the alternatives is neither simple nor obvious. A greater degree of aggregation of the three dimensions of risk increases situational awareness and the ability to communicate the result to decision-makers. At the same time, the comparability with other societal risks, and the usefulness of today's data and risk management methods, are reduced with a higher degree of aggregation.

An intermediate option, (2) 'Isolated', seems more appropriate. This option does not negate the current risk management work, and all historical data are fully useable. It also creates an opportunity to both present a comprehensive risk picture and generate a national priority, while still being comparable with other societal risks. The major disadvantage is that it imposes greater demands on all the actors involved in the risk management process, as the individual risks must be managed separately.

Aggregate and visualize the uncertainty

As described earlier, there are a number of uncertainties at several levels: scientific, model, information, the nature of the problem, and the effect of different remediation methods. The uncertainties are normally so extensive that they have a significant impact on assessed risk values. The possibility that, in some cases,

the uncertainties will be greater than the known conditions cannot be excluded. What impact does the aggregated uncertainty have on the risk picture presented to the decision-makers? How do you visualize and communicate uncertainties?

The problem involves a paradox, in terms of presenting facts about something unknown. How does one put a value on something one has no knowledge about?

However, the problem can be tackled more fundamentally. How can the degree of uncertainty be demonstrated, in order to convey a sense of its impact on an estimated/calculated risk value?

Figuratively, uncertainty can be said to constitute a tolerance from a given (risk) value, within which the actual risk lies. When a risk value has been calculated, this is supplemented by the effect of all the uncertainties in the assessment. These uncertainties give two limit values, a maximum and a minimum, which give the uncertainty interval. A large interval implies great uncertainty, and vice versa. See Figure 5.4.

The next challenge is how to aggregate the individual uncertainties into a total uncertainty. Even if the respective risk dimensions (environment, safety, and security) are handled separately, the task is complex. There are often several parallel uncertainties. Usually, neither their causal relationship nor their precise impact on the risk value can be determined. Is it even possible to give a weighting to the different impacts of various uncertainties on the risk value? For example, how do you quantify and weight the uncertainty of not knowing which ammunition has been fired in an area, in combination with the scientific uncertainty that knowledge about the sensitivity of unexploded munitions is non-existent?

Although it would be desirable to quantify the uncertainties, this is probably not possible. On the other hand, it is normally possible to roughly categorize the degree of uncertainty, for example, low, medium, or high. By doing so, one can still present differences in the level of uncertainty to the decision-makers.

Another challenge is how to communicate the total level of uncertainty. How do you create comparability between the different risks? Although the individual risk aspects should not be expressed in the same unit, their measurement value (y-axis) should be normalized to create conditions for visual comparability of the impact of uncertainties (Figure 5.5).

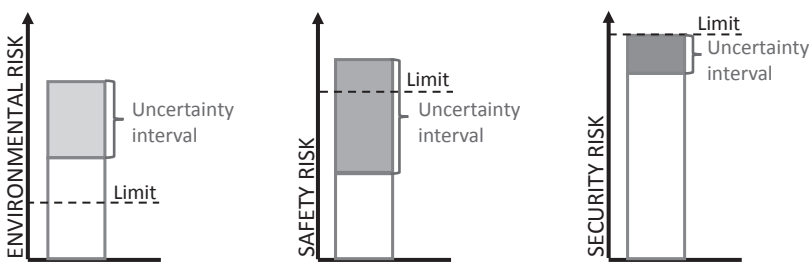

Figure 5.4 The level of uncertainty presented as intervals in relation to an acceptable risk limit.

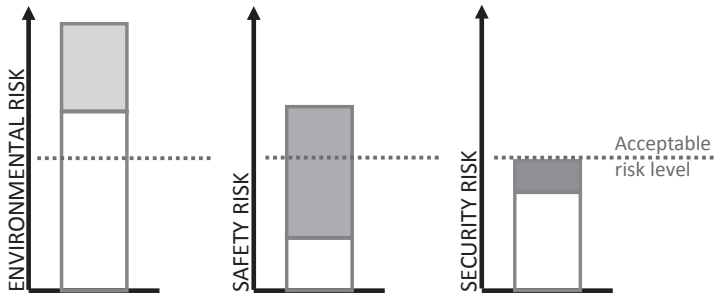

Figure 5.5 The acceptable risk level normalized between the three risk categories.

Define and visualize the acceptable risk level

The acceptable risk describes the limit of risk from explosive remnants that can be tolerated, from a societal perspective. Thus, the acceptable risk also defines the limit for whether or not remediation measures are required.

The value of the acceptable risk level depends on future land and water use. The limit is lower if large values (human as well as economic) are exposed to the risk. The risk acceptance for accidents would be lower if a school were to be built on the land than if the land were to be used for forestry. Likewise, the threshold for toxic substances would be lower for a lake that was going to be used as a freshwater source than for a lake that was going to be used for leisure activities.

At the same time, the acceptable risk is not defined for each individual case. Normally, different thresholds apply for different categories of applications, residential areas, industrial development, recreational areas, etc. On the other hand, the categories are different for each risk dimension, that is, environment, safety, and security. Existing categorization should therefore be mapped to scenarios to create comparability. For example, what safety risk is acceptable for a residential area?

Similar to the discussion about uncertainties, there is a problem with visualizing the acceptable risk limit value for the decision-makers. It is difficult to create comparability between the different risk aspects. In order to do so, a normalization of the value axis (x-axis) is proposed, so that the acceptable risk limit, based on the intended land or water use, is comparable between risks. The normalization is a graphical adjustment of the scale of the y-axis, so that the limit value 'acceptable risk level' is presented at the same level in the three graphs. See Figure 5.5.

Recommendation

At first glance, it may seem obvious that the risk from explosive remnants should be expressed in one merged value. This creates simplicity in the dialogue with decision-makers and, not least, a common base for all stakeholders involved.

However, on deeper analysis, it is clear that this is a complicated, perhaps impossible, standardization process to realize. In addition, several dimensions of the problem are lost with aggregation to a common risk value. A major reason for dealing with the different risk dimensions separately is comparability with other societal risks, which puts the problem of explosive remnants in a wider context.

A more expedient alternative means that each risk dimension is assessed separately but presented together − as part of a larger whole. Furthermore, it has been found necessary to normalize the value axis between the three dimensions, in order to clearly visualize and communicate to the decision-makers and stakeholders the impact of uncertainties and the relationship to acceptable risk.

It is important that there is a balance in the accuracy with which the risk picture is presented. The three parts – the calculated risk value, the uncertainty interval, and the acceptable risk limit – should be expressed to the same number of significant figures. The common denominator should be the part that has the least accuracy.

At an early stage, the level of knowledge about the problem is limited; see Figure 5.1. This lack of data makes it difficult to quantify a risk value, and the reliability of any calculated value is low. It is more realistic if, instead, the risk can be classified on the basis of a number of overall criteria, resulting in a rough risk categorization rather than a calculated risk value. In addition, as discussed above, it is not normally possible to assign a value to the uncertainties, which are significant, and only a rough categorization is possible. This leads to the conclusion that the entire risk picture should be expressed semi-quantitatively or semi-qualitatively (see Figure 5.6).

Overall, it is proposed that the individual risk aspects (i.e. environmental, safety, and security risks) are assessed separately but presented together as a whole. It is proposed that the assessment should be semi-quantitative or semi-qualitative, due to the limited knowledge available. The risk value presented should be based on a fixed scale, where the value axis is normalized between the three risk aspects. The threshold for what constitutes an acceptable risk should be normalized between the three risk aspects to create an overview and comparability. The aggregated uncertainty should be presented as an ‘uncertainty

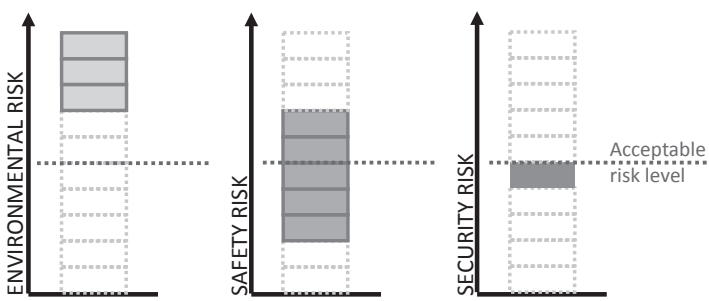

Figure 5.6 Presentation of a semi-quantitative risk value, uncertainty interval, and acceptable risk limit.

interval', within which the actual risk value is estimated to lie. By their very nature, only a few levels of uncertainty are distinguishable.

The utility of standardization

The example of explosive remnants described relates to a specific societal problem, but some conclusions are of a more general nature. Many of the threats and risks posed to our modern society have significant similarities to the example. The problems are often complex, with several parallel risk dimensions, great uncertainty, and many stakeholders involved, who act within their respective areas of interest, without any overall management and coordination. Standardization of a risk management approach to handle such problems means that some dilemmas need to be considered.

Standardization implies a common language among all stakeholders; however, it takes place at the expense of comparability with other societal risks. One of the main advantages of standardization is that it creates a common language and a unified set of concepts, critical prerequisites to communicate the problem. Communication is the key component of the risk governance framework, and all actors must share the same definitions, otherwise risks may be interpreted differently. To communicate the problem to the decision-makers, a common risk picture is required. An understandable common risk picture requires that the different 'sub-risks' are expressed in a uniform and comparable way. Both existing risk models and criteria must be adapted to a standard. This reduces comparability with other societal risks and the possibility of putting the risk in a wider context. The same standardization facilitates communication in one direction and counteracts communication in another.

Standardization is the key to making complex risks manageable; however, it takes resources from the handling of the risk. As soon as there are several stakeholders involved in the handling of complex risks, a consistent approach is required to ensure rational risk management. Standardization of the basic elements in a common risk management concept creates a foundation for effective cooperation across organizational boundaries and between responsibility areas. Standardization requires adaptation of routines, models, and procedures to a common approach. These changes are associated with costs, in terms of resources, time, and labour, to carry out the adaption: resources that could instead be used to handle the actual risk.

The level of standardization must be balanced – otherwise, the utility will be lost. As noted in this chapter, standardization has both advantages and disadvantages. Any general level of optimal standardization cannot be defined. If the level of standardization exceeds a certain threshold, the effect is counterproductive. Therefore, in each case, the level of standardization must be adapted to the nature of the problem; otherwise, its utility may be reduced − or even lost.

Conclusion

Explosive remnants from military activities are a complex and costly problem for Swedish society to deal with. The problem involves several risks that are

currently managed in isolation by different actors, leading to expensive sub-optimal measures.

Risk governance is a suitable framework for ensuring effective management, but further development is required to come up with a model that can be operationalized.

Standardization is a fundamental prerequisite for obtaining a comprehensive risk picture, so that all the actors involved can collaborate to achieve a common goal and communicate the problem to the decision-makers.

Standardization can be achieved in different ways with different pros and cons. There is no universal solution; the approach must be adapted to the nature of the problem.

Several critical choices are needed to define an appropriate standardization level. If the level of standardization is either too high or too low, the utility will be reduced.

Standardization, to obtain a comprehensive risk picture, must be based on a balance between available information and knowledge levels, in terms of:

- the ability to aggregate the assessment of the different risk dimensions;
- the aggregated impact of different uncertainties;
- what constitutes an acceptable risk.

For an initial prioritization of all contaminated areas in the country, a semi-quantitative or semi-qualitative model is proposed. The individual risk categories should be valued separately but presented as a combined risk picture. The model should also illustrate the degree of uncertainty and its impact on the assessed risk values. The individual risks should be presented in relation to a normalized level of acceptable risk, in order to clearly indicate to the decision-makers the need for risk remediation measures.

References

Andersson, A.-C., Eriksson, J., Nygren, Y., Hägglund, L., and Forsman, M. (1998). Miljöriskbedömning av oexploderad ammunition i akvatisk miljö: förstudie. FOA-R-98-00814-222 Umeå: Swedish Defence Research Institution (FOI). (In Swedish).

Aven, T. and Renn, O. (2010). *Risk management and governance: Concepts, guidelines and applications.* Berlin: Springer.

GICHD (Geneva International Centre for Humanitarian Demining) (2008). *A guide to land release: Non-technical methods*. Geneva: Geneva International Centre for Humanitarian Demining.

GICHD (Geneva International Centre for Humanitarian Demining (2011). *A guide to land release: Technical methods*. Geneva: Geneva International Centre for Humanitarian Demining.

GICHD (Geneva International Centre for Humanitarian Demining (2014). *A guide to mine action.* 5th ed. Geneva: Geneva International Centre for Humanitarian Demining.

IRGC (International Risk Governance Council) (2005). *Risk Governance – Towards an integrative approach*. Lausanne: The International Risk Governance Council.

IRGC (International Risk Governance Council) (2012). *An introduction to the IRGC Risk Governance Framework*. Lausanne: The International Risk Governance Council.

ISO (2009). *ISO 31000:2009 − Risk management − Principles and guidelines*. Geneva: International Organization for Standardization.

Johnsson, F. (2016). Explosive remnants: A risk governance challenge. In *Society of Risk Analysis – 2nd Nordic Chapter Meeting*. Göteborg: Society of Risk Analysis − Nordic Chapter.

Johnsson, F. and Vretblad, B. (2017). Explosive remnants: A societal risk challenge. In Proceedings of the 17th International Symposium on the Interaction of the Effects of Munitions with Structures (17th ISIEMS), Bad Neuenahr, Germany, p. 10.

MacDonald, J., Knopman, D. S., Lockwood, J. R., Cecchine, G., and Willis, H. (2004). *Unexploded ordnance: A critical review of risk assessment methods*. Santa Monica, CA: RAND.

Renn, O. (2008). *Risk governance: Coping with uncertainty in a complex world.* London: Earthscan.

Sjöström, J., Karlsson, R.-M., and Qvarfort, U. (2004). Environmental risk assessment of dumped ammunition in natural waters in Sweden: a summary. FOI-R-1307-SE. Umeå: Swedish Defence Research Agency (FOI).

SWEDEC (2015). Explosive remnants in Sweden: A problem to manage Eksjö: Swedish Armed Forces, Swedish EOD and Demining Centre. (In Swedish).

White, R. (2017). The challenge of long-term risk management in mine action. *Journal of Conventional Weapons Destruction*, 21(3), p. 17.

Zalasiewicz, J. and Zalasiewicz, M. (2015). Battle scars. *New Scientist*, 225(3014), pp. 36–39. http://doi.org/https://doi.org/10.1016/S0262-4079(15)30036-1.

6 Which crisis?

The promise of standardized risk ranking in the field of EU infectious disease control

Louise Bengtsson

Introduction

In society in general and in public health in particular, there seems to be little guidance regarding the relative importance we should give to different kinds of potentially risky phenomena. In a reality in which resources are always limited, should we spend money on the prevention of unlikely events that may be seen as posing an existential threat to societies – such as 'bioterrorism' or Ebola preparedness in Europe − or creeping but widespread public health challenges, such as tuberculosis or HIV/AIDS, often affecting large and vulnerable segments of populations? These kinds of questions point to a deeper philosophical tension about what kind of events we consider risky and why. Contributing to the debate, this chapter explores what may happen when so-called pre-emptive forms of governance, focusing on exceptional and disruptive events, are confronted with methodologies trying to make sense of and rank risky events. For this purpose, I use an illustrative example from the European Centre for Disease Prevention and Control (ECDC), the European Union (EU) expert agency for infectious disease. The example casts light on how different forms of knowledge about risk were exposed and negotiated, as experts were confronted with an internal initiative to develop a standardized risk ranking tool based on multi-criteria decision-making analysis. See also Morsut (Chapter 3, in this volume), who discusses the processes in the EU for establishing common standards and guidelines for risk governance and crisis management among member states.

The empirical material was collected through participant observation at the ECDC in Stockholm between November 2016 and February 2017. During this time, the author took part in the final stage of an internal project aiming to gauge the usefulness of a standardized risk ranking methodology for use at EU level and in the member states. Apart from participation in an exercise with member state experts at the agency's premises in Stockholm, February 14–16, 2017, the chapter also draws on official documents published by the ECDC at different stages of this project.

The chapter starts with an outline of how concepts can be studied as empirically sensitive analytical tools. It then introduces the theoretical debates in critical security studies around preparedness, risk, and 'health security', positioning the

chapter's contribution in relation to these discussions. It then offers a brief outline of the nature of standardized risk ranking methodologies, before moving on to the empirical study of the pilot project at the ECDC and a discussion of its implications. In conclusion, the chapter argues that risk-ranking methodologies have the advantage of exposing which kinds of normative input, estimations, and priorities may underpin knowledge about risk.

How to understand and study the concepts of risk and standardization

In this chapter, notions such as risk and standardization are treated as empirically sensitive and open-ended analytical tools, rather than words with a fixed meaning (see Juhl, Chapter 2, in this volume). In this regard, the understandings of risk and standardization are explored as mutually constitutive of prevailing practices in the expert communities studied. The meaning-making practices and stakes involved when it comes to shared knowledge about risk and standardization are thus at the core of the research question. Approaching risk and standardization as open and flexible concepts or 'thinking tools' (Leander, 2008) in this way helps to structure the empirical analysis. More precisely, the standardized methodology studied in this chapter is treated as part of the practices, through which the meaning of risk is shaped within expert communities. Standardization in this chapter should hence not be confused with the formal standard setting often implied in an EU or international context, such as those of the European Committee for Standardization (CEN) or the International Organization for Standardization (ISO). To sum up, studying risk-ranking methodologies as practices of meaning-making becomes relevant, since such processes serve as the foundation for knowledge that then becomes the basis for action. This has implications for the policies pursued, as it guides the allocation of resources and ultimately informs practices determining which situation is designated a crisis and which is not.

The chapter, however, requires some introduction to how certain notions in infectious disease control are currently enacted through practices in the EU context. First, a *risk assessment* is typically understood to be either a more substantial study, concerning long-term implications of known risks, or a so-called rapid risk assessment that may be produced upon early warning of a potential outbreak threatening public health. As opposed to *risk assessment*, *risk management*, on the other hand, is considered a more 'political' activity, in that the level of acceptable risk and feasible public health measures (such as case tracing and isolation, entry screening at borders, or mass vaccination) have to be carefully considered and weighed against other societal concerns.[1] Even though the legal mandate of the ECDC relates to risk assessment and preparedness *support* only, there have also been attempts to streamline risk management by its mother organization, the European Commission's department for health and food safety (DG SANTE), through best practices when it comes to pandemic preparedness plans and coordination of member state response measures in the so-called

Health Security Committee. Normally, however, risk management is carried out at member state level (see Morsut, Chapter 3, in this volume, for a discussion of the EU efforts to standardize risk-related issues).

In this chapter, risk ranking is understood as a collective, expert-led methodology in several steps, meant to facilitate prioritization among different infectious diseases. Such ranking of which risks may be used to inform the allocation of resources at all stages of infectious disease control, such as prevention, preparedness, surveillance, risk assessment, and risk management (also referred to in expert language as containment or response support). In this case, a tool was developed centrally by the EU authorities in the hope that the methodology would, at least to some extent, inspire a new standard practice in the EU member states, hence the notion 'standardized risk ranking'. Although the ranking tool developed at the ECDC was framed to inform preparedness planning, the method is considered internally as transferable to a range of other activities.[2] Typical concerns for preparedness planning are contingency planning, procurement of countermeasures and vaccination, together with disease-specific preparedness in hospitals and generic preparedness for health crises across other societal sectors. When it comes to expert practices within the ECDC, it should be mentioned that various approaches exist within the organization, and that attempts to generalize will always do injustice to the perspectives of certain officials or activities.

What is a health risk?

The idea of potentially sudden and disruptive 'health crises', assumed to imply above all certain disruptive infectious disease outbreaks, airborne pandemics, or 'bioterrorist attacks', tends to give such events a special connotation of urgency in public perception and policy-making. An example of this was the risk of the West African Ebola outbreak, in 2014 and 2015, reaching Europe. As much as the rest of the world can be accused of a slow reaction to the humanitarian concerns caused by the onslaught of the outbreak, as quickly did the same countries rush into preparedness measures at home for the potential arrival of Ebola cases at their own borders and hospitals. The fear that just one case of Ebola would arrive in Europe, creating havoc and panic, had vast effects on the prioritization of EU health authorities and governments. Even in low-income countries, a scramble for preparedness came to overshadow the existing, immediate burden of domestic infectious disease concerns.

To mitigate and pre-empt the occurrence of what are thought of as health crises, societies invest in surveillance for the purpose of early warning and preparedness planning, including vaccination, stockpiling of countermeasures, crisis management exercises, but also generic resilience capacities across various societal sectors. What is seldom discussed, however, is the prioritizations guiding such resource allocation. Which kind of risks are prepared for and in what way? In this regard, it is well known that perceived political or public pressure can affect the way resources are distributed at national, regional, and global

levels. More recently, it has also been argued that public health has seen the rise of certain forms of governance, focusing attention on detection and preparedness for exceptional events, such as pandemic influenza, 'bioterrorism', and certain kinds of emerging infectious disease (King, 2002; Diprose *et al.,* 2008; Kittelsen, 2009; Roberts and Elbe, 2017).

Pre-emptive logics in global health governance

By now, a considerable stream of literature has been dedicated to the rise of such anticipatory or *pre-emptive* logic, as a feature increasingly typical of a turn towards so-called health security, as a priority in global health governance (Collier, Lakoff, and Rabinow, 2004; Diprose *et al.,* 2008; Lakoff, 2008; Weir and Mykhalovskiy, 2012; Elbe, Roemer-Mahler, and Long, 2014). Characteristically, pre-emptive logic treats risk as incalculable, on the basis of past statistical evidence, turning instead to algorithms and real-time monitoring of 'Big Data' in order to detect suspicious disruptions that might indicate exceptionalities as they are happening (De Goede, 2008; Amoore, 2013; De Goede, Simon, and Hoijtink, 2014; Amoore and Raley, 2017). This pre-emptive trend in contemporary societies has been noted across several sectors and is typically concerned with profiling in order to detect indication (but not confirmation) of different kinds of behaviour. As an example, certain kinds of financial transactions or movements might cause individuals to be profiled as 'risky', which may then result in border checks or more intrusive measures, despite the absence of any criminal offence.

Another stream of literature has studied pre-emptive forms of governance as characteristic of a new focus on preparedness in public health and beyond (Collier and Lakoff, 2008, 2015; Elbe *et al.,* 2014). Arguably, such forms of governance may foster a sense of constant alert, which turns out to be unhelpful for addressing root causes and prevention. While pre-emptive governance in the health field is not concerned with the profiling of individuals, a limited but expanding body of literature has explored how the possibilities of Big Data, online monitoring, and algorithms have spurred new approaches to risk in the field of infectious disease control (Diprose *et al.,* 2008; Weir and Mykhalovskiy, 2012; Roberts and Elbe, 2017). Whereas previously dominant and still influential traditions in infectious disease control are based on official data from health authorities, reported according to standardized indicators (Paquet *et al.,* 2006; Santos-O'Connor, Pukkila, and Varela-Santos, 2014), the increasingly influential pre-emptive regime scans sources of informal information that might predict potentially risky 'events' (Roberts and Elbe, 2017). In expert language, such activities are referred to as 'events-based surveillance', 'epidemic intelligence', or activities of 'early warning' (Paquet *et al.,* 2006; Santos-O'Connor, *et al.,* 2014).

The nature of preventive governance in infectious disease control is such that it focuses not on past official reporting of diseases but on any kind of early sign that might *indicate* an urgent threat to public health. Such a sign might be a

disruption in data flows from social media or a rumour from a professional contact, relating to a *potential* onset of something that might turn into a crisis. Approaches to public health along these lines have become nested in institutions such as the US Centers for Disease Prevention and Control (US CDC) and their representations abroad, the World Health Organization (WHO) (Weir, 2012; Weir and Mykhalovskiy, 2012; Hanrieder and Kreuder-Sonnen, 2014), and, as we shall see later in this chapter, the EU and the ECDC in particular (Bengtsson, Borg, and Rhinard, 2017; Roberts and Elbe, 2017).

What is then distinctive about how pre-emptive forms of governance approach risk in the infectious disease field? First of all, the use of Big Data and algorithms, drawing on real-time monitoring of online and informal sources, contrasts with (still existing, parallel) traditional infectious disease surveillance, which plots trends of confirmed cases according to fixed indicators over time. Put in other words, instead of using past trends as a basis for action, a pre-emptive approach is concerned with 24/7 monitoring of informal sources, such as online mentions and transnational platforms for data sharing, aimed at early warning of events as they are unfolding. Roberts and Elbe have argued that this development has entailed a change, from plotting normality and deviations from normality, to anticipation of exceptional events that cannot be captured though traditional surveillance of confirmed cases (Roberts and Elbe, 2017, p. 48). Risk is thus seen as something unpredictable, and focus is placed on detecting exceptional but unlikely events.

Pre-emptive governance practices in infectious disease control in the EU

Since the 2001 anthrax attacks in the US and other events, including the SARS outbreak in 2004, EU health policies have developed a particular focus on infectious disease control and health security, nested in the European Commission's DG SANTE and the ECDC in Stockholm (Kittelsen, 2013; Santos-O'Connor *et al.,* 2014; Bengtsson *et al.,* 2017). The legal mandate of the ECDC encompasses the 'monitoring, early warning of and combating serious cross-border threats to health' (Article 168, TFEU). In practice, this mandate has come to be channelled through a division between risk management and risk assessment of infectious disease (Santos-O'Connor *et al.,* 2014). While EU-level risk assessments are carried out to guide member state action, risk management has largely remained the domain of the member states. The EU level has, however, also been able to carve out a mandate to support and coordinate member state monitoring, surveillance, and preparedness activities. Monitoring and surveillance, as well as rapid risk assessment and preparedness, are thus the major activities of the ECDC, which was founded in Stockholm in 2004 (Greer, 2012, 2013).

Above all, early detection of new outbreaks or 'cross-border health threats' has become an increasingly important part of ECDC activities. These events are approached by the ECDC through preparedness, events-based surveillance, and rapid risk assessments (Paquet *et al.,* 2006; Greer, 2013; Santos-O'Connor *et al.,*

2014). At the ECDC, a multitude of events detected through threat-tracking tools and web-based surveillance platforms and informal information pass through a daily decision-making procedure, in which it is decided which out of such events should receive a 'rapid risk assessment' (Santos-O'Connor *et al.,* 2014). This stage in the procedure has no formal method of prioritization, other than the expert judgement of the so-called round-table meeting. At this daily encounter, which is attended mainly by outbreak epidemiologists from the Surveillance and Response Support Unit, the follow-up actions to the findings of epidemic intelligence activities are decided. Apart from the criterion that the event should be of cross-border concern for EU citizens, the decision-making procedure is carried out largely ad hoc, going with the flow of current (potential signs of) disruptive events.

In the field of epidemic intelligence but also preparedness support at the ECDC, the strong standing of the Surveillance Unit has led to a focus on the monitoring of and resilience to what are understood as large-scale but yet unknown events affecting public health. While structured, 'indicator-based' surveillance of trends regarding common diseases in the member states is also shared by the member states and processed by the ECDC, 'events-based' data from digital monitoring of online mentions, information-sharing tools, and networks have gained an increasingly central importance for the agency. Together with rapid risk assessments, carried out ad hoc as signs of potential health threats are detected, the latter have resulted in a special focus on preparedness and early detection of exceptional events or, if you will, *health crises*. In a related vein, an important part of preparedness activities at the ECDC is framed as 'generic preparedness' and aims to prepare various sectors of society for highly disruptive but yet unknown events that might affect not just public health but societal functions more broadly. The idea of generic preparedness is that such measures are thought of as contributing to societal resilience, no matter what kind of health threat might hit next. While best practices and coordination of disease-specific preparedness in the member states are also part of the ECDC mandate, the way such activities relate to generic preparedness and what gains priority have so far been less clear.

While the disease-specific ECDC programmes work with indicator-based data and long-term perspectives, it can thus be argued that the focus of the agency's epidemic intelligence and preparedness activities is geared towards preemption. First of all, the events-based monitoring and the rapid risk assessments are performed on an ad hoc basis. Second, while the disease-specific preparedness activities of the ECDC allow the organization to go beyond early detection, the work on 'generic' preparedness again has introduced an element of uncertainty that tends towards 'preparing for the worst'. While other approaches exist in parallel under the same ECDC roof, such as the agency's work on scenario studies and drivers of infectious disease (Suk and Semenza, 2011), the crisis-oriented focus of its preparedness and epidemic intelligence work influences how it pursues its priorities and more broadly how it defines its added value at the EU level. In the section below, I illustrate how standardized risk-ranking

methodologies may provide a contrast to such pre-emptive forms of governance, through a particular project initiated within the ECDC itself.

How to understand and study risk-ranking methodologies

Risk-ranking methodologies have so far not been applied extensively in infectious disease control, despite being widely recognized in other sectors as a way to allocate resources according to likelihood and vulnerability incurred by a certain scenario. The justification of risk ranking is typically presented as that of informing 'sound' risk management. The purpose of such methodologies is precisely to avoid certain kinds of events receiving a disproportionate amount of attention, while others are neglected. Namely, without prioritization, certain risks may receive unjustified attention, while others may remain neglected (Fischhoff and Morgan, 2010, p. 1). A common argument used in favour of risk ranking is also that, while risk is often seen as omnipresent and abundant, resources for managing risk tend to be subject to limitation (ibid., p. 1). The task of a risk-ranking methodology thus becomes to establish a more or less standardized and controlled process, bringing transparency to why certain kinds of risk are prioritized over others (see Johnsson, Chapter 5, in this volume).

Risk ranking as a methodology has a long tradition in policy areas adjacent to public health, where risk management is seen as paramount. As an example, standardized risk ranking has been applied in order to prioritize hazards in the broader fields of food safety and environmental risk (ibid.). Early work on risk-ranking methodologies was carried out by the US Environmental Protection Agency, and pioneering methodologies for standardization of such methodologies were promoted by the Canadian Standardization Agency (ibid.). Risk ranking is thus a methodology with principles and procedures that can be applied in any field; however, it requires some sector-specific adjustments and input that are normally developed at expert level. Normally, the various steps in the risk-ranking process imply the close involvement of experts, who can feed their specific knowledge on certain occurrences (such as particular diseases, environmental problems, or whatever might be the subject of the ranking) into the stages of the process. The support of risk ranking may be used not only for different sectors but also for many different purposes. These include resource allocation, for instance, in order to plan activities in the fields of preparedness, risk assessment, or prevention.

At its most all-encompassing, global level, risk ranking may be seen as related to a broader aim of understanding drivers of risk. In this context, the so-called Sendai Framework of the UN has been instrumental in promoting better understanding of disaster risk. In a recent report, the UN body responsible went as far as to suggest that disaster risk management has indeed come to be understood primarily as disaster management, allegedly leading to a skewed allocation of resources, as human activities contributing to risk generation continue to prevail (UNISDR, 2015). When it comes to risk ranking in its more formal sense, the most prominent global example is perhaps the yearly World Economic

Forum World Risks Report in the run-up to Davos, which tends to receive some attention beyond that of experts.

Although the practice of ranking infectious disease risk is not widespread, various methodologies have been developed. Risk rankings have, for instance, been pursued by several expert organizations, including the WHO, as well as the prestigious Robert Koch Institute in Germany. In the case of the WHO, the organization recently carried out a ranking exercise, listing 'global priority pathogens' when it comes to resistant bacteria, which is expected to feed into and guide research on antimicrobial resistance (WHO, 2017). Similar studies have also been carried out by the authorities in the Netherlands and Sweden. While some methodologies for ranking risk in the infectious disease field are limited to a ranking according to mentions in scientific journals, most approaches are geared towards a more specific, chain-like process, which sets out scope, a predefined list for ranking, and different criteria for ranking (ECDC, 2015, p. 1). To fully appreciate the kind of knowledge that risk-ranking methodologies can produce, and how this may contrast with practices of pre-emptive governance, I propose drawing on the example of an attempted standardized risk-ranking methodology in the infectious disease field at the EU level. The pilot project studied in this chapter originated in the ECDC and aims to address prioritization in preparedness measures for infectious disease. The project in itself can be seen as part of a larger trend within the European Union institutions to comply with the spirit of the UN Sendai Framework, which aims at understanding disaster risk (see e.g. European Commission, 2017). At national level, this kind of broader, all-encompassing work takes the form of National Risk Assessments, which are being compared at EU level for best practices, in line with the EU guidelines, Risk Assessment and Mapping Guidelines for Disaster Management (European Commission, 2010). The empirical study below, however, is limited to the example of a risk-ranking project in the EU infectious disease field.

Case study: standardized risk ranking in EU infectious disease governance?

The aim of the risk-ranking project

The initiative of the ECDC risk-ranking project originated in the section of the agency concerned with preparedness activities and was meant to support such planning at EU and member state level. The origins and the rationale of the project can be traced back to a joint meeting between the ECDC and the WHO Europe in 2013 (ECDC and WHO Europe, 2013). The purpose of the project was not so much to be a formal, mandatory standardization of risk ranking as to open up the discussion about how national health authorities can be supported in their prioritization of different kinds of infectious disease risks. Questions to be approached through the ranking tool could include which kinds of outbreaks to prioritize when it comes to preparing hospitals and public health professionals

with training, expertise, and equipment. Alternatively, if the scope was set to that of vaccine-preventable disease, the ranking could inform decisions about which kinds of outbreaks to prepare for in terms of vaccine procurement. The aim of the project was thus to develop, together with the member states, a tentative methodology for prioritizing such purposes. The final delivery of the project was to become an Excel-based ranking tool, accompanied by a handbook with guidelines (ECDC, 2017) and a scientific article produced by ECDC staff on the topic (O'Brien *et al.,* 2016). The exact aim of the project was defined as that of 'distinguish[ing] pathogens according to their epidemic and societal impact properties, allowing for a relative comparison of the threats posed by these pathogens' (ECDC, 2017, p. 3). The hope of the ECDC project coordinators, however, was that these deliverables would open up a broader discussion about prioritization in infectious disease control at the EU level, potentially also passing on a generic tool to the member states. In the sections below, I outline the various steps and outcomes of the project.

Development and launch of the risk-ranking tool

The ECDC risk-ranking project was formally launched in 2014, when consultations started with member states and international experts to determine the feasibility of a common methodology for the purpose of infectious disease preparedness planning. The purpose of the prospective tool was to assist strategic decision-making for disease-specific preparedness. The following statement, however, reflects a more comprehensive spirit of the project, touching not only upon activities of preparedness planning but also, indirectly, risk reduction:

> Types of threats and the pathogens involved shift in response to changing factors, such as climate change, global travel, immigration patterns, environmental degradation, and social inequalities. In order to effectively target the use of resources to manage the risk of outbreak, it is necessary to formulate rankings or prioritization of human and/or animal pathogens.
>
> (ECDC, 2015a, p. 1)

The first major meeting at the beginning of the project was held with the ECDC's member state network, composed of the so-called National Focal Points for Preparedness and Response in Stockholm, in October 2014. Subsequently, the ECDC set out to evaluate pre-existing risk- ranking exercises and methodologies, including at the WHO, in order to present member states with an outline of best practices. This review was concluded with an emphasis on the benefits of a comprehensive process in several stages, weighed according to criteria in a so-called multi-criteria decision analysis (MCDA) (ibid.). In its first stage, MCDA models typically require a design, in which the scope of the ranking is set, such as, in the ECDC case, a limitation to vaccine-preventable diseases or a larger list of infectious diseases. It should also involve a delineation of the purpose, that is, whether the ranking should be used for preparedness,

or perhaps in-depth risk assessment, or some other activity. Moreover, the geographic scope, such as a national, EU-level, or global focus, also has to be determined. A reflection on the stakeholders and target populations that would benefit from the study, as well as a setting of the time frame, is also recommended (ECDC, 2017, p. 5). Once these parameters are set, MCDA can be used to score a chosen list of diseases according to weighed criteria, such as likelihood of introduction, exposure, and possible vulnerabilities incurred. The results may then be used to guide priorities within the scope that was set for the study.

Once the MCDA methodology had been singled out as a promising way forward, the next stage of the ECDC project included the presentation of a pilot methodology to the member states, in the hope that it would engage national experts in a discussion of the usefulness of such a tool. The pilot tool developed would then be gauged by member state experts during a large two-day exercise in Stockholm, in February 2017. Among the participants were senior-level experts in infectious disease control from national public health agencies and health ministries. Representatives from the US Centers for Disease Control and Prevention, the WHO, and the research community were also present. The two-day programme also featured some guest lectures, one of which was delivered by a UNISDR representative on the organization's approach to risk ranking and risk reduction. Participation in this ranking exercise was restricted to the network of National Focal Points for Preparedness and Response, that is, the member state experts responsible for preparedness in the infectious disease field at their ministries or national agencies. With the support of ECDC facilitators, they were then divided up into smaller panels and instructed to score a list of diseases using the pilot tool.

This list of 30 different diseases that were up for ranking in the exercise had been set by the project managers beforehand and ranged from Ebola virus to polio and resistant bacterial infections (ibid., p. 14). This selection was meant to mirror a range of diseases entailing

> life-threatening or otherwise serious hazard to health of biological … origin which spreads or entails a significant risk of spreading across the national borders of Member States, and which may necessitate coordination at Union level in order to ensure a high level of human health protection.
>
> (ibid., p. 14)[3]

These diseases were then to be ranked by the experts, according to a methodology drawing on MCDA. During the exercise, fact sheets were also provided for each disease, containing general information on pathogen transmission, groups at risk, symptoms, treatment, and other available data on the nature of the diseases to be ranked. This material was supposed to help the experts in scoring the diseases against the following criteria, which had been set by the project coordinators:

> 1) probability of introduction of a pathogen with the potential for onward transmission in humans into the EU in the next five years, 2) peak annual estimated incidence in the study population over the next five years, 3) case

> fatality proportion at peak incidence levels, 4) probability that the risk increases in the next five years in the study jurisdiction, 5) discomfort of a disease episode at the individual level, 6) economic impact of the disease.
>
> (ibid., p. 14)

The actual scoring of the diseases against the above criteria was then carried out by the participants in the exercise on a scale ranging from 'very low' to 'low', 'medium', and 'high'. Each criterion also contained a specified scale for the respective levels. As an example, the criterion on discomfort at personal level was to be measured according to a standard reference in public health, namely estimated years lived with disability (YLD) per 100 cases. At the end of the two-day workshop, the results of all the groups' scores for each of the diseases were combined to produce a group average. A weighting of the different criteria was then carried out according to the suggestion of the pilot tool, in order to reflect the relative priority of the different criteria (for the exact method, see ibid., p. 17).

As it turned out, both the exercise itself and the results of the ranking resulted in lively discussions and disagreements among the experts. These lengthy debates even caused some delay in the programme, as discussions arose about various aspects of the pilot tool. Even though the participants included some of the most distinguished outbreak epidemiologists in Europe, various opinions on how to interpret the criteria emerged. The experts not only disagreed among themselves about some of the seemingly more open-ended estimations but also about the criteria themselves; an external observer would perhaps have expected a greater degree of expert consensus. In a wrap-up session, the ECDC project managers emphasized that disagreement among the experts was not necessarily a problem, as part of the purpose of the exercise was to stimulate debate and expose 'biases' in the process of prioritizing risks. The ECDC representatives also stressed that the pilot tool was not the final product, and that the discussions during the workshop would feed into its refinement.

Following the exercise, a new version of the tool was produced as the final deliverable of the project, building on the input during the mock-ranking in Stockholm. In August 2017, this new revised version was launched, together with a handbook for its use (ibid.). As regards the functioning of the final Excel tool, it allows users not only to set the initial list of diseases for ranking but also to modify the criteria in order to better target the use of the methodology. The first step is thus up to the users, but up to 60 diseases can be entered in the tool (ibid., p. 3). The next step is then the setting of the criteria that are to be used for assessment. Here, the following instruction is provided in the handbook:

> The definition of ranking criteria is essential for the ranking process. The ranking criteria should clearly reflect the purpose of the ranking exercise, and they should be applicable to all diseases selected for the exercise. Ideally, ranking criteria should reflect the full definition of risk, typically understood as risk = hazard × exposure × vulnerabilities.
>
> (ibid., p. 5)

The impact of the risk-ranking project

The aim of the ECDC project was never to push through a compulsory standardized methodology, since the latter would be considered outside its legal mandate. Rather, the project was framed towards engaging member states in some form of discussion that would support rather than dictate prioritization. As such, the project explicitly emphasized 'the added benefit of bringing together stakeholders in the decision-making process' (ibid., p. 3). The final handbook mentions in several places that 'The process itself is valuable for infectious disease preparedness planning, because it requires structured discussions and information exchange among various experts and relevant stakeholders' (ibid., p. 3). Arguably, the ECDC risk-ranking project was indeed geared towards exposing what it refers to as potential 'biases' among different kinds of experts in the field:

> Expert opinion is an important information source when empirical data are lacking or uncertain. It is, however, undesirable to base planning on the input from just a few experts, even if they are highly qualified, as cognitive bias can never be completely ruled out. One way to mitigate bias is to pool expert opinion.
>
> (ibid., p. 3)

In addition, the project implicitly raises the concern that generic preparedness for unknowable all-hazards scenarios might be useful, but that a more transparent way of allocating resources is also needed: 'With regard to communicable diseases, preparedness plans can be based on an all-hazard approach, but in order to define and respond to priority risks, disease- or pathway-specific modules may need to be developed' (ibid., p. 2).

As an interesting anecdote, it can also be mentioned that the Dutch consultants, to which the project had partly been outsourced, initially included a final seventh criterion of the methodology: perceived severity of a particular disease according to public opinion. This assessment criterion, however, was rejected by the ECDC project coordinators. The reason behind this move was that the type of expertise required to both develop and deploy a criterion on public perception was lacking in both the consultants and the member state participants in the exercise. Trying to estimate such public worries and feeding them into the tool was, moreover, in a broader sense also not exactly in line with the purpose of the MCDA methodology. Taking into consideration the perceived public urgency of a particular scenario (such as in the case of the panic in Europe following the Ebola outbreak in West Africa) was indeed a kind of consideration that the risk-ranking project was supposed to compensate for.

As regards the broader potential of the ranking beyond preparedness, the handbook touches briefly upon the many human-induced drivers that are changing the landscape of infectious disease control:

> Based on the number of emergence events marked by new pathogens or pathogens that were not previously observed in a region, Europe could be

> characterized as a hotspot of emerging infectious diseases. Future global changes such as climate change, population growth, increasing mobility and ageing population can reasonably be expected to further affect these emerging risks. Consequently, there is a need for new methodologies which can be used to prioritize and rank infectious disease threats for preparedness planning purposes in order to mitigate the impact of these threats.
>
> (ibid., p. 2)

To conclude, it is worth mentioning that the particular methodology, produced by the ECDC and studied in this chapter, carries no formal role as regards the obligations of member states under EU law. Formal or informal standardization of risk-ranking methodology (i.e. processual or procedural standardization) may or may not become the end result of the EU pilot project. The deliverables, that is, the Excel-based tool and the handbook, as well as the scientific article, were presented by the ECDC as a possible 'addition to other available information that supports decision-making in preparedness planning' (ibid., p. 3). The extent to which the emerging risk-ranking activities at the ECDC have a real chance of altering practices more broadly thus remains to be seen. In the case of the EU mandate in public health, it is worth mentioning once again that the member states have a strong legal and perhaps even emotional commitment to national decision-making. This means that the project is unlikely to result in a formally standardized methodology shared by all member states. The results of the project, however, may still spread and feed into expert practices in different ways. As an example, the ranking tool produced by the ECDC has reportedly already been picked up by some member states and may eventually inform practices in the wider expert community.

Potential implications of risk-ranking methodologies

As regards normative discussions about the benefits and drawbacks of standardizing, the introductory chapters of this anthology focused on the observation that 'With so much inherent normativity and uncertainty involved, risk is more than anything characterized by diversity and variability. Hence, risk as such cannot be standardized' (Juhl, Chapter 2, and Olsen, Chapter 1, in this volume). Moreover, the Introduction also pointed to the potential risk of simplification brought by standardization processes. It was argued that standardization of risk assessment might lead to over-simplification, resulting in an unbalanced response, over- or under-estimating the need to act. In addition, another potential risk of standardization raised was that standardization may lead to complacency, as one might get a false impression of control, through fixed forms of meaning-making.

In this chapter, however, I have shown that particular aspects relating to knowledge about risk are subject to constant processes of sense-making among experts. The development of an informally standardized methodology for risk ranking can be seen as an example of such a process, in that it informs shared understandings of what is considered risky and why. In this chapter, moreover,

the pressing issue was neither standardization of risk per se nor standardization of risk assessment or risk management. Rather, the chapter explored methodologies aiming at a 'soft' standardization of risk ranking, for the purpose of planning and resource allocation. As put by Claudia Morsut in Chapter 3, in this volume, such soft standardization does *not* aim to formulate technical specifications in the formal sense of 'hard standardization'.[4] Instead, the purpose is to establish a common ground of understanding, when it comes to procedures, rules, and norms. As a response to the concerns raised about simplification and unbalanced responses, the very idea of risk ranking is indeed that it would help to address potentially unbalanced approaches to risk, where some scenarios are neglected, and others receive an unjustified amount of attention. As outlined in the empirical example from infectious disease control at the ECDC, the purpose was to find a method which, if it prioritizes one kind of risk over another, is explicit about why it does so. This is not to argue that standardized risk ranking produces 'neutral' results. However, one could say that it does provide a method in which considerations and estimations are exposed in a transparent and more systematic way. As seen in the case study, the ECDC project aimed at a transparent set of criteria, to be scored through the involvement of different kinds of experts in order to expose and handle biases.

Moreover, this chapter has explored the potential of risk ranking, in particular against the backdrop of increasingly widespread forms of pre-emptive governance, which tend to focus attention on exceptional but unlikely events. As touched upon above, infectious disease control in Europe and beyond has seen the rise of pre-emptive forms of governance in the field of epidemic intelligence and infectious disease preparedness, shaping how risk is understood and acted upon. An implication of such forms of governance is that the focus is placed on constant monitoring and early signs of *potentially* risky events as they emerge, rather than using past data to predict the likelihood or weigh the impact and vulnerabilities of a certain disease outbreak. The task of public authorities thus primarily becomes one of nipping potentially disruptive events in the bud as they unfold, rather than allocating resources to eliminate structural risk factors or investing in proportional preparedness activities. In a broader sense, ECDC experts in charge of the risk-ranking project in this chapter may thus be seen as actively having pursued practices informing the foundation of knowledge about risk. In doing so, they exposed the constant struggle over knowledge, which determines what is considered risky or threatening in the field of infectious disease. It became clear during the member states exercise, in particular, that a transparent way of allocating resources for epidemic intelligence and preparedness had not been discussed extensively in the expert community.

To take the implications of standardized risk ranking further, the latter may, against the backdrop of pre-emptive forms of governance, provide perspectives that can alter the focus from early detection and containment of hitherto unknown events to risk as hazard × exposure × vulnerabilities. As shown by the ECDC methodology, this perspective can be operationalized by estimating the expected impact and vulnerabilities involved, combined with other commonly

agreed criteria. In general, it can thus be argued that risk ranking as a methodology has the potential to challenge dominant practices of pre-emptive governance, by addressing risk reduction or preparedness according to a common set of criteria, such as likelihood of occurrence, actual societal exposure to the threat, and the vulnerabilities, suffering, and economic impact expected as a result. As an example, the ECDC risk-ranking methodology could serve to prevent certain potential events, typically those that we understand as looming and disruptive health scares, from receiving disproportionate attention, compared to other perhaps neglected but widespread health problems.

This is not to say, however, that the ranking methodology would be a guarantee of a 'neutral' or 'rational' allocation of resources. It is of course true that standardization of risk ranking means a large degree of estimation, simplification, and unavoidable exclusions. It will always rely on expert knowledge, which is in itself shaped by implicitly shared assumptions. Yet, without transparent attempts to prioritize one potential form of risk over another, the focus of expert practices may (sometimes inadvertently, such as in the case of pre-emptive governance) produce priorities that largely escape scrutiny and become considered matters of 'technical' rather than political consideration. Risk rankings thus have the advantage of exposing the kind of normative input, estimations, and priorities that go into a decision, making it more transparent. Making risk ranking available for public scrutiny, at least in theory, also opens up a broader discussion of the criteria and weighting factors beyond expert communities.

As shown by the UNISDR approach to understanding disaster risk (which of course goes far beyond the ECDC project in its scope, directly addressing drivers of risk), more transparent prioritization may also lead to a better overview of the bigger picture and greater effectiveness of resource allocation. By touching briefly upon how various human-induced factors, such as climate change and practices in the food chain, affect the spread of infectious disease, the ECDC project indirectly raised concerns relating to risk mitigation and long-term prevention beyond preparedness. To sum up, while risk rankings of course vary in their scope and purpose, they hold the potential to provide important perspectives in infectious disease control and beyond. The potential of risk-ranking methodologies might be exactly that of bringing transparency to the elements of human interpretation involved in managing risk.

Conclusion

This chapter originated from the puzzlement regarding the kinds of risk we are concerned about and why, since there is often no guidance for either experts or the general public in this regard. Variations of risk-ranking methodologies have informed risk management, research, and preparedness, in fields ranging from food safety to anti-microbial resistance and are often justified on the grounds that some form of standardized process is needed, in order to prioritize among different kinds of measures. The need for reflection on prioritization is especially pressing, this chapter has argued, against the backdrop of increasingly widespread

forms of governance in contemporary societies focusing attention on pre-emption of exceptional events. As an illustrative case study of the potential of standardized risk ranking in such a context, I examined a project initiated by the EU agency for infectious disease prevention and control, the ECDC. Through its definition of risk as 'hazard × exposure × vulnerabilities', the project gave rise to a set of practices indirectly challenging the prevailing focus, in the organization, on risk as a matter of exceptional events. While the lasting impact of the project is still to be seen, it gave rise to a lively debate and internal reflections, since it forced experts to consider their own bias in the relative priority given to different kinds of infectious disease. As such, this and similar kinds of discussion hold the potential to generate knowledge that contrasts with pre-emptive forms of governance, currently on the rise, which have tended to focus attention on unlikely but disruptive *potential* events. Risk ranking may thus be understood as a practice that complements or even challenges such increasingly prevalent understandings of risk.

As for the outcomes and future of the risk ranking tool developed at the ECDC, a formally standardized process at EU level is likely to be sensitive, due to the limited EU legal mandate vis-à-vis the member states in public health. More generally, however, the ECDC example serves as a reminder that risk and standardization ought not to be thought of as fixed concepts but as a site of struggle, where different practices shape what is considered legitimate knowledge about risk. Methodologies such as (more or less standardized) risk-ranking tools may become important in affecting meaning-making in this regard. Rather than producing a 'neutral' form of knowledge, I suggest that risk ranking has at least the potential to bring transparency to the elements of human interpretation involved in managing risk. Against a context in which human activities are increasingly contributing to an accumulation of risk factors (including climate change, environmental degradation, health inequalities, and disinvestment in health systems), treating risk as something that can be made sense of and reduced, rather than just pre-empted, should also be considered of political importance.

Notes

1 It should be noted, however, that crisis management more generally also includes a stage of risk *reduction*. Such measures tend to be more difficult to implement politically than risk *management*, which concerns the actual management of an unfolding crisis. See Tehler *et al.,* Chapter 4, in this volume.

2 Reportedly, several EU member states have already made use of the standardized risk-ranking tool at the member state level. The ECDC has also used the tool to inform work on anti-microbial resistance (ECDC *et al.,* 2017), as well as for guiding the production of more detailed, long-term risk assessments of various pathogens (Domanović *et al.,* 2017). See also Morsut, Chapter 3 in this volume, on challenges in cross-border and multi-institutional standardization efforts.

3 The 30 diseases ranked were filoviral diseases (Ebola and Marburg), salmonellosis, hepatitis E, poliomyelitis, HIV (including multidrug-resistant HIV), colistin-resistant Enterobacteriaceae (mainly K. pneumoniae and E. coli), hepatitis C, tick-borne encephalitis,

Zika, Dengue, coronavirus-related respiratory infections (SARS and MERS), carbapenem-resistant Enterobacteriaceae (mainly K. pneumoniae and E. coli), zoonotic influenza in humans, West Nile fever, campylobacteriosis, diphtheria, pandemic influenza, measles, tuberculosis, antimicrobial resistant gonorrhoea, cholera, tularaemia, meticillin-resistant Staphylococcus aureus (MRSA), toxoplasmosis, hepatitis A, carbapenem-resistant Acinetobacter baumannii, malaria, Lyme disease/borreliosis, Legionnaires' disease, ESBL (extended-spectrum beta-lactamase) producing Enterobacteriaceae (mainly K. pneumoniae and E. coli).

4 What Morsut (Chapter 3, in this volume) defines as 'hard standardization' refers to cases when the EU formulates technical specifications aimed at enhancing uniformity through three standardization bodies: the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization, and the European Telecommunications Standards Institute.

References

Amoore, L. (2013). *The politics of possibility: Risk and security beyond probability*, Durham, NC: Duke University Press.

Amoore, L. and Raley, R. (2017). Securing with algorithms: Knowledge, decision, sovereignty. *Security Dialogue*, 48(1), pp. 3–10.

Bengtsson, L., Borg, S., and Rhinard, M. (2017). European security and early warning systems: From risks to threats in the European Union's health security sector. *European Security*, 27(1), pp. 20–40.

Collier, S. J. and Lakoff, A. (2008). Distributed preparedness: The spatial logic of domestic security in the United States. *Environment and Planning D: Society and Space*, 26(1), pp. 7–28.

Collier, S. J. and Lakoff, A. (2015). Vital systems security: Reflexive biopolitics and the government of emergency. *Theory, Culture & Society*, 32(2), pp. 19–51.

Collier, S. J., Lakoff, A., and Rabinow, P. (2004). Biosecurity: Towards an anthropology of the contemporary. *Anthropology Today*, 20(5), pp. 3–7.

De Goede, M. (2008). The politics of preemption and the War on Terror in Europe. *European Journal of International Relations*, 14(1), pp. 161–185.

De Goede, M., Simon, S., and Hoijtink, M. (2014). Performing preemption. *Security Dialogue*, 45(5), pp. 411–422.

Diprose, R., Stephenson, N., Mills, C., Race, K., & Hawkins, G. (2008). Governing the future: The paradigm of prudence in political technologies of risk management. *Security Dialogue*, 39(2–3), pp. 267–288.

Domanović, D., Cassini, A., Bekeredjian-Ding, I., Bokhorst, A., Bouwknegt, M., *et al*. (2017). Prioritizing of bacterial infections transmitted through substances of human origin in Europe. *Transfusion*, 57, pp. 1311–1317.

ECDC (European Centre for Disease Prevention and Control) (2015a). Best practices in ranking emerging infectious disease threats. Stockholm: ECDC. [online]. Available at: https://ecdc.europa.eu/sites/portal/files/media/en/publications/Publications/emerging-infectious-disease-threats-best-practices-ranking.pdf (accessed 26 October 2017).

ECDC (European Centre for Disease Prevention and Control) (2015b). Outbreak of Ebola virus disease in West Africa: Twelfth update, 30 June 2015. Stockholm: ECDC. [online]. Available at: https://ecdc.europa.eu/sites/portal/files/media/en/publications/Publications/Ebola-RRA-West-Africa-8April2014.pdf (accessed 26 October 2017).

ECDC (European Centre for Disease Prevention and Control). (2016). Rapid Risk Assessment: Zika virus disease epidemic: Eighth update, 30 August 2016. Stockholm: ECDC.

[online]. Available at: https://ecdc.europa.eu/en/publications-data/rapid-risk-assessment-zika-virus-disease-epidemic-10th-update-4-april-2017 (accessed 26.10.2017).

ECDC (European Centre for Disease Prevention and Control) (2017). *ECDC tool for the prioritization of infectious disease threats: Handbook and manual*. Stockholm: ECDC. [online]. Available at: https://ecdc.europa.eu/sites/portal/files/documents/Tool-for-disease-priority-ranking_handbook_0_0.pdf (accessed 26.10.2017).

ECDC (European Centre for Disease Prevention and Control), EFSA BIOHAZ Panel (European Food Safety Authority Panel on Biological Hazards) and CVMP (EMA Committee for Medicinal Products for Veterinary Use) (2017). ECDC, EFSA and EMA Joint Scientific Opinion on a list of outcome indicators as regards surveillance of antimicrobial resistance and antimicrobial consumption in humans and food-producing animals. *EFSA Journal*, 10(5017), pp. 1–70. [online]. Available at: https://doi.org/10.2903/j.efsa.2017.5017 (accessed 26 October 2017).

ECDC (European Centre for Disease Prevention and Control) and WHO Regional Office for Europe (2013). Meeting report: Joint European Centre for Disease Prevention and Control and WHO Regional Office for Europe consultation on pandemic and all hazard preparedness, 20–21 November 2013, Bratislava, Slovakia. [online]. Available at: https://ecdc.europa.eu/sites/portal/files/media/en/publications/Publications/Joint-ECDC-WHO-Europe-Consultation-on-pandemic-and-all-hazard-preparedness-meeting-report.pdf (accessed 26 October 2017).

Elbe, S., Roemer-Mahler, A. and Long, C. (2014). Securing circulation pharmaceutically: Antiviral stockpiling and pandemic preparedness in the European Union. *Security Dialogue*, 45(5), pp. 440–457.

European Commission (2010). SEC(2010):1626 final. Risk assessment and mapping guidelines for disaster management. Commission staff working paper Brussels, 21 December 2010. [online]. Available at: https://ec.europa.eu/echo/files/about/COMM_PDF_SEC_2010_1626_F_staff_working_document_en.pdf (accessed 26 October 2017).

European Commission (2017). SWD(2017):176 final. Commission staff working paper. Overview of natural and man-made disaster risks the European Union may face. Brussels, 23 May 2017. [online]. Available at: https://ec.europa.eu/echo/sites/echo-site/files/swd_2017_176_overview_of_risks_2.pdf (accessed 26 October 2017).

Fischhoff, B. and Morgan, G. (2010). The science and practice of risk ranking. *Horizons*, 10(3), pp. 40–47.

Greer, S. L. (2012). The European Centre for Disease Prevention and Control: Hub or hollow core? *Journal of Health Politics, Policy and Law*, 37(6), pp. 1001–1030.

Greer, S. L. (2013). Catch me if you can: Communicable disease control. In S. L. Greer and P. Kurzer, eds. *European Union public health policy: Regional and global trends*. London: Routledge, pp. 141–154.

Hanrieder, T. and Kreuder-Sonnen, C. (2014). WHO decides on the exception? Securitization and emergency governance in global health. *Security Dialogue*, 45(4), pp. 331–348.

King, N. B. (2002). Security, disease, commerce: Ideologies of postcolonial global health. *Social Studies of Science*, 32(5), pp. 763–789.

Kittelsen, S. (2009). Conceptualizing biorisk: Dread risk and the threat of bioterrorism in Europe. *Security Dialogue*, 40(1), pp. 51–71.

Kittelsen, S. (2013). The EU and the securitization of pandemic influenza. PhD thesis, Aberystwyth University. [online]. Available at: http://cadair.aber.ac.uk/dspace/handle/2160/13193 (accessed 26 January.2018).

Lakoff, A. (2008). The generic biothreat, or, how we became unprepared. *Cultural Anthropology*, 23(3), pp. 399–428.

Leander, A. (2008). Thinking tools. In A. K. Deepa Prakash and A. D. P. Klotz, eds. *Qualitative methods in international relations*. New York: Palgrave, pp. 11–27.

O'Brien, E. C., Taft, R., Geary, K., Ciotti, M., and Suk, J. E. (2016). Best practices in ranking communicable disease threats: A literature review, 2015. *Eurosurveillance: Bulletin européen sur les Maladies Transmissibles = European Communicable Disease Bulletin*, 21(17). Available at: www.eurosurveillance.org/Public/Articles/Archives.aspx?PublicationId=11678

Paquet, C., Coulombier, D., Kaiser, R., and Ciotti, M. (2006). Epidemic intelligence: A new framework for strengthening disease surveillance in Europe. *Eurosurveillance: Bulletin européen sur les Maladies Transmissibles = European Communicable Disease Bulletin*, 11(12), pp. 212–214.

Roberts, S. L. and Elbe, S. (2017). Catching the flu: Syndromic surveillance, algorithmic governmentality and global health security. *Security Dialogue*, 48(1), pp. 46–62.

Santos-O'Connor, F., Pukkila, J., and Varela-Santos, C. (2014). The health security framework in Europe. In B. Rechel and M. McKee, eds. *Facets of public health in Europe*. New York: Open University Press, pp. 43–69.

Suk, J. E. and Semenza, J. C. (2011). Future infectious disease threats to Europe. *American Journal of Public Health*, 101(11), pp. 2068–2079.

UNISDR (2015). Global assessment report on disaster risk reduction. [online]. Available at: www.preventionweb.net/english/hyogo/gar/2015/en/gar-pdf/GAR2015_EN.pdf (accessed 26 October 2017).

Weir, L. (2012). A genealogy of global health security. *International Political Sociology*, 6(3), pp. 322–325.

Weir, L. and Mykhalovskiy, E. (2012). *Global public health vigilance: Creating a world on alert*. London: Routledge.

WHO (World Health Organization) (2017). Short summary. Global priority list of antibiotic-resistant bacteria to guide research, discovery, and development of new antibiotics. [online]. Available at: www.who.int/medicines/publications/WHO-PPL-Short_Summary_25Feb-ET_NM_WHO.pdf (accessed 26 October 2017).

7 Standardization and flexibility in surgical operations

A question of balancing risk

Sindre Aske Høyland

Introduction

This chapter begins by looking at standardization from a larger societal risk perspective, before describing standardization tendencies within the Norwegian health care system and surgical practices. Following the introduction, the chapter's research problem is identified and explored empirically.

The industrial and technical evolution has led our global society into an era of risk production, both global in nature and local in impact (Beck, 1992). In the risk society, the number of real and perceived threats keeps growing, and they have taken dynamic, unpredictable, and non-transparent forms. This is evident in nebulous terror networks, unpredictable flu outbreaks, and rapidly escalating infrastructure failures, resulting from extended integration of Internet-based ICT in critical infrastructures, urban planning and development, and the economy (Laursen and Meliciani, 2010; Zhang, van Donk, and van der Vaart, 2011; Line and Tøndel, 2012). In parallel with the complex and globalized threat pictures facing contemporary society, a growing bureaucratization and standardization tendency is witnessed, comprised of more controls, adherence to rigid procedures, attention to detail, and reliance on standards (Lodge and Hood, 2003; Power, 2004, 2007a). The bureaucratization and standardization produce static countermeasures that seek to address dynamic threats, implying that standardization may represent an insufficient response in handling today's changing/dynamic threats.

Furthermore, Norwegian society – similar to that of other industrialized countries – demonstrates a strong trend towards governance and control of risks through standards and standardizations in the management and analysis of risks, as well as in the production and services of critical industries. This can be seen in the increasing number of standards within the area of information security, aimed at achieving more structured and systematic work to improve the quality of information security in general and the implementation of risk-reducing measures specifically (NOU, 2015, p. 13). The standardization tendency can be related to a desire to simplify or reduce cumbersome bureaucratic procedures (Power, 2007b), as well as a preference for more detailed and harmonized instructions for how to analyse and assess risks among professionals working

with risk and vulnerability assessments (Månsson, Abrahamsson, Hassel, and Tehler, 2015). Standardization also addresses the concern for organizational vulnerability and individual safety. This is evident in situations where a low degree of standardization and a high degree of reliance on legacy systems have resulted in long response times during ICT incidents and associated ICT systems downtime, with reduced capacity for patient treatment in shorter time periods. These are some of the benefits of standardization. The flipside is that standards require knowledge and technical insight; renewal and development of standards are demanding; and the large and increasing number of standards creates complexity (NOU, 2015).

Research problem, empirical data, and key concepts

This chapter explores how standardization and flexibility in surgical operations influence safety practices and risks to the patient undergoing surgery. This issue will be examined by means of empirical data from a Norwegian doctoral project (hereafter Study 1) and a follow-up focus study (hereafter Study 2) (2008–2013) that explored safe work practices of operating personnel and their perceptions of time and safety in surgery (Høyland, Aase, and Hollund, 2011a, 2011b; Høyland, 2012, 2013; Høyland, Haugen, and Thomassen, 2014).

The three key concepts discussed in this chapter – standards, standardization, and risk – need to be clarified (see also Juhl, Chapter 2, in this volume, for definitions of these concepts). Standardization can be understood as the process undertaken by standardizers by which a standard is attained, where the standard 'provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose' (International Organization for Standardization (ISO), www.iso.org). Brunsson, Rasche, and Seidl (2012, p.615) state that standards reflect explicitly formulated and explicitly decided rules and thus differ from more implicit social norms, with the rule-based character of standards makings them important tools for regulating individual as well as collective behaviour and achieving social order. More precisely, in this chapter, standards concern how to act as defined by procedures, routines, processes, checklists, and so forth applied by operating room personnel (Brunsson and Jacobsson, 2000).

As for the risk concept used in this chapter, Rosa (1998, p. 28) suggests that risk can be defined as 'a situation or event where something of human value (including humans themselves) is at stake and where the outcome is uncertain'. Extending this perspective and that of others, Aven and Renn (2009, p. 10) understand risk as 'uncertainties about events and consequences and severity of these events and consequences (outcome stakes)'. The uncertainties associated with events and consequences imply that the concept of risk and the knowledge surrounding it are highly dynamic. Thus, instrumental approaches and compliance with procedures and standards, such as checklists, may be less suited to address risk, compared to flexible individual and collective assessments and practices (Aven, 2015). As suggested by Juhl (Chapter 2, in this volume), risk is

more than anything characterized by diversity and variability, whereas standardization implies abstracting from diversity and variability, proving a potentially dangerous prospect. As this chapter will discuss, it may be both necessary and feasible to reconcile standardization and flexibility in surgical operations.

Standardization and flexibility in Norwegian healthcare

Standardization features strongly in the Norwegian healthcare system. This is evident in White Papers and official Norwegian reports that highlight the importance of cross-organizational coordinated and integrated services, including standardized patient pathways, as a main strategy to improve quality of services, resource use, and work environments (NOU, 2005; HOD, 2006, 2012, 2015). The standardization tendency further encompasses information systems and the work practices of healthcare personnel, as can be seen in the transition from written patient records and oral handovers[1] to electronic patient records (EPR) and electronic handover accounts, respectively (Pedersen, 2012). Similar transformations are evident in the increased implementation of standardized checklists, targeted at improving aspects of work practices (team, task, and equipment awareness) and patient outcomes (morbidity, mortality, and length of in-hospital stay) in surgery, anaesthesia, and other fields (Thomassen *et al.,* 2010; Høyland, Haugen, and Thomassen, 2014; Haugen *et al.,* 2015). Common to the standardization efforts is their aim to improve efficiency, safety, and quality. However, these efforts can also detract from the same goals. As Pedersen states:

> A fundamental characteristic of [the work of healthcare personnel] is its pragmatic fluid character with complex work activities that requires ad hoc and pragmatic response. Healthcare work is further characterized by its distributed decision-making, by 'multiple viewpoints' and by its 'inconsistent and evolving knowledge base'.
>
> (2012, pp. 18–19)

Thus, health personnel require a certain amount of flexibility to approach the complexity of their work tasks, including assessments of risks in the operating room and associated safety responses or precautions, such as the use of safety procedures and checklists. Related to the topic of standardization, processes of standardization may not account for the complexity of everyday healthcare practices, including the various ways risks are addressed by thinking and acting flexibly when it comes to safety.

Context: the operating room

In order for the reader to better visualize the context of this chapter, Figure 7.1 provides an overview of the layout of the typical operating room (explored in the projects outlined above), accompanied by descriptions of the roles and work zones of the operating personnel.

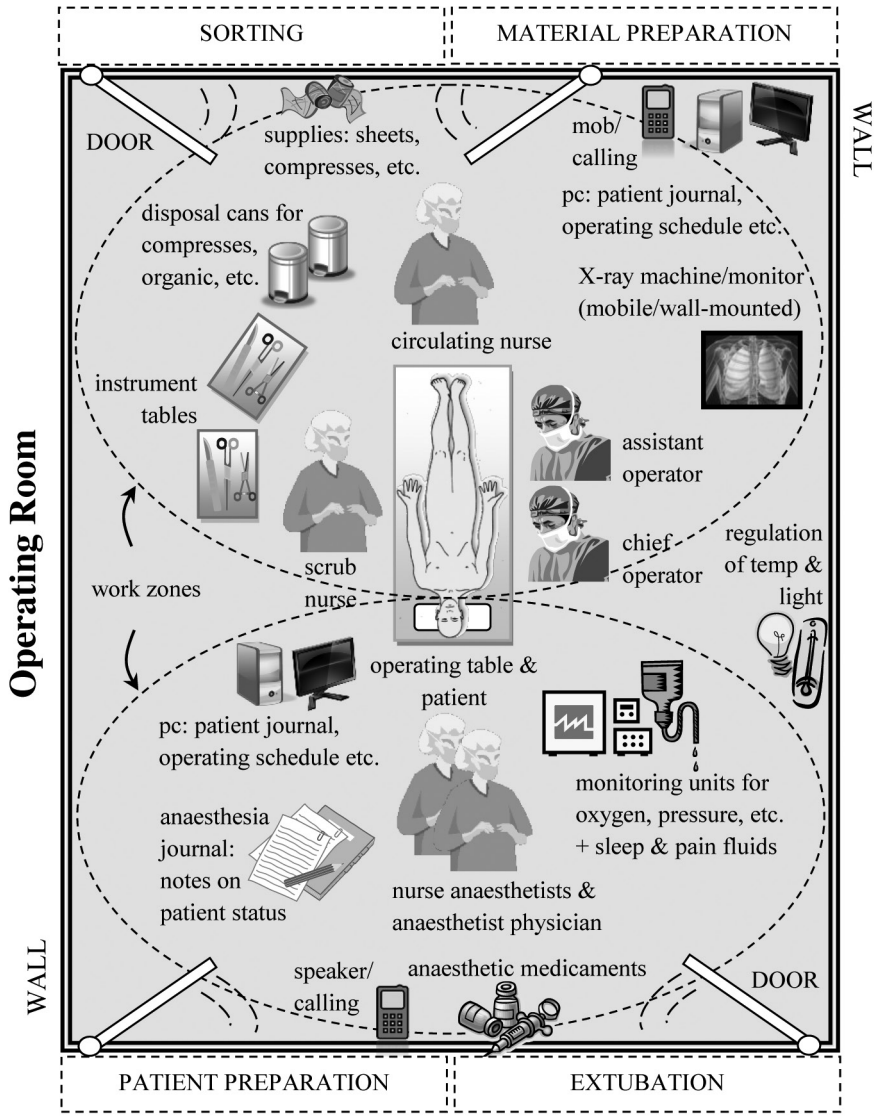

Figure 7.1 Layout of a typical operating room: zones, participants, and equipment.

Notes

- SORTING: In this room, operating room nurses prepare equipment and instruments for the particular operation.
- MATERIAL PREPARATION: In this room, the operators change into operating clothing before entering the operating room.
- PATIENT PREPARATION: Anaesthesia personnel prepare for the operation, receive patient, and enter the operating room (with patient) from this room.
- EXTUBATION: Upon completion of the operation, the patient is transported out of the operating room via this room. In case of intubation, tubes are also removed in this room.

The operating room consists of two specific work zones. One is associated with operating personnel (dashed circle at the top of Figure 7.1) and the other, with anaesthesia personnel (dashed circle at the bottom of Figure 7.1). The former is defined as the operating zone and the latter, as the anaesthesia zone. A work zone is the general area for which the particular team member is responsible and/or associated with from the beginning to the end of the operation.

The operating zone includes the operator(s) and operating room nurses (scrub nurse and circulating nurse). Specifically, a main operator is in charge of the procedure: making the incision, operating, and closing the (marked) operating area of the patient. The main operator relies on the scrub nurse to provide the necessary equipment and instruments (which the nurse has prepared on the instrument tables) and an assistant operator for input on progress and decisions to be made.

The main operator typically combines inputs both from colleagues and the X-rays (accessible from the wall monitor or mobile X-ray machine/monitor), to judge the procedure's progress. The scrub nurse's job is to hand the main operator the necessary instruments, so s/he rarely leaves the vicinity of the instrument tables. During certain procedures, the scrub nurse also assists the operator to maintain the patient in a steady position (for example, legs or arms) and helps the operator's access to the operating area. The circulating nurse keeps track of who is present during the operation (noting names and roles) and the upcoming operating schedule (planning and preparations) via the computer (upper right corner of Figure 7.1). The circulating nurse also observes and regulates who is allowed to enter and exit the operating room, maintaining sterile conditions as much as possible. In addition, the circulating nurse often obtains necessary supplies or equipment from the sorting room, other areas of the surgical unit, or even other areas of the hospital. However, both operating room nurses are responsible for managing equipment, instruments, and supplies in general, such as counting and sorting instruments before and after the operation.

The anaesthesia zone (bottom section/dashed circle in Figure 7.1) is on the opposite side of the operating room. Within this zone, the anaesthesia personnel administer general anaesthesia, if needed, and also continuously monitor the patient's status. The monitoring is done visually/physically by looking at and touching the patient, to determine whether the patient reacts negatively (for example, becomes cold or uneasy during general anaesthesia) to different aspects/phases of the surgical procedure. Monitoring is also done electronically, by observing the monitoring units (lower right corner of Figure 7.1). Combined, these efforts ensure that the correct dosages of sleep and pain-reducing medications are administered at any given time, and that oxygen, gases, and pressure levels are set correctly on the machines. Typically, one or two nurse anaesthetists take turns observing the vital data and writing it in the anaesthesia journal. The nurse anaesthetist also keeps track of calls from outside, via the speaker/calling function, and keeps an eye on the upcoming operation via operating schedules on the computer (ensuring preparedness). Anaesthetic medicaments are located directly behind the nurse anaesthetist, providing easy access to

preparing and administering new sleep and pain dosages. The second member of the anaesthesia zone is the anaesthetist physician, who is responsible for carrying out the more skilled anaesthetic procedures, such as insertion of an artery cannula for arterial blood pressure. The anaesthetist physician commonly stays directly outside the operating room, in the adjacent patient preparation room, where s/he monitors the patient's status from time to time but also prepares for the next operation by reviewing the next patient's journal. However, the anaesthetist physician is responsible for more than one operating room and often moves between several operating rooms, as needed.

In relation to the patient, the anaesthesia zone is from the neck up, because this zone focuses on respiratory functions. At this surgical unit, the operating zone is located from the neck down, focusing on back stabilizations, fractures, revisions, and extensions.

Methodology

Data collection and analysis for Study 1

With the aim of exploring how safety is achieved in surgical operations, Study 1 was conducted at an orthopaedic surgical section of a Norwegian hospital, with the interdisciplinary surgical team as the main research unit. The main methods of data collection included 27 non-participant observations of surgical operations, as well as 35 informal conversations and 15 semi-structured interviews with surgical team members (anaesthetist physicians, nurse anaesthetists, operating room nurses, and operators) and managers. The field work consisted of identifying emergent patterns during observations of the surgical operations, followed by the further exploration of these patterns during conversations and interviews, to gain a deeper understanding of the particular pattern and its validity. This represented a triangulation approach, understood as the act of combining multiple sources of data (observations, conversations, and interviews) to reach a deeper understanding and thereby validate an observation. Triangulation improves confidence in the research data and strengthens the credibility/validity of the research (Denzin, 1970; Thurmond, 2001). For more details on this study, see Høyland (2012).

Data collection and analysis for Study 2

The study was performed in a surgical section of a Norwegian university hospital, between November 2011 and January 2012. The study explored frontline operating personnel's perceptions of time spent on the World Health Organization's (WHO's) Surgical Safety Checklist.[2] Applied in the study was a focus group methodology (Krueger and Casey, 2000), which is understood as 'a way of collecting qualitative data, which – essentially – involves engaging a small number of people in informal group discussions, "focused" around a particular topic or set of issues' (Wilkinson, 2004, p. 177). Three focus group interviews

were conducted (Kyrkjebø, Brattebø, and Smith-Strøm, 2006). The first interview involved operating room nurses and nurse anaesthetists (n = 6), the second interview involved anaesthetists (n = 4), and the third, surgeons (n = 4). A purposeful sample was recruited from personnel who had more than one year of experience with the Surgical Safety Checklist. The participants were selected through consultation with the managers of the section, the leaders of each profession (nurses, physicians, surgeons), and the researchers involved in Study 2. Average experience with the checklist in the section as a whole, across all professions, was about two years. For more details about this study, see Høyland, Haugen, and Thomassen (2014).

Empirical findings

Based on data from Study 1 and Study 2, the purpose of the findings section is to shed empirical light on the research issue introduced in the research problem, empirical data, and key concepts section, specifically exploring the roles of standardization and flexibility in surgical operations, focused on their influence on risks to the patient undergoing surgery. The included findings highlight aspects of both standardization and flexibility that affect risk levels in everyday practices in the operating room.

Standardization, risk and flexibility in surgical teamwork: Study 1 findings

Study 1 documented several field observations that shed light on how knowledge and experience are expressed in interdisciplinary surgical operations. These observations reveal the importance of thinking and acting flexibly in the team's ability to handle uncertainty and reach a particular decision, specifically by means of gathering and combining multiple information sources, both technological and human in nature. This is illustrated in the following observation (Operation A): Before starting the procedure in this particular operation, the main operator (surgeon) gathers his team for a briefing by a monitor displaying the patient's X-rays. During the briefing, the main operator describes the patient's condition and history, and he also explains the specific steps involved in the coming procedure (pointing and illustrating via the X-rays). He seems to be seeking approval for the procedure. At a later time in the procedure, the main operator is confronted with a choice between method A and method B. He again gathers his team by the X-rays and receives inputs from his team and from what he sees in the pictures. The operator then makes his decision. Several X-rays are later taken, to confirm the decision. The practice of flexibly combining multiple information sources when faced by uncertainty can also be seen in Operation B: during preparations for this operation, uncertainty concerning the patient's position can be seen. Problem-solving then kicks in: The anaesthetist nurse checks the planning system, Orbit, for information on the pre-anaesthesia assessment of the patient from the day before. She also confers with the first operating room

nurse. Neither the system nor the operating room nurse provides any clear answers. The first operating room nurse takes over the problem-solving task and asks the second operating room nurse to make enquiries with the main operator. At last, an answer is obtained on the position of the patient.

Another aspect of surgical operations, demonstrating the importance of flexibility as well as standardization (through procedures) in reducing risks in the operating room, was revealed in the surgical team's awareness or anticipation of future events. Here, a combination of both explicit/procedure-based elements (such as preparing equipment) and tacit/experience-based elements (such as checking urine and preparing gloves and syringe) comes into play. This is reflected in observations of Operation C: during the preparations for this particular operation, the first nurse anaesthetist prepares the anaesthesia equipment, including back-up solutions, prior to the patient's arrival. These preparations are regulated by procedures, she explains. Before the operation begins, the first nurse anaesthetist scans the patient's urinary bladder to make sure it is empty. Upon enquiry, she explains that this activity is not regulated by procedures but the result of previous experience from situations where too much urine has accumulated in the patient's bladder. Before the operation begins, the first operating room nurse has also prepared several alternative sets of gloves. She explains this action by the need to be prepared, since a plastic surgeon she is unfamiliar with will be present. Later in the operation, the second nurse anaesthetist (who replaces the first, due to a break) notices that the large plastic syringe with the sleeping medicament is about to be depleted, but he has prepared a new one beforehand. At the end of the operation, the second nurse anaesthetist has already called on the patient for the upcoming operation.

The practice of combining aspects of procedures and experience, to improve awareness or anticipation of future events, can also be seen in Operation A: during this operation, the position of the patient is checked several times and at different stages by the anaesthetist nurses, the operating room nurses, and the main operator. Specifically, during preparations, belts and blankets are removed from the operating bench. This, we are told, is to prevent pressure injury when a patient remains in a given position for a prolonged period. When the main operator arrives in the operating room, he also reviews and confirms the patient's position. During the procedure, the operating room nurse massages and also lifts the arms and legs of the patient, in order to improve circulation and prevent damage. Near the end of the procedure, the operating room nurse checks the patient's position and makes sure no injury has occurred during the operation.

A content analysis of the empirical interview findings revealed further insight into the importance of flexibility in surgical operations (see Høyland, 2011). This can be seen in the individual's ability to disregard stress/pressure and apply the necessary time and considerations to do the job properly, including the decision to involve a second person/opinion during a procedure and/or the ability to think ahead by calling for assistance to save precious time in a critical situation. Moreover, flexibility in surgical operations was illustrated in the team's reliance on individuals' competency and ability to plan and improvise when challenged

by a problem or an unforeseen situation during an operation. Specifically, the reliance on the particular team member depended on trust in the competency levels of the individual/specialization. This meant that a nurse anaesthetist's medical judgement was heard during the operation and could result in the suspension of an operation.

In sum, the empirical findings so far indicate that flexibility plays a crucial role in reducing risks during surgical operations, as seen in the surgical team's ability to address uncertainty (which presents risks) and anticipate events, by combining different sources of information and knowledge (explicit and tacit), respectively. The importance of flexibility is also evident in the team's reliance on individual competency, planning, and improvisation, to handle the unforeseen.

Disruptions, system buffers, and risk in surgical teamwork: Study 1 findings

Study 1 also sheds light on how disruptions and vulnerabilities can arise, through various combinations of system factors surrounding surgical operations, which increase risk levels, and how the operating team was able to compensate for these disruptions by means of flexible system buffers, as well as exclusive exposure to one hospital section. The disruptions are illustrated in the following observation (Operation D): during preparations for this operation, the main operator enters the operating room and a discussion is triggered between the operator and the first operating room nurse (inexperienced) concerning the type of operation scheduled. The first operating room nurse has been informed of mobilization and testing in anaesthesia, but the main operator claims that an open surgery is scheduled. The nurse seems annoyed, seeing that she now needs to obtain unplanned-for equipment. Meanwhile, the main operator is seen walking restlessly across the floor. The discussion continues, regarding which patient was assigned to the operating room (of two patients that arrived simultaneously). The second operating room nurse (experienced) claims that they (the team) only followed the plan. She is supported by the nurse anaesthetist, who explains to the main operator that she selected the patient from the list in Orbit. The main operator replies by placing the responsibility for the two patients on another individual, suggesting that he did not make the priorities. Despite a heated discussion, the operation proceeds as normal and concludes with no remarks. Similar disruptions are observed in Operation A: early in this operation, the operator claims that the second operating room nurse should have more equipment prepared for this type of surgery. The nurse leaves the room to obtain what he asks for. This event is followed by a call from a colleague on his mobile phone. The operator decides to address it properly, even though the conversation does not concern the operation. At a later stage of the procedure, the main operator continues to request equipment. The equipment is not directly available in the operating room and is also hard to obtain right away. The operator seeks alternative solutions. He also becomes increasingly annoyed at the 'instrument service', particularly when the first operating room nurse demonstrates trouble

in obtaining the requested instruments. The annoyance seems to escalate with the nurse's displays of inexperience, when, finally, he decides to walk over and get the instruments himself. Again, the operation proceeds as normal and concludes with no remarks.

These and other observations revealed how various combinations of system factors contributed to disrupt the operational flow, although the particular operation continued and was completed as normal. Specifically, for an operation to become vulnerable and experience disruptions in the normal flow, a combination of local and external system factors typically needed to be simultaneously triggered. External structural factors (outside the operating room) included changes in the operating schedules, lack of planning in preparing operational equipment, less than ideal ad hoc team compositions (such as inexperience under immediate and/or demanding surgery), delays in equipment arrivals (once requested), and lapses in individual control checks at several organizational levels. Internal structural factors (within the operating room) included the team members' moods, mobile phone disruptions, equipment failure and lack of control, and lack of equipment in the operating room. Once the negative external and internal structural factors interacted in some way, operations became vulnerable.

However, various system factors appeared to compensate for the vulnerabilities and disruptions, because the observed operations proceeded despite interruptions (that is, the focus was on 'the job' and safety). Specifically, buffers, such as staffing, equipment, and operating rooms, constituted the outer structural factors of the system and part of the compensating ability during operations. An anaesthetist physician suggested that these buffers can reduce the individual workload and thereby strengthen the working environment. Overall, the buffers helped to explain why the operations continued as normal, despite disruptions, such as less than ideal ad hoc team compositions under demanding surgery interacting with team members' moods, for instance. Another compensating system factor was that operating personnel were exposed to only one hospital section, which over time boosted specialized knowledge, confidence levels, and the ability to become proficient with the equipment and select the right equipment at the right time.

Overall, the descriptions above illustrate flexibility in surgical operations comprising several system factors or elements, including staffing, equipment, and operating rooms buffers, as well as personnel exposure to one hospital section increasing individual knowledge and confidence levels. This level of flexibility compensates for disruptions and vulnerabilities in the operating room, and thereby reduces the risks to the patient undergoing surgery.

Spending checklist time can save operating room time: Study 2 findings

A short introduction to this section is necessary to familiarize the reader with the WHO's Surgical Safety Checklist, described in the Study 2 findings below. The Surgical Safety Checklist, understood as a formalized procedure and standardization approach used in the operating room, is divided into three sections or

phases: 'sign-in', 'time-out', and 'sign-out'. The sign-in focuses on the particular safety steps that must be performed prior to induction of anaesthesia, including communication with the patient. The time-out should be conducted when the entire operating team is present, immediately prior to the incision. Important discussion points during time-out include a 'roundtable introduction' of each team member (with name and role/function), the name of the patient and the planned procedure, site, risk factors, infection concerns, and so forth. Finally, the sign-out constitutes elements, such as the name of the performed procedure, counting instruments and swabs, messages to be passed along to post-operative care, and review of equipment (including difficulties).

Next, to the study findings. The study participants indicated that time spent on the Surgical Safety Checklist can improve awareness, preparedness, and systemizing, and can save operating room time in general, thus reducing risk levels, as exemplified in the following excerpts:

> I feel that, if we do a proper time-out, it doesn't take long. It takes very little time and is incredibly important. I think it's great that we have it, and it creates a sense of safety for everyone, especially the patient, who is the main focus.
>
> (Nurse anaesthetist 1)

> [The checklist] strengthens culture and the team's awareness of things in a systematic way. As a concrete example, I'm absolutely sure that the communication and performance of antibiotic administration [are] better than before [the list].
>
> (Anaesthetist 2)

> I believe a good time-out, where everyone agrees on the importance of this, is actually time-saving, because then you're more aware of what [equipment] to use and how to use it … so I believe we save time on a good time-out.
>
> (Operating room nurse 1)

Furthermore, the study participants suggested that time spent on the Surgical Safety Checklist depends on the team's familiarization levels, as seen in the following excerpts:

> It was a struggle to begin with; when there was opposition [to the use of the list], particularly among the physicians, it took time. I believe they (the physicians) have realized that we can actually save time by using it, and that it's really important.
>
> (Operating room nurse 2)

> To begin with, the conflict [referring to the lack of time and use of time on the checklist] was larger, since you were used to working without the

checklist. This made you feel that the list took time. Now that we have grown used to working with [the list], it's no longer a problem.

(Anaesthetist 3)

It's very person-dependent. You can predict beforehand how the checklist is going to be handled … almost.

(Operating room nurse 1)

Combined, the excerpts suggest that spending time on and becoming familiar with the Surgical Safety Checklist, as a standardized procedure, can strengthen the operating team's awareness and preparedness, in terms of what equipment to use, for example, and the team's ability to systemize aspects of surgical operations (such as communication and performance). Using the checklist can also save operating room time, due to improvements in the operating team's awareness, preparedness, and ability to systemize, and can improve the sense of safety for both the team and the patient. Overall, the study participants suggested that time spent on the Surgical Safety Checklist can reduce total operating room time, depending on the operating team's familiarization levels, with associated potential for reduction in risk levels in surgical operations.

Another finding of Study 2 concerns planning and rational use of time in surgical operations, as evident in the following two excerpts:

The use of time has much to do with planning, I believe. A major surgical procedure is to be undertaken and there are a lot of things that need to be prepared in advance. A lot of equipment for the operating and anaesthesia personnel must be in place … It has to do with rational use of time, during the anaesthesia, during the operation itself, that we're rational in our use of time … to avoid unforeseen events.

(Anaesthetist 1)

The surgeon who plans [the operation] can override [the average time the planning system produces] if he knows it is a complicated patient that will take longer time than the average … The most experienced surgeons should be aware of these things … However, it's my experience that they [the surgeons] leave many of the planning tasks –[data to be entered into the electronic planning system] to a secretary … and this has to do with [the surgeons' willingness] learning how to use the [planning system], and to spend time on this.

(Anaesthetist 4)

Judging by these study participants, an important planning element when attempting to avoid unforeseen events relates to the rational use of time on equipment preparation, anaesthesia, and the operation itself, while another planning element concerns how spending time and experience on the electronic planning system ensures that the necessary amount of time is assigned to the particular

operation and patient. Thus, planning becomes an experience-based tool, with which the surgeon can reduce or increase the time spent on a given patient, with potentially strengthening effects on patient safety, if the adjustment is applied with concern to reducing risks only.

The empirical findings combined suggest that standardization by means of checklists such as the Surgical Safety Checklist can improve the operating team's level of preparedness, awareness, and ability to systemize, which in turn can reduce total operating room time and thus the risks to the patient undergoing surgery. Similar risk reduction and patient safety benefits can be gained from spending time on planning and on standardized systems such as the electronic planning system to ensure that the necessary amount of time is spent on the particular patient.

Discussion

The empirical findings highlight the complexity present in everyday surgical operations, where operating personnel need to think outside of the rules, procedures, and textbook knowledge, to achieve safe operations and patient safety. This thinking is reflected in several of the findings, such as: (1) the individual's ability to disregard stress/pressure and apply the necessary time and considerations to do the job properly; (2) the team's reliance on individuals' competency and ability to plan and improvise when challenged by a problem or an unforeseen situation during an operation; (3) the team's ability to handle uncertainty and reach a particular decision, by means of gathering and combining multiple information sources; and (4) the surgical team's awareness or anticipation of future events, by combining both procedure and experience elements. The empirical findings also highlighted that system buffers, such as staffing, equipment, operating rooms, and exposure to one hospital section (improving competency, skills, confidence), are needed to compensate for disruptions and vulnerabilities related to human behaviour (lack of planning, control checks, mood swings), technology (equipment failure, mobile phone disruptions) and organization (changes in operating schedules, delays in equipment arrival).

Overall, the findings on surgical operations and practices suggest that having the room and ability to think and act flexibly is needed at an individual and team level, as well as at a structural and organizational level surrounding operations, in order to reduce risk levels and achieve a safe outcome for the patient during surgical operations. The characteristics of flexibility in surgical operations, as described in this chapter, are strikingly similar to the ideas presented in theories on high-reliability organizations (HROs), that is, organizations that have low accident rates, despite working under high pressure and trying conditions. The main principles behind these organizations' ability to achieve and maintain such success can be classified as standard operation procedures in normal operations, sensitivity to operations, and resilient design, as demonstrated in their ability to pre-programme operational procedures, to sense the need for local operational adaptions, and to treat signals of failure as having the potential to result in catastrophic

system events (Almklov and Antonsen, 2010). A number of existing safety research concepts encompass variants of these core principles, including the concepts of latent errors (Reason, 1997; Ramanujam and Goodman, 2003; Putz *et al.,* 2013), mindfulness (Weick and Sutcliffe, 2001; Weick and Putnam, 2006; Vogus and Sutcliffe, 2012), and organizational resilience (Kantur and_Iseri-Say, 2012; Aleksic *et al.,* 2013; Sahebjamnia, Torabi, and Mansouri, 2015).[3] The mindfulness concept is particularly interesting, since its principles, 'sensitivity to operations', 'reluctance to simplify', 'preoccupation with failure', 'commitment to resilience' and 'deference to expertise', focus both on the operational and the organizational/system levels evident in the empirical data (Weick and Sutcliffe, 2001; Weick and Putnam, 2006; Sellnow *et al.,* 2009; Vogus and Sutcliffe, 2012; Hales and Chakravorty, 2016).

Consider the sensitivity to operations, reluctance to simplify, and deference to expertise principles. The first principle is understood as an awareness of the situation surrounding a particular operation or process that enables abnormalities to be recognized and addressed, while the third principle concerns deferring decisions downwards or around the organization to the individual who works most closely with the procedure or problem in question and therefore possesses the most relevant expertise and experience. The middle principle, reluctance to simplify, implies a careful and limited use of categories, to ensure that details about events, experiences, and opinions of organizational members are preserved, and simplifications are kept to a minimum. All three principles are reflected in the empirical understanding that procedures and decisions are founded on experience and expertise, tacit knowledge, situational awareness, and a flat leadership and decisional structure. Specifically, the findings indicate that there is a flat decisional structure in the operating room, with expertise governing responsibilities and decision-making. Consequently, the team member with the most experience and also natural responsibility, for a given work task or procedure, determines leadership and decision-making in the operating room (deference to expertise). The findings also indicate that the team as a whole is sensitive to the particular patient and potential situations (sensitivity to operations), where, for instance, the nurse is aware that several different complications may ensue during an operation and is mentally prepared for this, by planning and thinking ahead about how to respond to any situations that may occur (reluctance to simplify). Individually and combined, the practices of surgical teams, characterized by flexibility, appear to reduce risks and strengthen patient safety in the surgical operating environment.

On the other hand, while flexibility in surgical operations might reduce risks and thus enhance patient safety, the empirical data also describe the importance of standardization through planning systems, checklists, and other procedures. Most notably, the findings indicate that the Surgical Safety Checklist can strengthen the operating team's awareness, preparedness, and ability to systemize and, above all, it can save operating room time, which is of critical importance to risk levels and patient safety during operations. Specifically, in the literature, operating room time is portrayed as being a concern to performance and outcome

in surgery and an obstacle that must be controlled to ensure optimal performance and outcome (Høyland *et al.,* 2014). Moreover, the observations described in the empirical findings highlighted an interesting interplay or symbiosis between standardization and flexibility in surgical operations, where standardization expressed through explicit procedures is combined with experience-based elements, such as the surgical team's awareness or anticipation of future events. This interplay empirically documents how standardization and flexibility can go hand in hand when it comes to reducing risks and strengthening patient safety in surgical operations. The interplay may in fact be a natural aspect of surgery, which should be subjected to further empirical exploration. Finally, one could also extend the notion of standardization to encompass having a 'standard for operational buffers', such as staffing, equipment, and operating rooms, to compensate for disruptions and interruptions during surgery, as evident in the empirical data. Whether establishing a standard for operational buffers is at all feasible, given the constraints put on resources and with the demand for efficiency in healthcare and the hospital system, is a question that needs to be pursued elsewhere and compared to the potential benefits to reducing risks and improving patient safety in surgery.

Conclusion

In conclusion, the findings indicate that standardization in surgical operations can only go so far before compromising operating personnel's ability to think and act flexibly when it comes to the safety of the patient. At the same time, standardization through the WHO Surgical Safety Checklist has become an invaluable tool to prevent wrong-site surgery, higher-than-planned-for blood loss, and other complications during surgery, thus reducing the risk levels to patients. To address the research issue introduced in the research problem, empirical data and key concepts section – 'to explore the roles of standardization and flexibility in surgical operations, focused on their influence on risks to the patient undergoing surgery' – the central issue is not standardization *or* flexibility, it is about combining them to be practised in sensible doses. The risks of surgical practice moving too far in either a standardization or flexibility direction are directly reflected in the safety concept of normalization; normalization can be seen in local practices that gradually become detached from written procedures, or irregularities and deviations that are normalized, where the results can be serious or catastrophic incidents or accidents (Vaughan, 1996; Snook, 2000). In other words, if thinking and acting outside the rules, regulations, and procedures become the norm, the risks to the patient undergoing surgery increase considerably.

Furthermore, the healthcare system – down to the specific hospital and operating room – constitutes a complex work domain, comprised of multiple human agents that work under uncertainty, time pressure, multiple interacting goals (productivity and safety), and potentially high consequences of failure (loss of human/patient life) (Johansen, Almklov, and Mohammad, 2016; Watts-Englert,

Woods, and Patterson, 2018). In such a setting, standardization is easier to apply in more stable operational phases, for example, through the WHO Surgical Safety Checklist and procedures for preparing the patient in advance of the operation. However, standardization becomes a lot harder when time is critical and the stakes high, for instance, when operational personnel face complications and risks to the patient, due to errors and/or patient physiology. It follows that the balancing act between standardization and flexibility is closely related to and dependent on the degree of stability or instability present in a given time and context.

In terms of implications of the empirical findings, it is important to consider the association between standardization and perceptions of sameness, suppression, or uniformity, which promote control but also restrain freedom (Timmermans and Epstein, 2010). This restraint can be at odds with the freedom or autonomy expected and practised by different healthcare professions – and by physicians and surgeons, in particular. In other words, it is necessary to balance explicitly formulated rules for regulating individual and collective behaviour, as manifested in formalized procedures such as checklists, and the ability to perform one's job in a flexible manner that comprises knowledge, experience, improvisation, and so forth. Given the potential that flexible practices might reduce risks in the operating environment, it follows that political, regulatory, and hospital actors involved in the current organization of the healthcare system in Norway should be careful not to overstimulate efforts at standardization, and to allow for flexibility when needed. The findings also indicate that risk levels and patient safety can benefit from surgical personnel being exposed to one hospital section over time, combined with less ad hoc team compositions, given the associated potential for boosting specialized knowledge, confidence levels, and equipment proficiency.

Notes

1 The process when information about patients and work responsibilities is transferred from one shift to the next.
2 The Surgical Safety Checklist is explained in the results section.
3 See Høyland *et al*. (2018) for an empirical exploration of different HRO safety principles across the healthcare sector and construction industry in Norway.

References

Aleksic, A., Stefanovic, M., Arsovski, S. and Tadic, D. (2013). An assessment of organizational resilience potential in SMEs of the process industry: A fuzzy approach. *Journal of Loss Prevention in the Process Industry*, 26, pp. 1238–1245.

Almklov, P. G. and Antonsen, S. (2010). The commoditization of societal safety. *Journal of Contingencies and Crisis Management*, 18, pp. 132–144.

Aven, T. (2015). Implications of black swans to the foundations and practice of risk assessment and management. *Reliability Engineering & System Safety*, 134, pp. 83–91.

Aven, T. and Renn, O. (2009). On risk defined as an event where the outcome is uncertain. *Journal of Risk Research*, 12, pp. 1–11.

Beck, U. (1992). *Risk society: Towards a new modernity*, London: Sage.

Brunsson, N. and Jacobsson, B. (2000). *A world of standards.* New York: Oxford University Press Inc.

Brunsson, N., Rasche, A. and Seidl, D. (2012). The dynamics of standardization: Three perspectives on standards in organization studies. *Organization Studies*, 33, pp. 613–632.

Denzin, N. K. (1970). *The research act: A theoretical introduction to sociological methods.* Chicago: Aldine.

Hales, D. N. and Chakravorty, S. S. (2016). Creating high reliability organizations using mindfulness. *Journal of Business Research*, 69, pp. 2873–2881.

Haugen, A. S., Softeland, E., Almeland, S. K., *et al*. (2015). Effect of the World Health Organization checklist on patient outcomes: A stepped wedge cluster randomized controlled trial. *Annals of Surgery*, 261, pp. 821–828.

HOD (2006). Report to the Storting no. 1 (2007–2010). National health plan for Norway. White Paper. Oslo: The Norwegian Ministry of Health and Care Services.

HOD (2012). Report to the Storting no. 10 (2012–2013). Good quality – safe services: Quality and patient safety in health and care services. White Paper,. Oslo: The Norwegian Ministry of Health and Care Services.

HOD (2015). Report to the Storting no. 11 (2015–2016). National health and hospital plan (2016–2019). White Paper, Oslo: The Norwegian Ministry of Health and Care Services.

Høyland, S. (2011). Exploring safe work practices in surgical operations: the role of time, patient, and operation. In S. Albolino, S. Bagnara, T. Bellandi, *et al.,* eds. *Healthcare systems ergonomics and patient safety 2011: Risks in OR, ICU and ER*. AK Leiden, The Netherlands: CRC Press.

Høyland, S. (2012). Developing and validating a scientific model for exploring safe work practices in interdisciplinary teams. *Safety Science*, 50, pp. 316–325.

Høyland, S. (2013). Safe work practices in interdisciplinary surgical teamwork: Model development and validation. PhD thesis, University of Stavanger.

Høyland, S., Aase, K., and Hollund, J. G. (2011a). Exploring varieties of knowledge in safe work practices: An ethnographic study of surgical teams. *Patient Safety in Surgery*, 5(21).

Høyland, S., Aase, K., and Hollund, J. G. (2011b). Understanding the system in relation to safe medical work practices. *Safety Science Monitor*, 12, Article 5.

Høyland, S., Haugen, A. S., and Thomassen, Ø. (2014). Perceptions of time spent on safety tasks in surgical operations: A focus group study. *Safety Science*, 70, pp. 70–79.

Høyland, S. A., Skotnes, R. Ø., and Holte, K. A. (2018). An empirical exploration of the presence of HRO safety principles across the health care sector and construction industry in Norway. *Safety Science*, 107, pp. 161–172.

Johansen, J. P., Almklov, P. G., and Mohammad, A. B. (2016). What can possibly go wrong? Anticipatory work in space operations. *Cognition, Technology & Work*, 18, pp. 333–350.

Kantur, D. and Iseri-Say, A. (2012). Organizational resilience: A conceptual integrative framework. *Journal of Management and Organization*, 18, pp. 762–773.

Krueger, R. A. and Casey, M. A. (2000). *Focus groups: A practical guide for applied research.* London: Sage.

Kyrkjebø, J. M., Brattebø, G., and Smith-Strøm, H. (2006). Improving patient safety by using interprofessional simulation training in health professional education. *Journal of Interprofessional Care*, 20, pp. 507–516.

Laursen, K. and Meliciani, V. (2010). The role of ICT knowledge flows for international market share dynamics. *Research Policy*, 39, pp. 687–697.

Line, M. B. and Tøndel, I. A. (2012). Information and communication technology: Enabling and challenging critical infrastructure. In P. Hokstad, I. B. Utne, and J. Vatn, eds. *Risk and interdependencies in critical infrastructures.* London: Springer.

Lodge, M. and Hood, C. (2003). Competency and bureaucracy: Diffusion, application and appropriate response? *West European Politics*, 26, pp. 131–152.

Månsson, P., Abrahamsson, M., Hassel, H., and Tehler, H. (2015). On common terms with shared risks: Studying the communication of risk between local, regional and national authorities in Sweden. *International Journal of Disaster Risk Reduction*, 13, pp. 441–453.

NOU (2005). *From stepwise to complete: A coherent health service* (NOU 2005:3). Oslo: State Administration Services.

NOU (2015). *Digital vulnerability – secure society: Protecting individuals and society in a digitalized world* (NOU 2015:13). Oslo: Norwegian Government Security and Service Organisation.

Pedersen, R. (2012). Standardizing work in healthcare through architecture, routines and technologies. In J. Dugdale, C. Masclet, M. A. Grasso, J-F. Boujut, and P. Hassanaly, eds. *From research to practice in the design of cooperative systems: Results and open challenges.* London: Springer.

Power, M. (2004). The risk management of everything. *The Journal of Risk Finance*, 5, pp. 58–65.

Power, M. (2007a). Corporate governance, reputation, and environmental risk. *Environment and Planning C: Government and Policy*, 25, pp. 90–97.

Power, M. (2007b). *Organized uncertainty: Designing a world of risk management*. Oxford: Oxford University Press.

Putz, D., Schilling, J., Kluge, A., and Stangenberg, C. (2013). Measuring organizational learning from errors: Development and validation of an integrated model and questionnaire. *Management Learning*, 44, pp. 511–536.

Ramanujam, R. and Goodman, P. S. (2003). Latent errors and adverse organizational consequences: A conceptualization. *Journal of Organizational Behavior*, 24, pp. 815–836.

Reason, J. (1997). *Managing the risks of organizational accidents.* Aldershot: Ashgate.

Rosa, E. A. (1998). Metatheoretical foundations for post-normal risk. *Journal of Risk Research*, 1, pp. 15–44.

Sahebjamnia, N., Torabi, S. A., and Mansouri, S. A. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. *European Journal of Operational Research*, 242, pp. 261–273.

Sellnow, T. L., Ulmer, R. R., Seeger, M. W., and Littlefield, R. (2009). *Effective risk communication: A message-centered approach*. New York: Springer Science+Business Media, LLC.

Snook, S. A. (2000). *Friendly fire: The accidental shootdown of U.S. Black Hawks over Northern Iraq*. Princeton, NJ: Princeton University Press.

Thomassen, O., Brattebo, G., Heltne, J. K., Softeland, E., and Espeland, A. (2010). Checklists in the operating room: Help or hurdle? A qualitative study on health workers' experiences. *BMC Health Services Research*, 10(342).

Thurmond, V. A. (2001). The point of triangulation. *Journal of Nursing Scholarship*, 33, pp. 253–258.

Timmermans, S. and Epstein, S. (2010). A world of standards but not a standard world: Towards a sociology of standards and standardization. *Annual Review of Sociology*, 36, pp. 69–89.

Vaughan, D. (1996). *The Challenger launch decision: Risky technology, culture, and deviance at NASA*. Chicago: University of Chicago Press.

Vogus, T. J. and Sutcliffe, K. M. (2012). Organizational mindfulness and mindful organizing: A reconciliation and path forward. *Academy of Management Learning & Education*, 11, pp. 722–735.

Watts-Englert, J., Woods, D. D., and Patterson, E. S. (2018). Resilient anomaly response in Mission Control Center. In B. Kanki, J. F. Clervoy, and G. M. Sandal, eds. *Space safety and human performance*. Cambridge, MA: Butterworth-Heinemann.

Weick, K. E. and Putnam, T. (2006). Organizing for mindfulness: Eastern wisdom and Western knowledge. *Journal of Management Inquiry*, 15, pp. 275–287.

Weick, K. E. and Sutcliffe, K. M. (2001). *Managing the unexpected*, San Francisco, CA: Jossey-Bass.

Wilkinson, S. (2004). Focus group research. In D. Silverman, ed. *Qualitative research: Theory, method, and practice*. London: Sage.

Zhang, X., Pieter van Donk, D. and van der Vaart, T. (2011). Does ICT influence supply chain management and performance? *International Journal of Operations & Production Management*, 31, pp. 1215–1247.

Part III

Impact of standardization processes

8 Pre-crime and standardization of security risks

Sirpa Virta

Introduction

> Pre-crime, like risk, is future-oriented and linked to the pursuit of security.
> (McCulloch and Wilson, 2016, p. 2)

This chapter discusses *pre-crime* as a special frame and approach of contemporary criminal justice systems. It has been argued that, once security and risk became integral to criminal justice in the last decades of the twentieth century, the stage was set for the emergence of pre-crime. Security and threats have become driving forces in criminal justice. Within the pre-crime frame, the standardization of security risks, and, for instance, terrorism prevention, operate through decision-making, norms, and legislation. Terrorism, radicalization, and violent extremism are seen not as incalculable unknowns and uncertain future crimes but as manageable risks. The logic of anticipatory risk has featured heavily in the European Union and other international legislation, through the implementation of procedures that are preventative. In general, in pre-crime, uncertain, often imagined, forthcoming events and risks have been the focus of direct contemporary decision-making (see e.g. Mythen, 2011, p. 175). According to Niklas Luhmann (1995), more and more dangerous situations and risks are not, as in older societal forms, the result of nature, God, or destiny, but the result of decisions. It is argued that pre-crime as a strategy to fight terrorism can create new risks and threats, posed by crime control measures.

This chapter deals with the relationship between pre-crime, the standardization of security risks, and decision-making. The empirical example is the European Union (EU) and other international legislation and norms regarding, in particular, terrorism, radicalization, and extremism. In criminal justice systems, pre-crime approaches are distinct from more recent risk-based approaches. They move beyond risk-based crime prevention, by pre-empting threats and looking to less proximate and incalculable catastrophic futures (McCulloch and Wilson, 2016, p. 3). International legislation on terrorism, radicalization, and extremism builds on pre-crime. Pre-crime formalizes pre-emptive policing into law (see also Jore, Chapter 9, in this volume).

The point of departure in the analysis is the contingent nature of security (see Virta and Branders, 2016). It has been argued that governing security is

governing at the limit of knowledge, due to the fundamental attributes of security: incalculability and radical contingency (Zedner, 2009, p. 85) Accordingly, decision-making about security is decision-making at the limits of knowledge. Take, for instance, the principle of differential technological development: 'Retard the development of dangerous and harmful technologies, especially ones that raise the level of existential risk; and accelerate the development of beneficial technologies, especially those that reduce the existential risk posed by nature or by other technologies' (Bostrom, 2014, p. 282). If security is defined in its broadest sense as existence and survival, for instance, artificial intelligence can mean both existential risk-causing technologies and risk-reducing technologies. In addition to this most radical contingency, there are many other contingencies of security (conceptual, contextual, political, practical).

Pre-crime and terrorism legislation

The term 'pre-crime' is originally taken from Philip K. Dick's 1956 science fiction short story, *The Minority Report*. The story's philosophical heart highlights the interplay between human agency and fate, questioning whether the future is multiple and contingent or predetermined and predictable. In this fantasy world, a police pre-crime unit stops murders before they happen (McCulloch and Wilson, 2016, p. 1). Policing terrorism, extremism, and radicalization as a subdomain of policing is not new but has particularly emerged as a global concern since 9/11. International norms are capable of harmonizing legislation relevant to the policing of terrorism, extremism, and radicalization globally and in highly harmonized polities such as the EU. However, how terrorism is understood and defined legally is central to the practices of counterterrorism. Compared to the approach of the United States of America (USA) in the Global War on Terror and its concept of preventive war, the criminal justice approach of the EU relies on a different kind of logic (den Boer, Mankkinen, and Virta, 2018, p. 175).

Increasingly, security agents and, more specifically, police officers are equipped with powers to monitor and control the so-called 'pre-emptive' aspects of criminals and terrorists. Various national and international frameworks have criminalized elements of pre-crime (thoughts, plans, indications). The question is how evidence can be obtained about a situation that has not yet materialized but which might happen in the future – just as well that it may not happen. Perhaps one of the most challenging issues in the policing of terrorism, extremism, and radicalization is the unpredictable and ambivalent nature of the phenomena themselves. The prediction of future crime is one of the enduring challenges for the security community. The logic of pre-crime is most evident in the context of terrorism, but it increasingly spills over to other regions of criminal justice. The growing anxiety about terrorism has encouraged the emergence of a strategy of prevention, pre-emption, and precaution. The policy-making and legislation processes have integrated the 'Precautionary Principle' (Virta, 2011, p. 186.) In terrorism research, too, the principle has been identified in the introduction of the notion of preventive war (see Ranstorp, 2007, p. 15), while criminologists have been more familiar with conventional crime

prevention policy and its methods, like situational crime prevention (den Boer *et al.,* 2018, p. 186).

Imagination is a key aspect of pre-crime. Donald Rumsfeld argued that you can only know more about the unknown unknowns by imagining what they might be. Promoting the need for pre-crime counterterrorism laws in 2008, the former British Minister of State for Security, Counterterrorism, Crime and Policy, McNulty urged people to imagine two or three 9/11s. However, the role of imagination is denied in the implementation of pre-crime. The language of science, mathematics, police and intelligence expertise, and political authority is used to mask the central place of imagination in pre-crime. The establishment of pre-crime as a major trend in criminal justice coincided substantially with the 9/11 attacks on the US, the declaration of the War on Terror, and a more pre-emptive approach to security (McCulloch and Wilson, 2016, pp. 7–8).

The international clamp-down on terrorism has contributed to a growing set of international legal rules and standards that find their way to national legislation through binding implementation routes. Counterterrorism involves the multiplication of efforts by several law enforcement agencies: This drive for multi-agency cooperation has involved far-fetching legislation on the sharing of information between public security providers as well as private actors. It has been argued that counterterrorism has produced significant legal spill-over, that is to say, that legal instruments that were originally invoked for counterterrorism purposes can now also be applied to regular criminal offences. If there is one phenomenon that has been heavily influenced by the fear of terrorism, it is the emergence of the trans-boundary surveillance society, by means of instituting legal norms on retention, interception, screening, monitoring, and sharing (real-time) data with the help of modern technology such as biometrics. 9/11 has infused our collective anxiety about terrorism and has subsequently induced a tremendous arsenal of laws, regulations, and agreements (den Boer *et al.,* 2018, p. 174).

The increasingly high volume of international counterterrorism legal instruments becomes apparent from the electronic Legal Resources on International Terrorism database of the United Nations on Drugs and Crime (UNODC) Terrorism Prevention Branch. It has three categories: (1) international legal resources; (2) national legal resources; and (3) additional legal resources. Universal instruments against terrorism include all international legal instruments against terrorism and their ratification status database (country by country). International legal resources include the UN Action to counter terrorism and feature the list of Security Council and General Assembly resolutions on terrorism, including states' reports to the Counter-Terrorism Committee and other Security Council committees. They also include Regional Action against Terrorism (counterterrorism conventions adopted by regional organizations) and international jurisprudence (a selection of case law of international tribunals and other relevant bodies on terrorism-related matters) (www.unodc.org).

The influence of counterterrorism legislation is a two-directional interaction: On one hand, international agreements against terrorism have been complemented by legislative efforts at the national level (Deflem, 2010, p. 14) and, on

the other hand, national counterterrorism legislation has been affected by international legislation. The latter is particularly the case within the EU, which is a regional legal community with high levels of legal approximation. International criminal law regimes have been established by the UN and the EU, followed by national legislation that imposes travel bans, confiscation and freezing orders, transfer of suspects, and criminalization of group membership or prohibits the provision of material support to listed groups (terrorism financing) (Dudouet, 2011, p. 4). International norms form a particular category of norms, as they specifically govern the actions of states (Finnemore and Sikkink, 1998, p. 893).

At the international level, there are international conventions that deal with some aspects of terrorism. They compel signatory states to adopt national legislation that penalizes a variety of terrorist activities, including supporting or financing terrorist activity. These include, for instance, violence at airports (Montreal 1988), terrorist bombings (New York 1997), and terrorism financing (New York 1999) (Crelinsten, 2009, p. 55). These terrorism conventions can jointly be considered a legal acquis that attempts to create a common discourse and – to the extent possible – an international consensus on combating terrorism throughout the international system of states. In addition to the global conventions, there are also regional conventions like the European Convention on the Prevention of Terrorism (Strasbourg 1977) and the Council of Europe Convention on the Prevention of Terrorism (Warsaw 2005) (den Boer *et al.,* 2018, pp. 175–176).

The UN General Secretary´s Plan of Action to Prevent Violent Extremism was published in January 2016. The counterterrorism agenda was replaced by the wider approach regarding the prevention of violent extremism. According to this approach, prevention should also include measures that address the potential breeding grounds for terrorism. Subsequently, the counter-extremism and counterterrorism agenda should have three stages: (1) preventing violent radicalization and extremism; (2) countering extremism; and (3) countering terrorism. An interesting question is how the prevention of violent radicalization and extremism should be included in the UN structures: Is it about increasing social cohesion or about countering terrorism? At the moment, it seems that the majority of the UN member states would include preventing violent radicalization and extremism in the structures countering terrorism. For a status of signature and ratification of UN instruments, see Extract from the Report of the Secretary-General on Measures to Eliminate International Terrorism (Doc. A/63/173) (Status of International Legal Instruments Related to the Prevention and Suppression of International Terrorism) (30 instruments, of which 16 are universal).

In more recent times, EU policy-makers have become increasingly alarmed by the growing number of European citizens and residents training and fighting with the Islamist State and other terrorist groups in the Middle East and North Africa, and the need to control the 'foreign fighter' phenomenon. In 2015, an estimated 19 per cent of the total number of foreign fighters in Syria and Iraq originated from the EU, which amounted to 3,000–5,000 individuals. As concerns mounted in 2014 and 2015 about the foreign fighter threat, the EU urged

national authorities to make full use of available security tools, including intensified electronic checks at the EU's external borders, provided by the revised Schengen Borders Code, which is the detailed set of rules governing external and internal border controls in the Schengen Area. Recently, based on the work of the group of EU member states most affected by the foreign terrorist fighter phenomenon (G13+), an urgent objective has been to define a common approach with regard to foreign terrorist fighter returnees. In 2016, the group of EU member states most affected by the foreign fighter issue were Austria, Belgium, Denmark, France, Germany, Ireland, Italy, Luxembourg, the Netherlands, Poland, Spain, Sweden, and the UK, plus the associated Schengen signatories, Norway and Switzerland (European Commission, 2016, p. 5). Hence, the EU legislator has gradually assumed a more active role as a security actor in the field of counterterrorism, illustrating that terrorism is no longer regarded merely as an external threat but as one that is also integral to European societies (den Boer *et al.,* 2018, p. 177).

In many countries, reforms were introduced into previously existing counterterrorism legislation, and there was a call for new legislation. In some other countries, European legislation – in particular, the adoption of the EU Framework Decision on Terrorism – helped to stamp out entirely new national counterterrorism legislation (den Boer and Wiegand, 2015) such as in The Netherlands (den Boer, 2007). In Finland, the legislation regarding terrorist crime has been reviewed in recent years. This has been influenced by the international developments and the increasing threat of terrorism. The guidelines have mainly been set by international organizations, such as the UN and the EU. Of particular interest is Article 34a of the Finnish penal code – Crimes committed for terrorist purposes – which contains the main piece of legislation regarding terrorist crimes. According to this, the following acts are regarded as terrorist crimes:

- preparing to commit a terrorist crime;
- leading a terrorist group;
- promoting terrorist activities;
- educating and training;
- recruiting and financing terrorism and terrorist groups.

The Finnish Parliament adopted the government's proposal to criminalize travelling for terrorist purposes, including the financing and promoting of travel, and the new piece of legislation came into force on 1 December 2016. The new legislation grants more possibilities to the police to prevent travel to conflict zones. In addition, any crime can be regarded as a terrorist crime if there is evidence that it has been committed for terrorist purposes. Another piece of legislation that is commonly used is legislation regarding war crimes.

The challenge, in the cases where terrorist legislation is adopted, is the difficulty in getting sufficient evidence regarding the crimes. This is especially the problem with crimes that have allegedly been committed in conflict zones and in

failing states. Some countries have criminalized the membership of groups that are regarded as terrorist groups. In Finland, this is not the case (yet) because these lists of terrorist organizations are regarded as political, and membership of a political group is not subject to criminalization (den Boer *et al.,* 2018, p. 181).

In the new Finnish National Action Plan for the Prevention of Violent Radicalisation and Extremism, violent extremism refers to using, threatening with, encouraging, or justifying violence on ideological grounds. Crimes motivated by hate or racism can also be categorized as extremist crimes. In the analysis of how to prevent terrorism and crime by legislative means, one should aim to study extremist crimes. Extremist crimes tend to be very closely linked to terrorist crimes. The similarities between these two types of crime are that they are both motivated by ideologies, and the use of violence is a means to achieve goals. Terrorist crimes and violent extremism pose a threat to the state and to international organizations. Extremist crimes are targeted at individuals or communities who are regarded as enemies by the members of the extremist groups. Extremist crimes increase fear in society, and they decrease the sense of security experienced by individuals and communities who are the potential targets of these crimes. Crime is regarded as extremist if the motivation of the crime is extremist or the offender is (visibly) a member of an extremist group (Ministry of the Interior, 2016).

All this is evidence about the failure of standardization of security risks (posed by possible future violent extremism and terrorist attack) through pre-crime legislation. An intention is not a crime. A purpose to commit a crime is not a crime as such, or at least it is difficult to obtain evidence of a crime for the courts. Part of the selective nature of risk, linked to the state-centric notions of security, is the failure to take seriously the risk posed by these crime control measures themselves: for instance, the risk of being falsely suspected or accused, or the risk of being deemed a future criminal and treated as if one had already committed the predicted future crime (McCulloch and Wilson, 2016, p. 39).

In several countries, democratic processes have tended to slow down the scrutiny and adoption of counterterrorism legislation. However, governments have sought to persuade legislative bodies of the appropriateness of the measures, and there has been a comparatively marginal space for parliamentary input or scrutiny (Goldsmith, 2008, p. 142; Virta, 2011, p. 191). Legislation processes may be long and tedious, which is again due to the ambiguous nature of counterterrorism measures. For instance, there is little evidence, as well as ample suspicion and contradictory information, about the effectiveness of mass surveillance and intelligence gathering, and therefore the situation politically tends to be rather challenging for legislators.

National legal resources include laws and provisions relating to the implementation of the universal instruments against terrorism, and relevant national judicial decisions. In addition, legislation on special subjects is offered by other UN legislative databases, such as the IMoLIN (International Money Laundering Information Network), and the 1540 Committee Legislative Database on Weapons of Mass Destruction. The national legal resources section of the database contains legislation relevant to counterterrorism and international cooperation

from more than 190 countries. Legislative provisions for each state are presented according to a uniform structure and are subdivided into the categories:

- laws in full text;
- international cooperation in criminal matters;
- substantive criminal law (including crimes of conspiracy and incitement, and nuclear, maritime, and aviation terrorism);
- procedural law;
- case law (www.unodc.org).

A legal-comparative perspective on policing terrorism is challenging, primarily due to the lack of systematic and comparable data. The UN and Europol, for instance, collect information country by country, but their databases are updated based on and dependent on the member states' willingness to submit and share information. The EU Terrorism Situation and Trend Report 2015 (TE-SAT) is illustrative in this sense: Annex 6 at the end of the report includes amendments in national legislation on terrorism in 2014 from three countries (France, Greece, and the United Kingdom). In France, the amendments are in the Criminal Code, the Code of Criminal Procedure and administrative provisions. In Greece, amendments have been introduced in the Criminal Code, Laws 4267/2014 and 4274/2014. In the United Kingdom, the Data Retention and Investigatory Powers Act 2014 was included. The information provided by the EU member states is not congruent and therefore not informative from a comparative perspective. The report includes copied pieces from national legislations. However, Europol's TE-SAT offers good comparative data from other terrorism-related issues in the member states. For instance, the statistics on arrests, convictions, and penalties concerning terrorist attacks are significant in showing how legal instruments have worked in practice, *after* the attacks. There is a need for proper comparative research and analysis of national level CT (counterterrorism) legislation and implementation. However, a pre-definition is required regarding which kind of legislation is interpreted as CT legislation, as well as the ability to translate from national languages. It is also a challenge to set viable criteria for legal-comparative research purposes (den Boer *et al.,* 2018, p. 179).

Nevertheless, the reports of the EU and other organizations provide insight into the situation. For instance, the US Department of State Country Report, 'Europe Overview', describes the CT legislation situation in 23 European countries. The report does not explain why and how the 23 have been selected or included in the report or why some countries, like Finland, are not included. All 23 countries have a legal framework to combat terrorism and all have implemented activities like countering the financing of terrorism and violent extremism. In the report, regional co-operation means mainly European co-operation, organizations like the OSCE (Organization for Security and Co-operation in Europe), but also the 'Balkan states' and the 'Nordic states'. The alignment of national counterterrorism legislation with EU legislation has progressed at a fast pace in the past four to five years. Most of the legislation initiatives strengthening

the existing legal frameworks, notably against foreign fighters, were passed in national parliaments of the EU member states during 2014–2016. This was the case, for instance, in Austria in 2015, Belgium in 2015, Bulgaria in 2015, France in 2015, and Ireland in 2015 (US Department of State, 2015).

The EU seeks to approximate counterterrorism measures in national criminal systems, while respecting national sovereignty. The EU Framework Decision on combating terrorism, adopted in 2002 and to be replaced by the formerly discussed Directive, required member states to introduce into their criminal codes provisions penalizing terrorism and harmonizing punishments for terrorist offences. The instrument was amended in 2008 in order to criminalize offences related to provocation, recruitment, and training for terrorist purposes. The decision needs a comprehensive revision, among other things, to align its provisions with a United Nations Security Council Resolution on foreign fighters (UNSCR 2178, 2014). The UN Resolution requires countries to penalize travelling, or planning to travel, to foreign countries with the intention of preparing, or training for, a terrorist attack. It also criminalizes terrorism financing and facilitating such activities (see also Morsut, Chapter 3, in this volume).

According to the first progress report on an effective and genuine *Security Union*, the EU will strengthen its fight against terrorism, by developing a further legal framework for combating terrorism and cutting access to financing and firearms (European Commission, 2016). The complementary report on the implementation of the counterterrorism agenda set by the EU to the first progress report draws recommendations regarding legislative measures. The Council is of opinion that the EU information systems such as SIS II, VIS and Eurodac should take into account interoperability, as well as the business needs of Europol, and facilitate the systematic cross-matching of and biometric data against Europol systems (den Boer *et al.,* 2018, p. 180).

Decision-making and the contingencies of security

In this chapter, societal security, and within it the criminal justice system, are seen as a social system *sensu stricto* (Luhmann, 1995), in which security strategies, security risks, and resilience are interdependent and in a complex relationship with each other and in relation to multiple contingencies. Pre-crime legislation, security strategies, and policies are decisions made by various security systems like networks, organizations, or governments. According to Niklas Luhmann's system theoretical approach, standardization of security is a decision made by a typical second-order contract of security systems. In these second-order contracts (networks, partnerships), the most important elements are common interests and future and common visions, not operational exact goals and objectives (see also Engen, Chapter 15, in this volume). In this context, standardization means 'a way of organizing society' on the societal level (see Brunsson, Rasche, and Seidl, 2012), a special dynamic of attempts to govern security through decisions (strategies, policies) of standardization of security risks. The European Union and other international legislation and norms are an example of this type

of organizing through the standardization principle. When conventional crime risk prevention uses past offending to calculate the future probability of offending and the basis for coercive state intervention, pre-crime concentrates on uncertain possibilities and imaginations that underpin a precautionary approach and rationale for coercive state intervention (McCulloch and Wilson, 2016, p. 9).

According to Luhmann, to combine the problem of complexity and systems theory requires a renewed treatment of the concept of complexity. Complexity means the necessity to make selections. In decision-making, complexity means being forced to select; being forced to select means contingency; and contingency means risk (Luhmann, 1995, pp. 25–26). In recent security studies, and according to its contemporary interpretation, contingency means risk, unexpectedness, unpredictability, and a possibility of alternatives (see e.g. ibid.; Eräsaari, 2005; Aradau, 2014; Virta and Branders, 2016, pp. 1–3). Therefore, according to Luhmann's definition, contingency (1995, p. 25) means 'also being possible otherwise', and the selection then positions and qualifies the elements, although other elements would have been possible. Reducing complexity is the task of decision-making. Standardization of security risks can be seen as a strategy, decision, and attempt to reduce complexity and risks (contingencies).

As has been noted (de Lint and Virta, 2004), security arguments are made within a hierarchy of political truth, an ordering principle. In addition, and moreover, they must provide a predetermined course to secure finite relations over abstract ideas. *Securitization*, to this way of thinking, serves to close options and minimize political contingency. In other words, a political order will prefer to view security as a synonym for certainty of outcomes. It holds that the more indeterminate the political outcome, the less secure it is. Security policy from this vantage point seeks to present itself as exchanging indeterminate and uncertain relations for something with less ambiguity.

Standards are particularly important in the context of international regulation, because most state legislation remains bound to a national territory and standards are often the only type of rule that can be applied internationally, especially where there are no common cultural elements to serve as a basis for regulating mechanisms (Brunsson *et al.,* 2012, p. 621). International legislation and regulation, for instance of counterterrorism measures, have been very challenging and difficult (see Grayson, 2016; den Boer *et al.,* 2018;). The strategic purpose of the security standardization talk in the EU is to convince member states that, through the standardization of security risks, they become more governable. Standardization is seen as a tool for the effectiveness of security measures, for the convergence of strategies and models in countering terrorism and fighting crime, and, indeed, a way of creating at least some degree of consensus about the complex field of interdependent threats and phenomena. However, as a way of organizing society, standardization of security risks is seen – ironically – as a risk in itself (to democracy and human rights; see e.g. Kundnani and Hayes, 2018).

There are no standard definitions of security across different disciplines, to be accepted as the universal meaning and concept of security. Criminology has taken much of its terminology from international relations and political science,

as part of the securitization process of criminology (see e.g. Zedner, 2009). The following example is from the *SAGE Dictionary of Criminology* (2nd and 3rd editions, also to be included in the 4th edition in 2019):

> Security is the state of being secure, specifically freedom from fear, danger, risk, care, poverty or anxiety. Security also implies certainty. The roots of the term are in the Latin securitas/secures, derived from *se* (meaning without) *cura* (fear, anxiety, pains, worry). Safety is closely related to security. Safety also means freedom from danger or risk. However, it has additional connotations which have more to do with physical conditions, e.g. freedom from injury, the safety of the body and of property. In this context certainty refers to certainty of order, assurance and predictability.
>
> (Virta, 2006, p. 371; 2013, p. 312)

When security is defined mainly as 'freedom from' something, like risk, we can assume that prevention and the elimination of risks increase security. The ambivalence of the definition is an illustration of the contingent nature of security; certainty, assurance and predictability refer to the fundamental political nature of security (status quo, order, continuity).

In criminological security studies, there have been discussions about the relationship between security and risk (see e.g. Zedner, 2009). Risk has been discussed in the context and in relation to uncertainty and insecurity. According to Zedner (ibid., p. 153), risk has positive and negative possibilities that tend to be dismissed in writings on security. In our earlier article (de Lint and Virta, 2004, p. 480), we observed that criminology has failed to question the assumption that security is an unqualified good, whose pursuit trumps all other goods. Privileging security undermines the value of uncertainty and ambiguity that lie at the heart of political debate and a healthy democracy. Rejecting the conventional association of security with certainty, we found a 'security in ambiguity' approach to be more fruitful in analysis. Today, we can find similarities in discourses of ambiguity and complexity; complexity creates ambiguity.

The merging of criminal justice and security led to the emergence of the concept of risk as a key rationale for crime control. As security became integrated into criminal justice from the 1980s, preventive measures nascent in the traditional law were pursued more vigorously, and new preventive measures were developed to deal with crime risks. Subsequently, crime risk prevention has been pushed along a temporal spectrum towards pre-emption and pre-crime. *Pre-crime* reflects a changing attitude to crime, risk, and the future. Pre-crime discourse emerged in the criminological and policing research first, in the context of terrorism and counterterrorism research (McCulloch and Wilson, 2016; Virta and Taponen, 2017).

The contingent nature of security is the main argument against the possibility to standardize security. Contingency, as a philosophical concept and according to its contemporary interpretations in social science, refers to a possibility (e.g. of alternative interpretations of security in a given context), that is, a

possibility of occurrence, something that is incidental, surprising, not intentional, unexpectable, and unpredictable (see e.g. Luhmann, 1995; Eräsaari, 2005; Aradau, 2014). Politics and the political are the most significant *contingencies of security*, but there are others too, like secrecy and closure, the role of the state and order institutions, the political and other paradoxes of security, and the limits of knowledge. In decision-making processes, contingencies are seen as risks, and, therefore, the contingent nature of security is risk in itself. Therefore, standardization of security risks is seen as a means and strategy, as a political decision, to tame the contingencies of security. In decision-making processes, the taming often operates through intentional depoliticization of security, which means that standardization as a decision is a political act. Within the pre-crime frame, legislation is an act of standardization of counterterrorism measures, aiming to tame the contingencies of security.

Contingency represents a complex discourse about the knowledge of uncertainty. Aradau (2014) draws on the distinction between three epistemic regimes that problematize contingency differently: *ignorance/secrecy*; *risk/uncertainty*; and *surprise/novelty*. Surprise and novelty indicate an epistemic regime, in which events are always emergent and potential. As complexity theorists argue, surprise is inevitable, and novelty, always already in the making. In this discourse, preparedness and risk management are the answers to the surprising event and its emergent novelty. Contingency is not tamed but incorporated, literally lived with. *Resilience* and risk management are proactive responses to a world that is complex, unstable, unknowable, and unpredictable. Surprise becomes an ontological characteristic of all complex adaptive systems. It is its unexpected and always emergent quality that becomes the main concern for security and governance (ibid., pp. 77–78).

The many contingencies of security, by their nature and characteristics – for instance, the essence of the state, the power of the state over the life and death of citizens, national security, and the states of exception, secrecy, closure, and confidentiality – mean that security cannot be subjected to standardization (Virta and Branders, 2016, p. 1160). However, pre-crime, as national and international criminal justice systems' means to pre-empt and prevent terrorism, radicalization and violent extremism, relies on standardization of these threats and risks, through regulation and legislation. International legislation and norms, as well as European threat assessments and other common intelligence products, are based on commonly accepted definitions of the phenomena. These definitions are seen as standards, created in international decision-making processes as part of security politics.

Conclusion

Uncertainty is a hallmark of pre-crime, and pre-crime terrorism laws have been widely criticized for being overly broad and vague. The threat of future catastrophe shifts the basis for decision from risk and evidence to uncertainty and suspicious imagination; decisions are made not in the context of certainty but of

doubt, challenge, mistrust, fear, and anxiety (McCulloch and Wilson, 2016, p. 51). The international and European counterterrorism legislation and regulations are based on a myriad of internationally and nationally funded research, common and member states' government policies and strategies and, of course, the increasingly felt need to control terrorism risks and threats.

Pre-crime legislation and the emergence of predictive policing are the indicators that the technologies and science of pre-crime are floating downstream from the threat of terrorism and into the local policing spaces of crime and low-level disorder. It has been argued that the police need to start thinking of crimes in the way that seismologists think of earthquakes and aftershocks (ibid., p. 84). However, terrorism, radicalization, and violent extremism, as well as other crimes, are not risks like natural disasters, because they are results of intentional (criminal, political) human behaviour. Due to the fundamentally paradoxical and political nature of security (see Berki, 1986) and the many contingencies of security (see Virta and Branders, 2016), it is argued that security risks cannot be standardized in the context of pre-crime legislation and terrorism prevention.

References

Aradau, C. (2014). The promise of security: Resilience, surprise and epistemic politics. *Resilience: International Policies, Practices and Discourses*, 2, pp. 73–87.

Berki, R. N. (1986). *Security and society: Reflections on law, order and politics*. London: Dent.

Bostrom, N. (2014). *Superintelligence: Paths, dangers, strategies*. Oxford: Oxford University Press.

Brunsson, N., Rasche, A., and Seidl, D. (2012). The dynamics of standardization: Three perspectives on standards in organization studies. *Organization Studies*, 33(5–6), pp. 613–632.

Crelinsten, R. (2009.) *Counterterrorism.* London: Polity Press.

Deflem, M. (2010). *Policing terrorism*. New York: Routledge.

de Lint, W. and Virta, S. (2004) Security in ambiguity. Towards a radical security politics. *Theoretical Criminology*, 8(4), pp. 465–489.

Den Boer, M. (2007). Wake-up call for the Lowlands: Dutch counterterrorism from a comparative perspective. *Cambridge Review of International Affairs*, 20(2), pp. 285–302.

Den Boer, M., Mankkinen, T., and Virta, S. (2018). Policing terrorism, extremism and radicalization: A legal-comparative perspective. In M. den Boer, ed. *Comparative policing from a legal perspective*. Cheltenham: Edward Elgar Publishing, pp. 173–191.

Den Boer, M. and Wiegand, I. (2015). From convergence to deep integration: Evaluating the impact of EU counter-terrorism strategies on domestic arenas. *Journal of Intelligence and National Security*, 30(2–3), pp. 377–401.

Dudouet, V. (2011). Anti-terrorism legislation: Impediments to conflict transformation. *Berghof Policy Brief 02*. Berlin: Berghof Foundation.

Eräsaari, R. (2005). Täyttymättömien tilojen passiivinen fantasia. Robert Musilin kontingenssin käsitteen jäljillä. In U. Kovala *et al.,* eds. *Tarkkoja siirtoja*. Jyväskylä, Finland: Nykykulttuurin tutkimuskeskus, pp. 53–58.

European Commission (2016). Communication from the Commission to the European Parliament, the European Council and the Council. First Progress Report Towards an Effective and Genuine Security Union. 12 October 2016. Brussels.

Extract from the Report of the Secretary-General on Measures to Eliminate International Terrorism (Doc. A/63/173). Status of International Legal Instruments Related to the Prevention and Suppression of International Terrorism. [online]. Available at: www.un.org/en/ga/sixth/63/Terrorism_Table_63rd.pdf (accessed 14 December 2016).

Finnemore, M. and Sikkink, K. (1998). International norm dynamics and political change. *International Organization*, 52(4), pp. 887–917.

Goldsmith, A. (2008). The governance of terror: Precautionary logic and counterterrorism law reform after September 11. *Law & Policy*, 30(2), pp. 141–163.

Grayson, K. (2016). *Cultural politics of targeted killing*. London: Routledge.

Kundnani, A. and Hayes, B. (2018). *The globalisation of countering violent extremism policies: Undermining human rights, instrumentalising civil society*. Amsterdam: Transnational Institute.

Luhmann, N. (1995). *Social systems*. Stanford, CA: Stanford University Press.

McCulloch, J. and Wilson, D. (2016). *Pre-crime: Pre-emption, precaution and the future*. London: Routledge.

Ministry of the Interior (2016). *National Action Plan for the Prevention of Violent Radicalisation and Extremism*. Finland: Ministry of the Interior Publications 17/2016.

Mythen, G. (2011). The pre-emptive mode of regulation. In V. Bajc and W. de Lint, eds. *Security and everyday life*. New York: Routledge, pp. 168–184.

Ranstorp, M. ed. (2007). *Mapping terrorism research: State of the art, gaps and future direction.* London: Routledge.

U.S. Department of State (2015). *Country Reports on Terrorism: Europe overview*. [online]. Available at: www.state.gov/j/ct/rls/crt/2015/ (accessed 23 January 2017).

Virta, S. (2006). Security. In *The SAGE dictionary of criminology.* 2nd ed. London: SAGE, pp. 371–374.

Virta, S. (2011). Re-building the EU: Governing through counterterrorism. In V. Bajc and W. de Lint, eds. *Security and everyday life*. New York: Routledge, pp. 185–211.

Virta, S. (2013). Security. In *The SAGE dictionary of criminology.* 3rd ed. London: SAGE, pp. 312–314.

Virta, S. and Branders, M. (2016). Legitimate security? Understanding the contingencies of security and deliberation. *British Journal of Criminology*, 56(6), pp. 1146–1164.

Virta, S. and Taponen, J. (2017). Policing regimes in transition in the Nordic countries: Some critical notes from the Nordic reality. In E. Devroe, A. Edwards, and P. Ponsaers, eds. *Policing European metropolises: The politics of security in city-regions*. London: Routledge, pp. 121–143.

Zedner, L. (2009). *Security*. London: Routledge.

9 Standardization of terrorism risk analysis

A means or an obstacle to achieving security?

Sissel H. Jore

Introduction

The threat of terrorism has emerged as one of the most prominent security challenges in Western countries in recent years. Numerous attacks, targeting innocent civilians in European cities, have received massive media attention and led to a demand for public and private places to be secured from the unfolding of such horrific scenes. After such attacks, the public calls for action to be taken and requires that security should be provided. However, how to prevent, and protect society from, the occurrence of such devastating attacks is a question without a straightforward answer.

The management of terrorism and other intentional crimes is often denoted 'security', in contrast to the management of unintentional crimes, which is often referred to as 'safety' (Jore, 2017). Since the 1970s, safety management has revolved around bureaucratization, formalized rules, and standardization (Dekker, 2014). Standardization of safety has brought the kind of benefits envisaged by modernism, including reduction of harm and a major decrease in industrial accidents. Consequently, different forms of standardization lie as the basis of safety management, building on the assumption that it is possible to identify, predict, and control the circumstances that produce accidents (Antonsen, Skarholt, and Ringstad, 2012).

In recent years, this tendency to bureaucratize and standardize has also reached the security domain. Since the terrorist attack on the US on September 11, 2001 (9/11), a bureaucratization of security has gradually taken place, and the tools for governing security have become similar to safety management tools. Nowadays, risk analysis, risk awareness programmes, and organizational culture programmes, once exclusively applied in the realm of safety, have become tools that private and public organizations use for security governance. However, managing security risks, such as terrorism, is different from managing safety risks, such as industrial accidents. Consequently, it is reasonable to ask whether all risk problems are suitable for standardization. Are there certain types of risks, for example, terrorism, that we might be more reluctant to standardize than others, and could standardization actually hamper security, instead of fostering it?

In this chapter, the standardization of terrorism risk management that has taken place in Norway during recent years is investigated. First, we give a short introduction to Norwegian terrorism risk management. Thereafter, we discuss the logic of standardization and how standards should be seen as a result of a specific discourse on terrorism. Next, we discuss the underlying implications of risk management and the characteristics of terrorism risk, and we discuss whether terrorism risk fits the logic of risk management and what challenges terrorism risk management entails for organizations. Subsequently, we discuss what security is and whether security can be achieved by standardization. We conclude that, although standardization of terrorism management will contribute to a more hegemonic cross-organizational and cross-sectoral risk management regime, trapping a systemic risk such as terrorism into fixed categories entails that the risk of terrorism is made predictable and value-free, and thereby the risk of terrorism is simplified and depoliticized. Thus, standardization of terrorism risk involves paradoxes, meaning that it is not evident that standardization of terrorism risk management will lead to a more secure society (see Virta, Chapter 8, in this volume).

Norwegian terrorism management in context

There is an expectation in contemporary Western societies that authorities, and multiple other actors in society, are responsible for protecting citizens from acts of terrorism. This is reflected in the many investigation reports that have been published in the aftermath of major terrorist attacks in recent years, where numerous official bodies and private companies have been criticized for not taken appropriate responsibility for the mitigation and protection of citizens from acts of terrorism (The 9/11 Commission Report, 2004; Gjørv *et al.,* 2012; Statoil, 2013). Although most citizens nowadays take this notion for granted, this assumption is relatively new in a historical perspective (Crelinsten, 2009). Until the 9/11 terrorist attacks, there was little focus on terrorism in research or the media; few states had terrorist legislation; there were few institutions in society appointed to deal with the topic; and terrorism risk analysis was certainly not a topic that organizations dealt with at the time.

The terrorist attacks on 9/11 led to a major focus on the necessity of protecting societies from the threat of terrorism. In the aftermath of this event, many countries, including Norway, highlighted risk analysis as the appropriate tool for terrorist mitigation and preparedness. Despite this, risk assessments as arguments behind the implementation of counterterrorism measures were absent from the public discussions on terrorism security in the first decade after 9/11. Although Norway implemented a raft of counterterrorism measures after 9/11, arguments, such as precaution, compliance, solidarity, and moral obligations, dominated the justification of the implementation of countermeasures in the public sphere (Jore, 2012, 2014). This can be attributed to the perception of Norway as a low-risk society with no former history of major terrorist activity prior to 2011.

On July 22, 2011, Norway became the target of a major terrorist attack. The attack was directed against the Norwegian Government complex and a youth camp on the island of Utøya, where a total of 77 people were killed. Additionally, in January 2013, five Norwegians were killed in a terrorist attack against an oil facility in In Amenas, Algeria (Statoil, 2013). As a response to the criticism directed at the Norwegian authorities and the Norwegian petroleum company, Statoil, in the evaluation commissions following these attacks, the focus on private and public companies' responsibility for security risk management increased. Massive media coverage of terrorism and the occurrence of many terrorist attacks in Europe after these events, including the escalation of attacks on civilians in public places by the terrorist group, Islamic State, have further highlighted citizens' expectation of protection from terrorism in private and public spaces.

Consequently, current security management is no longer limited to high profile targets. Counterterrorism, once national and sectoral in nature, has become a shared responsibility, with multiple actors in society having an obligation for mitigation and protection. The corollary of this shared responsibility of counterterrorism is reflected in the laws, regulations, and counterterrorism strategies published in recent years. In 2011, in Norway, a new Object Security regulation was passed, which made the owners of so-called critical objects those responsible for national security protection (Ministry of Defence, 2011), and in 2018 Norway passed a new National Security Law (National Security Law, 2018). These regulations build on a 'functional' or 'soft' regulation approach to security, where the implementation of security measures should be based on risk assessments instead of prescriptive requirements. Consequently, official bodies have published guidelines for how to conduct security risk analysis for objects critical to national security but also for organizations that do not fall under the jurisdiction of the National Security Law. Additionally, three new security risk analysis standards have been published (Standards Norway, 2012, 2014a, 2014b).

The commonality of these standardized approaches to security risk management is that they all recommend the same approach to security risk analysis. These documents describe the procedure for how to conduct security risk analysis, where risk should be understood as a combination of threats, values, and vulnerabilities (National Security Agency *et al.,* 2015; Standards Norway, 2012, 2014a, 2014b). This definition differs from well-recognized standards within the safety field, such as Norwegian Standard 5814 and ISO 3100, which describe risk mainly as a combination of probability with associated uncertainty.

Many aspects of these new standards have led to debates in the academic and practical communities. The debates have mainly centred on the new risk concept proposed in the standards (Askeland, Flage, and Aven, 2017; Jore, 2017), the problems of excluding probability and uncertainty assessments from security risk analysis (Jore and Egeli, 2015; Maal, Busmundrud, and Endregard, 2017), and the problematic implications of constructing a different risk concept for security from that for safety (Askeland, Flage, and Aven, 2017; Jore, 2017). However, no one seems to ask the overall question: Is counterterrorism a phenomenon that fits the logic of standardization?

The logic of standardization

The process of standardization is widely used to refer to how organizations can deal with different risks, hazards, and dangers. The term 'standardization' can broadly be defined as the process of 'rendering things uniform' (Timmermans and Berg, 2003, p. 24); thus, standards are generalized and formalized rules that serve to prescribe and document efficiency, similarities, hegemony, and control within and across organizations. Standardization enhances the predictability of normal operations, as well as facilitating the transfer of lessons learnt across organizational contexts (Bowker and Star, 2000; Antonsen, Skarholt, and Ringstad, 2012). For many decades, there has been a major increase in the publication of safety standards, and standards have become a central feature of organizations' safety work in most sectors (Antonsen, Skarholt, and Ringstad, 2012). Despite this, standards are seldom the topic of public or academic discussions.

Since the new laws and regulations on security in Norway are based on a functional regulation regime, the security risk analysis standards can be useful tools for organizations with a lack of experience in performing terrorism risk assessments. The standards will facilitate a hegemonic cross-organization and cross-sector risk management process. The standards and guidelines give a formalized description of how to conduct terrorism risk analysis, but they do not give directions for how organizations should set up their security management system. Consequently, the standards are what Mintzberg (1983, 1989) refers to as 'standardization of work processes'.

Standardization can contribute to building a hegemonic approach to the management of terrorism risk that is especially helpful in an area where most Norwegian organizations have little experience. Thus, security standards give those who work with security a procedure for how to think about terrorism risk, and they also provide risk assessors with the concepts and categories that should be applied in the risk management process. Consequently, security standards aim at conformity or uniformity and provide organizations with a norm for how security risk should be perceived and approached, regardless of how good or bad these standards might be (see Olsen, Chapter 1, and Juhl, Chapter 2, in this volume).

However, standards are more than just directions to follow. They tell us what is relevant, what is valued, what is important, and they function as epistemological and ontological devices; they not only tell people what to do but they also 'make' the realities that they claim to describe (Busch 2011a). Standards have a tendency to become taken for granted and natural, and subsequently they justify certain orderings of aspects of the world, tending to make these aspects appear obvious and unworthy of reflection (ibid.; Busch, 2011b). As a result, security risk analysis standards should not just be seen as neutral directions for how to protect society from terrorism; instead, they should be seen in relation to how terrorism is perceived and understood in the historical-political context.

Standards are institutionalizations of the current perception of terrorism

According to Busch (2011a, 2011b), standards are related to what is considered 'right or wrong', because they provide us with concepts for classifying the world. Inherent in standards is the proposal for the hegemonic way of performing a certain procedure. Busch refers to the work of Foucault, who claimed that in a society there is a set of rules that is historically conditioned and that decides which arguments are seen as true or meaningful. Foucault (1989) considered discourses to be the macro-level formation of specialist knowledge that determines what can be said or thought about a specific subject. This implies that when different actors speak about terrorism, they will draw on different discourses, to make sense of the kind of risk the phenomenon of terrorism is. The concept of terrorism is not a neutral word used to refer to an independent, objective, ontological phenomenon. On the contrary, the concept of terrorism functions as a frame that shapes and constructs how individuals and society view a phenomenon of violence, associated threats, and countermeasures. In a world of multiple threats, the fact that some groups are defined as terrorist threats against Norwegian society is a result of the social-political construction of specific groups of activists being framed as an extraordinary type of risk that has a dimension other than that of just being political activists or criminals. Subsequently, what is perceived as a terrorism threat is contingent on historical, cultural, and political framing and influences what are seen as relevant and legitimate ways to counter the threat.

This implies that what society perceives as effective ways to counter terrorism depends on how society comprehends terrorism as a threat. If terrorism is understood as a kind of evil, states will eradicate it through any means (Jackson, 2005). If terrorism is perceived as a type of crime, appropriate means will be policing and criminal justice. If terrorism is seen as an outcome of oppression and political injustice, dialogue, political reforms, and conflict resolutions will be appropriate means (Crelinsten, 2009; Jore, 2012). This means that terrorism countermeasures are not neutral means to reduce the threat. Counterterrorism measures such as risk analysis standards are related to how terrorism as a phenomenon is perceived and what are considered effective and legitimate ways to counter it.

When many people use the same discourse to conceptualize the world, it often solidifies into an institution (Hajer, 1995). In the case of terrorism risk, discourse institutionalization of terrorism is reflected in the practices of how to deal with terrorism, for example, negotiation, imprisonment, or military operations. From this perspective, terrorism countermeasures such as risk management standards are institutionalizations of terrorism discourses in society. An important aspect of discourse institutionalizations is that, when a discourse has solidified into an institutionalization, this will facilitate the reproduction of a given discourse. Individuals socialized to see terrorism in a specific framework, for example, to see terrorism as a manageable risk, reinterpret the phenomenon of terrorism within this framework. Thus, security risk analysis standards are not

only a means for coping with the threat of terrorism but also a concrete discourse institutionalization that supports a specific view on the phenomenon of terrorism. From this perspective, we should investigate the underlying implications of terrorism risk management, in order to reflect upon whether terrorism risk fits the logic of standardization.

The underlying implications of terrorism risk management

One of the key assumptions of risk management is that the circumstances that produce major accidents can be identified, predicted, and controlled (Petersen, 1978). Thus, risk management involves the ability to describe what may happen in the future, to assess associated risks and uncertainties, and to choose among alternatives (Aven, 2003). The assumption is that risk assessments should function as a foundation in a decision-making process, in order to make rational, optimal, cost-effective decisions about how to make a safer society. A risk-based approach to terrorism conceptualizes terrorism risk as a manageable, predictable, and measurable phenomenon and, subsequently, a risk that could be minimized with the right prevention measures. This means that risk management involves simplification and de-politicization of a highly complex and political phenomenon, to make the phenomenon of terrorism measurable, identifiable, and comparable, in order to make rational decisions on how to distribute resources in the most cost-effective manner (Juhl, Chapter 2, in this volume). Thus, risk management builds on the idea that it is possible to describe the uncertainties related to the likelihood of where, how, and when the threat will manifest itself. Additionally, this approach to terrorism has an underpinning assumption that rational decision-making in organizations and society can reduce either the likelihood or the consequences of a terrorist attack. A risk management approach to terrorism builds on the notion that the risk should be reduced to an acceptable level and weighted against other values and costs. However, does the logic of risk management fit the risk of terrorism?

The characteristics of terrorism risk

For some risks, uncertainty is low, and there is hardly any ambiguity with regard to the interpretation of the risk. Such risks, often referred to as ‘simple risks’, are recurrent, statistics are available, and the application of statistics to assess the risks is meaningful (Renn, Klinke, and van Asselt, 2011). Such risks are risks that can easily be an object for standardization, because the degree of knowledge for the optimal way of handling them is high, as is the possibility for sharing lessons learned between organizations.

On the contrary, terrorism is a ‘systemic risk’. The term ‘systemic’ describes the extent to which a risk is embedded in the larger contexts of societal processes. Systemic risks such as terrorism are not restricted to national borders or a single sector and do not fit the linear, mono-causal model of risk. They are complex, multi-causal, and surrounded by uncertainty and ambiguity (ibid.).

The ambiguity of terrorism is related to terrorism being a political phenomenon. If an attack is labelled 'terrorism', it will often have high consequences, not necessarily in terms of casualties or physical damage, but a terrorist attack gains enormous media coverage and can have major political consequences in its aftermath. The aim of a terrorist attack is not only to cause damage but also to produce a signal effect of meanings. Thus, terrorism is also a crime against the mind. Consequently, the risk of terrorism has a symbolic and political dimension. This implies that, although an organization might be the scene of an attack, the aim of the perpetrator is not necessarily to harm the company's production but to draw attention to a political case. The symbolic aspect of terrorism risk also influences which counterterrorism measures are seen as relevant and which assets should be protected. The demand for security measures is often more related to public discourses on what might be legitimate terrorist targets than the actual risk-reducing effect of such measures (Pache and Santos, 2010; Jore, 2012). The ambiguous and political aspect of terrorism entails that when risk assessments are performed, there are no neutral ways to conduct them, and that the input and the output of a risk analysis are not value-free or neutral. On the contrary, all risk assessments are value judgements (Juhl, Chapter 2, in this volume), and these aspects are not taken into account in the standards.

It is obvious that managing systemic risks like terrorism poses a challenge to actors on many scales. However, given the downscaling of counterterrorism responsibility that has taken place in Norway and other Western countries during the last decade, organizations now play a crucial part in counterterrorism, and it is at this scale that the Norwegians standards are intended. However, from an organization mitigation perspective, the management of security risks such as terrorism is fundamentally different from managing safety risks.

Managing terrorism risk from an organizational perspective

Most safety risks such as industrial accidents are frequently associated with an organization's production and profit. Production of goods and services is always connected with some kind of risk. These risks are risks that the organization is willing to take to produce its desired outcome and to gain profit. The sources of these risks are generally well known, and the organization can use reliable historical data in the risk management process. Since organizations have knowledge concerning the source of these risks, they usually also know how these risks can be mitigated. The decisions on whether to implement risk-reducing measures are often a result of quantitative probability assessments and cost-benefit assessments. Since organizations have extensive experience with how to deal with these risks, standardized management approaches are often applied, to facilitate the risk management process.

Conversely, terrorism is a risk to which organizations are exposed. The risk of terrorism is not necessarily directly linked to the production of an organization and is therefore less controllable from an organizational perspective (Petersen, 2013). In contrast to safety risks, terrorism risk is of a dynamic character. Terrorist

attacks are carried out by strategically thinking human beings, who can adapt and alter targets and their *modus operandi* to changing realities. This implies that an organization that is carrying out a terrorism risk analysis must consider the possibility of innovation in target selection and weapons; thus, for terrorism risks, there is almost an infinitive number of possible attack scenarios, which makes it difficult to assess the effects of employing mitigating and protective measures. This challenges the simplification logic that underpins risk management and standardization. In order to fit possible threat scenarios into this logic, there is a need to simplify and focus on what is considered to be the most likely threat scenarios and, as such, diversity, complexity, and variability are reduced.

Since security threats are not directly linked to their production, organizations do not have the same knowledge regarding possible risk scenarios for security risks as for safety risks. Security risks are characterized by low frequency and low predictability. Terrorists can strike suddenly, without warning, because, for a terrorist attack to be effective, the terrorists must keep a low profile. This means that, in contrast to many safety risks, early warning signals will not be possible to detect. Moreover, since terrorist attacks are low-frequency events, limited relevant available historical data exist, which leads to enormous uncertainties in risk assessments.

The dynamic and secret nature of terrorism indicates that it is almost impossible to envision exactly where, how, and when terrorists will strike. Uncertainties will be involved at many levels in a risk analysis. There will be uncertainties related to what might happen, how likely it is that a scenario will unfold, and to the potential consequences of an incident and the possible cascading effects. To develop plans that will work for the endless array of complex, chaotic, and destructive scenarios that arise from terrorism is impossible (Boin and McConnell, 2007). Because of the uncertainties related to assessing the risk of terrorism, many scholars argue for resilience-driven strategies. While risk analysis focuses on plausible scenarios, resilience analysis focuses more on how a system can adapt to changing conditions and various threats. However, this field remains relatively new and underdeveloped, and many of the newer perspectives to resilience analysis trap the risk into strict classification frameworks (Linkov, Trump, and Fox-Lent, 2016).

When simplified predefined categories are used, this could easily lead to simplifications, thereby reducing uncertainties instead of exploring them. Thus, standardized procedures can hamper the creativity and foresight that are needed to create flexible and adjustable security approaches that take into account the fact that terrorism risk stems from rational individuals, who can alter their plans in accordance with security measures. Security planning should not be directed exclusively towards specific scenarios with perpetrators deemed probable. Planning for improvisation and flexibility is a much more promising trajectory for building organizational security than traditional risk management approaches. However, improvisation involves a low degree of pre-defined structures and a high degree of situational flexibility (Barrett, 1998). While a high degree of standardization may be a highly efficient way of securing predictability in

everyday operations, it may have adverse effects for the ability to deal with unexpected events such as terrorism. According to Antonsen, Skarholt, and Ringstad (2012), too strong an emphasis on standardization can involve unintended negative consequences for organizations' crisis-handling capabilities. Moreover, the relationship between bureaucratization, proceduralization, and safety has been questioned by several authors (Amalberti, 2001; Bieder and Bourrier, 2013). More rules do not necessarily increase safety, so why should they increase security, which is even more difficult to handle?

Some of the literature suggests that safety policies developed or enforced bureaucratically by those at a distance from operations do not well represent risk nor how to manage or govern it in practice (Dekker, 2014). The implication of this is that standardization might lay the foundation for a false sense of security. Instead of laying the foundation for resilience, flexibility, and improvisation, standardization of security risk analysis might lead to an illusion of a secure organization, where the focus is on protecting certain assets or places, without taking into consideration the dynamic character of a terrorism threat.

Despite these challenges of managing terrorism from an organizational perspective, many actors in Norway seem to believe that security can be achieved by the use of risk analysis on an organizational scale. However, in order to discuss whether security can be achieved through the use of risk analysis, we need to discuss what security is and how it can be achieved.

Security is a non-event with no best practice

Although security has become an omnipresent aspect of modern societies, the concept of security in itself has drawn surprisingly little scholarly attention, compared to similar concepts such as risk and safety. In everyday use, the word 'security' invokes the association of absence of threats, promising some measures of assurance and certainty of being free from harm (Jarvis and Holland, 2014). Consequently, the concept of security implies the feeling of being safe and secure, the lack of threats, and nowadays also the management of future risks.

However, the concept of security not only evokes positive connotations such as being safe and free from danger. Inherent in the concept is also the association of objects, such as guns, security technologies, and even wars – objects that could, in some cases, have a counterproductive effect on security. This is what Jarvis and Holland (ibid.) refer to as the paradoxical element of security. The paradoxical element of security implies that it is not sufficient to understand security in terms of an absolute optimal situation but more in terms of finding the optimal level of security, where the benefits are weighed against the negative outcomes of security – an argument that fits the logic of risk management.

The management of future risks is central to the current understanding of both safety and security. The term 'safety management' has no clear definition, and the term often refers to all organizational measures that are taken to ensure that an acceptable level of safety is maintained in an activity or throughout the

life cycle of an installation or an organization (e.g. Kettunen, Reiman, and Wahlström, 2007). Security and security management often have similar definitions but focus on protection from actors' malicious intent. Jore claims that the current understanding of security includes much more than just focusing on the actor's intent, and defines security as:

> The ability to prepare for, adapt to, withstand and recover from dangers and crises caused by the deliberate, intentional, malicious acts of people, such as terrorism, sabotage, organized crime and hacking.
>
> Security risk management includes assessing and reducing the likelihood and consequences of possible attacks by employing various types of risk-reducing measures such as critical infrastructure protection and building organizational and societal resilience.
>
> (2017, p. 855)

Today, both safety and security are seen as the outcomes of active risk management. However, the concept of security is related to multiple dimensions, such as individuals, organizations, states, or the international level, and it is related not only to the management of risks but to perceptions and discourses on what are seen as threats to security. Security is, thus, multidimensional in nature and diverse in practice. Consequently, security cannot be achieved exclusively by organizational management of risks.

One problem with measuring security is that security, in parallel with safety, may be seen as a 'dynamic non-event' (Weick and Sutcliffe, 2011). Safety and security are achieved when unwanted events do not happen. This challenges the logic of standardization and risk management. If security is achieved when nothing happens, is it then possible to rationally steer against non-events? Since security is a non-event, it is not possible to really know when you have received your desired level of security. You cannot know that you have achieved security, when security is when nothing happens. This also makes it problematic to evaluate the outcomes of a risk management regime, because it is almost impossible to know if an absence of unwanted events is the result of a successful risk management regime or if the non-event simply is a result of a lack of threats in the first place. This means that security is also invisible. The only way to observe security is when threats materialize and security is not achieved. In this respect, it is possible to observe 'insecurity' but not security.

One consequence of this is that security management relies on measurements that refer to the absence of security rather than to the presence of security, which makes standardization of security quite a contradiction. Because the focus is on things that could go wrong, there will be something to measure when security is absent but, paradoxically, nothing to measure when security is present. This way of thinking corresponds to what Hollnagel (2014) refers to as a 'causality credo', which can be formulated as follows: (1) adverse outcomes happen when something goes wrong; (2) adverse outcomes therefore have causes, which can be found; and (3) treating – and preferably eliminating – the causes will increase

security by preventing future accidents (e.g. Schröder-Hinrichs, Hollnagel, and Baldauf, 2012).

Since security risk analysis focuses on what could go wrong, it is the process of describing insecurities that has been standardized. This is further complicated by the fact that standards are supposed to be generalized and formalized rules that serve to prescribe and document efficiency, similarities, hegemony, and control, within and across organizations, in order to facilitate the transfer of lessons learnt across organizational contexts (Antonsen, Skarholt. and Ringstad, 2012; Bowker and Star, 2000). Nevertheless, a literature review of the current state of affairs of security risk analysis concluded that no 'best practice' exists for how to conduct security risk analysis (Maal, Busmundrud, and Endregard, 2017). Although a variety of risk assessment tools are available, a robust empirical foundation does not yet exist for understanding the risk of terrorism, or involvement, or the outcomes of violent extremist activity (Borum, 2015). There are several reasons why the theoretical field of security risk management is not yet developed to the same extent as safety risk management. First, historically, security has not been an area of organizational responsibility. Second, organizations that have a tradition of dealing with security risks have mainly been the military and the police – organizations that have a tradition for classification and, in general, have not been open to research or critical perspectives. Third, while safety science has been a broad research field, covering multiple disciplines and levels, not until recently has this been the case for the security field, which has been mainly a subject in criminology or international relations, and these disciplines have not focused on the topic of risk management. This is problematic from a standardization point of view. If no best practice exists for how to conduct risk assessments, how is it possible to standardize such a best practice of lessons learned? The implies that the standardization process is not a standardization of the optimal way of conducting risk analysis but an attempt to force and uphold what is considered the correct view on how to conduct risk assessments held by some stakeholders.

Discussion: the paradoxes of standardization of security

It is important to keep in mind that standardization of security is not a new phenomenon. For centuries, military operations have been based on standardization, to provide hegemonic guidelines for soldiers to follow in the field. The new element today is the novel role of organizations in counterterrorism, and subsequently there is a demand to clarify how to carry out this responsibility. It is in this context that the standardization of terrorism management should be understood.

Despite the obvious need for standards for how to conduct security risk analysis, we conclude that, in particular, there are three paradoxes associated with standardizing terrorism risk management, which entail that it is not evident that standardization of terrorism risk management will lead to a more secure society.

Standards should build security but could instead lead to more insecurity

To build security against terrorism, it is not enough for each organization with a responsibility for terrorism security to perform an isolated security risk analysis, because a systemic risk such as terrorism does not follow a certain sector or organization's responsibility. In the current multi-agency counterterrorism cooperation, standardization could be beneficial because it gives a hegemonic and similar guide to how to perform security risk assessments. However, since most risk analysis will be limited to organizational boundaries, it is questionable whether security will actually be achieved, because there are multiple challenges to cross-organizational cooperation, such as classifications, time, and resources. Additionally, boundaries within organizations exist as obstacles to achieving optimal security management. Although decisions regarding security should be based on normative, rational risk assessments, decisions concerning security are often influenced by the blame that organizations expect from failing to prevent attacks (Hood, 2002; McGraw, Todorov, and Kunreuther, 2011). Accordingly, standardization of terrorism security might lead to an overemphasis on following standards, instead of focusing on building security.

The institutionalization of the standardization of terrorism risk management has consequences for the perception of the threat that goes beyond the illusion of creating a secure society. The practical tools of risk management aimed at organizations that do not have a specific responsibility for counterterrorism imply that the threat of terrorism is ubiquitous and can target everyone everywhere; thus, the discourse on terrorism as an omnipresent societal threat is sustained, and this notion functions as a constant reminder that terrorism is an omnipresent threat. Thus, standardization can lead to more insecurity, in the form of creating fear of terrorism, by constantly reminding us about the uncertainties and dangers terrorism possesses, instead of building a feeling of security.

Standardization traps an uncertain, political risk into value-free and non-political categories

Standardization of terrorism risk management implies that organizations follow rules and conform procedurally to enable decision-making. A security risk analysis involves 'agreed-upon procedures for inquiry, categories into which observations are fitted, including beliefs about cause effect relationships and standards of practice in relation to it' (Vaughan, 1997). This implies that, in carrying out risk assessments, there is a need to make simplifications concerning the risk involved.

The political and symbolic value dimension of risk influences what society includes in the concept of terrorism and thus what becomes a relevant topic of risk management. If a crime such as a shooting spree is denoted terrorism, it becomes a threat to the existence of democracy and freedom. If the same crime is labelled 'hate crime' or 'mass murder', the same political dimension will not be present. When the risk is linked to something with high value, such as democracy or the

existence of society itself, the frequency or probability loses relevance, because the thought of losing what is valuable is more important than considering the likelihood of the incident happening. This might make it difficult to fit terrorism into the language of risk management. The risk concept presented in the Norwegian standards has excluded probability assessments from the analysis. On the one hand, it might seem logical to exclude the probability aspect, given that terrorism involves low-frequency events and representative historical data to base risk assessments on do not exist. On the other hand, excluding probability entails that the focus is shifted from what is probable to what is possible and could lay the foundation for too great a focus on worst-case scenarios and mean that too many resources are spent on scenarios that will probably never become a reality.

The value aspect of risk also entails that the assessments that are done include value judgements, and that these value judgements are inseparable from the risk assessments. Despite the presence of a value aspect in the notion of risk in the security risk analysis, the impression is given that it is possible for an organization to neutrally outline the values that the organization should protect. As such, the standards give an impression that it is possible to perform objective value judgements, if the procedures are followed, and they do not take into account that risk assessments and value judgement are based on normative judgements. By so doing, the political risk of terrorism is de-politicized.

Through standardization, an unmanageable risk is made manageable, giving the illusion of security

Power (2004) states that contemporary societies are obsessed with taming and controlling all sorts of risks, and that risk management is applied by different organizations and authorities to create an illusion of a safer society. Risks must be made auditable and governable, because there are functional and political needs to maintain myths of control and manageability. According to Power, 'Risk management organizes what cannot be organized, because individuals, corporations and governments have little choice but to do so' (ibid., p. 10).

This is also the case for terrorism risk management. Organizations currently have the responsibility to manage terrorism risk, despite the fact that their ability to actually reduce the threat of terrorism is minimal, given that most security threats are rooted outside the organizational context, and that it is the state that has the mandate to detect, arrest, and prosecute potential terrorists. As a result, organizations are forced to take precautionary actions against terrorism, even though organizations do not necessarily have the corresponding tools at their disposal. Through the lens of risk management, terrorism has been transformed into a manageable and calculable risk. This creates an illusion of control and manageability.

Conclusion

Security risk analysis is not the only area in counterterrorism for which guidelines have recently been published. In parallel with the increased number of

foreign fighters returning to Europe and in line with an increased number of low-tech terrorist attacks in European countries, de-radicalization programmes in schools and prisons have been initiated. Consequently, standardization of terrorism management takes different forms and currently covers several guidelines for how to prevent radicalization. This implies that the risk management standards are a part of a broader tendency to standardize counterterrorism. The variety of actors in society that presently have a counterterrorism responsibility need some form of guideline to fulfil their role. Thus, there is reason to believe that we will be seeing even more standardization of terrorism management in the future. Through the language of risk management, the image is given that uncertainties can be tamed and that some form of predictability exists that will make us safe from terrorism. Consequently, the illusion of the ability to manage the unmanageable risk of terrorism is sustained. Although standardization will contribute to a hegemonic terrorism management regime, it is not evident that standardization will lead to a more secure society, given the paradoxes associated with the standardization of terrorism risk.

References

Amalberti, R. (2001). The paradoxes of almost totally safe transportation systems. *Safety Science*, 37(2), pp. 109–126.

Antonsen, S., Skarholt, K., and Ringstad, A. J. (2012). The role of standardization in safety management: A case study of a major oil and gas company. *Safety Science*, 50(10), pp. 2001–2009.

Askeland, T., Flage, R., and Aven, T. (2017). Moving beyond probabilities: Strength of knowledge characterisations applied to security. *Reliability Engineering & System Safety*, 159, pp. 196–205.

Aven, T. (2003). *Foundations of risk analysis: A knowledge and decision-oriented perspective*. Chichester: John Wiley & Sons, Ltd.

Barrett, F. J. (1998). Coda—creativity and improvisation in jazz and organizations: Implications for organizational learning. *Organization Science*, 9(5), pp. 605–622.

Bieder, C. and Bourrier, M. (2013). *Trapping safety into rules: How desirable or avoidable is proceduralization?* Ashgate: CRC Press.

Boin, A. and McConnell, A. (2007). Preparing for critical infrastructure breakdowns: The limits of crisis management and the need for resilience. *Journal of Contingencies and Crisis Management*, 15(1), pp. 50–59.

Borum, R. (2015). Assessing risk for terrorism involvement. *Journal of Threat Assessment and Management*, 2(2), pp. 63–87.

Bowker, G. C. and Star, S. L. (2000). *Sorting things out: Classification and its consequences*. Cambridge, MA: MIT Press.

Busch, L. (2011a). Food standards: The cacophony of governance. *Journal of Experimental Botany*, 62(10), pp. 3247–3250.

Busch, L. (2011b). *Standards: Recipes for reality*. Cambridge, MA: MIT Press.

Crelinsten, R. D. (2009). *Counterterrorism*. Cambridge: Polity.

Dekker, S. W. (2014). The bureaucratization of safety. *Safety Science*, 70, pp. 348–357.

Foucault, M. (1989). *The order of things: An archaeology of the human sciences*. London: Routledge.

Gjørv, A. B. *et al*. (2012). *Rapport fra 22. juli-kommisjonen: oppnevnt ved kongelig resolusjon 12. august 2011 for å gjennomgå og trekke lærdom fra angrepene på regjeringskvartalet og Utøya 22. juli 2011*. Avgitt til statsministeren 13. august 2012 (NOU 2012:14). Oslo: Statens forvaltningstjeneste. Informasjonsforvaltning.

Hajer, M. A. (1995). *The politics of environmental discourse: Ecological modernization and the policy process*. Oxford: Clarendon Press.

Hollnagel, E. (2014). Is safety a subject for science? *Safety Science*, 67, pp. 21–24.

Hood, C. (2002). The risk game and the blame game. *Government and Opposition*, 37(1), pp. 15–37.

Jackson, R. (2005). *Writing the war on terrorism: Language, politics and counter-terrorism*. Manchester: Manchester University Press.

Jarvis, L. and Holland, J. (2014). *Security: A critical introduction*. Basingstoke: Palgrave Macmillan.

Jore, S. H. (2012). *Counterterrorism as risk management strategies.* Vol. 178. Stavanger: UiS.

Jore, S. H. (2014). Norwegian media substantiation of counterterrorism measures. *Journal of Risk Research*, 19(1), pp. 101–118.

Jore, S. H. (2017). The conceptual and scientific demarcation of security in contrast to safety. *European Journal for Security Research*. doi:10.1007/s41125-017-0021-9.

Jore, S. H. and Egeli, A. (2015). Risk management methodology for protecting against malicious acts: Are probabilities adequate means for describing terrorism and other security risks? *Safety and Reliability of Complex Engineered Systems*, pp. 807–815. doi:10.1201/b19094-10910.1201/b19094-109.

Kettunen, J., Reiman, T., and Wahlström, B. (2007). Safety management challenges and tensions in the European nuclear power industry. *Scandinavian Journal of Management*, 23(4), pp. 424–444.

Linkov, I., Trump, B. D., and Fox-Lent, C. (2016). Resilience: Approaches to risk analysis and governance. In M.-V. Florin and I. Linkov, eds. *IRGC Resource guide on resilience*. Lausanne: EPFL International Risk Governance Center (IRGC). [online]. Available at: irgc.epfl.ch (accessed 4 November 2017).

Maal, M., Busmundrud, O., and Endregard, M. (2017). Methodology for security risk assessments: Is there a best practice? In L. Walls, M. Revie, and T. Bedford, eds. *Risk, reliability and safety: Innovation theory and practice.* London: Routledge, pp. 860–866.

McGraw, A. P., Todorov, A., and Kunreuther, H. (2011). A policy maker's dilemma: Preventing terrorism or preventing blame. *Organizational Behavior and Human Decision Processes*, 115(1), pp. 25–34.

Ministry of Defence (2011). *Forskrift om objektsikkerhet (2011).* LOV-1998-03-20-10-§17. Oslo: Ministry of Defence.

Mintzberg, H. (1983). *Structures in fives. Designing effective organizations*. Harlow: Pearson.

Mintzberg, H. (1989). The structuring of organizations. In D. Asch and C. Bowman, eds. *Readings in strategic management.* Berlin: Springer, pp. 322–352.

National Security Agency *et al*. (2015). *Terrorsikring. En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger*. [online]. Available at: www.nsm.stat.no/globalassets/dokumenter/veiledninger/veileder_terrorsikring_2015_enkelts_final.pdf (accessed 15 August 2016).

National Security Law [Lov om nasjonal sikkerhet] (2018). [online]. Available at: https://lovdata.no/dokument/NL/lov/2018-06-01-24 (in Norwegian) (accessed 15 August 2018).

Pache, A.-C. and Santos, F. (2010). When worlds collide: The internal dynamics of organizational responses to conflicting institutional demands. *Academy of Management Review*, 35(3), pp. 455–476.

Petersen, D. (1978). *Techniques of safety management*. New York: McGraw-Hill Companies.

Petersen, K. L. (2013). The corporate security professional: A hybrid agent between corporate and national security. *Security Journal*, 26(3), pp. 222–235.

Power, M. (2004). *The risk management of everything: Rethinking the politics of uncertainty*. London: Demos.

Renn, O., Klinke, A., and van Asselt, M. (2011). Coping with complexity, uncertainty and ambiguity in risk governance: A synthesis. *AMBIO: A Journal of the Human Environment*, 40(2), pp. 231–246.

Schröder-Hinrichs, J. U., Hollnagel, E., and Baldauf, M. (2012). From *Titanic* to *Costa Concordia*: A century of lessons not learned. *WMU Journal of Maritime Affairs*, 11(2), pp. 151–167.

Standards Norway (2012). *NS 5830 – Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Terminologi*. Oslo.

Standards Norway (2014a). *NS 5831 – Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sik-ringsrisikohåndtering*. Oslo.

Standards Norway (2014b). *NS 5832 – Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikoanalyse*. Oslo.

Statoil (2013). *The In Amenas attack – Report of the investigation into the terrorist attack on In Amenas, prepared for Statoil ASA's Board of Directors.* [online]. Available at: www.statoil.com/en/NewsAndMedia/News/2013/Downloads/In%20Amenas%20report.pdf (accessed 20 January 2014).

The 9/11 Commission Report (2004). *Final report of the national commission on terrorist attacks upon the United States*. Washington, DC: Government Printing Office. [online]. Available at: www.9-11commission.gov/report/ (accessed 20 April 2009).

Timmermans, S. and Berg, M. (2003). *The gold standard. The challenge of evidence-based medicine and standardization in health care*. Philadelphia, PA: Temple University Press.

Vaughan, D. (1997). The trickle-down effect: Policy decisions, risky work and the *Challenger* tragedy. *California Management Review*, 39(2), pp. 80–102.

Weick, K. E. and Sutcliffe, K. M. (2011). *Managing the unexpected: Resilient performance in an age of uncertainty*. Vol. 8. Chichester: John Wiley & Sons, Ltd.

10 Standardization of cybersecurity for critical infrastructures

The role of sensemaking and translation

Ruth Østgaard Skotnes

Introduction

The aim of this chapter is to discuss how processes of sensemaking and translation impact the development of global standards for cybersecurity for critical infrastructures. Cybertechnology and associated cybersecurity are today central to our economic and social lives (Schneider, Sedenberg, and Mulligan, 2016), and cyber risk has become a matter of global interest and importance (von Solms and van Niekerk, 2013). In the digital age, society's critical infrastructures rely on the functioning of information and communication technology (ICT) systems, as ICT software and hardware are integrated in the ability of other sectors to uphold their services (Almklov, Antonsen, and Fenstad., 2012). Securing ICT systems can contribute to creating a sense of confidence that the technologies and processes aimed at improving performance and welfare will not endanger data privacy, confidentiality, integrity, or availability, which are areas of value to both people and businesses (Schneider, Sedenberg, and Mulligan, 2016).

According to Scott (2008), the institutional construction of a risk management process is expressed and materialized in standards and guidelines. Standards formalize the fundamental design principles for the organizational self-management of risk and establish baselines against which organizations must evaluate themselves. As a means to protect ICT systems from malfunctions or attacks, national and international industrial (technical) standards and public guidelines for ICT safety and security management have been developed, to provide a wide range of different safety and security measures and activities.

Nevertheless, many industrial standards are sufficiently complex and ambiguous that they do not provide clear prescriptions for conduct. In such cases, the use of standards can be better conceived as occasions for sensemaking and collective interpretation (ibid.). According to Weick (2001), organizational members selectively attend to their environments and then, in interaction, make collective sense of what is happening. Weick's ideas are consistent with ideas of the scholars within organizational neo-institutionalism, who emphasize the diffusion of ideas through a process of 'translation'. Instead of treating institutionally prescribed structures and practices as 'out there' and as adopted more or less 'as is',

translation assumes that ideas and practices are interpreted and reformulated during the process of adoption.

Sensemaking and translation theory

In this chapter, the theories of translation and sensemaking are viewed as closely connected. Researchers in the tradition of Scandinavian (neo-)institutionalism (e.g. Czarniawska and Joerges, 1996; Sahlin-Andersson, 1996) and actor-network theory (e.g. Callon, 1986; Latour, 1986) use the term 'translation' to refer to situations where new ideas and practices are adapted to local contexts, as they travel during the diffusion process (Ansari, Fiss, and Zajac, 2010). In the global world, ideas travel around the planet but are then locally translated. The result may be that the same idea differs in every place it lands, that different ideas may lead to similar practices, and that the final combination of global ideas and local practices is almost inevitably difficult to foresee (Czarniawska, 2012). A text (e.g. a standard, regulation, guideline, etc.) is taken from its cultural/historical context to fit into another (Power, 2007), and no standard, no best practice description, no manual can guarantee that actions inspired by it will be identical (Czarniawska, 2012). According to Ansari, Fiss, and Zajac (2010), transfer and diffusion of practices among different local contexts consist of translation, co-construction, and editing activities in different cultural and social contexts and may lead to divergence and variability in practices that are being adopted, enacted, and adapted.

Niemimaa and Niemimaa (2017) have also found that practices across organizations may not emerge as identical simply by following the same set of best practices. On an abstract level, it may be possible to identify common characteristics of practices across organizations. However, closer analysis will likely show that the actual performances of these practices are never quite the same in all contexts. The best practices are translated in relation to local needs and peculiarities. According to Niemimaa and Niemimaa, translation is the process whereby abstract practices are transformed and implemented in organizations. Global or international prescriptions translate to situated (local context) practices.

Czarniawska and Joerges (1996) stress that attention, or perceptual readiness, is important in the translation process. Perception involves an act of categorization, that is, placing or giving an identity to an object, event, or idea (Bruner, 1957). We cannot translate what is wholly unrecognizable. We cannot perceive something unless it somehow relates to what we already know. People reading the same texts see in them different ideas, depending on what they expect to see and what they are able to notice in terms of categories accessible to them. According to Czarniawska and Joerges (1996), the context of organizational decision-making is influenced by taken-for-granted political arrangements or structures and cultural structures: a taken-for-granted social reality. Ideas must be fitted into already existing action patterns, that is, through local labelling, as it reflects the broader, social categorizing which tells us what to see.

According to Ansari, Fiss, and Zajac (2010), the diffusion process across time and across adopter should be assessed as an issue of dynamic fit between idea or practice and adopter, and this fit is influenced by technical, cultural, and political factors. Different forms of fit and its absence will trigger different patterns of adaption. There are also certain key characteristics of affordances that make it more or less likely that a practice will be adapted. These are the interpretive viability, divisibility, and complexity of the ideas or practices.

The perceived attributes of an idea, the perceived characteristics of a problem and the match between them are all created, negotiated, or imposed during a collective translation process, in the never-ending activity of sensemaking (Czarniawska and Joerges, 1996). Sensemaking comes from pre-existing symbols, norms, and social structures that people reproduce and transform rather than create from scratch (Weick, 2001). According to Weick, new technologies, such as complex production systems that use computers (e.g. critical infrastructures) have created unusual problems in sensemaking for the operators. The use of computer (ICT) systems involves the self-contained, invisible material process that is actually unfolding, as well as the equally self-contained, equally invisible imagined process that is mentally unfolding in the mind of an individual or a team.

ICT systems store digital data, and digital data are themselves translations of people, things, behaviours, and relations into information that can be stored, computed, and visualized by computers (Bellanova, 2017). Humans and digital data are continuously entangled in sociotechnical assemblages. According to Kaufmann and Jeandesboz (2017), digital information is never raw or universally accessible but is always fabricated and interpreted. The digital cannot be divorced from the social, and, thus, the digital is best examined within existing sociotechnical configurations and as an artifact with a set of affordances that are shaped and filled with meaning by social practice.

Furthermore, there is continuous improvement intervention and redesign (technological innovations) in computer technologies, which means that the implementation state of development never stops, and these technologies require ongoing structuring and sensemaking if they are to be managed (Weick, 2001). As previously mentioned, Weick's ideas are consistent with the ideas of the scholars in organizational institutionalism, who emphasize the diffusion of ideas through a process of translation. Organizations are not seen as conforming to institutional demands but as making sense of them, adapting them, enacting them, and working upon them.

Cybersecurity in critical infrastructures

ICT security is about the protection of ICTs, that is, hardware and software, and the term 'cybersecurity' refers to securing things that are vulnerable through the use of ICT (CCIS, 2014). The Association for Computing Machinery (ACM) Joint Task Force on Cybersecurity Education, which is a collaboration between major international computing societies, defines cybersecurity as

> [a] computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries.
>
> (CSEC, 2017)

According to the European Union Agency for Network and Information Security (ENISA), securing cyberspace has become one of the most important challenges of the twenty-first century (ENISA, 2016).

Industrial control systems (ICS) are vital to the operation of critical infrastructures, which are increasingly highly interconnected and mutually dependent systems. ICS include supervisory control and data acquisition (SCADA) systems and other control system configurations (Leith and Piper, 2013). ICS/SCADA systems are deployed worldwide and are traditionally used by utilities and industries in the areas of electric power supply, oil and natural gas, rail transportation, water, and wastewater. These systems support many aspects of our day-to-day lives, and in many cases are critical to our well-being and the very existence of our economy (Nicholson *et al.,* 2012).

Intricate interdependencies are the result of the computerization and automation of infrastructures of recent decades. As an example, computers and software depend on electricity, but the very same computers and software are strongly integrated into the production of electricity. The existence of such 'feedback loops' means that the potential for cascading effects will increase, at the same time as the intersections between infrastructures are becoming more and more opaque. This combination may lead to surprising interactional effects, and it is thus a vulnerability of increasing importance (Almklov, Antonsen, and Fenstad, 2012).

Historically, ICS have had little resemblance to traditional ICT systems, in that ICS were 'isolated systems', running proprietary control protocols using specialized hardware and software. However, according to Leith and Piper (2013), ICS owners are increasingly adopting ICT solutions to promote connectivity and remote access capabilities of corporate business systems. This integration supports new ICT capabilities but reduces the isolation of ICS from the outside world, creating a greater need for ICS security. According to the US Industrial Control Systems Emergency Response Team (ICS-CERT), infrastructure assets that use ICS have become high profile targets (Piggin, 2015), and there has been a significant increase in the number of plant disruptions and shutdowns, due to cybersecurity issues in the control networks at industrial facilities (Byres, 2011).

Stuxnet, discovered in 2010, was the first malware (malicious software) to specifically target SCADA systems and programmable logic controllers, and was responsible for causing substantial damage to Iran's nuclear programme. In 2013, Havex, a remote access Trojan, was used as part of a widespread espionage campaign, targeting ICS environments across numerous industries.

The malware, BlackEnergy 2, was used in a cyberattack that took down the Ukrainian power grid in December 2015, and ICS in the Ukrainian power grid were also hacked in December 2016, resulting in power cuts in Kiev lasting more than an hour. The malware used in the 2016 attack was named Crash Override/Industroyer and is the first known malware designed to attack electricity grid systems. It is a completely new malware and far more advanced than the general-purpose tools used to attack Ukraine's power grid in 2015. Another malware variant specifically designed to attack industrial safety systems, named TRITON, was discovered in December 2017. TRITON was apparently used to cause an operational outage at a critical infrastructure facility in the Middle East. According to Perelman (2018), these examples signal that operational networks, which have been largely immune to cyberthreats, are now in the cross-hairs of attackers.

What are standards and why use them?

Institutional capacities to organize in the face of uncertainty have been challenged and threatened by failures, scandals, and disasters, and, as a response to this, visionary documents and designs in the form of standards and guidelines for individuals and organizations have been produced, to maintain perceptions of control and manageability (Power, 2007). These recipes and recommendations have constituted a new normativity for safety and security management. The organization of uncertainty in the form of safety and security management designs and standards is related to expectations of governance and demands for defendable, auditable processes. Standards cover a broad range of types, serve a wide variety of purposes, and may be classified in numerous ways. The term 'standard' is given many different definitions, which it is important to remember when discussing the development of international and global standards (see Olsen, Chapter 1; Juhl, Chapter 2, in this volume).

A significant feature of standards and standardization is that expert knowledge is stored in rules and technical solutions (Brunsson and Jacobsson, 2000). Several researchers in organizational neo-institutionalism have focused on the emergence of 'soft' regulations, and the institutional change they are interested in is the displacement of coercive, state-level regulations by more voluntary regulations, such as standards, rankings, and accreditations (Greenwood *et al.,* 2008). In recent decades, most industrialized countries have made attempts to modernize their regulation of risk, by introducing new principles of regulation, coined with terms such as 'enforced self-regulation', 'functional regulation', and 'internal control'. These new regulatory regimes replace former 'command and control' regimes, by delegating part of the regulatory process to the stakeholders but under conditions given by the authority as regulator. Within this framework of enforced self-regulation, legal norms and standards are combined with industrial norms and standards (Lindøe, 2010; Lindøe and Baram, Chapter 14, in this volume). The dominant rationale behind this has been the process of mobilizing the self-regulatory capacity of high-risk industries. The industries have to make safety-critical judgements on their own and not just rely on government

prescriptions. This is meant to empower industries, engage them actively in the risk management processes, and make them accountable for the solutions adopted (Kringen, 2014; Lindøe and Baram, Chapter 14, in this volume).

However, the consistent application of a function-based regulation requires a comprehensive and systematic review of how the various provisions are to be understood and how the appropriate standards should be used to meet the requirements (Lindøe, 2010; Lindøe and Baram, Chapter 14, in this volume). Authorities are continually confronted with the need to know what is 'good enough'. The primary response has been to provide guidelines that, if adhered to, could optionally meet functional requirements, but other options are possible if an equally satisfactory effect is to be documented. Nevertheless, the maintenance of detailed guidelines generally has high costs, and the technology advances before them. Thus, the next step has been to replace guidelines with industrial standards (Kringen, 2014). These softer regulatory structures are developed and applied by non-governmental agencies and elicit compliance because they provide legitimacy (Greenwood *et al.,* 2008). By replacing much of the content in the guidelines with references to industrial standards, the role of the authorities has largely been to participate in standardization groups on a professional basis. To the extent that these standards are referred to in the guidelines, compliance with the standard would normally equal compliance with the regulation to which it is linked (Kringen, 2014; Lindøe and Baram, Chapter 14, in this volume).

A multiplicity of organizations have been created at 'the world level' to provide coordination and direction for risk management, including international standards organizations, such as the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the Committee of Sponsoring Organizations of the Treadway Committee (COSO). Variants of generic risk management create isomorphic pressures on organizations to conform to these models and to apply them (Scheytt *et al.,* 2006). Standards establish a conceptual framework to which organizations need to relate to be legitimate. A 'good' organization is now one which manages risk in accordance with established frameworks; organizations that value their reputation must adopt legitimate practices (ibid.). The distinction between mandated and voluntary norms has become blurred. Some standards become institutionalized in that, in practice, actors take it for granted that they should be followed (Brunsson and Jacobsson, 2000; Lindøe and Baram, Chapter 14, in this volume).

According to ISO (2017), 'A standard is a document that provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose.' The European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC) define a standard as

> [a] document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.

A European Standard 'carries with it the obligation to be implemented at national level by being given the status of a national standard and by withdrawal of any conflicting national standard'. Therefore, a European Standard automatically becomes a national standard in each of the 34 CEN-CENELEC member countries. CEN and CENELEC also cooperate with ISO and IEC to reach agreements on common standards that can be applied throughout the whole world (CEN and CENELEC, 2017).

Yet another very common way of understanding standards and standardization is 'everyone doing things in the same way'.[1] For example, the QualityTraining-Portal, which is a company that helps businesses and organizations implement and sustain quality and productivity improvement, defines standardization as: '[s)]tandardization is about creating best practices and then getting everyone to "copy exactly", using the established best practices the same way, everywhere, and every time' (QualityTrainingPortal, 2017). According to the *Handbook of Healthcare Management*:

> Once the process is simplified, it must be standardized, meaning everyone does it in the same way. Procedures, instructions, checklists, and other related documents are created to support the streamlined process, and training is undertaken to make sure everyone knows how to follow the new standard process.
>
> (Fottler, Malvey, and Slovensky, 2015, p. 57)

Another example is the *Practical Guide to Software Quality Management*, which states:

> Standards are the keystones of a Software Quality System. They provide the basis against which activities can be measured and evaluated. Further, they provide common methods and practices so that the same task can be accomplished the same way each time it is done.
>
> (Horch, 2003, p. 36)

However, standards are often general and abstract, and it can be difficult to do exactly what a standard says (Brunsson and Jacobsson, 2000). Furthermore, companies are not rational, in the sense that they do not neatly follow prescribed or formal paths (e.g. procedures, standards, processes). They have to rely on the expertise of individuals (and an informal world of practices) to fill in the gaps between expectations and real-life situations, through adaptive strategies and interactions in a constant flow of changes (Le Coze *et al.,* 2017). In this chapter, unlike in the previous definitions, standards are rather understood as ways of guiding the behaviour of various actors (Brunsson and Jacobsson, 2000) and as an opportunity to share expert advice and good practices to increase safety and security.

In many of the above-mentioned definitions of standards and European and US documents about cybersecurity, the terms 'standards', 'best practice', and

'guidelines' are used interchangeably. An example is from a review of cybersecurity best practices and lessons learned in the area of safety-critical electronic control systems, performed by the US National Highway Traffic Safety Administration in 2014, where they write: 'NIST [the National Institute of Standards and Technology] creates many of the standards, guidelines, and best practices that are used for security standards for operational systems in each sector' (McCarthy, Harnett, and Carter, 2014). However, according to Knowles *et al*. (2015), there is a distinction between the three types of formal security publications.

- Standards explicitly declare requirements to meet policies.
- Guidelines provide recommendations about what should be done.
- Best practices are guidelines that specify what should ideally be done in particular situations.

On the other hand, standards may be both mandatory and voluntary, and the definitions will vary in practice. Furthermore, according to Knowles *et al.,* it is important to use standards *in combination with* guidelines and best practices. In the remainder of this chapter, the terms 'standards', 'guidelines', and 'best practices' will to a certain extent be used interchangeably when referring to other work.

Standards for cybersecurity

An increasing number of standards are used as a basis for cybersecurity. Many of these standards overlap, in that they regulate the implementation of a management system for cybersecurity, with the aim of more structured and systematic work to generally improve the quality of cybersecurity and the implementation of risk-mitigating measures in particular (NOU, 2015). Knowles *et al*. (2015) presented an international survey of approaches for measuring and managing security in ICS environments. The study revealed that a multitude of ICS-specific security solutions had been developed by industry and academia across the full spectrum of risk management topics.

However, in the last few years, a lot of work has been done to attempt to develop and establish international standards and even global standards for cybersecurity, both for critical infrastructures and for cybersecurity in general. An example of these standards is the 'Framework for Improving Critical Infrastructure Cybersecurity', developed in the US by NIST, published in 2014 and updated in 2018, based on President Obama's Executive Order 13636. Another example is the holistic guidelines for cybersecurity, '10 Steps to Cyber Security', developed by the British Government Communication Headquarters, Centre for the Protection of National Infrastructure, and Department for Business Innovation and Skills, and launched in 2012 (re-launched in 2015) (NOU, 2015).

In Europe, the European Commission has set up a working group, the European Reference Network for Critical Infrastructure Protection, to look at how a European certification scheme could improve the cybersecurity of ICS

(ERNCIP, 2016). Cybersecurity is one of the priority areas of the European Commission initiative on ICT standards, which is part of the Digitising European Industry strategy, launched in 2016 (European Commission, 2016). These standards indicate a move towards a 'whole of community' approach to risk management, security, and robustness (NOU, 2015). According to the International Risk Governance Council, it is important to pursue international collaboration in both harmonizing technical choices and institutional and regulatory measures (Schneider, Sedenberg, and Mulligan, 2016). And, according to the Information Technology Industry Council, whose members are global technology companies located in various countries, globally developed security standards form the foundation of cybersecurity risk management.

Discussion

According to Westby (2004), cybersecurity standards and best practices typically apply over a large area, both geographically and in many infrastructure sectors. They may be issued by governments, quasi-government bodies, or private organizations. They can be global, international, regional, or national. They can be vendor-specific or industry sector-specific or generic. Overall, there is a myriad of laws, regulations, best practices, standards, and certifications that relate to information assurance and cybersecurity.

As previously mentioned, Knowles *et al*. (2015) presented a survey of approaches for measuring and managing security in ICS environments. They did a thorough analysis of standards, guidelines, and best practices, originating from government, industry and standardization bodies, and publications specific to ICS. They concluded that, although information security and assurance standards did not completely address security requirements of ICS, they were still used extensively in ICS environments. However, guidelines vastly outnumbered standards for ICS security. They found that US publications dominated in both categories and only a limited number of international or multinational (e.g. EU-wide) standards addressed ICS security in comprehensive terms. They also found it noteworthy that the standards with regulatory grounding were almost predominantly US-based. This was not surprising because the US has one of the most mature ICS security industries. However, it posed some interesting questions about how other countries can improve their own ICS industries. Would other countries be better off developing their own standards for ICS operations? Would the adoption rates of standards increase because of this? Would the existence of country-specific standards improve security because countries can enforce them with regulations?

There are many different types of ICS, with varying levels of potential risk and impact, which means that there are also many different methods and techniques for securing these systems. According to NIST 800–82, to properly address security in an ICS, it is essential for a cross-functional cybersecurity team to share their varied domain knowledge and experiences, to evaluate and mitigate risk to the ICS. And it is recommended that the cybersecurity team also

consults with the control system vendor and/or system integrator (Stouffer, Falco, and Scarfone, 2011).

However, the companies need to translate the standards, to be able to use them for their specific ICS system. As mentioned in the Introduction, many industrial standards are sufficiently complex and ambiguous that they do not provide clear prescriptions for conduct. In such cases, the use of standards can be better conceived as occasions for sensemaking and collective interpretation (Scott, 2008). The people carrying out the translation in this context are the people responsible for ICT safety and security/cybersecurity of ICS, and for implementing the measures prescribed in the standards in the different companies, such as ICT managers or coordinators and their teams.

A previous study in the Norwegian electricity power supply sector showed that very few of the electricity power supply network (distribution) companies used industrial standards for ICT safety and security for their ICS but used different types of guidelines and checklists instead. Because of the complexity of ICT systems, the industrial standards for ICT safety and security may be perceived as too complicated and difficult to follow; it is easier just to cross off items on a checklist. Considerable knowledge and technical skill are often required to use the industrial standards. Furthermore, according to the Norwegian companies, the different industrial standards were divergent when it came to methodology and approach to safety and security for ICS, and this made it difficult for the network companies to choose the right standard (Skotnes, 2012).

Contrary to the above, one of the recommendations from an official Norwegian report on digital vulnerabilities in society (NOU 2015, p. 13) was to increase the use of internationally recognized standards for ICT safety and security. According to the report, the employment of standards for risk management of ICT systems is useful, to ensure that analyses are as complete as possible and to cover all relevant areas. Referring to standards is also useful for achieving the most effective safety and security measures. However, the report also commented that the large and increasing number of standards contributes to complexity (NOU, 2015).

Hagen, Albrechtsen, and Hovden (2008) found that, even though information security guidelines were of a prescriptive nature and imperative, often the users still failed to apply the guidelines as intended. The result of this can be that the guidelines are not effective for the purpose of influencing human behaviour and attitudes. According to Brunsson and Jacobsson (2000), practising a standard is mostly about adapting practice, so that the standard describes it with reasonable accuracy. There may be substantial differences between presentation and practice, between formal structure and actual operations, and between what people say and what they do. Actors may have dual systems, which are decoupled from each other, and they may argue that they follow a standard, while not doing so in practice. However, according to Brunsson and Jacobsson, standardizers do not seem to notice this phenomenon, or at least they seldom discuss it in public. Standardizers seem to assume that standards that change presentation always change practice.

Hopkins states, 'It is not possible to give a simple answer to the question of whether or not a duty holder is in compliance. The very concept of compliance has to some extent lost its meaning' (2007, p. 7). One problem is that these 'beyond compliance' realities are often invisible to a formal and procedure-based approach to organizations. These realities are hidden behind the rational façades that safety management systems can create. The discourse about the existence of a formal organization seems to reflect the activities behind the scenes. It is supported by auditing techniques, which have been criticized precisely for their limitations regarding looking into complex realities (Power, 2007). Following procedures, standards, or processes is no guarantee of safety or security, because reality exceeds them. Procedures, standards, and processes are important, but there is a need for a better appreciation of context, what happens in real-life situations (Le Coze *et al.,* 2017). According to Gunningham and Sinclair (2009), only when the formal systems (audits, reporting, monitoring, etc.) are supported by informal systems (trust, commitment, engagement, means of overcoming conflicting loyalties, etc.) will they be fully effective.

Niemimaa and Niemimaa (2017) studied how an information technology service provider translated the information systems security (ISS) best practice of information classification into an ISS policy and into situated practices. As found in the study of the Norwegian electricity power supply sector, they note that the international ISS standards, such as ISO/IEC 27001 and ISO/IEC 27002, are universal and general in their scope and provide little guidance for the organizations that wish to adopt them (Siponen, 2006; Siponen and Wilson, 2009). Many organizations face the challenge of understanding and translating the standards' requirements into something concrete and actionable. The ISS policies will only materialize in the enactment of situated practices in a given context, and in organizations these policies must be crafted into material form by ISS practitioners. The translated practices Niemimaa and Niemimaa found at the IT service provider were neither exact copies of the best practices nor completely new but sustained a resemblance to and a connection with the best practices in ways that fitted their particular context and patterns of work. They found that it was important to engage in employees' work in order to reveal the possible incongruence between the ISS policy and local organizational practice. A new ISS practice should also be communicated and discussed with employees in a continuous manner rather than in a one-off effort to increase employees' motivation and skills to enact the new practice (Niemimaa and Niemimaa, 2017).

Following on from the above, the people performing the translation of the standards for cybersecurity can come from very different organizational contexts, for example, private companies, public organizations, governments, large or small organizations, different national, local, and organizational cultures, and so on. These different contexts will affect the outcome of the translation. The people doing the translation will try to individually and collectively make sense of the content of the standards, and the standards will be adapted and made to fit their own real-life context. Translation is not always a conscious choice; it is necessary to be able to implement and use the standards in the specific organizations.

On the other hand, according to the Information Technology Industry Council, it is important to stress that there is no one 'cybersecurity standard' or set of practices that is applicable across the board. Cybersecurity risk management is complex, including many moving parts, responsible parties, and standards. In addition, the global ICT industry continually establishes new standardization efforts, addressing emerging cybersecurity risk concerns. And, according to the 'Framework for Improving Critical Infrastructure Cybersecurity', a key point is that it is not a prescription. The framework complements, and does not replace, an organization's own risk management process and cybersecurity programme. The organization can use its current processes and leverage the framework to identify opportunities to strengthen and communicate its management of cybersecurity risk, while aligning with industry practices. Just as the framework is not industry-specific, the common taxonomy of standards, guidelines, and practices that it provides is not country-specific. Organizations outside the US may also use the framework to strengthen their own cybersecurity efforts, and the framework can contribute to developing a common language for international cooperation on critical infrastructure cybersecurity.

Conclusion

It is important to take into account the impact of sensemaking and translation on the development and use of standards and how this may affect the actual cybersecurity practices in local contexts. If global standards are developed, they will still have to be translated into the specific local context before they are used. This may result in very different practices in different countries and in different companies, even though they are using the same standards.

Different risk problems can be distinguished according to their degree of complexity, uncertainty, and ambiguity (Aven and Renn, 2010), and some approaches to risk problems are better suited to standardization than others. If standardization is understood as attempts to make risks more comparable and thereby more manageable, that is, 'everyone doing things in the same way', then cybersecurity for critical infrastructures is less suited to standardization. Cyberattacks can be seen as transboundary risks; they can cross geographical borders, affect multiple jurisdictions, undermine the functioning of various policy sectors and critical infrastructures, and escalate rapidly because of interdependencies between systems (Ansell, Boin, and Keller, 2010). If this is not taken into consideration, the global standardization of risk may lead to a poorer understanding of the mechanisms producing transboundary risks, which can lead to a reduced capacity to implement an efficient means of mitigation and preparation (see Olsen, Chapter 1, in this volume).

On the other hand, in the realm of cybersecurity for critical infrastructures, there *does* seem to be an understanding of the necessity to adapt and adjust the standards to the industry-specific, local context. If we acknowledge that standards are more an opportunity for interpretation and sensemaking, then creating international and global standards can rather be an opportunity to share expert

advice and good practices to increase cybersecurity. We can think of best practices not as prescriptive recipes of policy implementation but as ideas about the implementation (Niemimaa and Niemimaa, 2017). However, it is also important to remember that formal systems, such as the use of standards, will need to be supported by informal systems, such as awareness, trust, commitment, and engagement, to be effective.

Note

1 See also Juhl, Chapter 2, in this volume, for a thorough discussion of the semantic and pragmatic meanings of the concepts of standards and standardization.

References

Almklov, P., Antonsen, S., and Fenstad, J. (2012). Organizational challenges regarding risk management in critical infrastructures. In P. Hokstad, I. B. Utne, and J. Vatn, eds. *Risk and interdependencies in critical infrastructures: A guideline for analysis*. London: Springer, pp. 211–225.

Ansari, S. M., Fiss, P. C., and Zajac, E. J. (2010). Made to fit: How practices vary as they diffuse. *Academy of Management Review*, 35(1), pp. 67–92.

Ansell, C., Boin, A., and Keller, A. (2010). Managing transboundary crises: Identifying the building blocks of an effective response system. *Journal of Contingencies and Crisis Management*, 18(4), pp. 196–207.

Aven, T. and Renn, O. (2010). *Risk management and governance: Concepts, guidelines and application*. Heidelberg: Springer.

Bellanova, R. (2017). Digital, politics, and algorithms: Governing digital data through the lens of data protection. *European Journal of Social Theory*, 20(3), pp. 329–347.

Bruner, J. S. (1957). On perceptual readiness. *Psychological Review*, 64(2), pp. 123–145.

Brunsson, N. and Jacobsson, B. (2000). *A world of standards*. New York: Oxford University Press.

Byres, E. (2011). System integration – Revealing network threats, fears: How to use ANSI/ISA-99 standards to improve control system security. The International Society of Automation (ISA). [online]. Available at: www.isa.org/link/networkthreats (accessed 23 March 2019).

Callon, M. (1986). Some elements of a sociology of translation: Domestication of the scallops and the fishermen of St. Brieuc Bay. In J. Law, ed. *Power, action, and belief: A new sociology of knowledge?* London: Routledge & Kegan Paul, pp. 196–229.

CCIS (Center for Cyber and Information Security) (2014). Cyber security versus information security. [online] Available at: https://ccis.no/cyber-security-versus-information-security/ (accessed 2 January 2017).

CEN and CENELEC (2017). What is a European standard (EN)? [online]. The European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC). Available at: www.cencenelec.eu/standards/DefEN/Pages/default.aspx (accessed 28 February 2017).

CSEC (2017). CSEC2017 v. 0.5 Report. [online]. Cyber Security Education Consortium (CSEC). Available at: www.csec2017.org (accessed 2 January 2017).

Czarniawska, B. (2012). Operational risk, translation, and globalization. *Contemporary Economics*, 6, pp. 26–39.

Czarniawska, B. and Joerges, B. (1996). Travels of ideas. In B. Czarniawska and G. Sevón, eds. *Translating organizational change*. Berlin: Walter de Gruyter, pp. 13–47.

ENISA (2016). Stocktaking, analysis and recommendations on the protection of CIIs. Heraklion, Greece: European Union Agency for Network and Information Security (ENISA). [online]. Available at: www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis (accessed 23 March 2019).

ERNCIP (2016). The ERNCIP Project Platform, European Reference Network for Critical Infrastructure Protection (ERNCIP). [online]. Available at: https://erncip-project.jrc.ec.europa.eu/ (accessed 1 March 2017).

European Commission (2016). Cybersecurity industry, digital single market. [online]. Available at: https://ec.europa.eu/digital-single-market/en/cybersecurity-industry (accessed 2 January 2017).

Fottler, M. D., Malvey, D., and Slovensky, D. J. (2015). *Handbook of healthcare management.* Cheltenham: Edward Elgar Publishing.

Greenwood, R., Oliver, C., Suddaby, R., and Sahlin, K. (2008). *The SAGE handbook of organizational institutionalism.* London: SAGE.

Gunningham, N. and Sinclair, D. (2009). Organizational trust and the limits of management-based regulation. *Law and Society Review*, 43(4), pp. 865–900.

Hagen, J. M., Albrechtsen, E,. and Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, 16(4), pp. 377–397.

Hopkins, A. (2007). Beyond compliance monitoring: New strategies for safety regulators. *Law & Policy*, 29(2), pp. 210–225.

Horch, J. W. (2003). *Practical guide to software quality management*. 2nd ed. London: Artech House.

ISO (International Organization for Standardization) (2017). Standards. [online]. Available at: www.iso.org/iso/home/standards.htm (accessed 9 January 2017).

Kaufmann, M. and Jeandesboz, J. (2017). Politics and 'the digital': From singularity to specificity. *European Journal of Social Theory*, 20(3), pp. 309–328.

Knowles, W., Prince, D., Hutchison, D., Pagna Disso, J. F., and Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, 9, pp. 52–80.

Kringen, J. (2014). Liability, blame, and causation in Norwegian risk regulation. *Journal of Risk Research*, 17(6), pp. 765–779.

Latour, B. (1986). The powers of association. In J. Law, ed. *Power, action, and belief: A new sociology of knowledge?* London: Routledge & Kegan Paul, pp. 261–277.

Le Coze, J.-C., Pettersen, K., Engen, O. A., *et al*. (2017). *Sociotechnical systems theory and the regulation of safety in high-risk industries*. White Paper. Finland: VTT Technical Research Centre of Finland, p. 293.

Leith, H. M. and Piper, J. W. (2013). Identification and application of security measures for petrochemical industrial control systems. *Journal of Loss Prevention in the Process Industries*, 26, pp. 982–993.

Lindøe, P. H. (2010). Complex roles and mixed norms: A dilemma for safety inspections? Paper presented at the Working on Safety (WOS) 5th International Conference, Røros, 7–10 September.

McCarthy, C., Harnett, K., and Carter, A. (2014). *A summary of cybersecurity best practices (Report No. DOT HS 812 075)*. Washington, DC: National Highway Traffic Safety Administration (NHTSA).

Nicholson, A., Webber, S., Dyer, S., Patel, T., and Janicke, H. (2012). SCADA security in the light of cyber-warfare. *Computers and Security*, 31, pp. 418–436.

Niemimaa, E. and Niemimaa, M. (2017). Information systems security policy implementation in practice: From best practices to situated practices. *European Journal of Information Systems*, 26(1), pp. 1–20.

NOU (Norsk Offentlig Utredning)(2015). *Digital sårbarhet – sikkert samfunn – Beskytte enkeltmennesker og samfunn i en digitalisert verden*. Oslo. Norsk Offentlig Utredning (NOU 2015:13.

Perelman, B. (2018). The rise of ICS malware: How industrial security threats are becoming more surgical. *Security Week*, 21 February. [online]. Available at: www.securityweek.com/rise-ics-malware-how-industrial-security-threats-are-becoming-more-surgical (accessed 18 June 2018).

Piggin, R. (2015). Are industrial control systems ready for the cloud? *International Journal of Critical Infrastructure Protection*, 9(C), pp. 38–40.

Power, M. (2007). *Organized uncertainty: Designing a world of risk management*. Oxford: Oxford University Press.

QualityTrainingPortal (2017). 5S Resource Center: 5S Defined. [online]. Available at: www.qualitytrainingportal.com/resources/5S/standardize.htm (accessed 9 January 2017).

Sahlin-Andersson, K. (1996). Imitating by editing success: The construction of organizational fields. In B. Czarniawska and G. Sevón, eds. *Translating organizational change*. New York: Walter de Gruyter, pp. 69–93.

Scheytt, T., Soin, K., Sahlin-Andersson, K., and Power M. (2006). Special Research Symposium: Organizations and the management of risk. Introduction: organizations, risk and regulations. *Journal of Management Studies*, 43(6), pp. 1331–1337.

Schneider, F., Sedenberg, E., and Mulligan, D. (2016). *Public cybersecurity and rationalizing information sharing. Opinion piece for the International Risk Governance Center (IRGC)*. Lausanne: IRGC.

Scott, W. R. (2008). *Institutions and organizations: Ideas and interest*. 3rd ed. Thousand Oaks, CA: SAGE.

Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM*, 49(8), pp. 97–100.

Siponen, M. and Wilson, R. (2009). Information security management standards: Problems and solutions. *Information and Management*, 46(5), pp. 267–270.

Skotnes, R. Ø. (2012). Strengths and weaknesses of technical standards for management of ICT safety and security in electric power supply network companies. *Journal of Risk and Governance*, 3(2), pp. 119–134.

Stouffer, K., Falco, J., and Scarfone, K. (2011). *Guide to industrial control systems (ICS) security: Recommendations of the National Institute of Standards and Technology*. Washington, DC: US Department of Commerce, Special Publication 800–82.

von Solms, R. and van Niekerk, J. (2013). From information security to cybersecurity. *Computers and Security*, 38, pp. 97–102.

Weick, K. E. (2001). *Making sense of the organization.* Oxford: Blackwell Business.

Westby, J. R. (2004). *International guide to cyber security*. Chicago: American Bar Association, Privacy and Computer Crime Committee, Section of Science & Technology Law.

11 Standardizations and risk mapping

Strengths and weaknesses

Lene Jørgensen and Preben H. Lindøe

Introduction

This chapter aims to investigate the role of the *risk matrix* in standardization of risk work. The risk matrix is one of the most prominent tools within risk management, being traced back to the 1980s (COSO, 2004a, 2004b; Collier, Berry, and Burke, 2007; Power, 2007; Woods, 2009; Jordan, Jørgensen, and Mitterhofer, 2013; Goerlandt and Reniers, 2016). Only a few studies investigate the actual use of risk matrices in practice (Woods, 2009; Boholm, 2010; Jordan, Jørgensen, and Mitterhofer, 2013). The chapter examines different standardization processes linked to risk mapping and discusses the positive and negative effects of these formal and informal standardization processes.

The research context is *inter-organizational collaboration*. As work life becomes ever more specialized and complex, inter-organizational collaborations in projects are becoming increasingly common, making risk management even more challenging, as it involves collaboration between different actors, disciplines, and organizations (Bourrier, 2005; Milch and Laumann, 2016). The concept of *mediating instruments* (Miller and O'Leary, 2007) directs the attention towards how particular management tools such as the risk matrix mediate the relationship between distributed actors, distinct imperatives, and domains within a socio-technic network.

In her analysis of the concept of standardization (Chapter 2, in this volume), Juhl explores many alternative interpretations. The understanding and interpretation of 'standards' are comprehensive, taking into account the diversity of 'local standards' and 'best practice' within organizations. In this chapter, we follow up the issue, by assessing how standardized procedures, tools, and practices are organizationally enacted in specialized and complex inter-organizational collaborations. An in-depth analysis of a case study provides a window into risk management practices in an inter-organizational project, where standardization manifests itself in formal and informal ways with wanted and unwanted outcomes.

The chapter is organized as follows; first, we introduce the risk matrix as a tool and some theoretical perspectives related to standardization, use, and effects. Then the context of the study, methods and empirical findings follow. Finally, the findings are analysed and discussed before concluding.

Perspectives on the risk matrix

Risk matrices, because they have several useful qualities, are representations of hazardous situations, events, or actions, where a complex reality is translated into a form that facilitates control at a distance (Zuboff, 1988). Within this framework, operational risks, risk related to HSE (health, safety, and environment), technical risks, reputational risk, etc. are made commensurable. The risk matrix offers a diagrammatic, simplified image, which is appealing to users (Quattrone, 2009), offering an opportunity of 'knowledge at a glance' (Cooper, 1992; Jordan, Jørgensen, and Mitterhofer, 2013).

Risk matrices consist of a diagram with two axes, describing respectively the probability of an unwanted event (the x-axis) and the severity or consequences of that event (the y-axis). Different types of risks are identified and placed in the matrix, according to the assessment of their probability and severity. The matrix is usually presented using the traffic-light metaphor of red, amber, and green. An observed 'risk' placed in the red zone will be identified as 'no go' or not acceptable. Risks placed in the green zone mean that the situation is acceptable. The amber zone in between indicates that the risk must be followed up with attention. Figure 11.1 presents a 'standard' risk matrix format.

Many researchers have stressed that standardization of risk management is problematic (Schrader-Frechette, 1991; Power, 2004; Busch, 2011). Practitioners and other stakeholders can get the impression that risks are easily identifiable, quantifiable, and manageable. The development and use of risk matrices mean a considerable reduction and simplification of a complex reality. Several authors have questioned the functionality and precision of a risk matrix (Ward and Chapman, 2003; Cox, Babayev, and Huber, 2005; Cox, 2008; Pickering and Cowley, 2010; Aven, 2011; Brünger, 2011; Ball and Watt, 2013; Jordan, Mitterhofer, and

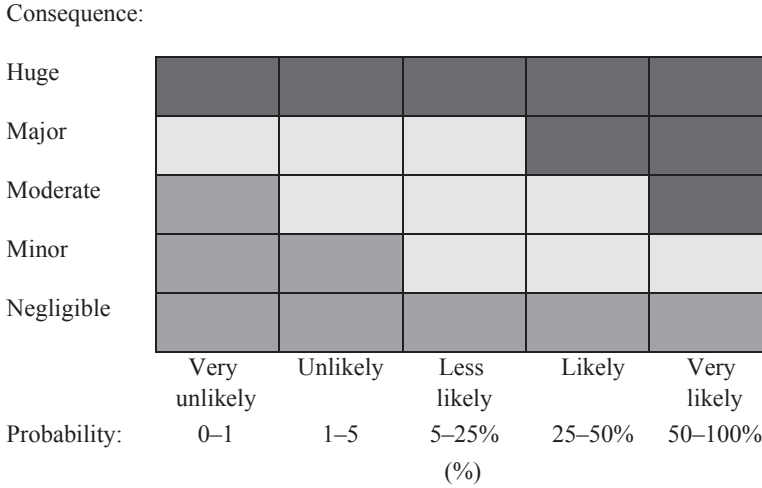

Figure 11.1 Ideal-type risk matrix

Jørgensen, 2018). However, such testimonies of technical 'imprecision' and misrepresentation have not reduced the popularity of risk matrices. On the contrary, their application and use are promoted in guidelines from authorities and consultants.[1]

As already demonstrated in previous chapters (see Part II), there is a gap between the diversity and complexity of risk and standardization as concepts and the need to simplify the practical use of standardized methods and tools. This chapter provides better insight into these challenges by following up perspectives of organizational translation and sensemaking, as discussed by Skotnes in Chapter 10, in this volume. With the aim of exploring the effects of standardized tools within risk mapping, we will introduce some useful theoretical perspectives.

Theoretical perspectives

Risk management textbooks and guidelines often present risk management as protecting the organization from loss by avoiding risk (Collier, 2009). Before the promotion of 'enterprise risk management' (ERM), risk management was implemented within separate disciplines, such as HSE risks, technical/operational risks, and cost risks, which could lead to silo-based or functional approaches. Since the rise of ERM from the middle of the 1990s, more and more 'risk events' have been seen and described as organizational 'risk objects' (Power, 2004, 2007), looking at risks in a more overall and integrated manner. ERM has become a standardized way of managing organizations, promoted by an ever-growing body of risk management textbooks, standards, and guidelines. Within this toolbox, the risk matrix is particularly suited for displaying different types of risks and for mediating between different actors and actor groups (Power, 2007; Jordan, Jørgensen, and Mitterhofer, 2013). Most likely, there is a link between the rise of ERM and the increased popularity and use of the risk matrix.

In contrast to overall ERM, *project risk management* focuses on a specific task within a short-term span. Project management is about planning, organizing, and managing resources for the successful completion of a specific task and its unique goals, within the right time frame and within budget. Collier (2009, p. 197) says that project risk management 'provides a holistic view of project risks, identifies potential problems and builds processes to help the service provider monitor and manage those risks'. In this context, risk matrices are often used for two purposes: (1) as templates in the ongoing discussions within teams throughout the project; and (2) in reporting to senior management within and across inter-organizational settings (Jordan, Jørgensen, and Mitterhofer, 2013).

Risks are usually managed within the areas of HSE, technical integrity, costs, time schedule, and reputation, making different types of risks commensurable. The impact of the risks can either be quantitatively or qualitatively assessed, depending on the nature of the risk. In either case, it is possible and common

practice to estimate an economic calculation of the impact (Busch, 2011, pp. 278–286). This will trigger an already strong focus on costs, and the omnipresent trade-off between costs and safety will be very relevant, as a major task in management (Reason, 1997; Aven, 2012).

As presented by Juhl in Chapter 2, in this volume, the standard responses in risk management analysis rely on simplifications of a complex reality and are posited as normal, universal, and unproblematic (Jordan, Jørgensen, and Mitterhofer, 2013). High reliability theory (HRT) is a critical voice against simplifications of organizational practice. HRT identifies key processes to explain how organizations manage to avoid major accidents and mistakes, labelling them 'the mindful infrastructure for reliable performance' (Weick, Sutcliffe, and Obstfeld, 1999). Reluctance to simplify interpretations is one of several identified 'processes of mindful organizing' that can promote error detection and the capacity to contain consequences of error. According to HRT, simplifications may undermine robust risk assessment. The researchers argue that successful high reliability organizations (HROs) have developed a 'reluctance to simplify interpretations' that works as an antidote against mindless operations that may miss weak signals of danger or suppress dissenting voices. 'Mindlessness' in their view is characterized as 'reliance on past categories, acting on "automatic pilot" and fixation on a single perspective without awareness that things could be otherwise' (ibid., p. 38). In contrast, in a state of 'mindfulness', awareness tends to be high and broad, with routines being constantly renegotiated, and assumptions and decisions questioned. 'Simplifying interpretations', as characterized by Weick and his co-authors, refers to the commonly observed way of handling complexity, in which people tend to ignore new information that contradicts their existing 'worldviews', 'frameworks', or 'mindsets' (ibid.).

Simplifications are, to a certain degree, also necessary in risk management: The critical issue is whether these simplifications are accurate enough to ensure the organizational or project goals. Simplifications also means making decisions on which aspects of the problems can be ignored and which must be attended to and followed up. Interdisciplinary teams increase the possibility of identifying risks. However, having divergent views and perspectives may lead to discussions, conflict, and time consumption in project teams. Therefore, HROs need institutionalized mechanisms that enable the involved actors to constructively deal with disagreement and conflicts that may arise as results of divergent views.

Project teams normally consist of representatives from different relevant disciplines. These teams have great potential for organizing work, focusing effort, making good decisions, and solving problems (Janis, 1989). Diversity in background, perspective, and experience are important to increase cognitive skills in the group and get the overall job done. Janis argues that, in diverse teams, case-oriented conflicts and intellectual sharpening of different perspectives will increase the number of suggestions and solutions. The outcome can be decisions of higher quality, where compromising is an important part of the process. Bourrier (1996) explains that cooperation implies that individuals mutually adjust their strategies and renegotiate participation and responsibility. Effective collaboration

in divergent teams relies on a common understanding of the objectives of the work, the challenges, and risks, as well as the time schedule. As a rule, shared understanding does not exist at the outset of the collaboration. In a project team and inter-organizational collaboration, divergent actors have to engage in a process of alignment to create common ground, which facilitates progress and develops mutual trust and confidence as competent project partners (Jordan, Jørgensen, and Mitterhofer, 2013).

Formal standardization using risk management procedures and tools (such as the risk matrix) and diverse project teams are important steps in ensuring quality in the management process. However, the informal parts of the system also come into account in this matter. Informal work practices, based on custom, convention, or general consent, will develop over time (Schein, 1985). Work practices should exploit the potential of diverse teamwork in such a way that the intentions and potential are realized. This might not be the case. Some researchers point to factors which negatively influence the potential high-quality group processes. Particularly due to communication patterns and cognitive limitations, some of the information is not shared in diverse teams (Weick and Roberts, 1993). Other potential negative factors are that procedures and documentation in themselves produce trust in the control processes (Pentland, 1993; Power, 1997, 2003, 2007), which in turn could lead actors to withhold discussion and judgement. All these factors may have a negative effect on the quality of decision-making and problem-solving. Janis (1989) argues that consensus in groups can become more important than the quality of their individual decisions. Through *passive conformity*, actors adapt their behaviour and opinions, so that they fit the behaviour and attitudes of the others in the group. *Active conformity* happens when actors are persuaded to adjust, in order to fit the group´s attitudes and behaviour.

Description of case and research methods

The empirical case study was part of a PhD thesis (Jørgensen, 2017), and the project studied was a so-called upgrading project within two gas-processing plants in Norway. The Norwegian petroleum sector is organized in accordance with European Union requirements from the late 1990s, which secures independence within the gas-value chain and third-party access to infrastructure for transportation of natural gas to the market. This requirement resulted in a separation of ownership and operator along the gas-transportation value chain. In some cases, the operator has outsourced the daily operations to a technical operator company (TOC). The inter-organizational collaboration in the case under study consists of three actor groups, as illustrated in Figure 11.2.

The owner group is a joint venture of different companies, funding investments and making decisions about the project's decision gates. A 'decision gate' denotes the necessary decisions to be taken when activities move from one main project phase to another. The operator in this case is a non-profit public organization, responsible for overseeing the TOC and for looking after the owners' interests. The technical operator company´s mandate is to run the daily operations

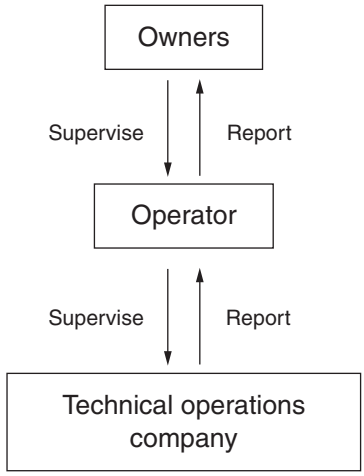

Figure 11.2 Main actor groups and their inter-organizational relationship.

at high quality in a safe and cost-efficient manner. The operations require tight collaboration between the operator and the TOC. The owner organization has a very important but more peripheral role. Both the operator and the TOC had their own inter-disciplinary project team.

The project went through four project phases, which are illustrated in Figure 11.3. The feasibility phase is about specifying the problem and looking for three possible solutions. The solutions are worked on to a point of 'maturity', where the owners have enough information to make a decision in the concept phase. In the definition phase, the concept chosen is matured and everything is developed further in preparation for the execution phase. In this case, this stage is the actual upgrading taking place at the plants.

The research method used was an ethnographic approach, following the project for a period of two and a half years. The project owner provided access to project meetings, procedures, guidelines, and project documents. Updates and reviews related to project activities were described in project-governing procedures within each organization. The most relevant documents were analysed, in order to understand how risk management in the different project phases was defined and regulated. In total, 52 documents were selected for analysis. The most important inter-organizational arenas were the monthly meetings between the operator and TOC, the base-line updates, the independent project review (IPR), at each decision gate, and the operator's risk reviews. The latter was carried out every six months. The monthly TOC risk reviews were another important arena for observations, although were not inter-organizational. In total, 50 project meetings were observed. Depending on the agenda, between 3 and 20 people were present in these meetings. Finally, 17 interviews of project team members were conducted.

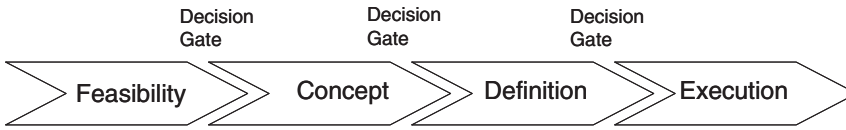

Figure 11.3 Blueprint of project phases (D-TOC-1).

Findings

Formal standards refer to codifications of rules and procedures into written documents (see Juhl, Chapter 2, in this volume). Project management and risk management were highly standardized in the studied case. In regulations and procedures, the necessity and relevance of identifying, representing, and managing risks are explained with reference to an 'enterprise-wide risk management approach' and 'to make sure that our operations are safe, and to reach our corporate goals in compliance with our requirements' (D-TOC-5).[2] At the same time, the particular rationale for using risk matrices is presented in governing documents as increasing efficiency in reporting and decision-making (D-TOC-3, p. 4), stressing its relevance for efficiently complying with external accountability requirements as well as for supporting internal decision-making processes.

There was a 'collaboration agreement' contract, regulating the relationship between the operator and the TOC. Furthermore, several procedures were related to project management, risk management, and risk management in projects. The risk matrix and other tools and blueprints were integrated into software programmes and used by both parties. This standardization implies the choices already made about what is important and how different tasks should be performed. This is meant to ensure risk management of a certain quality, and that work processes are efficient and effective. Standardization means complexity reduction, where a complex reality is made simpler and more manageable.

In carrying out risk reviews and filling out reports, past categories, based on experience from other relevant projects and operations, were the starting point for establishing risk matrices in the start-up of projects. When the operator and the TOC establish the risk matrix for the first time, they both rely on pre-existing categories. There is a list of frequent risk issues in projects, which the risk facilitator goes through, before the brainstorming in the divergent project team begins. This practice saves time compared to starting from scratch and letting the actors come up with categories themselves.

We will give two examples of enacting formal and informal processes of 'risk mapping' among the main actors within the inter-organizational relationship (see Figure 11.2). The examples highlight some important issues, followed up in the analysis. The first example illustrates the challenges of openness and balancing trust and mistrust in the hierarchical partnership of owner, operator, and TOC. The second example exposes the formal and informal negotiation

process taking place in mapping and re-mapping a diversity of risk issues within a limited matrix format.

Example 1: Inter-organizational collaboration

The first empirical example relates to the inter-organizational collaboration between the operator and the TOC. The complexity of the work itself and the management system called for methods to simplify work practices and reporting practices. A vast amount of information about all the different aspects and activities in the project needed to be filtered, to suit the needs of the project management level in each organization, the inter-organizational level, and the top level (owner arenas and senior management levels in both organizations). The actor groups had formalized their collaboration in an agreement, which, among other things, specified the kind of information that should be included in the monthly report, the decision gate support package, the sorts of meetings that the operator had access to, and so on. The monthly meeting template is a formal, standardized report, including the issues and level of information the actors had agreed upon. However, attempts were made to negotiate over attending more meetings and gaining access to more underlying information. The monthly meeting report in general and the provision of information about risks through the risk matrix were, at times, not perceived as 'sufficient' for the operator.

The operator occasionally asked for permission to be an observer at the TOC's internal meetings and was sometimes refused access. One example was the TOC's monthly risk reviews, where the operator very much wanted to gain access but never did during this project. The argument for denying access was that these processes were internal to the TOC. The operator thought more underlying information, through observing meetings and receiving more documents, would increase their ability to oversee and monitor the TOC. Such information could prepare them better to answer questions from the owner group and thereby justify passing the decision gate to the next project phase. The TOC, on the other hand, stated that the operator should trust them and that they did not see a need to reveal background material. The TOC had also had the experience that giving more details to an operator led to even more questions and extra work, shifting the focus away from more important issues, which could also influence cost and schedule.

The following episode from a monthly meeting illustrates the tension arising when the project partners negotiated over access to more information and underlying documents. In this meeting, the operator requested more details regarding criticality issues in the schedule (project flow) to be included in a presentation meant for the owners. The TOC asked why the operator needed this extra information, arguing that they used the risk matrix for risk-related information, including the time schedule and progress in every monthly meeting. The operator said there could be issues related to the schedule that were not serious enough to be among the 'top ten' risks in the risk matrix. They, therefore, wanted to have more detailed information about this.

Here is an example of a discussion between the TOC project member and the operator:

PROJECT MEMBER TOC (1): You [the operator] have to balance your demands for access and details. Yes [representative from the operator], you can raise your eyebrows, but it is true. You [the operator] can kill our organization with all this; you have to find a balance.

PROJECT MEMBER OPERATOR: We must be allowed to ask whether you [TOC] have an overview over all the critical activities.

PROJECT MEMBER TOC (1): Yes, we have; the question is whether this is going to be included in the presentation.

PROJECT MEMBER TOC (2): This is a typical discussion. We have improved and developed the risk matrix, but we are not willing to use it fully. We want the underlying information in addition, we want both.

Another project team member from the TOC said that this discussion had to be handled at a higher level in the organizations. A third representative from the operator then concluded that the TOC did not have to include the information in question in the presentation but needed to have an overview and have answers ready if the owners came up with some questions about the issues.

On another occasion, in an outburst, one TOC team member demanded of the operator's project manager:

PROJECT MEMBER TOC: How many nuts and bolts are you going to get yourself involved in? … Why don't you trust us?

The operator was aware that requiring more information from the TOC might make the TOC feel they were not trusted, and that this could influence the collaboration climate. Combining the role as a collaborator and supervisor, the operator said that they took care not to tell the TOC what to do. If the operator instructed them to do something and the TOC did not feel ownership of it, it would probably not get done. The TOC experienced the same dilemma regarding their relationship with their contractors. They needed to balance being both a collaborative partner and a supervisor. From time to time, the TOC felt the need for more detailed control, but they were aware that this might be regarded as lack of trust. For that reason, the TOC gave their subcontractors some leeway and made sure they felt ownership of their tasks.

Example 2: Informal practices

Informal practices refer to standards that have grown out of custom, convention, general consent, and 'best practice'. In essence, they are behaviour standards, laying down codes of conduct in given situations, based on a specific mindset (see Juhl, Chapter 2, in this volume). According to the procedures laid down in the project management system, the risk matrix should give an updated picture

of the risk status. In practice, the risk matrix was quite stable over time. The established practice was to make sure the different risk themes were covered in the matrix (HSE, cost, schedule, technical risks, reputation) and give them abstract names. Each of the risks would then include several issues, involving a lot of mitigating activities. The abstract, overview risks mapped in the risk matrix did not have much meaning in themselves (abstracts such as 'technical integration', 'subcontractor performance'), and, therefore, the matrix did not reflect the actual activities that were performed in the projects. The effects of these standardized practices caused concern among project team members. An excerpt from an interview will illustrate this point: 'I think the biggest risk, once you have established the risk matrix, is that you become blind. You get blinkers on, and you ignore things that are happening outside of them. I´d say that is the biggest issue' (1-OP-01).

An excerpt from an observed monthly TOC risk review meeting shows that risks usually remained in the matrix over time, and few new risks were included. This caused concern for team members during the project (M-OP-08):

PROJECT MANAGER:It worries us that we never get to close risks; we drag risks along all the time.

ENGINEER REPRESENTATIVE: The projects are processes; there are changes and developments all the time.

PROJECT MEMBER: We are talking about two different things; we are on different levels of detail. Can we just close this risk [engineer representative]?

ENGINEER REPRESENTATIVE: Go ahead and close it as far as I am concerned, but it is not realistic.

PROJECT MANAGER: (Reads out the title of the risk) We have performed [the task].

ENGINEER REPRESENTATIVE: Yes, but there have been some changes. I perceive it like this: We establish a risk and then we comment on what happens as the project moves along.

PROJECT MEMBER (RISK DEPT.): We always have to close that particular risk and then establish a new one. We can't change the names of old risks.

PROJECT MANAGER: If we make new ones for each of the concerns we have, it becomes easier to handle them and close them one by one.

What happened next in the meeting was that they closed that particular risk issue and established a new one. Later in the project, they merged somewhat related risks. Too many quite similar risks were difficult to handle. This discussion went back and forth several times as an issue they struggled with quite a lot when working with the risk matrix.

Few new risks were included in the risk matrix during the project period. The operator's project manager did not always ask whether new risks had emerged in monthly meetings (ME-OP-TOC-18). When serious problems and risk issues arose, they were discussed, but they were mostly handled outside the meetings, which also demonstrates that the risk matrix did not reflect everything that was going on.

Seeking alignment

Alignment of divergent teams and actor groups is an important part of any inter-organizational collaboration, and the many benefits of alignment are documented well in the research (Cicmil and Marchall, 2005; Ravishankar, Pan, and Leidner, 2011; Ika and Donnelly, 2015; Mok and Shen, 2015; Bygballe, Swärd, and Vaagaasar, 2016; Tantalo and Priem, 2016). In their study of inter-organizational project collaboration, Jordan, Jørgensen, and Mitterhofer (2013) identified such alignment as a major effect of risk matrices. Also, in our case study, alignment on objectives, major challenges, and risk issues was important for ensuring trust in each other's ability and commitment to the project and its performance. Such alignment facilitates the collaboration and the progress of the project. Negative effects of alignment have been less focused; one exception is group think (Janis, 1989).

One informant in the TOC, who had considerable experience in project management, said that he used the risk matrices to render the objectives visible for the different actors and actor groups. People could have different views on what the actual objectives were, and views could shift over time, so it was important to focus on the goals and make sure people were aligned. Another informant from the operator put it like this: 'You need to remind yourself of what you agreed on. It [the risk matrix] helps align people on what the challenges are, either within a group or across groups …' When questioned what alignment mean, he answered: 'Alignment means that you agree, at least, on what the major challenges are. It's an agreement on what the main challenges are in the project, what the agenda should be, and what we should be looking at' (I-TOC-01).

The distributed actors and actor groups seemed to need this kind of 'aligning' process on targets. Alignment on the major risks in the project was regarded as a good result of inter-organizational meetings and risk reviews, as illustrated in the following conversation at the end of a risk review meeting (M-OPTOC-09):

PROJECT MANAGER OPERATOR: I think this has been a good review, it is a good thing that we are aligned.
PROJECT MANAGER TOC: We are well aligned, that's true.

The different actor groups also copied and pasted some of the risks from each other's risk matrices. This practice also ensured alignment and a common understanding of the project and the main risks. The operator copied risks from the TOC and the TOC copied risks from the subcontractors. Some actors perceived these practices as problematic. It could lead to insufficient updating and stand in the way of engaging in the specific risks that each organization was exposed to. The following quotes from operator project team members illustrate this point:

> It can become a security blanket for us, using the TOC's risk matrix. We must consider where WE are exposed ourselves. There must be a correlation between the gut feeling of the project management and the risks displayed in the risk matrix.
>
> (I-OP-01)

> If we have a common risk picture with the TOC, it could turn out to be dangerous. We should not have the same mindsets.
>
> (M-OP-09)

Project team members in the TOC were also aware of the same dangers related to copying and pasting from the subcontractors' risk matrix.

Avoiding discussions and questions

When observing 50 project meetings, it was puzzling to notice how quickly the participants went through the different risk issues in the matrix and how little discussion there was in these meetings. On several occasions, when a discussion started, the project managers said there was not time to go into detail or that they would come back to the issue on another occasion. In addition to perceived lack of time, the participants representing different disciplines in the project teams were given a lot of autonomy and trust. Often these experts acted a great deal on their own professional basis, when identifying, positioning risks, and deciding on mitigating actions, as long as the project manager agreed the risk should be displayed in the risk matrix in the first place.

When preparing for inter-organizational meetings and working on documents that would be presented to another actor group, there was a concern about reporting the right level of detail to make the other actor happ. and discourage them from asking follow-up questions, requiring more background information or more studies. This was particularly the case when reporting to the owners. Both too few and too many details could raise questions and generate more work. Concern over details was observed in the operator and in the TOC meetings and in inter-organizations meetings, as the following citation from an inter-organizational meeting by an operator illustrates: 'The owners will probably ask questions about this [cost figure presented at portfolio level instead of per project]. All questions that can be stopped beforehand are a good thing' (M-OP-TOC-11b).

On some occasions, information believed to make the owners confused or suspicious was withheld. An example of such information was that this particular project had less priority, due to another, more challenging project in the same project portfolio. In another case, the operator and the TOC jointly planned how to present the project, to avoid the owners looking at the opportunity to organize this project as a stand-alone project, instead of including it in the portfolio.

To have decisions made and approvals given at the right time was identified as the greatest risk in any project in the studied case (I-TOC-02). A bad case scenario was that too many questions and too much uncertainty could result in a lack of approval for further funding and thereby a lack of acceptance to enter the next project phase. A less serious consequence could be prolonged meetings and a request for follow-ups, such as more tests and extra reviews. Questions and discussions would result in prolonged meetings, which they tried to avoid for several reasons: the extra time spent and the extra work would negatively affect the cost and the schedule.

Discussion

As presented in the Introduction, a precise representation of risk issues is not seen as an end in itself, and there has been no expectation of risk matrices as 'representational of the truth' (cf. Robson, 1992). Rather and in contrast, the lack of precision and calculative sophistication can be seen as productive, as an imprecise and subjective judgement in enabling activities, such as cost-efficient screening, entrepreneurial self-management, and integration. This could explain why the criticisms focusing on the imprecision, subjectivity, and simplification of risk have not impeded the popularity of risk matrices.

Inter-disciplinary teams offer the possibility of increased intellectual skills and different perspectives, which can increase the number of suggestions and solutions. Different disciplines have different understandings of risks and different competences (Aven, 2012), and a joint effort would thus result in decisions of higher quality (Janis, 1989; Weick, Sutcliffe, and Obstfeld, 1999). However, discussion of assumptions made, risks, and different solutions for their mitigation takes time, and time is a critical factor. In project management, the main focus is on progress and completion of the project within the planned budget and time frame. Controlling the schedule and the cost are two interrelated objectives in any project, as well as controlling risks and the trade-off between costs and safety (Reason, 1997; Aven, 2012).

The project teams consisted of members from different disciplines. During a project, there were many arenas, in which interdisciplinary groups came together and focused on the project's status and future plans. However, the focus in these meetings seemed to be to get all actors aligned, by raising confidence in each other as committed and capable project partners. In an inter-organizational project collaboration, it is important to ensure that all actor groups have understood the scope of the project and the work to be done. They need to agree on the objectives and challenges in the project. Furthermore, the actor groups must choose to prioritize the project and demonstrate their ability and obligation. However, in ensuring risk management, these rationales should be balanced with an open-minded and critical attitude. In the studied project, attempts were observed, in fact, to *avoid* questions and discussions, in order to avoid prolonged meetings. This happened so many times among both the operator and the TOC that it could be labelled standardized practice. In preparing for inter-organizational meetings, the focus was on delivering information in ways that would reduce the chance of questions and discussions. Prolonged meetings and follow-up activities, such as providing underlying information, carrying out more tests and so forth, were seen as potentially delaying the project and increasing the costs. This practice results in a reduced space for and missed opportunities for discussions of risks.

Projects in this context are very complex, and actors need to be reminded of the different project objectives, their challenges, and the status. The risk matrix provides an opportunity to aggregate information and integrate the different objectives, challenges, and status, giving an instant overview. In such projects, many simultaneous activities are taking place and many risks that are defined

within different relevant disciplines are mitigated. Communicating risk to higher-level management within the organization and to inter-organizational partners requires filtering and prioritizing, to avoid information overload and the use of extra time. In risk management, however, background information and details can be very important. Therefore, reluctance to simplify interpretations and interdisciplinary input in the discussions are regarded as highly relevant, to ensure reliability (Weick, Sutcliffe, and Obstfeld, 1999). Standardized risk matrix practices imply complexity reduction, where the multiple qualities and contextual specificities of the depicted social processes disappear, as they are reduced to the spatial relation of 'dots' in the matrix. As a result, the complexity of the risk issues is often poorly understood; the social processes become simplified, and issues seem to be more manageable.

Many precautionary activities also took place in the studied project. Practices, involving diverse teams in different committees, meetings, and reviews, were institutionalized and integrated into procedures. Scepticism regarding several issues, a trait identified in high reliability organizations (ibid.), was often given voice in the studied project. Questions were raised, such as 'Are sufficient precautions in place?' and 'Do the people involved sufficiently understand their tasks?' Such scepticism was especially directed towards subcontractors but also from time to time towards the collaboration between the operator and the TOC. These concerns sometimes resulted in the operator or the TOC initiating double checks. When scepticism increased, the trust decreased, and attempts had to be made to increase the trust to a level where the collaboration could once again progress smoothly. When concerns were raised in team conversations, personal hunches and intuition tended to be drawn upon. High reliability theory holds that intuition should not be disregarded, as it is necessary in order to increase the state of mindfulness. The project managers, in both the operator organization and the TOC, challenged project members regarding their gut feeling and whether they felt comfortable. In such cases, paying attention to body signals was regarded as important.

Conclusion

Do these findings imply that the organizations involved in this project are 'mindless' organizations, with the ERM process acting as an autopilot? Not at all. This particular project went well, and the installations were put in place without any injuries to personnel or other significant unwanted incidents or accidents. The records of accomplishment of the involved plants are also good, so it would be wrong to assume that the success was down to pure luck. In fact, the organizations involved have a high international reputation for their reliability.

On the other hand, this chapter describes several examples of formal and informal standardization practices that result in tensions affecting the complex, inter-organizational project collaboration that potentially could decrease the quality of risk management.

First, it relates to the need for simplification. Through the collaboration agreement, standardized layouts for the monthly report, the 'decision gate support

package', and the risk matrix are used as a means to reduce the complexity and level of detail and information to communicate. At the same time, 'the devil lies in the detail': certain details are of crucial importance in risk management.

Second, there is a need for alignment of divergent, inter-disciplinary team members and actor groups in the project. However, divergent, inter-disciplinary teams, committees, and actor groups are not primarily established to become aligned. On the contrary, they are meant to assess risks, problems, and alternatives from different perspectives and to discuss them in order to identify more risks and alternatives for mitigation and to enhance quality in decisions. To ensure an efficient, smooth collaboration, everybody had to be in agreement on the project's main objectives and challenges. Alignment facilitated the collaboration and increased the trust in each other as competent, reliable project partners. By making sure that the project had collaborating partners on board, aligned over project goals, risks, and securing good progress through the different project phases, the project manager and his team mitigated two of the major risks in all projects: cost and schedule.

Third, in the hierarchy of actors, ranging from the technical operators/suppliers to the operators and owners, power relations may dominate and overrule conflicts of interest. In the process of simplification and alignment, these power relations amplify the risk of overlooking 'the devil embedded in the detail'. Open and free discussions of assumptions and implications of risk issues, from different perspectives, and their mitigation could be missed.

We may therefore conclude with a paradox: standardizing risk assessment and communicating risk through a standardized and decontextualized format could, in fact, increase the risk.

Notes

1 See examples, such as: AS/NZS (2004); COSO (2004b); U.S. Department of Defense (2006); Institute of Management Accountants (2007); International Risk Governance Council (2005); ISO (2009); integrative risk and project management technologies (e.g. Project Information Management System PIMS; MITRE risk management toolkit; SAP-GRC) and consultants (e.g. Clarke and Varma, 1999; Curtis and Carey, 2012).
2 The coded data is organized as follows: The first part of the code refers to where the data originate from (D: document, I: interview, or M: meeting observation). The second part indicates whether it is collected in a single company (operator or TOC) or in an inter-organizational setting. The last part of the code is a serial number; documents, interviews, and meeting observations are numbered from 1 onwards.

References

AS/NZS (2004). *4360 Risk management*. Sydney: Standards Australia/Wellington: Standards New Zealand.

Aven, T. (2011). Selective critique of risk assessments with recommendations for improving methodology and practice. *Safety Science*, 49, pp. 1080–1086.

Aven, T. (2012). *Foundations of risk analysis: A knowledge and decision-oriented perspective*. Chichester: John Wiley & Sons, Ltd.

Ball, D. J. and Watt, J. (2013). Further thoughts on the utility of risk matrices. *Risk Analysis*, 33(11), pp. 2068–2078.

Boholm, A. (2010). On the organizational practice of expert-based risk management. *Risk Management*, 12(4), pp. 235–255.

Bourrier, M. (1996). Organizing maintenance work at two nuclear power plants. *Journal of Contingency and Crisis Management*, 4, pp. 104–112.

Bourrier, M. (2005). An interview with Karlene Roberts. *European Management Journal*, 23(1), pp. 93–97.

Brünger, C. (2011). *Nutzenkonsistente Risikopriorisierung. Die Risk-Map in Kontextrelationaler Entscheidungen*. Wiesbaden: Gabler/Springer.

Busch, L. (2011). *Standards: Recipes for reality*. Cambridge, MA: MIT Press.

Bygballe, L. E., Swärd, A. R., and Vaagaasar, A. L. (2016). Coordinating in construction projects and the emergence of synchronized readiness. *International Journal of Project Management*, 34, pp. 1479–1492.

Cicmil, S. and Marchall, D. (2005). Insights into collaboration at the project level: Complexity, social interaction and procurement mechanisms. *Building Research and Information*, 33(6), pp. 323–332.

Clarke, C. J. and Varma, S. (1999). Strategic risk management: The new competitive edge. *Long Range Planning*, 32(4), pp. 414–424.

Collier, P. M. (2009). *Fundamentals of risk management for accountants and managers. Tools and techniques*. Oxford: Elsevier/CIMA Publishing.

Collier, P. M., Berry, A. J., and Burke, G. T. (2007). *Risk and management accounting: Best practice guidelines for enterprise-wide internal control procedures*. Oxford: Elsevier/CIMA Publishing.

Cooper, R. (1992). Formal organization as representation: Remote control, displacement and abbreviation. In M. D. Hughes and M. Reed, eds. *Rethinking organization: New directions in organization theory and analysis*. London: Sage.

COSO (Committee of the Sponsoring Organizations of the Treadway Commission) (2004a). Enterprise risk management – Integrated framework: Executive summary framework. Available at: www.coso.org.

COSO (Committee of the Sponsoring Organizations of the Treadway Commission) (2004b). Enterprise risk management – Integrated framework: Application techniques. Available at: www.coso.org.

Cox, L. A. (2008). What's wrong with risk matrices? *Risk Analysis*, 28(2), pp. 497–512.

Cox, L. A., Babayev, D., and Huber, W. (2005). Some limitations of qualitative risk rating systems. *Risk Analysis*, 27(2), pp. 439–445.

Curtis, P. and Carey, M. (2012). *Risk assessment in practice*. London: Deloitte and Touche LLP, commissioned by COSO.

Goerlandt, F. and Reniers, G. (2016). On the assessment of uncertainty in risk diagrams. *Safety Science*, 84, pp. 67–77.

Ika, L. A. and Donnelly, J. (2015). Success conditions for international development capacity building projects. *International Journal of Project Management*, 35(1), pp. 44–63.

IMA (Institute of Management Accountants). (2007). *Enterprise risk management: Tools and techniques for effective implementation*. Montvale, NJ: Institute of Management Accountants.

International Risk Governance Council (2005). Towards an integrative approach. IRGC White Paper No. 1 Risk governance .Geneva: IRGC. [online]. Available at: http://irgc.org/wp-content/uploads/2012/04/IRGC_WP_No_1_Risk_Governance__reprinted_version_3.pdf (accessed 30 September 2013).

ISO (2009). *ISO/IEC 31010:2009. Risk management: Risk assessment techniques*. Geneva: International Organization for Standardization.

Janis, L. I. (1989). *Crucial decisions: Leadership in policy making and crisis management*. New York: Simon & Schuster.

Jordan, S., Jørgensen, L., and Mitterhofer, H. (2013). Performing risk and the project: Risk maps as mediating instruments. *Management Accounting Research*, 24, pp. 156–174.

Jordan S., Mitterhofer, H., and Jørgensen, L. (2018). The interdiscursive appeal of risk matrices: Collective symbols, flexibility normalism and the interplay of 'risk' and 'uncertainty'. *Accounting, Organization and Society*, 67 (May), pp. 34–55.

Jørgensen, L. (2017). The appeal, use and effects of the risk matrix. Risk communication in an inter-organization project. PhD thesis, Faculty of Social Science, University of Stavanger, no. 353.

Milch, V. and Laumann, K. (2016). Interorganizational complexity and organizational accident risk: A literature review. *Safety Science*, 82, pp. 9–17.

Miller, P. and O'Leary, T. (2007). Mediating instruments and making markets: Capital budgeting, science and the economy. *Accounting, Organizations and Society*, 32(7/8), pp. 701–734.

Mok, K. Y. and Shen, G. Q. (2015). Stakeholder management studies in mega construct projects: A review and further directions. *Journal of Project Management*, 33(2), pp. 446–457.

Pentland, B. T. (1993). Getting comfortable with the numbers: Auditing and the micro production of macro order. *Accounting, Organizations and Society*, 18(7–8), pp. 605–620.

Pickering, A. and Cowley, S. (2010). Risk matrices: Implied accuracy and false assumptions. *Journal of Health and Safety Research and Practice*, 2(1), pp. 9–16.

Power, M. (1997). *The audit society: Rituals of verification*. Oxford: Oxford University Press.

Power, M. (2003). Auditing and the production of legitimacy. *Accounting, Organizations and Society*, 28(4), pp. 379–394.

Power, M. (2004). *The risk management of everything. Rethinking the politics of uncertainty*. London: Demos.

Power, M. (2007). *Organized uncertainty: Designing a world of risk management*. Oxford: Oxford University Press.

Quattrone, P. (2009). Books to be practiced: Memory, the power of the visual, and the success of accounting. *Accounting, Organization and Society*, 34, pp. 85–118.

Ravishankar, M. N., Pan, S. L., and Leidner, D. E. (2011). Examining the strategic alignment and implementation success of a KMS: A subculture-based multilevel analysis. *Information System Research*, 22(1), pp. 39–59.

Reason, J. (1997). *Managing the risks of organizational accident*. Farnham: Ashgate.

Robson, K. (1992). Accounting numbers as "inscriptions": Action at a distance and the development of accounting. *Accounting, Organization and Society*, 17, pp. 685–708.

Schein, E. H. (1985). *Organizational culture and leadership*. San Francisco: Jossey-Bass.

Schrader-Frechette, K. S. (1991). *Risk and rationality: Philosophical foundations for populist reforms*. Berkeley, CA: University of California Press.

Tantalo, C. and Priem, R. L. (2016). Value creation through stakeholder synergy. *Strategic Management Journal*, 37(2), pp. 314–329.

U.S. Department of Defense (2006). Risk management guide for DOD acquisitions. Washington, DC: US Department of Defense. [online]. Available at: www.acq.osd.mill/se/doc/2006-RM-Guide-4Aug06-final-version.pdf (accessed 30 September 2013).

Ward, S. and Chapman, C. (2003). Transforming project risk management into project uncertainty management. *International Journal of Project Management*, 21, pp. 97–105.

Weick, K. E. and Roberts, K. H. (1993). Collective mind in organizations: Heedful interrelating on flight decks. *Administrative Science Quarterly*, 38, pp. 357–381.

Weick, K. E., Sutcliffe, K. M., and Obstfeld, D. (1999). Organizing for high reliability: Processes of collective mindfulness. *Research in Organizational Behavior*, 21, pp. 81–123.

Woods, M. (2009). A contingency theory perspective on the risk management control system within Birmingham City Council. *Management Accounting Research*, 20, pp. 69–81.

Zuboff, S. (1988). *In the age of the smart machine: The future of work and power*. New York: Basic Books.

Part IV

Standardization of risk in business activity

12 Standardization, risk dispersion, and trading

Grahame F. Thompson

Introduction

This chapter examines several features of the financial system that involve issues of standardization and what is termed 'risk dispersion'. Standardization as a mechanism of risk dispersion operates in many areas of social life, and these are raised here before moving on to the specifics of the commercial and financial system. An early example is illustrated in Figure 12.1: a bond from the Dutch East India Company (Vereenigde Oostindische Compagnie), dating from November 7, 1622, for the amount of 2,400 florins, written out and authorized in Middelburg but signed in Amsterdam in the name of Jacop van Necq.

Risk dispersion is not to be confused with risk aversion – though these may be related, as will become clear later. To put it simply, risk dispersion refers to the way certain technologies for dealing with risk have the effect of dispersing it rather than eliminating it. To scatter risk implies both to redistribute it so that no one party bears the full burden of it and – at the systemic level – to reduce its overall impact so that the system as a whole becomes more robust.

There are several tactics of dispersion in dealing with risk. One of these is 'hedging'. Hedging is a formal strategy of offloading risk to third parties, by buying and selling securities with differing terms and maturities to minimize exposure to the owned but vulnerable asset.[1] Then there is the policy of 'insurance', designed to spread the risk associated with the possibility of unexpected or unforeseen events in the future among the insured parties, aggregating that exposure through contractual arrangements in the present. But the situations discussed later in this chapter address this by means of standardization. If a standard is established and adhered to by everyone, this is a way of lowering the risks to all, or of lowering the risks associated with going it alone. Standards provide a collective pre-response to what could otherwise turn out to be risky situations. If a standard is adhered to, parties know where they are, so to speak – they commit ex-ante to increase the level of ex-post certainty. Of course, standards do other things as well. They obviously facilitate commerce and provide mechanisms for accountability. But their role in relationship to risk has so far been underestimated. And their role in facilitating the governance of risk via its

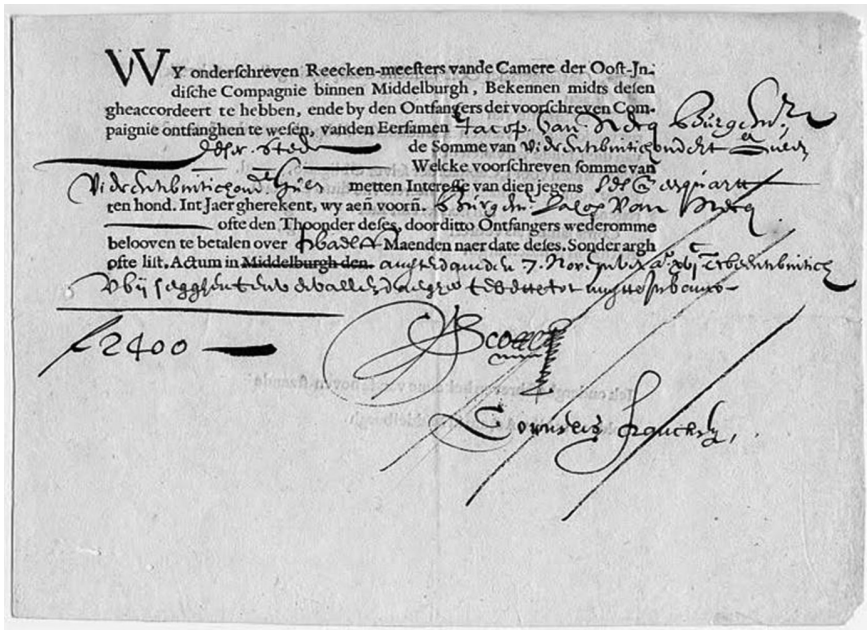

Figure 12.1 Early example of a financial security.
Source: www.tschoepe.de/auktion51/auktion51.htm

dispersion is further neglected.[2] Furthermore, the context for this analysis is that risk and standardization considered in this way are closely related to societal security, so this connection also needs to be discussed.

The substantive analysis of this chapter thus opens with a discussion of security in its various guises. Then it moves directly into a consideration of standards and the process of standardization. This raises several general issues associated with the characteristics of standards, which are not all directly related to the following discussion of the types of standardization to be found in the commercial world and the financial system. But they serve to establish a framework for that subsequent analysis and deal with issues that typify all processes of standardization. Thus, this section of the chapter provides a discussion of matters that have a wider significance for the analysis of all standards. The way these various considerations impact upon the commercial world and financial arrangements is weaved into the discussion as the analysis proceeds, but near the end a rather specific sense of standardization is investigated in the context of algorithmic trading in particular. This involves recognizing that standardization can be the consequence of the informal adoption of a codified social norm rather than the result of a formal process of overt construction and implementation.

Financial security and societal security

If standardization effectively disperses risk and thereby reduces its potential operational impact, then various aspects of security are enhanced. So, we need to consider the notion of security more closely, and – for the purposes of this chapter in particular – that of financial security.

A financial security (an early example of which is shown in Figure 12.1) is a negotiable financial instrument, like a share certificate (a common stock), a debt obligation (bond, debenture, currency, repo), or a derivative asset (futures, forwards, options, and swaps). Financial securities of this type are often collectively referred to as 'assets'. But security is also a kind of 'state of mind': the feeling that you are not worried about your income being enough to cover your expenses in the foreseeable future. The relationship between 'financial instruments' and 'financial security' in an emotional sense is, of course, the subject of a huge amount of commentary, highly variable, and fiendishly complex. In addition, there is the matter of the overall financial security of the system as a whole and its relationship to societal security more generally. A convenient discussion of these matters in the context of contemporary financial developments can be found in de Goede (2010) and Boy (2015a, 2015b, 2015c).

For the purposes of this chapter, we define financial security in terms of a concern not to lose money: the aim of financial security is not to make a financial loss.[3] This is distinct from other forms of security, which have different objects of investigation: national security is concerned to maintain the sovereign integrity of a territory or jurisdiction; energy security to maintain energy supply; environmental security to preserve or sustain environmental reproduction; welfare or social security to maintain a population fit for work (or military service), etc. Taken together, all these forms and objects of analysis amount to an overall concern with 'societal security' as a whole. Indeed, when considered together, these forms of security may be refashioning the nature of society as a whole rather than just being added into the configuration of an already existing social order.

Of course, the content of a concern not to lose money differs with respect to say, the providers of finance and the consumers of the services those providers offer. Thus, financial security might have different implications for these two groups (among others, e.g. the government). Indeed, these two parties might have quite opposite views. What offers financial institutions security might be at the expense of the security of consumers of financial services. Financial institutions are out to make money – and their ultimate security depends on their ability to competitively produce financial returns. This they do by 'selling' their services to consumers (wholesale and retail) – providing them with funds and expertise. And the experience over recent years is that financial institutions have often been less than honest in their dealings with their customers: fraudulently selling them products or manipulating markets so as to maximize their own profits at the expense of the consumers and society at large (Thompson, 2017c). What is more, these misdemeanours by financial institutions – in the aggregate – were

partly to blame for the 2007/08 financial crisis, which thereby undermined its security profile. Finance is increasingly at the heart of all economic conduct and affects all social relations (so-called 'financialization'; Martin, 2002; van der Zwan, 2014), so what happens to financial security is central to societal security.

But it is important to note that the 'play' of financial security, as that between providers and consumers of financial services, is not necessarily a zero-sum game – what providers gain, receivers necessarily lose. Indeed, the idea would be that the provision of financial services adds to a positive sum game – both parties win and gain something through the exchange involved in funding opportunities (a variant of the 'mutual gains from trade' argument – financial security overall is enhanced). However, the 2007/08 financial crises would surely have seen a case of a negative sum outcome – both parties lost. In the big picture of the financial meltdown, losses by consumers were paralleled by losses in those financial institutions involved in triggering the crisis. And financial security of the system overall fragmented. This could have been temporary but, in fact, the uncertainty generated has persisted and the consequences of an aggregated negative outcome continue as overall societal security falters. We are all worse off as a result.

As we will see, the way risk is woven into the analysis is variable. Although risk is mostly viewed negatively, as something to be avoided, in the financial system in particular, it also has a positive connotation: It provides opportunities to make money. Indeed, in many areas of financial activity, it is risk itself that is the tradable instrument: 'Volatility indexes' are a tradable commodity. And more generally, risk is often thought of positively as a means for social advance and as a stimulus to innovation (so-called 'entrepreneurialism').

However, like any analysis involving risk, mechanisms designed to address it (whether hedging, insurance, or, as here, standardization) end up reconstructing what the particular risks involved are. So, any approach to risk reconstructs its object. There is no one thing 'out there' called risk, which is then addressed by these tactics or attitudes. Rather, risk is only constituted relative to the mechanisms designed to deal with it. Effectively, this means there are always *risks*, never risk in the singular. So, as we will see, dispersion actually constitutes a particular kind of risky situation in the various contexts in which it is examined, as well as being a response to those situations. Several concrete examples of this will be discussed later.

Sorting out standards

Standards seem to be everywhere (Brunsson, 2000; Büthe and Mattli, 2010; Ponte, Gibbon, and Vestergaard, 2011). They have become a ubiquitous feature of our modernity. One way of classifying *de jure* standards is shown in Figure 12.2. Important for the standard setting process is who is responsible for initiating and policing the standard and for what reason standards are established. This can involve either the public authorities or private interests. In addition, the issue of whether these are scientific or ethical in character is another fundamental distinction

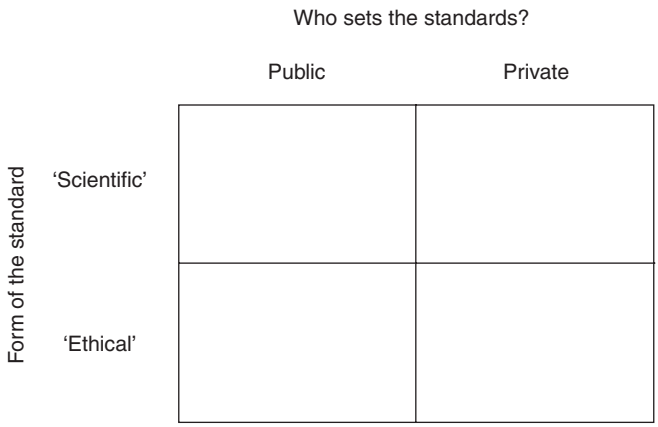

Figure 12.2 Sorting out standards.

(the 'ethical' dimension might be expanded to include the 'social' as a type of standard). So, we have a basic matrix, as shown in Figure 12.2, into which we could place most standards. I use these distinctions below to further develop the categorization of standards.

As we will see later, the sharp distinctions outlined in this matrix become muddied in any practical setting: There is no stark distinction between the public and private realm, for instance, and scientific and ethical/social norms are inevitably intertwined (see Virta, Chapter 8, in this volume). But the matrix provides an analytical starting point for considering standard formation and implementation. It is not a 'model' in the conventional sense but a framework for investigation and a means for providing a 'thick description' of standard setting (Geertz, 1973): one that is theoretically modest but illustratively ambitious.

Another important aspect of sorting out standards is whether they appear as 'rules' or as 'principles'. Are standards operationalized through rules or principles? Or are they perhaps 'gap fillers', acting in some way to articulate rules with principles?

If they are *based upon principles*, standards become something to which agents 'aspire' only. An example of this in the commercial world might be ISO 2600. This is a standard for corporate social responsibility, developed by the International Standards Office in Geneva, one which is only voluntarily agreed to by companies if they wish to be recognized by the ISO and has no mandatory standing (www.iso.org/news/2010/11/Ref1378.html). ISO 26000 only provides guidance on what social responsibility is and how organizations can operate in a socially responsible manner.

If they are *based upon rules*, however, they need to be 'obeyed', so certification becomes a key governance technique. An example of this from within the same ISO organization is the ISO 9000 family of production quality standards, which have effectively become mandatory for companies if they want to be recognized as

viable and reliable commercial partners and trade internationally (www.iso.org/iso-9001-quality-management.html). Third-party certification bodies provide independent confirmation that organizations meet the requirements of ISO 9000. Any accredited certification body audits an organization's management system and issues a certificate, confirming that it conforms to the requirements of the standard.

As 'gap fillers', standards would be more difficult to clearly identify, but an example could be the *issuance of guidelines*. These are not exactly rules or principles but indicators of best practice procedures that somehow fit in between the other two, offering a way of supplementing or modifying their respective strengths and weaknesses through a different performative arrangement.

Of course, all of this acutely raises issues about policing and enforcement. Whether standards are considered as principles or rules (or guidelines), there is an obvious problem of oversight, inspection, and implementation, features associated with all standards. Thus, a key question is what is happening to standards functioning as principles or as rules? In fact, these are not polar opposites, as might be thought from the discussion so far because – in many instances – it is not easy to distinguish between principles and rules. This is illustrated by the ISO case just described, since the ISO is a private body, with no ultimate sanctioning powers that can forcefully implement its standards. So, the principles vs rules distinction in this case is one of degree.

In economic terms, standards are public goods or merit goods. A pure public good displays the characteristics of non-excludability and non-discrimination in consumption: traditional examples are law, defence, environmental protection. Merit goods, on the other hand, while demonstrating some of these characteristics, could in principle be provided discriminately, though it is generally thought best not to do so, to maximize beneficial uptake: examples would be education, health provision, some welfare services. Once established and adopted, pure public goods are something from which everybody benefits – the 'cost' of one extra consumer is zero and it is difficult to exclude anyone from using the standard (indeed, there is an incentive to recruit more users, since this expands their effectiveness – risks are dispersed more widely).

But one of the features of standards considered as public goods is something that reintroduces the matrix of 'sorting out standards' pointed out above. There is no necessity for public goods to be provided by the public authorities – as illustrated by the ISO case. Indeed, one of the major contentious features of the contemporary standard setting process is the way standards are increasingly being promoted by private bodies. In many ways, the state is withdrawing from the standard setting process with the emergence of private organizations, claiming and exercising a 'public power' in setting standards.

The shadow of hierarchy and the shadow of the market

There are several modalities operating in the context of private and public standard setting, which are discussed here under the headings, 'the shadow of the hierarchy' and 'the shadow of the market' (Thompson, 2003). Although

there is a certain autonomy for standard setting processes, there is never a complete escape from either state sponsorship and oversight, on the one hand, or market-driven competitive interests and calculations, on the other. The state and the market thus appear as a backdrop context for standard setting, providing a framework environment for the operationalization of any regime of standardization. The actual day-to-day processes of standard setting and their enforcement thus exist in the shadows of either of these two overall societal mechanisms of coordination. Any standard setting process cannot completely escape considerations and influences arising from elsewhere: from issues ultimately associated with state or market relationships. These I term 'the shadow of hierarchy' or 'the shadow of the market', respectively.

Most private-body standard setting still operates under 'the shadow of hierarchy' because it is ultimately shaped by, and dependent upon, legal mechanisms for its characterization and enforcement. But the extent of this is vitally dependent on quite how and under what circumstances the public authorities have authorized and sanctioned the shift of powers to private interests. If this shift takes the form of a *delegated* capacity, it quite easily can be reversed by the public authorities. Under these conditions, private standard setting exists for a limited set of circumstances and is implicitly only granted for a limited period. A delegated capacity is strongly articulated, with hierarchy as a result.

Less strongly articulated are *devolved* powers to set standards. Devolution represents a granting of powers to a separate body that displays more autonomy and runs more deeply than does delegation. Devolved powers grant substantial capacities of autonomy, ones not easy to reverse or regain should the desire emerge to do so. However, even with devolution, a granting authority like a state retains ultimate capacity to reverse the process and recoup the powers so devolved, if it really wants to and has the will to proceed. The ISO referred to above is a case of devolved powers, I would suggest. Interestingly, perhaps, this is part of a 'double movement': states devolve powers to bodies like the ISO, which in turn contract the state back in as an authorized certificating agent – the British Standard Office, for instance, 'polices' ISO 9000 standards at the domestic level.

However, the 'shadow of the market' falls more heavily on standard setting, if the state has either *abandoned* the capacity to initiate and control standard setting or that capacity has simply been *seized or captured* by some other party. Here, private interests prevail more readily, and the shadow of the market operates more forcefully to determine the characteristics of standards. We live in a period in which the state has progressively abandoned many aspects of its traditional fields of operation. Often, the constraints on the state are argued to be so great that it can no longer afford to support these activities and it operates a 'politics of abandonment' with respect to them: leaving those so affected to fend for themselves in whatever way they can. And this is sometimes accompanied by an argument that the state has failed so badly and lost competences so widely that the only answer is to hand this capacity over to private agencies. In whatever way, however, the shadow of hierarchy recedes, and the shadow of the market grows.

And, as a result, this process is even more obvious in the case of private interests just seizing new areas of capacity to work in their own interests. The market has simply captured many areas of social life, as its status as the only efficient mechanism for social governance has advanced. Standard setting under these circumstances becomes almost a purely private matter. In Anglo-American jurisdictional contexts, the setting of accounting standards for corporate entities would be a case in point.

Thus, we have complex relationships between standards, rules, and principles and between the shadow of hierarchy and the shadow of the market in the determination of standards. But there is another dimension to standards that needs consideration, in relationship to their robustness, which is termed here the 'texture' of standards.

The texture of standards

The matter of the texture of standards relates to issues of whether they are 'thin' or 'thick' in character. Thin standards are loose, flexible, all-embracing attempts to cater for everyone. Thick standards are tight and focused, more like rules than principles. Thin standards allow discretion and judgement in the process of compliance. Thick standards demand close supervision and proper certification as part of compliance (see Lindøe and Baram, Chapter 14, in this volume).

One area where this distinction becomes particularly focused is in the context of 'globalization'. Are all international standards necessarily thin? As the standardization process goes global, with the intention of including as many different parties as possible, to give the standard its global credibility, some flexibility and looseness seem inevitable – even for rules; hence, the standard would be *fragile* (Tate, 2001; Teubner, 2001, 2011). The argument here is that legal and other standards that are devised to harmonize activities across national jurisdictions just result in new disruptions, new perturbations, and new differences that undermine the original intention. Thus, fragility would seem to be a consequence of thinness. If discretion and judgement become a built-in feature for all standards, what does this say about their 'failure'? Is failure in some sense an inevitable feature of standards, just like every other form of societal governance (Malpas and Wickham, 1995)? In fact, there is some evidence that commercial standards are more supra-nationally regional in character than they are global, with a strong element of continued national determination (Thompson, 2005). But the point is that while ultimate 'failure' would seem to be the destiny of all standard setting processes, that failure needs to be registered against original (often limited) intentions not against some ideal of a total and universal comprehensive 'global' standard (which would probably be unachievable anyway, see below).

Related to this is a further aspect of standards: They foster 'sameness' over 'difference'. If thick standards were ever to be completely and successfully devised and implemented, they would lead to a homogenization and harmonization of activity and behaviour. But it is differences that encourage innovation. Any ecological system thrives on difference: this is what gives it its dynamism.

Pluralism encourages heterogeneity, just the opposite of the normalizing dynamic of standardization. Thus, what are we losing as the attempts at standardization sweep the social world? I return to this in the concluding comments.

Consequences: 'top down' vs 'bottom up' standardization?

Where should the locus or the direction of standardization be situated? The above discussion has indicated the inherent difficulties of establishing effective and sustainable standards, particularly in international settings. However, this has not prevented the continued commitment to such standard setting among policy-makers and regulators in these areas. Most of these take the form of grand initiatives from above, devised by international governance bodies like the UN (The Global Compact), the BIS (bank capital adequacy ratios, known as the 'Basel rules'), the International Monetary Fund, and many bodies dealing with functional areas of commerce like accounting (international accounting standards), the legal apparatuses and tax authorities (the Organisation for Economic Co-operation and Development), or labour standards (the International Labour Organization). All these initiatives are directed at providing security and stability for those involved. But they look to a comprehensive coverage, with various attempts at enforced compliance – difficult though this has proved, given the ambiguous status of standards under international law and the fact that many of these initiatives arise from what are actually 'private-bodies-claiming-a-public-power' (see above).

But the international commercial system is best viewed as a complex system, with multiple feedback mechanisms and looped interconnections. Under these circumstances, instead of elaborate thick unitary standards originating from above, the need is for simpler regimes of decentralized and thin standards, geared up to preparedness and resilience in the face of the particularities of complexity and the seeming inevitability of failure (as detailed in respect to various functional areas in Thompson (2015a, Chapter 6) – see also Lentzos and Rose (2009)). A robust regulatory/standardization system should pragmatically prepare for failure by providing multiple bottom-up initiatives, loosely configured together as far as possible but flexible enough to withstand complete destruction as circumstances and conditions change, that is, an 'ecology' of varied and dispersed standards rather than a singular centralized arrangement. Standards would emerge here as a type of codified social norm. A particular example of this will be discussed later, in connection to algorithmic trading.

Standards as a (neoliberal) technology of governance?

Standards could be a way of 'governing at a distance'. If a standard is set by a body, and those adopting the standard organize its implementation themselves, following the standard as suits their purpose, they are in effect 'governing themselves'. This could strongly be the case in the context of standards considered as principles. The standard setting 'regulator' does not intervene directly to administer

the standard on a day-to-day basis but pushes this off to those who adopt it and who thereby 'discipline' themselves.

One important aspect of neoliberalism is that it fosters this kind of a governance regime (Rose, 2018). It governs not just in the name of freedom but also *through* freedom – cultivating a sense of freedom by those subjected to its operation ('We are free to adopt this standard if we wish to', etc.). Standards are thereby rendered a governmental technique for shaping expectations, engendering preparedness, and anticipating the future. And this technology of governance is so prevalent that standardization might be considered one of the supreme examples of such contemporary neoliberal governance. We should remember, however, that standardization has a very long history. UK financial institutions set credit rating standards in the late nineteenth and early twentieth centuries, Norway and the UK captured the setting of marine classification standards early in the twentieth century, and the Federal Aviation Administration in the United States effectively did the same for international air transport in the 1960s. Thus, there is nothing to necessarily link globalization or neoliberalism directly to standardization as such but only to the particular characteristic of it as a 'technology of the self'. Governing through standards is so widespread that it has become part of the 'taken-for-grantedness' of the everyday and an almost unnoticed part of the popular political imagination. In so doing, it constitutes or engenders a certain subjectivity, organized around performance, measured against benchmarks, norms, standards, etc. Thus, it cultivates a particular type of *personae*: all agents are increasingly and continuously monitored by, assessed in the name of, scrutinized by, rewarded and paid as a consequence of, congratulated and praised in the name of and, it must be said, energized and motivated by performance measures, indicators, and standards. And this not only applies to individual agents but also to corporate agents and to whole countries: they are continually ranked and judged – rendered into a common standard for comparison – and subject to a performance monitoring regime that hands out rewards and punishments, dependent upon their 'competitiveness', 'efficiency', 'success', etc. (Ponte, Gibbon, and Vestergaard, 2011).

What have been provided in this section are some rather general considerations of the consequences of the processes of standardization: how they might, in part at least, be reorganizing the social terrain in a period of neoliberal governance. The next section moves into the concrete case of the financial system. It will illustrate some, but not all, of the features discussed in this section. It will pick up on themes explored above, but in doing so in an empirical setting, it will have to be selective in how it tackles and incorporates these. This is an inevitable consequence of the way rather abstract concerns can become embedded into what was characterized above as a 'thick description'.

Financial markets and trading

The rationale for a safe modern social order is to be found in the reciprocal relationships between wealth and security. That is why both of these – security and

wealth – became the twin objects of 'the interests of states', as the formation of national state territories consolidated (in Europe in the first instance) in the latter part of the seventeenth and early part of the eighteenth centuries (Walter, 2011). Ever since, the fate of the state has been closely tied to the performance of the economy. But both wealth and security pose their own dimensions of risk and standardization.

In the case of modern financial markets, as key features of the economic system, these are moving from 'fixed role' to 'switch role' characteristics (Castelle *et al.,* 2016). Fixed role is typified by the separation of sellers and buyers into different categories of agent: the provider of a financial asset is different from the purchaser of that asset. Switch-role markets are where the seller and the buyer are the same agent – they switch roles and operate in the same market to exploit small differences in offer and bid prices of assets. These markets are driven by ultra-high-speed algorithmic trading and a 'dealing' culture. The foremost algorithm deployed here is the 'matching algorithm' – this matches buyers and sellers (in nanoseconds) in an almost continuous trading environment.

One consequence of this is that traditional 'scopic'-based trading is on the decline (Figure 12.3). Traditionally, financial traders would sit at desks, with a series of monitors in front of them displaying information on market conditions and trends in individual company share prices, etc. Traders then accessed this information via a single keyboard. They would make their own trades based upon this scopic information. But this type of activity is being displaced by algorithmic

Figure 12.3 A 'scopic' trading environment (the trading room at Sydbank in Aabenraa, Denmark).

trading (80 per cent of US equity trading is now done automatically with these methods – and this is increasing in respect to bond trading and Forex trading but still to a lesser extent, see Thompson (2017a)).

What are trading algorithms looking for? There are two types of activity; see Thompson (2017a) for details. Either they are looking for small differences in offer and bid prices for securities in the same market where they think a profitable trade can be made – that is, where there is an 'expectation' that the offer/bid price is somehow 'wrong', so that the security can be subsequently sold on at a higher price (itself in milliseconds: the companies involved in this business do not want to hold large – indeed any – inventories of securities for more than a few moments), or they are seeking different prices of the same securities in different market contexts, so they can profitably trade between the one and the other (say, between different jurisdictions or currencies – classic arbitrage business). So, the role of the matching algorithm is to bring all these heterogeneous securities into some commensurate standard framework to make trading of them possible – often rendered into an index, which itself is the tradable vehicle (so-called 'exchange traded funds', ETF). A further point to note is that a lot of this involves prediction. Based upon probability calculations derived from macro-market and firm-based information – which itself now increasingly appears in an online standardized computer-readable form – the algorithm makes a prediction as to the 'proper' price, and trades accordingly. This means high frequency trading algorithms algorithms have to be anticipatory: proactive rather than reactive, with the latter being the case for the fast-disappearing scopic mode of coordination just discussed. High frequency trading is future-orientated and thus anticipatory in a risk context (characterized by 'futurity', Palan, 2015).

As suggested above, these kinds of trading strategies are all instances of 'matching' algorithms. The history of matching algorithms began in the 1960s (Gale and Shapley, 1962). In a technical sense, these are referred to as 'deferred acceptance algorithms' (Roth, 2007) and they are deployed in a wide variety of contexts. The recent popularity of such algorithms has much to do with the work of Alvin Roth on market design (Roth, 2015), who, along with Lloyd Shapley, won the Nobel Prize for economics in 2012. The argument is that the use of matching algorithms in more colloquial contemporary settings has much to do with certain aspects of the modern condition that transcend the purely technical character of the algorithm. While these take several forms, they share a common underlying structure – one akin to the matching activities involved with dating sites, for instance. In these cases, each party lists a set of personal characteristics according to a common template, and the dating algorithm compares these, to come up with a compatible match. This is similar to 'profiling' in a traditional security or policing context. A list of supposed characteristics associated with likely criminal or terrorist activity is developed, then any particular individual is compared to these to come up with a matching profile and is thereby rendered a suspect. Thus, there is a certain continuity in the logic of these activities, working across quite diverse sites of societal existence: dating, criminal, and terrorist activity, and financial trading. And while it might be tempting to suggest

that these are newly invigorated because they are easily rendered into an electronic computable algorithmic form, that is, in respect to a technology, what is more important is that they also share a common syndrome: a consequence of perceived anxiety and precariousness: in the case of dating, that we will be left alone without a partner; in the case of criminality/terrorism, that we are vulnerable to theft or violence; and in the case of financial trading, that a profitable opportunity will be missed and picked up by someone else.[4] There seems to be a common logic working across domains here.

What this raises, however, is the fact that matching algorithms of this type have now become a kind of standard technique that is deployed across many different social contexts. However, this may be a new or different kind of standardization to the ones focused upon so far: a surrogate de facto standardization, not one that is the product of any deliberate act to develop it but one that has emerged 'spontaneously', so to speak. We might therefore describe matching algorithms as a 'calculative social norm': they appear in the form of a standard that has not been deliberately fostered by some recognized agency or authority – then implemented and monitored by that authority – but as an instance of a practical 'surface of emergence', with no deliberative centre or single stable institutional location.

Matching, however, is above all a 'conservative', risk-averse trading strategy (Cowen, 2017). It is precautionary in that it does not step outside the ambit of existing relationships and practices: it matches (almost) like with like. It is not innovatory or creative in this respect. So, despite its seemingly radical technical nature, switch-role algorithmic trading is a way in which private economic agents in these markets are ensuring their 'security'. They may not be doing this 'consciously', as it were, but this is the effect of their activity. They always want to ensure the least risk to themselves as possible, despite taking risks in the process of trading. However, from the point of view of the regulatory authorities, this is far from a 'secure' system. It requires constant monitoring and threatens to spin out of control and foster systemic contagion across financial markets. Elsewhere, I have shown how this operates in the concrete contexts of secondary banking, repo-markets, and derivatives contracts (Thompson, 2017b). This illustrates one of the major differences between private security and public security in financial markets: that which may be 'good' for individual private financial institutions is not necessarily 'good' for the financial stability of the system as a whole and societal security beyond.

Conclusion

This chapter has delved into some general matters associated with standards, as well as investigating the particularities of commercial and financial standard setting in several contexts. The main focus in the latter part of the chapter was on the nature of high frequency trading and how a de facto standard seems to have emerged here, associated with the matching algorithm: what was termed a 'calculative social norm'. Such a calculative social norm has the effect of

dealing with the risks associated with calculative practices by dispersing them widely among players in the system. But this is all part of a ubiquitous trend of the 'standardization of everything' in the contemporary world, which raises the question: What don't we have, now that we have standards everywhere? Now that we are ruled and governed by/through standards, what have we lost, and should we regret it? We have become so accustomed to being governed by and through standards that a certain conformity creeps up upon us almost unnoticed, perhaps dulling the ability to innovate – dampening creativity. But it might also make us more resilient and self-responsible. So, like all governmental techniques, standardization is potentially double-edged: it both constrains and enables in various ways. Such is also the nature of societal existence, it might be added. Standardization has ambiguous consequences for security and insecurity, for freedom and control, discipline and liberty. This is its legacy and the dilemmas it presents.

Notes

1 Maturity specifies the length of time left before a security expires and the principal must be repaid. See below for a discussion of different senses of 'security'.
2 There may be a parallel example of 'risk dispersion' operating in the context of the generation of trust via cooperative gaming. The wider the information circulating about cooperation among participants, the more the level of trust increases and the risk of losses to all diminishes (Yamagishi *et al.,* 2005). The level of their collective security is enhanced. I thank Kirsten Voigt Juhl for drawing my attention to this possibility.
3 People often go through long periods of what we might colloquially term 'insecurity': periods of dependency as children, as students, when they are unhealthy, when they are disabled, and when they are old. Conventional economics deals with this problem by expecting people to buy security in financial markets – by saving or by buying insurance or financial securities when necessary. This is one instance where security in our sense abuts security considered in a more colloquial manner.
4 For a discussion of the reaction to 'failure' on the part of algorithms, see Dietvorst, Simmons, and Massey (2015). In the case of dating matching algorithms, this failure has in part to do with the fact that, while these might provide a wider range of possible contacts than one would ordinarily come across in daily life, their record in matching compatibilities, leading to long-term attachments, is no better than ordinary 'random' collisions of the everyday life variety (Finkel *et al.,* 2012).

References

Boy, N. (2015a). *D5.1 Report on the theory of risk as a societal security instrument*. Oslo: PRIO/Brussels: European Commission.

Boy, N. (2015b). *D5.2 Report on the role of financial regulation in the provision of security*. Oslo: PRIO/Brussels: European Commission.

Boy, N. (2015c). *D5.3 Analytical report on the impact of the global financial crisis on societal security*. Oslo: PRIO/Brussels: European Commission.

Brunsson, N. (2000). *A world of standards*. Oxford: Oxford University Press.

Büthe, T. and Mattli, W. (2010). *International standards and standard-setting bodies.* Oxford: Oxford University Press.

Castelle, M., Millo, Y., Beunza, D., and Lubin, D. C. (2016). Where do electronic markets come from? Regulation and the transformation of financial exchanges. *Economy and Society*, 45(2), pp. 166–200.

Cowen, T. (2017). *The complacent class: The self-defeating quest for the American dream*. New York: St Martin's Press.

de Goede, M. (2010). Financial security. In J. P. Burges, ed. *The Routledge handbook of new security studies*. London: Routledge.

Dietvorst, B. J., Simmons, J. P., and Massey, C. (2015). Algorithm aversion: People erroneously avoid algorithms after seeing them err. *Journal of Experimental Psychology*, 144(1), pp. 114–126.

Finkel, E. J., Eastwick, P. W., Karney, B. R., *et al*. (2012). Online dating: A critical analysis from the perspective of psychological science. *Psychological Science in the Public Interest*, 13(1), pp. 3–66.

Gale, D. and Shapley, L. (1962). College admissions and the stability of marriage. *American Mathematical Monthly*, 69, pp. 9–15.

Geertz, C. (1973). Thick description: Toward an interpretive theory of culture. In C. Geertz, *The interpretation of culture: Selected essays.* New York: Basic Books, pp. 3–30.

Lentzos, F. and Rose, N. (2009). Governing insecurity: Contingency planning, protection, resilience. *Economy and Society*, 38(2), pp. 230–254.

Malpas, J. and Wickham, G. (1995). Governance and failure: On the limits of sociology. *The Australian and New Zealand Journal of Sociology*, 31(3), pp. 37–50.

Martin, R. (2002). *Financialization of daily life*. Philadelphia, PA: Temple University Press.

Palan, R. (2015). Futurity, pro-cyclicality and financial crises. *New Political Economy*, 20(3), pp. 367–385.

Ponte, S., Gibbon, P., and Vestergaard, J. (2011). *Governing through standards: Origins, drivers and limitations.* Basingstoke: Palgrave Macmillan.

Rose, N. (2018). Still 'like birds on the wire'? Freedom after neoliberalism. *Economy and Society*, 64(3–4), pp. 303–323.

Roth, A. E. (2007). Deferred acceptance algorithms: History, theory, practice, and open questions. NBER Working Paper No. 1322. Cambridge, MA: NBER, July.

Roth, A. E. (2015). *Who gets what and why: The hidden world of matchmaking and market design.* London: Collins.

Tate, J. (2001). National varieties of standardization. In P. A. Hall and D. Soskice, eds. *Varieties of capitalism: The institutional foundations of comparative advantage*. Oxford: Oxford University Press, pp. 442–473.

Teubner, G. (2001). Legal irritants: How unifying law ends up in new divergences. In P. A. Hall and D. Soskice, eds. *Varieties of capitalism: The institutional foundations of comparative advantage*. Oxford: Oxford University Press, pp. 417–441.

Teubner, G. (2011). *Networks as connected contracts*. Oxford: Hart.

Thompson, G. F. (2003). *Between hierarchies and markets: The logic and limits of network forms of organization*. Oxford: Oxford University Press.

Thompson, G. F. (2005). Is the future 'regional' for global standards? *Environment and Planning A*, 37(11), pp. 2053–2071.

Thompson, G. F. (2015a). *Globalization revisited.* London: Routledge.

Thompson, G. F. (2015b). Post-Katrina and post-financial crises: Competing logics of risk, uncertainty, and security. In W. M. Taylor, M. P. Levine, O. Rooksby, and J-K. Sobott, eds. *The 'Katrina effect': On the nature of catastrophe*. London: Bloomsbury Publishers, pp. 177–194.

Thompson, G. F. (2017a). Time, trading and algorithms in financial sector security. *New Political Economy*, 22(1), pp. 1–11.

Thompson, G. F. (2017b). Reform from within? Central banks and the reconfiguration of neoliberal monetary policy. In B. Jones and M. O'Donnell, eds. *Alternatives to neoliberalism: Towards equality and democracy.* Bristol: Policy Press, pp. 139–157.

Thompson, G. F. (2017c). Reforming the culture of banking. In I. Erturk and D. Gabor, eds. *The Routledge companion to banking regulation and reform*. London: Routledge, pp. 398–410.

van der Zwan, N. (2014). Making sense of financialization. *Socio-Economic Review*, 12(1), pp. 99–129.

Walter, R. (2011). *A critical history of the economy: On the birth of national and international economies*. London: Routledge.

Yamagishi, T., Kanazawa, S., Mashima, R., and Terai, S. (2005). Separating trust from cooperation in a dynamic relationship: Prisoner's dilemma with variable dependence. *Rationality and Society*, 17(3), pp. 275–308.

13 UN Guiding Principles on Business and Human Rights

Ian Higham

Introduction

The challenges of managing two radically different forms of risk (economic and human rights risk) within the same framework are discussed in this chapter. It problematizes the concept of 'human rights risk' in the context of corporate human rights due diligence. It shows that, in the United Nations Guiding Principles on Business and Human Rights, the concept of human rights risk is modelled on existing business risk management practices. Building on recent contributions to the business and human rights literature, it is argued that, if the goal of the standards is supposedly to prevent human rights abuses, older risk management systems are not necessarily the most appropriate templates for human rights risk assessments. Human rights risk is generally understood as the risk that human rights will be violated by a certain activity. The risk logic employed in other corporate risk assessments is economic in nature, calculating the best ratio of risk to economic return. Yet this economic logic of risk is incompatible with the intention and spirit of international human rights norms: If one takes the position that any severe human rights violation is unacceptable, no matter the economic return, then a different logic should be required to inform human rights due diligence. Due diligence 'is normally understood to refer to a process of investigation conducted by a business to identify and manage commercial risks' (Bonnitcha and McCorquodale, 2017). Building on Fasterling's (2017) critique of human rights as risk management, the chapter connects it to other literatures, and extends the critique to empirical case studies.

The globalization literature is replete with examples of how the nature of corporations has changed over the past several decades. Corporations now frequently operate across national borders and may take in revenues that exceed some developing countries' gross domestic product (GDP). This enormous concentration of corporate power and the many different jurisdictions in which a single corporation can operate may create governance gaps and conflicting regulations that result in corporations acting irresponsibly and violating human rights. It therefore makes sense that some actors have moved to standardize corporate human rights practices globally.

The political debate over standardizing corporate conduct globally has been ongoing in international forums since at least the 1970s. Yet most efforts such as a United Nations (UN) code of conduct failed, and other standardization initiatives, such as the Organisation for Economic Co-operation and Development (OECD) Guidelines for Multinational Enterprises are limited in scope or reach. These standards were also not initially human rights-specific but rather addressed general corporate responsibilities. The UN Global Compact, launched in 2000, listed ten principles for companies committed to reporting on social responsibility, but these principles did not include any actionable guidelines or true 'standards' to which companies could be held; they were primarily aspirational in nature. However, over the past decade, developments at the UN Human Rights Council (UNHRC) have finally led to a global standard for business and human rights: the UN Framework and Guiding Principles on Business and Human Rights, central to which is the concept of human rights due diligence for corporations.

This chapter questions whether corporate human rights practices are always appropriate for this type of standardization. While a basic process of due diligence may be replicable across corporations, it is not obvious that all companies are capable of conducting human rights impact assessments on the same scale. Moreover, without the backbone of government regulation, companies may only concern themselves with their human rights impacts if their operations fall under a category specifically designated in the guidelines as 'high risk'. While I maintain that the Guiding Principles are an example of transparent policy-making and an innovative approach to global governance (Aaronson and Higham, 2013), I show that their shortcomings must be addressed critically, to ensure consistent implementation and actual improvement of corporate human rights performance.

In 2005, then-Secretary-General of the UN, Kofi Annan, appointed Harvard professor, John Ruggie, as his special representative on the issue of human rights and transnational corporations and other business enterprises. Ruggie was tasked with mapping out the human rights responsibilities of companies and governments on the issue of business and human rights and with defining key concepts in the area, such as corporate spheres of influence and complicity. Ruggie produced a 2008 'framework' for business and human rights called *Protect, Respect and Remedy* (A/HRC/8/5, 2008; hereafter called the framework). The structure of the framework was based on three different pillars: (1) the state's duty to protect citizens against human rights abuses from business; (2) the corporate responsibility to respect human rights; and (3) the need for victims' access to effective remedies when their human rights are violated.

Ruggie produced follow-up reports on implementing the framework and ultimately drafted the Guiding Principles on Business and Human Rights, which the UNHRC unanimously endorsed in 2011, creating a political commitment for member states to uphold the guidelines. The Guiding Principles were intended as a blueprint for implementing the framework. These principles were also structured on the three pillars and gave specific recommendations for governments to develop business and human rights policies, including through

regulation, legislation, providing incentives, and other measures. They also prescribed specific components of human rights due diligence that companies could conduct, to mitigate 'human rights risks'. In addition, the Guiding Principles detailed criteria for effective judicial and non-judicial grievance mechanisms for incidents of corporate human rights violations.

The Guiding Principles are a unique type of policy instrument. They are a set of standards for both governments and corporations:

- standards that states should follow, to produce the most effective business and human rights policies;
- standards that companies should follow, to ensure respect for human rights;
- standards that states, companies, and multi-stakeholder organizations should follow, to establish effective grievance mechanisms for victims of corporate human rights abuse.

The Guiding Principles assume a concern with standardizing *risk management*. This chapter thus deals only with the first two pillars of the Guiding Principles.[1, 2] They prescribe appropriate conduct for both states and corporations in managing human rights risks. These standards specify appropriate conduct for states to mitigate the risk that firms operating under their jurisdictions will violate human rights and for companies to mitigate the risk that *they* will violate human rights. The key concept in the Guiding Principles' conception of risk management is human rights due diligence: Companies should do this, and governments should incentivize or require them to do it, to manage human rights risks. The human rights impact assessment is the means by which a company becomes aware of the level of human rights risk to which it is exposed.

The chapter proceeds as follows: First, it defines the different risk logics competing in the human rights due diligence discourse. Then, it shows how the content of the Guiding Principles hinges on an economic risk logic. It then critically assesses this logic in light of its ability to have a positive effect on human rights. In order to assess how the targets of standardization have interpreted the Guiding Principles and translated them into practices, a case study of the Danish government's early implementation of the Guiding Principles and the implementation by A.P. Moller-Maersk, a large Danish company that also acted early to implement the standards, is presented.

The logic of risk management and the standardization of corporate conduct

Risks

As made clear by Juhl in Chapter 2 in this volume, a generally accepted definition of risk is 'the possibility of *undesirable, adverse* outcome(s) of something happening'. Risk is thus conceptually distinct from chance or opportunity in its normative judgement of the possible outcome: Risk is generally assigned to a judgement of a negative, or 'bad', outcome, while an opportunity provides the

possibility of a positive outcome. Juhl (Chapter 2) shows that operationalizations of risk may be expanded to allow for a normatively neutral conceptualization of risk, whereby opportunities are also considered.

What, then, should the concept of human rights risk mean? According to the more normative approach, a human rights risk is one in which there is a negative outcome for human rights, that is, human rights are not respected and are even violated. A normatively neutral approach would also consider opportunities for ensuring respect for human rights. For business, this would mean any action taken by a corporation that may result in a human rights violation – as well as, possibly, an opportunity for the business to strengthen support for the realization of human rights. The latter 'opportunity' approach could include examples such as pressing governments over which a corporation has influence to ensure respect for particular rights; it should not be understood solely as an opportunity to increase profits.

Risk, however, is frequently associated with the bottom line for corporations. In most discourses, actors apply, whether explicitly or implicitly, an economic logic in the management or standardization of risk. The mainstream position in risk studies is that which is informed by economic and actuarial theory. In this approach, the main concern is 'how to anticipate and control future risks by taking the necessary preventive action' (Petersen, 2011). Accordingly, the economic approach to risk most frequently uses statistical methods and economic models, on the assumption that risks can be classified, quantified, and predicted, as well as managed by rational behaviour (ibid.).

The economic approach to risk is informed by two logics, one of which includes corporate or governmental decision-making. This is usually based on whether a given action is beneficial, based on the probability that certain events will result. This is the logic that informs enterprise risk management (ERM) (ibid.). Thompson (Chapter 12, in this volume) has also shown that corporate management of (financial) risks is really about dispersion of the risk to the business: scattering risk to disperse it, rather than eliminate it, through a redistribution, such that no one party bears the full burden of the risk, and to reduce its overall impact. This financial/economic approach to risk is problematic when the discussion is of corporate human rights risk management, as it is not obvious either that human rights risks could be 'dispersed' in any meaningful way, or that minimizing human rights violations is sufficient compared with eliminating them altogether.

Standards

The Guiding Principles are at their core a set of standards for managing human rights risks by conducting human rights due diligence. The other chapters in this volume discuss the concepts of standards and standardization at length. Juhl (Chapter 2, in this volume) shows that setting a standard is analytically identical to establishing a norm. As norms, standards bear an oughtness – they prescribe something that is deemed best practice and thereby confer normative judgements.

These concepts need particular attention, as this chapter is closely linked to the international relations literature, where the definition of a norm is often contested. A norm may be a 'standard' of what governments, individuals, corporations, organizations, and other actors ought to do. To speak of standards is to imply that something should be evaluated against the standard or brought into compliance with it using comparable metrics (see Juhl, Chapter 2, in this volume). Jore (Chapter 9, in this volume) shows that standards are a form of discourse, telling us what is relevant, valued, or important and how standards can construct the realities that they claim to describe.

While a norm is usually regarded as soft law in the international relations field, standards can also be binding. Some standards are enshrined in law or are issued directly by government regulatory bodies. There is thus a scale of gradation for standardization, from basic accepted practices deemed the minimum socially appropriate action, called soft standards, to mandatory rules implemented by a government with enforcement mechanisms, called hard standards (Lindøe and Baram, Chapter 14, in this volume).

The Guiding Principles are a unique type of standard. While Ruggie frequently refers to them as 'principles', 'guidelines', or 'a blueprint', they are essentially a set of soft standards. The second pillar of the Guiding Principles offers standards for companies conducting human rights due diligence. The first pillar offers a set of standards for national governments to encourage or mandate the second pillar. In that sense, the Guiding Principles are potentially a soft standard for implementing hard standards. These standards span the spectrum from softer norms to hard rules: It depends on how national governments interpret the first pillar to enforce the second pillar, that is, whether they rely on policy incentives, binding legislation, or a combination of the two. This in turn depends on the particular regulatory state's political machinations that lead to policy adoption and implementation.

Human rights due diligence

What is the human rights due diligence that the Guiding Principles seek to standardize? Human rights risks can be a legal risk – that is, the likelihood that the company will be sued for violations of human rights – but the risk of legal liability 'is simply another commercial consideration to be identified and managed in the context of a particular transaction' (Bonnitcha and McCorquodale, 2017). Due diligence could also be understood as a standard of conduct required to discharge an obligation, which in international law has meant supplying a standard of care against which fault can be assessed. Bonnitcha and McCorquodale argue that the Guiding Principles invoke both concepts without explaining their interconnections.

ERM includes the assessment and management of so-called 'social risks' with which human rights due diligence is frequently conflated in both Ruggie's reports to the UN and other writing on the subject of the Guiding Principles. Corporate social risks are the 'actual and potential leverage that people or

groups of people with a negative perception of corporate activity have on the business's (financial) value' (Fasterling, 2017). Human rights risk, however, refers to the risk that the company will violate human rights, which is hardly compatible with the economic approach to risk that focuses on quantifying and weighing potential losses against potential gains. I analyse the text of the framework and Guiding Principles in the next section to show how Ruggie privileges the economic approach to risk.

Protect, Respect and Remedy and the Guiding Principles for business and human rights

Global public policy innovations

Elaborating on the full content of Ruggie's framework and the Guiding Principles on Business and Human Rights is beyond the scope of this chapter; more thorough overviews of these standards and the historical evolution of business and human rights norms can be found in Bernaz (2017) and Aaronson and Higham (2013). In this section, I will outline the contents of these policy guidelines, with a focus on their emphasis on risk.

In the framework, Ruggie developed a tripartite structure for addressing the business and human rights policy challenge. In the first pillar, Ruggie focused on the state's duty to protect against corporate human rights abuses. The framework outlined four key areas on which governments should focus, to prevent corporate human rights violations in their jurisdictions:

- creating a corporate culture respectful of human rights;
- aligning policies across departments to ensure consistency;
- improving guidance and support at the international level for states to achieve greater policy coherence;
- addressing businesses operating in human rights-sensitive conflict zones (A/HRC/8/5, 2008, para. 27–50).

The second pillar of the framework regards the corporate responsibility to respect human rights. This pillar focuses on the need for companies to respect human rights as part of their social licence to operate in particular contexts. It also prescribes a due diligence process for companies. The due diligence process for human rights, Ruggie argued, should look, at a minimum, to the International Bill of Human Rights (the Universal Declaration of Human Rights and the two international covenants that codify the declaration into law) and the core conventions of the International Labour Organization. Human rights due diligence includes developing a human rights policy for the company, conducting human rights impact assessments, integrating the policy throughout the company, and tracking performance. This pillar also attempted to set out clearer definitions for what qualifies as a company's 'sphere of influence' and what counts as 'complicity' in human rights violations when the company is not directly responsible for the abuse (A/HRC/8/5, 2008, para. 51–81).

The Guiding Principles in some ways supplant the framework with more specific and actionable guidelines for its implementation. Ruggie called on states and companies to take on a mix of actions. For states, this includes enforcing existing laws, providing guidance to companies, and encouraging or mandating firms to conduct (components of) human rights due diligence. The first pillar of the Guiding Principles also provided specific recommendations for state-owned businesses and businesses operating in conflict zones. The second pillar of the Guiding Principles again focused on the corporate responsibility to respect, with specific recommendations for best practices in conducting human rights due diligence (A/HRC/17/31, 2011, para. 1–24). Both the framework and the Guiding Principles also advanced the agenda for access to remedy. While grievance mechanisms can inform the due diligence process and are important for the realization of human rights – and should indeed be subjected to critical assessment – this portion of the business and human rights policy agenda is outside the scope of this chapter, which focuses primarily on the standardization of human rights risk management.

Risk in the UN Guiding Principles

The framework notes that the less governments do to provide guidance for, and regulation of, the human rights impacts of corporate activities, 'the more they increase reputational and other risks to business' (A/HRC/8/5, 2008, para. 22). In this document, corporate human rights due diligence is defined as 'a process whereby companies not only ensure compliance with national laws but also manage the risk of human rights harm with a view to avoiding it' (A/HRC/8/5, 2008, para. 25).

The framework and the Guiding Principles frame some operating contexts as riskier than others. For example, both have extensive guidelines on corporate activities in conflict zones and on complicity when operating in specific high-risk regions or contracting with certain regimes. By including specific sections on these high-risk contexts, Ruggie implicitly prioritizes particular operating contexts for the application of risk management processes, based on the notion that such areas posed a higher 'human rights risk' for companies. According to the framework, for example, the state duty to protect includes providing or facilitating access to information and advice 'to help businesses address the heightened human rights risks' of operating in conflict zones (A/HRC/8/5, 2008, para. 49).

The Guiding Principles maintain these special criteria for companies operating in conflict zones, discursively facilitating a 'riskification' of particular operating contexts. The seventh principle states, 'Because the risk of gross human rights violations is heightened in conflict-affected areas, States should help ensure that business enterprises operating in those contexts are not involved with such abuses', including by

- engaging with businesses at an early stage to help them 'identify, prevent and mitigate the human rights-related risks of their activities and business relationships';

- assisting businesses to 'assess and address the heightened risks of abuses, paying special attention to both gender-based and sexual violence';
- denying access to public support for businesses involved with gross human rights abuses;
- ensuring that existing policies, legislation, regulation, and enforcement measures 'are effective in addressing the risk of business involvement in gross human rights abuses' (A/HRC/17/31, 2011, para. 7).

Although Ruggie had stated that no list of specific human rights should be prioritized by companies (since they could theoretically violate any human right), it is clear that the Guiding Principles highlight certain operating contexts as being particularly in need of government policy innovation due to a logic of calculable 'human rights risk'.

The more general guidelines (not related to a specific operating context) contained in the Guiding Principles for states similarly focus on applying risk logics when creating public policy. In the third principle, which focuses on general state regulatory and policy functions, the Guiding Principles prescribe that states should enforce existing human rights laws, ensure that other laws and policies governing the creation of enterprises do not constrain business respect for human rights, provide guidance to businesses on how to respect human rights, and '[e]ncourage, and where appropriate require, business enterprises to communicate how they address their human rights impacts' (A/HRC/17/31, 2011, para. 3). For a government to determine where it is 'appropriate' to require business communication on addressing human rights impacts appears also to be based on a risk logic. The commentary on this principle states: 'A requirement to communicate can be particularly appropriate where the nature of business operations or operating contexts pose a significant risk to human rights' (A/HRC/17/31, 2011, para. 3). Thus, the first pillar of the Guiding Principles encourages governments to use a calculable risk-based approach when deciding upon which policy or regulation to pursue.

The second pillar of the Guiding Principles also employs the economic logic of risk in prescribing standards for corporate human rights due diligence. This pillar is based on the responsibility to respect, which the Guiding Principles define as companies' need to 'avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur' and 'seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts' (A/HRC/17/31, 2011, para. 13). This responsibility is ascribed to all enterprises of all sizes, sectors, operating contexts, etc. However, the Guiding Principles specify that, 'Nevertheless, the scale and complexity of the means through which enterprises meet that responsibility may vary according to these factors and with the severity of the enterprise's adverse human rights impacts' (A/HRC/17/31, 2011, para. 14), suggesting that some companies pose a higher risk than others.

The Guiding Principles lay out specific steps for meeting this responsibility. The first is to make a human rights policy commitment that is approved at the

most senior level of the company, is informed by relevant expertise, stipulates the enterprise's human rights expectations, is publicly available and communicated internally and externally, and is embedded throughout the enterprises (A/HRC/17/31, 2011, para. 16). The next component of the corporate responsibility is for companies to conduct human rights due diligence '[i]n order to identify, prevent, mitigate and account for how they address their human rights impacts' (A/HRC/17/31, 2011, para. 17).

The commentary on Principle 17 justifies the need for due diligence through an explicit connection to risk and goes on to provide a definition of human rights risk: 'Human rights risks are understood to be the business enterprise's potential adverse human rights impacts' (A/HRC/17/31, 2011, para. 17). Ruggie argues explicitly that human rights due diligence is consistent with existing conceptions of corporate risk: 'Human rights due diligence can be included within broader enterprise risk-management systems, provided that it goes beyond simply identifying and managing material risks to the company itself, to include risks to rights-holders' (A/HRC/17/31, 2011, para. 17). Like other risks managed by such systems, 'Human rights risks can be increased or mitigated already at the stage of structuring contracts or other agreements and may be inherited through mergers or acquisitions' (A/HRC/17/31, 2011, para. 17). The definition here goes beyond the economic logic risk to address the risk to rights-holders, but it suggests that ERM systems operating on an economic logic are compatible with this competing and expanded definition of risk.

This principle also suggests that the decision of when and where to conduct due diligence may be based more explicitly on economic risk logic approaches:

> Where business enterprises have large numbers of entities in their value chains it may be unreasonably difficult to conduct due diligence for adverse human rights impacts across them all. If so, business enterprises should identify general areas where the risk of adverse human rights impacts is most significant, whether due to certain suppliers' or clients' operating context, the particular operations, products or services involved, or other relevant considerations, and prioritize these for human rights due diligence.
> (A/HRC/17/31, 2011, para. 17)

Principle 17 ties the concept of human rights risk to a more traditional concept of material risk by highlighting the legal risks associated with corporate human rights violations. Ruggie's commentary on the principle states: 'Conducting appropriate human rights due diligence should help business enterprises address the risk of legal claims against them by showing tha t they took every reasonable step to avoid involvement with an alleged human rights abuse' (A/HRC/17/31, 2011, para. 17).

The following principles in the second pillar provide guidance on how to implement this concept of due diligence. Principle 18 states:

> In order to gauge human rights risks, business enterprises should identify and assess any actual or potential adverse human rights impacts with which

> they may be involved either through their own activities or as a result of their business relationships. This process should:
>
> (a) Draw on internal and/or independent external human rights expertise;
> (b) Involve meaningful consultation with potentially affected groups and other relevant stakeholders, as appropriate to the size of the business enterprise and the nature and context of the operation.
>
> (A/HRC/17/31, 2011, para. 18)

The focus on actual and potential impacts employs a classic risk logic of imagining the future and acting accordingly. Ruggie embeds Principle 18 again in existing risk-management systems, with a qualifier: the commentary states, 'While processes for assessing human rights impacts can be incorporated within other processes such as risk assessments or environmental and social impact assessments, they should include all internationally recognized human rights as a reference point' (A/HRC/17/31, 2011, para. 18). He also states that such assessments must be carried out at regular intervals.

Critiquing the economic risk logic of the Guiding Principles

From the outset, Ruggie concerned himself largely with the interconnections of human rights and business risk. One can conceive of risk in different ways, and I argue that the Guiding Principles' conception is primarily based on an economic logic insofar as they advocate an integration of human rights due diligence into existing ERM practices, rendering human rights risk as managerially analogous to social risk. As stated above, the main concern in economic approaches to risk is to predict and mitigate probabilities of events. It is precisely this logic of risk that is deployed in the UN Framework and Guiding Principles on Business and Human Rights – even if the goal is ostensibly the mitigation of human rights violations. This is clearly demonstrated by the section of the Guiding Principles (see above) in which Ruggie stated that 'Human rights due diligence can be included within broader enterprise risk-management systems, provided that it goes beyond simply identifying and managing material risks to the company itself, to include risks to rights-holders' (A/HRC/17/31, 2011, para. 17). It is also evidenced by Ruggie's tethering of the concept of human rights risk to legal risk, which is a material risk to the firm in the most traditional sense and eschews the need for concern with the affected individuals beyond the extent to which they can bring charges against the firm and be awarded damages.

The economic logic of risk as a means for ensuring respect for human rights appears highly problematic. I make two main points. First, by privileging particular areas as 'higher risk' for human rights violations, the UN guidelines may dissuade companies not operating in such contexts from taking seriously their human rights obligations in the absence of more stringent government regulation. The Guiding Principles discursively removes the responsibility from companies with complex operations to assess risks throughout their value chains and

instead encourage a focus on areas of particular risk. Yet the standards do not provide clarity on how these risks should be calculated, and companies themselves are left to decide what constitutes a high-risk area. There is no clear guidance, either, on how many tiers fall under the scope of due diligence: tier 1 and 2 suppliers[3] might not operate in high-risk areas, but what if tier 3 suppliers do? The Guiding Principles are not specific.

Risk management is not normatively neutral – the risk literature broadly accepts that risk is socially constructed with a normative basis (e.g. Fasterling, 2017). Companies may normatively decide that certain human rights or certain vulnerable populations are more worthy of risk than others and assess impacts accordingly to the detriment of rights-holders elsewhere. If the aim of human rights due diligence is to mitigate or eliminate human rights risks, and if there is, as Ruggie has said, no hierarchy of human rights and no limit to the rights that a company can violate, then removing the responsibility from a company not obviously operating in 'riskier' contexts fails to meet the goal of advancing respect for all human rights in all contexts. The Guiding Principles can thus be interpreted and implemented in a manner that contradicts their stated goal.

Second, I argue that human rights due diligence in particular is not necessarily appropriate for standardization according to existing models of ERM and social impact assessments. This is so, provided that the goal of human rights due diligence is not the minimization of financial losses but rather the prevention of human rights violations. Fasterling (ibid., p. 230) made a similar argument:

> The normative justification for social risk management [as defined above] is that managers fulfil responsibilities that they owe to the stakeholders that have a legitimate interest in the perenniality and profitability of the business corporation. … Social risk management's objective … is to secure the acceptance or approval by local communities and stakeholders of a business enterprise's operations or projects in a certain area.

If a company cannot obtain a social licence to operate, it faces financial losses related to those operations that are shut down, interfered with or unable to commence. Fasterling contrasts social risk with the concept of human rights risk that the Guiding Principles claim to want to address: 'While the UNGPs have been drawn up against the backdrop of corporate risk management practice, the corporate responsibility to respect human rights has a different normative trajectory mandating social risk management' (ibid., p. 231).

Human rights risk is the relevant risk for fulfilling the second pillar of the Guiding Principles. This risk comes from the potential occurrence of an adverse human rights impact, which means that assessing human rights risks not only requires analysing potential harm but also making a normative judgement about whether such harm qualifies as a human rights violation. The purpose of human rights risk management therefore is not to fulfil responsibilities owed to individuals whose rights may be exposed due to corporate activities (ibid.).

Thus, the economic logic of managing risks is incompatible with the very purpose of human rights risk management, but the Guiding Principles deploy these competing logics interchangeably, without clarity on which approach is best. This confusion of competing logics provides no guarantee that a company or government adopting the Guiding Principles' standards will have a 'standard' approach to human rights risk management: Some will be left to look at human rights as a legal (financial/economic) risk; others will focus on the stated goal of mitigating human rights violations whatever the cost to firms. Resolving this type of 'fundamental conceptual confusion within the Guiding Principles' has practical relevance, as 'Business enterprises seeking to implement the Guiding Principles need clarity about the standard of conduct that they are expected to meet in avoiding adverse human rights impacts', since

> Victims of corporate human rights abuse and non-governmental organizations advocating on their behalf need clarity as to whether the remedial responsibilities recognized by the Guiding Principles apply only in cases in which human rights infringements are the result of a lack of diligence by a business enterprise.

and because 'It is relevant to the future of the Guiding Principles as a basis for national and international regulations and voluntary codes of conduct' (Bonnitcha and McCorquodale, 2017).

Government implementation of the Guiding Principles: the Nordic conception of risk

I have argued above that, in the absence of government regulation, companies may not take seriously their human rights responsibilities outside of particular operating contexts. I have also shown how there are competing 'risk logics' in the business and human rights discourse. It is therefore crucial to understand how governments have interpreted the UN policy guidance on business and human rights and translated (or not) this guidance into domestic policy or legislation. The four Nordic countries – Denmark, Finland, Norway, and Sweden – were all relatively early adopters of National Action Plans (NAPs) for business and human rights. NAPs are policy documents that outline what a government has done and/or plans to do to address the human rights impacts of business.

In the following case studies, I assess how the Danish government, through its NAP, and one of the biggest and most influential companies in Denmark have implemented the Guiding Principles. I consider the extent to which their implementations have been informed by the economic risk logic at play in the Guiding Principles. I do this because the Guiding Principles' conception of risk may discursively limit the options for governments and companies seeking to keep their policies consistent with the source material of the Guiding Principles. The desire to implement and conform to the Guiding Principles reproduces the principles' logic at the national and company levels and defines what states and

companies are capable of and willing to do within this construction of risk. Choosing to implement the standards (or not) and deciding how to do so are political decisions. As Karen Lund Petersen (2011) puts it:

> The concept of risk is contingent on political action … The concept of risk cannot be reduced to a mere description of a certain empirical political reality; rather, the concept must also be understood as a medium for defining the possibility of politics.

First pillar case study: Denmark

The case of Denmark is particularly interesting for further study and has important political implications. Denmark was the second country to adopt a National Action Plan (NAP) on implementing the Guiding Principles in April 2014, although the Danish government had public policies for corporate social responsibility (CSR),[4] including human rights-specific provisions, before the publication of the Danish NAP. Denmark was thus a pioneer of public policies for business and human rights. Moreover, the Danish government used its presidency of the European Union in 2012 to convene a conference that pressed other EU member states to begin working on NAPs for business and human rights (Danish EU Presidency, 2012).

The Danish NAP outlined measures taken to date, including that the government mandates some aspects of human rights due diligence. For instance, Denmark requires the largest Danish companies to disclose their CSR practices, including their practices related to human rights (Danish Government, 2014, p. 14). The NAP also proposed new policy measures to be taken to promote corporate respect for human rights.

Many components of existing and proposed Danish public policies for business and human rights use risk analysis as a key concept. The Danish government is explicit that its policies are risk-based:

> In the National Action plan for CSR, the Danish Government sets out clear expectations to Danish companies that they must take responsibility to respect human rights when operating abroad – especially in developing countries where there can be an increased risk of having an adverse impact on human rights (GP2).
>
> (ibid., p. 11)[5]

Immediately, the government discursively restricted the scope of its policy to companies in particular operating contexts, namely, developing countries. The government explicitly references Guiding Principle 2, which says that states should set out clearly their expectation that businesses domiciled in their territory/jurisdiction respect human rights throughout their operations, as a source of this limitation. Yet this risk-focused target illustrates my first critique of the

standards: One operating context (developing countries) is normatively privileged as being more risk-sensitive for human rights abuses.

One might reasonably expect human rights to be more at risk in developing countries, but companies interpreting and translating Danish public policy into company-level policy might be inclined to ignore human rights risks in developed countries. Services-based economies still pose great risks to human rights, including the right to freedom from employment discrimination, which is plainly prevalent in some developed countries, where effective redress remains difficult to access for many social groups. It is also increasingly obvious that economic development is no guarantee of the rights to privacy and to the freedom to receive and impart information – rights that can be violated virtually anywhere companies collect personal data or facilitate communications.

Specific policy measures included in the NAP go on to demonstrate the focus on economic logics of risk. Danida Business Partnerships are an instrument that facilitate economic support to develop commercial partnerships between Danish companies and partners from developing countries. Companies involved are required to integrate CSR in their business operations and 'demonstrate due diligence' on human rights issues (ibid., p. 12). In order to be approved for financing, Danida Business Finance 'analyses potential human rights related risks including local legislation and policies and other CSR issues' (ibid., p. 28).

The Danish Export Credit Agency (EKF) has an Environmental and Social Due Diligence Policy that includes a commitment to Guiding Principle 4, which says that states should take additional steps to protect against human rights abuses by business enterprises that are owned or controlled by the state or that receive support and services from state agencies, such as export credit agencies.

> The EKF has initiated the development of a model that provides an overview of the business risks that could potentially be related to human rights, labour rights, environment and climate in the countries where EKF is investing. EKF is screening the companies involved in the EKF's transactions.
>
> (ibid., p. 13)

The EKF focuses especially on operating contexts, per Danish policy above, specifically on companies operating in conflict zones (ibid., p. 28).

Analysing the entire document is beyond the scope of this article, but suffice it to say that the NAP focuses heavily on due diligence: both incentivizing human rights due diligence by laying out clearly the government's expectation of companies, mandating due diligence where export credit financing is sought, and mandating the reporting component of due diligence for all major companies.[6] Yet nowhere in the NAP does the Danish government differentiate between the different logics of risk (economic/social or human rights abuse-mitigating) to conceptually guide Danish firms seeking clarity on how they are to best identify a human rights risks and manage their responsibilities. Since the principles are not only largely voluntary – that is, not codified in Danish law – companies are left to determine for themselves whether to implement the standards.

Lacking conceptual clarification from the state where the Guiding Principles have not provided any, companies are also mostly left to work out for themselves *how* to implement the standards. I therefore turn to a case study of one of Denmark's largest corporations that claims to be implementing the Guiding Principles.

Second pillar case study: A.P. Moller-Maersk Group

Danish companies were among the earliest adopters of human rights-focused CSR practices in line with the Guiding Principles, among which A.P. Moller-Maersk Group (commonly referred to as Maersk) was one of the first globally to include a reference to the Guiding Principles in its human rights policies and to begin assessing human rights impacts (Aaronson and Higham, 2013). Maersk has a long history of close relations with the Danish state and an important role in the Danish economy. It is therefore a likely target for regulation and for having its human rights practices in the public spotlight in Denmark.

The company makes clear on its website that these practices are based on risk calculations. Maersk states: 'In every country where we operate, whether high or low risk, conflict-affected or not, our goal is to ensure that we do not have adverse impact on human rights' (A.P. Moller-Maersk, 2017). Maersk's human rights webpage continues with more details on its human rights programme, with a heavy emphasis on risk. 'We work to ensure that we respect human rights in line with our Maersk values and the UNGPs. We strive to integrate human rights risk management into existing business processes across A.P. Moller-Maersk operations' (ibid.).[7] Here, the company indicates that they have taken up the Guiding Principles' standard of using existing risk management processes – those discussed above as driven by an economic logic of return and loss – to manage human rights risks.

Yet the rhetoric is at least partially inconsistent with the economic logic of the ERM systems into which Maersk claims they have integrated human rights risk management. According to Maersk, operating context is irrelevant to its goal of avoiding human rights abuse. Yet the Guiding Principles emphasize the need to assess risks in particular operating contexts and recommend integration with risk level-focused management processes. Also, despite the discursive nod to broad human rights risk management beyond targeted areas, the company lists five priority human rights issues for which it has developed action plans, and one of these is 'the use of security services in high risk settings' (ibid.).

Maersk outlines its approach to corporate governance in the area of business and human rights. The company states that human rights risks are managed as part of its various programmes, such as Responsible Procurement, Global Labour Principles, Anti-Corruption, Health and Safety, the enterprise risk management system, and in due diligence processes for mergers and acquisitions. 'The management of human rights risks is the responsibility of Maersk's businesses, including government relations and social investments in host countries' to assist in their economic development' (ibid.).

The company thus not only integrates human rights risks into existing ERM practices, but it also divides responsibility among multiple businesses and departments. Such a division of human rights risk management may suggest integration of a human rights policy throughout the enterprise. Yet it may also suggest that the company does not fully recognize human rights risks as distinct from other risks that are managed by departments with specialist business functions and who may lack the necessary human rights content training that a centralized CSR operation could provide. More research is desirable to determine how companies manage human rights risks internally and which units in which companies are delegated such responsibilities. Such research could shed further light on which of the risk logics companies interpret in reading and implementing the Guiding Principles.

Conclusion

As I have previously argued (Aaronson and Higham, 2013), the Guiding Principles were a remarkable governance innovation that provide a model for inclusive, multi-stakeholder deliberation and policy-making. The purpose of this critique is not to detract from the initial successes of the Guiding Principles but to highlight and build upon existing identifications of the conceptual confusion contained within these standards. I have reviewed the literature on the confusion between different risk approaches within the Guiding Principles and argued that, without clarity, there remains doubt as to whether 'human rights' are appropriate for standardization for corporate risk management. It is also possible that there is a need for explicit standards like the Guiding Principles but with a clearer demarcation of the standards' human rights risk logic from traditional economic logics of risk. Standards help governments to benchmark their own policies and companies to operate on a level playing field, but standards that confuse different mechanisms can be unhelpful to both.

Empirically, I have discussed the Danish government's approach to implementing the Guiding Principles, as well as the approach of perhaps the most famous Danish firm. So far, Denmark leaves companies to decide for themselves whether to implement the standards in most cases; the Guiding Principles have largely failed to find their way into binding Danish legislation. States were not necessarily meant to translate each principle into law in a standard manner, but they are uniquely positioned to 'speak' to their home firms in a way that the UN cannot: Regulatory bodies have authority and connections to domestic firms that international organizations lack. The Danish state has so far squandered the opportunity to provide clear guidance on precisely how human rights are to be conceptualized and, thereby, managed. It is apparent from the A.P. Moller-Maersk case that companies, lacking such guidance, follow the economic approach that the Guiding Principles seem to suggest. This is a significant and potentially problematic development, as this approach has been shown to be logically inconsistent with the stated goal of minimizing risk to the rights-holders; instead, the firm focuses on minimizing risk to itself. Firms also may present

competing risk approaches in their own CSR literature, as is seen in the Maersk case. While the world may need standards for managing human rights risks, such standards need to be clearer about what this management really means.

Notes

1 While the third pillar also contains standards of state and business conduct, it is primarily concerned with redressing violations after they have occurred and not with assessing or mitigating the risk of such violations occurring. Some scholars and practitioners have noted that grievance mechanisms could also inform future risk management practices.
2 For the remainder of the chapter, I refer to the Guiding Principles independent of the *Protect, Respect and Remedy* framework. Both texts contain the same three pillars, with the framework laying out ideas and aspirations and the Guiding Principles providing concrete recommendations.
3 Tier 1 suppliers supply products or product components directly to the firm; tier 2 suppliers supply the tier 1 suppliers; and so on.
4 CSR is distinct from, but overlaps with, business and human rights. For a discussion, see Bernaz (2017, pp. 3–8).
5 Denmark's National Action Plan for Corporate Social Responsibility is distinct from, though overlaps with, its National Action Plan for Business and Human Rights. CSR is defined here as a broader set of corporate responsibilities, including not only human rights but also environmental sustainability and anti-corruption.
6 Companies can also disclose merely that they do nothing on the issue of business and human rights. While this may amount to public shaming that the company prefers to avoid, and while it may encourage companies to begin thinking about their baseline human rights performance, this may not technically be considered a 'mandatory' component of due diligence insofar as companies do not actually have to do anything other than issue a statement that they do nothing.
7 www.maersk.com/business/sustainability/responsibility/human-rights (accessed 16 January 2017).

References

Aaronson, S. A. and Higham, I. (2013). Re-righting business: John Ruggie and the struggle to develop international human rights standards for transnational firms. *Human Rights Quarterly*, 35(2), pp. 333–364.

A/HRC/8/5 (2008). *Protect, Respect and Remedy: A Framework for Business and Human Rights*. Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises. New York: UN.

A/HRC/17/31 (2011). *Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework*. Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises. New York: UN.

A.P. Moller-Maersk (2017). Human rights [online] Available at: www.maersk.com/en/about/sustainability/responsibility/human-rights (accessed 16 January 2017).

Bernaz, N. (2017). *Business and human rights: History, law and policy – Bridging the accountability gap*. London: Routledge.

Bonnitcha, J. and McCorquodale, R. (2017). The concept of 'due diligence' in the UN Guiding Principles on Business and Human Rights. *The European Journal of International Law*, 28(3), pp. 899–919.

Danish EU Presidency (2012). From principles to practice: The European Union operationalizing the United Nations Guiding Principles on Business and Human Rights [online]. Available at: www.ihrb.org/pdf/2012-05-07-Danish-EU-Presidency-Conference-Report.pdf (accessed 31 March 2019).

Danish Government (2014). Danish National Action Plan: Implementation of the UN Guiding Principles on Business and Human Rights [online] Available at: www.ohchr.org/Documents/Issues/Business/NationalPlans/Denmark_NationalPlanBHR.pdf (accessed 16 January 2017).

Fasterling, B. (2017). Human rights due diligence as risk management: Social risk versus human rights risk. *Business and Human Rights Journal*, 2, pp. 225–247.

Petersen, K. L. (2011). Risk analysis: A field within security studies? *European Journal of International Relations*, 18(4), pp. 693–717.

14 The role of standards in hard and soft approaches to safety regulation

Preben H. Lindøe and Michael S. Baram

Introduction

Regulation of industrial safety has developed over decades. The traditional 'hard law' approach that involves government development and enforcement of detailed prescriptive rules in 'command and control' fashion is yielding to, or being applied in combination with, a more flexible 'soft law' approach (Lindøe, Baram, and Paterson, 2013). A prime example is safety regulations to prevent major accidents. There are several versions of the soft law approach, but common features are its use of rules that set goals but allow industrial enterprises to devise the means of achieving the goals, additional rules that assign broadly defined functional responsibilities to the managers of such entities, and the creation of a regulatory ethos that fosters government-industry collaboration and industry self-regulation (Lindøe, Baram, and Renn, 2014).

This transition has raised many questions about the efficacy, credibility, accountability, and even the legitimacy of a soft law regime in which industrial self-regulation is a prominent feature (Verkuil, 2007; Baram and Lindøe, 2014). To address these questions, policy analysts and other interested parties are examining how soft law approaches are being implemented. Their endeavours show that regulators and industry look to and rely on numerous detailed technical and management standards, instructive guidance, and well-established norms, in order to administer and implement broadly defined soft law mandates.

More urgent attention is being given to such standards, guidelines, and norms by the regulators, companies, industrial associations, professionals, and consultants, who are most closely involved in regulatory implementation of soft law mandates. These mandates require compliance but often lack the details that would be instructive about achieving compliance in order to allow the flexibility needed by government and industry to cooperate in fashioning an optimal approach to safety for each industrial enterprise. Thus, uncertainties about compliance, as well as meeting other obligations (to stakeholders, shareholders, contractors, etc.), draws their attention to relevant standards and guidelines that would be instructive about achieving compliance, especially those that are adopted or favourably referenced by regulators.

This chapter reviews the characteristics of hard and soft regulatory modes and examines their reliance on standards, standardization organizations and processes, and stakeholder interests. Lessons learned from offshore oil and gas regulation are highlighted, to reveal how implementation problems are dealt with; a discussion of findings and public policy issues then follows and leads to conclusions about standardization as a core feature of risk governance in industrial democracies.

The structure of a regulatory regime

A regulatory regime consists of several layers of action-forcing features and can be depicted as a pyramidal structure, as shown in Figure 14.1. First and foremost is the law or other government action that mandates the regulation of a designated set of industrial actors. This top level also includes the regulations (e.g. rules, permit requirements) that are subsequently enacted. The middle level encompasses the standards and recommended practices developed by private organizations, that have been adopted by or favourably referenced by regulators, as well as regulator-developed guidelines that are considered authoritative and therefore constitute *de jure* or de facto requirements that must be heeded by the targeted set of private actors.[1]

The bottom level is comprised of other relevant standards and guidelines, whose application is left to the discretion of the regulated entity, including those developed by each industrial actor for its operational purposes (e.g. quality control, efficiency, interchangeability of operations, etc.). It includes the many methodological and behavioural guidelines (individual and organizational) that infuse and shape regulatory regimes (e.g. court decisions, professional codes, societal norms, and moral principles).

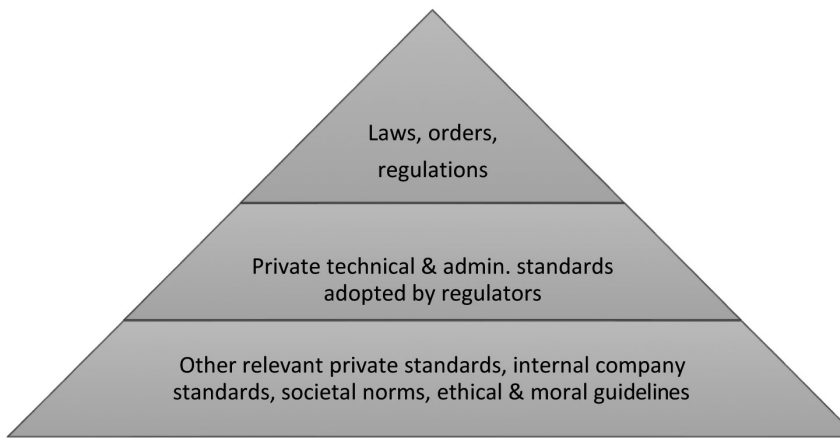

Figure 14.1 The pyramidal structure of a regulatory regime.

The top layer establishes whether the regime will pursue a hard or soft law approach. A hard law regulatory approach is generally considered to be one whose main purpose is to force regulated entities into compliance with prescriptive rules developed by government entities, whereas a soft law approach has the purpose of fostering co-regulatory risk management and socially responsible self-regulation (Gilad, 2010; Short and Toffel, 2010).

However, making such a clear-cut distinction has been questioned (Hopkins, 2011; Lytton, 2018) and can be misleading in the real world, where the overall regulatory regime is likely to have a blend of elements from both approaches (Sinclair, 1997). A good example is seen in the hard law approach taken by the regulator of offshore oil and gas operations in the US, in which many voluntary standards and recommended practices developed by the leading industrial association are subsequently adopted and enacted by the regulator as legally enforceable prescriptive rules (Baram, 2014; National Academies of Science, Engineering, and Medicine, 2016).

Further refuting any sharp distinction between the two approaches, the regulator is often empowered to develop and enforce both types of rules, to the extent that their content, implementation, and enforcement are consistent with the mandate that authorizes the regulatory regime (Baldwin and Cave, 2012). Even when self-regulation is authorized for a soft law approach, the regulator has an important role to play because self-regulation can be seen as a 'negotiation occurring between the state and individual firms to establish regulations that are particularized to each firm' (Ayres and Braithwaite, 1992, p. 101).

The middle level of the pyramid is comprised of standards and recommended practices that have been privately developed and subsequently selected and adopted, or favourably referenced, by the regulator. Regulators frequently prompt and participate in the development of such standards, to improve the technical quality of the regime's requirements. Subsequently such standards are adopted as prescriptive rules or used in other ways to provide more technical detail for industry and reduce uncertainties about compliance with vaguely defined performance or goal-based rules.

Thus, the regulator capitalizes on private expertise and experience to develop a more robust regime and one that is better able to keep pace in a changing technological environment. Zwesloot (2000) shows how standards capitalize on the organizational capabilities and motives of many industrial, technical, and certification organizations that engage in standardization, such as the International Organization for Standardization (ISO), the Organisation for Economic Co-operation and Development (OECD), and highly-qualified technical entities like DNV-GL, TUV Rheinland, and the American Petroleum Institute (API). Further discussion on the use of standards in different types of regimes appears later in this chapter.

The base level of the pyramid encompasses a broad range of principles, policies, standards, and guidelines that influence individual and organizational behaviour within any regulatory regime, as noted above. However, their selection and application are left to the discretion of the regulated entity. They

include internal company policies and standards that are developed and applied by each industrial actor for operational purposes, such as quality control, efficiency, interchangeability of operations, training levels, equipment specifications, supplier qualifications, and management functions. In addition, there are numerous behavioural guidelines, stemming from court decisions and liability doctrines, contractual commitments, professional codes of ethics, and prevailing societal norms and moral principles that need to be heeded to build and maintain trust.

The regulator as regime manager

The regulator has the challenge of coordinating and harmonizing the diverse approaches and activities of the regime and ensuring appropriate messages are sent to the regulated industry about compliance. Combining modes of regulation within a regime structure that incorporates hard and soft approaches can be depicted as shown in Figure 14.2.

Top down, the regulator is empowered to develop and enforce rules to protect the public and workers, and, together with inspectorates, to oversee and enforce compliance by issuing orders and imposing sanctions. In taking this instrumental approach, the regulator has the opportunity to reference or incorporate selected voluntary standards and technical guidelines developed by industrial and professional organizations, recommend best practices and provide instructive materials to facilitate compliance, and determine the acceptability of each company's self-regulatory efforts.

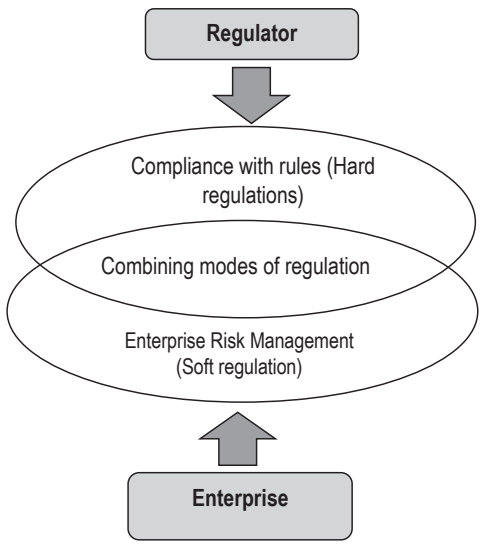

Figure 14.2 Convergence of hard and soft law approaches.
Source: Lindøe (2017).

Bottom-up, in addition to complying with any top-down, hard law rules, the regulated enterprise acts as a self-regulatory agent and establishes the internal controls needed for assessing risk and implementing its own safety management system. Although it may have substantial expertise, it will usually seek to follow the voluntary standards and best practice guidelines of its industrial sector, especially those developed by associations of industrial peers, allied professional groups, influential standard-setting organizations, such as the ISO and the OECD, and, of course, any standards and guidelines recommended or favoured by the regulator.

In the middle zone, the two approaches converge, resulting in a co-regulatory regime that has elements of both approaches and a mixture of rules, standards, and guidelines, some of which may apply across the industrial sector and others that are only applicable to a specific regulated entity. Among the challenges for the regulator are coordinating and managing the hard and soft approaches, mentoring and enforcing compliance with the regime's prescriptive rules, evaluating the quality and performance of self-regulatory activities by each enterprise, and heeding requirements and norms regarding stakeholders and other public sector involvement.

Standards and guidelines for regulation and self-regulation

The most visible part of the pyramidal regulatory regime, discussed earlier (Figure 14.1), is its top level of legally enforceable laws, rules, and administrative procedures. However, like an iceberg, the largest part of the pyramidal regime is its less-visible middle and base level sets of standards, guidelines, and norms from various external sources that provide the detailed substantive content of prescriptive rules and the substantive guidance for implementing performance-based rules and self-regulation.

Beyond their value to a risk-managing regulatory regime, standards can be used to provide economic value in the private sector. Some industrial and professional associations, such as the ISO and the International Association of Drilling Contractors (IADC), certify members, who adhere to, or are trained to meet, the standards set by such associations. Companies that adhere to standards that reflect best practices have a better defence against claims of negligence and liability. Further, standards have value in defining commitments between the parties to a contract, in supporting claims in company advertisements, and in gaining public trust.

For many years, the vast majority of private standards pertained to products made for use by consumers or companies. As such product markets expanded with the globalization of commerce and competition, the economic value for industry of adhering to such standards prompted a substantial increase in their development and use at national and global levels. Nevertheless, among the policy-analytic community, there has been scant research or interest in standardization processes and outcomes and their societal consequences (Brunsson and Jacobsson, 2000; Mattli and Büthe, 2003).

Since the growing acceptance and deployment of soft law, with its emphasis on self-regulation, internal control, and the uncertainties about compliance that are posed by performance-based and management-based rules, private standard-setting organizations have responded by developing consensus standards that are claimed to represent best practices. These standards essentially consist of principles and methods for the conduct of industrial operations and management functions and may also incorporate or reference other standards for the products to be used in the operations and the qualifications of managers and workers.

One example is the largest private standard-setter, ISO, offering a global catalogue of voluntary standards for quality management, auditing practices, sustainable development, environmental management, corporate social responsibility, sustainable procurement practices, ecolabelling, information security, and health and safety at work.[2] In this expansion of its standards portfolio, ISO has created what can be called a global knowledge infrastructure (Edwards *et al.,* 2013). Each standard that involves coordination with numerous other standard-setting entities, such as the International Techno-electrical Commission, the global chemical industry's Responsible Care Management (RC) System, and entities such as DIN, BSI, and API, brings industrial and national interests into standardization processes. These elaborate arrangements can involve thousands of experts, organized in many national committees, interacting and ultimately producing several types of standards. These can be standards serving as a sort of global currency for risk governance used for the certification of companies shown to be in compliance, thereby endowing them with reputational and commercial advantages (e.g. ISO standards for quality control). Others can serve as interim guidelines en route to building a global consensus about basic principles and detailed practices with other standard-setters (e.g. with OECD and its Guidelines for Preventing Chemical Accidents).[3]

For our purposes, we focus on the subset of private voluntary standards and guidelines that provide detailed technical and organizational instructions that can be used for safety regulation and industrial safety management. These have usually been developed by an industrial standard-setting entity, such as IADC and API, to define methods, processes, products, and practices, and are documented for use by regulators, legislators, companies, and other industrial enterprises, researchers, and professional groups.

A company's own internal standards also encompass the unique set of internal norms, policies, and guidelines about business operations that are developed and voluntarily adopted by each regulated company for its own governance. They need to be compatible with and facilitate company compliance with regulatory requirements and with certification standards set by ISO and others, for example, organizational standards needed to establish the internal controls that will enable the fulfilment of soft law rules and self-regulation initiatives. They reflect organizational judgements and address many other issues, such as relations with suppliers and customers, setting contractual obligations for production, allocating resources for maintenance, improving the resilience of critical facilities, outsourcing hazardous operations, designating job functions, worker training, reporting and evaluation of near miss incidents, etc.

Standards and stakeholders

The standardization process involves the interaction of many players with various interests at stake. The diversity of such stakeholders is determined by the organization that manages the process. If the organization is a professional or industrial association, such as NORSOK or API, participants are likely to be limited to members of the association (e.g. companies), who have similar interests as stakeholders, and selected outsiders, who have relevant expertise.

But if the organization is one that sets standards for broader purposes and societal benefit, such as facilitating global trade or developing a principled approach to a new technology, as is done by ISO, global stakeholders with diverse interests are enlisted in a lengthy negotiation process. These stakeholders may therefore represent the interests of industrial, commercial, financial, and governmental organizations, non-governmental organizations and public interest and advocacy organizations, labour unions, national standards organizations, and relevant professional and industrial standard-setting entities. Thus, the ISO model creates a global network of knowledgeable stakeholders for each subject it selects for standardization.

However, it is an oversimplification to distinguish between these two main types of standard-setting bodies on the basis of whether they are primarily intended to serve the private interests of an industrial or professional sector or to serve broader societal interests. For example, when it is carried out for private interest, as in the case of developing detailed technical standards for offshore drilling operations, enlightened beneficiaries may include companies who need to improve performance, regulators who want gap-filling expertise, and society at large, which wants more industrial self-regulation.

Lessons learned from Norwegian and US offshore oil and gas regulation

This section draws on experience and lessons learned from a comparative study of risk governance in Norway and the US to prevent major accidents in offshore oil and gas operations and focuses on the different approaches to standardization in these soft and hard law regimes. Further discussion of standardization issues in Norway is presented by Engen in Chapter 15, in this volume.

US regulation and its dependency on industry standards

The US regulatory regime for offshore oil and gas operations is known for its development and use of detailed prescriptive rules to define the methods and practices that companies must follow, and ensures compliance by strict enforcement when necessary. But many of its rules are based on technical and operational standards developed by the American Petroleum Institute (API, see www.api.org/), the most influential industrial association in the global oil and gas industry. API's members include producers, refiners, pipeline and marine

transport firms, and service and supply companies; drawing on their collective expertise, it has enacted hundreds of technical standards and recommended practices for voluntary adoption by its member companies, with some 86, at the last count, for exploration and production activities, and many others, for example, for automation, security, and fracking.

Over several decades, many of its standards have been adopted or incorporated by reference by government regulators, in the US and elsewhere, and have thereby become made mandatory and legally enforceable, and others have been favourably referenced or recommended as acceptable means of meeting the requirements of prescriptive and performance-based rules.[4]

Similar reliance on industry standards is a feature of other regulatory programmes in the US, such as regulation of workplace safety on offshore platforms by the Coast Guard, which boasts that it saves $1.5 million annually by routinely adopting industry standards. According to the National Institute of Standards and Technology (NIST), 'Government agencies use externally developed standards in a wide variety of ways.' That includes formal adoption as their own regulations or by officially referencing a voluntary standard, by permitting adherence to a voluntary standard, or recommending it as an acceptable course of action for industry, or by otherwise deferring to the voluntary standard in lieu of taking other action (http://standards.gov/regulations.cfm). Indeed, such practices are mandated by federal law, the Technology Transfer and Advancement Act (TTAA), which requires that all federal agencies, in carrying out agency activities, use technical standards that are developed by voluntary consensus standards organizations, unless inconsistent with other law or impractical. The 15 USC 3701 Act on 'Standards Conformity' (Section 12(d)) states:

> All Federal agencies and departments shall use technical standards (defined as 'performance-based or design-specific technical specifications and related management systems practices') that are developed and adopted by voluntary consensus standards bodies, using such technical standards as a means to carry out policy objectives or activities determined by the agencies and departments.

The Act further states that 'Federal agencies and departments shall consult with voluntary, private sector, consensus standards bodies, and shall … participate with such bodies in the development of technical standards.' See also http://standards.gov/nttaa.cfm for implementation information.

Thus, it can be said that prescriptive regulation in the United States has co-regulatory features and encourages self-regulation because of several factors, including the regulator's need for technical expertise and desire to avoid the lengthy and costly processes of developing the substantive content of its own rules. Taking the 'short cut' of adopting standards that were developed by the industry itself is also motivated by the assumption that rules based on such standards will avoid conflicts with industry, which could lead to lengthy lawsuits challenging the rules. From an industrial perspective, the regulator's reliance on

its standards provides it with the opportunity to tailor the regime's actions to serve its own self-interest (Mattli and Büthe, 2003; Verkuil, 2007).

Virtually all the numerous rules and standards that the US regulator of offshore operations (previously the Minerals Management Service, MMS, currently the Bureau of Safety and Environmental Enforcement, BSEE) has enacted or adopted by reference from API are prescriptive and technically detailed and require company compliance in the design and conduct of a proposed operation. Reliance on API has therefore enabled the regulator to capitalize on API's technical expertise and ability to gain industry consensus. But it has also created a situation in which API controls the pace at which advances in safety become part of the regulatory regime. This became apparent in the aftermath of the massive BP Macondo oil spill in 2011, when it was revealed that neither the regulator nor the API had developed rules and standards that could have prevented some of the root causes of the accident, namely, those that stem from the industry's failure to address unique features of deep water drilling operations, such as cementing stability and blowout prevention methods (Baram, 2014). A manifestation of the 'drift' problem was highlighted earlier by Rasmussen and Svedung (2000).

A regulator's reliance on industry standards and practices must be supervised, to avoid deterioration of its own technical competence and prevent industry takeover of its programme to the extent that the agency does no more than accommodate standards that maintain 'business as usual'. However, more than supervision is needed; it is also necessary to ensure the integrity and objectivity of the industrial and technical organizations that regulators look to for technical support and other expertise. This need is apparent when one considers the conflicting roles played by the API, the leading association of offshore operators. It has developed some 500 standards and practices, many of which were incorporated by the regulatory regime, but it also spends millions of dollars annually to aggressively lobby and coordinate campaigns and public demonstrations against new laws and regulatory initiatives for improving safety, because its members oppose new rules and additional compliance costs.[5]

Another problem arising from dependence on the API and other private organizations is that their development of voluntary standards and practices occurs in private proceedings that have excluded the presence and participation of unions, workers, other industries (e.g. commercial fishing and recreation), and other stakeholders. They may have concerns and intimate knowledge about safety issues and harmful consequences that deserve consideration. To sum up, there is a need to democratize the private standardization process whenever the standards are destined for adoption by regulators, a problem further discussed later in this chapter.

Stakeholders and standardization in the Norwegian regime

Major and fatal accidents, especially the blowout at Ekofisk Bravo in 1977 and the capsizing of the Alexander Kielland platform in 1980, gave momentum to the rethinking and redesign of the regulatory principles in Norway for the safety of offshore oil and gas production. While mobile drilling rigs were classified and

regulated similarly to ships, integrated and fixed platforms on the seabed proved to be too difficult to handle within the same regime.

The technically expert standard-setting organization, Det Norske Veritas (DNV), came into conflict with the newly established Norwegian Petroleum Directorate (NPD). The dispute lasted for some years and, from September 1977, several 'framework agreements' established the future division of regulatory roles (Paulsen *et al.,* 2014). NPD promoted a regulatory model, based on internal controls and enforced self-regulation with harmonization of legal rules on offshore safety, health, and environment. Control functions established by several laws and ministries were delegated to NPD, as was done by the broader Health and Safety Executive in the UK.

The Norwegian regime has been developed step by step in the direction of increased use of functional requirements that are expressed in legislation as *legal standards* (Braut and Lindøe, 2010; Bang and Thuestad, 2014). The framework regulation calls for the creation of 'a sound health, environment and safety culture' by promoting operators' self-regulation (Kringen, 2009).[6] It directly requires them to develop and apply internal control systems, aimed at reducing risks and preventing and responding to accidents. An important element of this regulatory regime is the tripartite system, legally embedded in the Work Environment Act of 1977, with complete collective bargaining rights and a comprehensive network of safety representatives recruited from the unions. The basic principles in the law also became mandatory for the offshore industry (Karlsen and Lindøe, 2006).

At the end of the 1990s, the tripartite governance was strengthened and expanded by new arenas for cooperation. The tripartite group was extended by the Pollution Control Authority and the health authorities and labelled the Regulatory Forum. In the context of offshore safety, an initiative taken by the authority was to create a Safety Forum, where the most important actors meet regularly. The industry initiated two programmes: (1) working together for safety, addressing activities with high-risk potential, and making improvements on installations, industrial standards, and procedures; and (2) organizing the training programme for offshore workers, 'Competence in Rules and Regulations for the Petroleum Industry'.[7]

In 2004, as part of a comprehensive restructuring of the regulatory system in Norway, safety regulation was transferred from the NPD to a new agency, the Petroleum Safety Authority (PSA), leaving the resource management administration with the NPD (Hovden, 2004; Lindøe and Olsen, 2009). Responsibility for a number of petroleum-related land facilities was transferred to the PSA as part of the deal. As part of the tripartite cooperation, a monitoring programme, covering all risk aspects within the PSA´s jurisdiction, has been developed (Vinnem, 2010). Since 2000, annual update reports have been produced, in cooperation with the industry and unions and with support from the researcher community. The programme uses statistical, engineering, and social science methods, including risk perception and cultural factors.

The interpretation and the practice of the legal standards are facilitated by the use of the tripartite arenas presented above and reinforced by regulatory oversight

by the PSA. As discussed by Engen in Chapter 15, in this volume, this may open up conflicts of interests among tripartite actors regarding the use of legal standards and multitudes of possible interpretations of regulatory practice. It also results in proceduralization (Bieder and Bourrier, 2013, p. 3) with the adoption of consensus standards and practices that set precise and quantified safety objectives and, at the same time, instructing how to achieve such objectives. Thus, use of common law concepts does not mean that detailed proceduralization is absent from the Norwegian system. The tripartite cooperation of authorities, operators, and labour unions in problem-solving has created a PSA-managed, non-adversarial approach to building safety systems within each company.

Discussion

Polycentric risk governance and standardization

Risk governance of a hazardous industrial sector involves a regulatory regime with the capacity to prevent and mitigate major accidents. The regime is shaped by the unique interaction of laws, traditions, and norms, institutional and political contexts, harmful accidents, and many economic and societal factors, including industrial policies and practices.

But the regime co-exists with many other entities, national, sub-national, and international, that develop standards based on their mandates, motives, and interests. Thus, risk governance is polycentric in that it involves multiple independent entities in the public and private sectors, addressing various aspects of the risks being dealt with by the regulatory regime. As noted earlier, these entities include industrial and professional associations, labour unions, insurers, and others who engage in setting voluntary standards that command attention and shape regulatory regimes (Carlisle and Gruby, 2017).

Left to itself, this polycentric condition can lead to a diversity of standards that enrich the risk discourse but do not necessarily add up to provide a coherent menu for the regulatory regime. However, it does afford the regulator the opportunity to adopt and enforce any such standards or to propose the development of new standards by these sources, to fill gaps and otherwise enhance the regulatory regime. As previously discussed, both the hard US and the soft Norwegian regulatory approaches encourage and benefit from such standards.

Laws, rules, standards, norms, and guidelines

The convergence of hard and soft regulation presented in this chapter (see Figure 14.2) implies interconnections between laws, rules, standards, norms, and guidelines that occur within the regulatory regime. These connections and the interplay between them are further developed in Figure 14.3.

The top layer (I) of Figure 14.3 consists of laws and the rules enacted by the regulator pursuant to such laws, including any standards that the regulator has adopted and made enforceable, as is often done in the US.

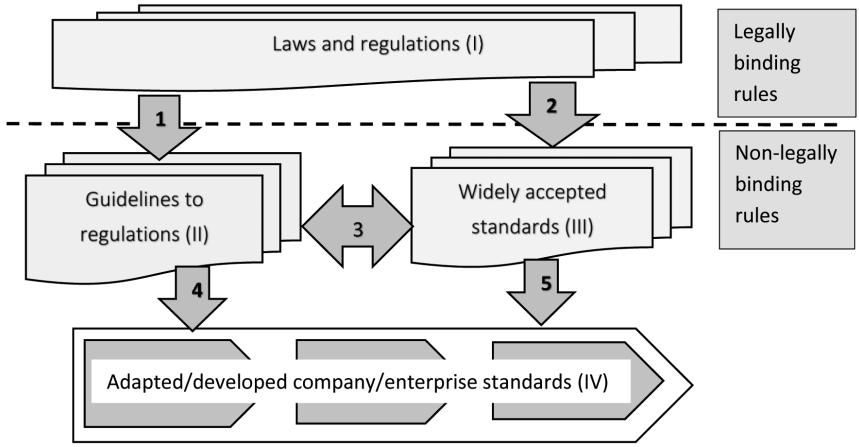

Figure 14.3 Interconnections between laws, rules, standards, and guidelines.

The left track indicates any guidelines to regulations (II) issued by the regulator that are provided to facilitate compliance by the regulated enterprises by adapting and developing internal company/enterprise standards (IV). Such guidelines may be developed by the regulator for a specific enterprise activity, or for an industrial sector, and in either case may be derived by the regulator from widely accepted standards and practices (III). That is the case, as we have seen, in the Norwegian offshore industry.

The right track indicates widely accepted standards (III) that have been voluntarily accepted by regulated enterprises without regulator action or, as mentioned immediately above, may have been taken by the regulator to serve as guidelines (II) and suggested to the enterprises for their adoption (IV).

The applicable laws, rules, selected standards, and guidelines therefore converge on the regulated enterprises and are instrumental in their development of internal policies and internal standards (IV) that shape the conduct of their activities.

As discussed in the offshore cases, numerous technically detailed voluntary standards developed by private sources often become prescriptive rules and require industrial compliance in the design and conduct of their operations, as in the US regime, or are recommended as guidelines for acceptable self-regulation, as in Norway. Thus, in both regimes, the regulator capitalizes on private sector technical expertise and the ability of private standard setters to gain industry consensus.

By developing enterprise management systems (EMS), enterprises relate to laws and rules (I) and guidelines (II), as well as to widely accepted standards (III), in developing their own internal standards, policies, and 'best practices' for design, management, operations, services, and products (IV).

The link between the left and the right tracks points at combining modes of regulation as a convergence of hard and soft law approaches, as earlier presented

in Figure 14.1. Balancing a hard/prescriptive and a soft/performance-based approach presupposes a combined and coordinated use of two tracks. The coordinated approach needs a certain degree of cooperation, confidence, and trust between the regulator and the industrial actors, as well as resources and competence to maintain and develop the industrial standards. A soft and risk-based regulatory regime requires mature industrial actors, with high competence, motivation, and resources to keep technical and industrial standards updated, in the same manner as in the principles of resilience engineering (Hollnagel *et al.,* 2011). One illustrative case on this challenge is presented and discussed by Engen in Chapter 15, in this volume.

Combining rules and roles

The model of converging hard and soft law approaches introduced previously can be described as a hybrid mechanism of the company's bottom-up enterprise risk management (soft regulation) and the harder approach from regulators, involving compliance with legally binding rules. Combining these modes of regulation introduces a possible opening, where the actors have to develop frameworks and rules for interaction. It requires a mutual understanding of how the authorities and industry exercise their roles, how they understand the hierarchy of rules and regulations, how they practise the rules, and how responsibility and authority are distributed.

Figure 14.4 comprises four different areas, A, B, C and D, defined by the two dimensions: horizontally by the two different roles exercised by authorities and vertically by legally binding and non-legally binding rules. Acting with legally binding rules, there is an asymmetric power relation between regulators and the regulated (A and C). By executing the role of facilitator, the regulator needs a symmetrical power balance with the regulated industry (B and D).

Within this leeway, there are two areas with fairly clear rules of the game. In area (A), the regulator exercises Command and Control, based on clear and detailed legal rules as binding entities. In area (D), the process of self-regulation presupposes a dialogue on the same footing, facilitating and developing 'best practice' and continuous improvement. In area (B), regulators guide the industry in implementing laws and regulations, interpreted as widely accepted standards and best practice. In area (C), the regulators engage in the process of developing standards.

Challenges following the combination of rules and roles are further developed in Chapter 15, in this volume. Here, Engen describes dilemmas in conveying conflicting interests within the tripartite organizational field, aiming to maintain a unified standardization process of NORSOK standards.

Standards and legitimacy

When enacting or modifying a rule, the regulator must meet several substantive and procedural requirements, in order to ensure the legitimacy of the rule from a societal perspective and the legality of the rule from a legalistic perspective. The

	Forms of influence	
	Legal control Asymmetrical power relation	Facilitator Symmetrical power relation
Legally binding rules	A Detailed prescriptive 'Command and Control'	B Guidance for implementing legally binding rules
Non-legally binding rules	C Participation in development of technical standards	D Dialogue and cooperation with industry

Figure 14.4 Combining rules and roles.

requirements are those set by the laws that established and empowered the regime, such as the Norwegian and US laws authorizing the regulation of offshore drilling, and additional requirements set by other laws of generic applicability to national regulatory regimes, such as Norway's Working Environment Act and the National Environmental Policy Act in the US (NEPA, 42 USC 4321).

For example, the major US law on offshore drilling, the Outer Continental Shelf Lands Act (OCSLA, 43 USC 1333), directs the regulator (BSEE) to enact rules that require industrial use of 'best available and safest technology' (BAST) and use cost-benefit analysis in making such determinations. In addition, the regulator must comply with generic rule-making requirements of the Administrative Procedure Act (APA, 5 USC 551) for public notifications, transparency of proceedings, and opportunities for public comments that must be responded to by the regulator. Other generic laws also require the regulator to adopt technical standards, as discussed below, and conform to a wide range of social policies, for example, to protect minorities and the disabled against discrimination. Finally, the APA holds that a rule can be appealed to a federal court for judicial review, where it may be rejected if it can be shown that the regulator failed to follow required procedures or enacted a rule that was beyond the scope of its mandate, unsupported by the facts, or arbitrary.

These features of US law provide for democratic anchoring or societal legitimization of regulatory regimes and improve the quality of rules, even though they add complexity, costs, and delays to proceedings (Scalia, 2017). As discussed earlier, opening up the rule-making process to public involvement brings diversity of views and often new facts that enhance the quality and credibility of rules.

Thus, a legitimacy problem arises when regulators disregard democratic anchoring and act summarily by announcing they have favourably referenced or adopted highly detailed, private voluntary standards to amplify their rules and thereby made the standards as mandatory and enforceable as the rules. These standards are most often created by private standards development organizations (SDO), to whom rule-making requirements do not apply. Of most concern are the detailed technical standards developed by industrial or professional SDOs such as API that serve a narrow range of industrial interests, exclude stakeholders, such as labour, environmental, and human rights groups from their deliberations, limit access to their documents and deliberations, and even require that copies of the standards be purchased (Baram, 2014; Mendelson, 2015).

Nevertheless, it is well established that many societal benefits accrue from having industry associations and other SDOs use their expertise to define best practices, set voluntary standards, educate regulators, and reduce the costs of agency rule making.

Regulators in the US and elsewhere must therefore find ways to derive value from SDO activities, while complying with national legitimacy requirements. For the US offshore drilling regime, BSEE outlined its approach in its prescriptive rule on Oil and Gas Production Safety Systems (30 CFR 250, December 27, 2018), and in its responses to over 700 comments from industry and various stakeholder groups, including many that were critical of BSEE's routine adoption of API's standards.

In its explanation, BSEE points to a federal law, the National Technology Transfer and Advancement Act (NTTA Act, 15 USC 3701), as previously noted in this chapter, that requires federal regulators to 'use technical standards that are developed or adopted by voluntary consensus standards bodies as a means to carry out policy objectives', and its adoption of numerous technical standards that thereafter apply to operators, lessees, and other offshore entities. It then claims that legitimacy concerns are satisfied by its practice of briefly summarizing any adopted standards in the preamble it provides for each rule and instructing stakeholders and the public that the full text of such standards can be viewed at its six regional offices and at API for 'read only' or purchase. It also notes that it refrains from printing and disseminating the actual text of such standards because copyright law protects many SDO standards.

This approach to legitimizing the use of standards is unlikely to satisfy critics of offshore operations and other industrial activities, sceptics who worry about industrial capture of regulatory regimes, and advocates of openness and stakeholder involvement in all aspects of risk governance. A deeper approach to the legitimacy issue would require national legislation to extend the reach of a country's rule-making framework to private SDO proceedings or the securing of SDO acquiescence to voluntarily heed the national framework. This would encounter several obstacles: Can national authorities impose such requirements on private standards organizations, especially when the private entities are based in other jurisdictions (e.g. ISO in Switzerland)? Would it call for an international treaty or other global arrangements, and would IMO, Codex Alimentarius, or the World

Trade Organization serve as models for such an undertaking? Clearly, these and other issues would need to be addressed but lie beyond the scope of this chapter.

Regulators as 'orchestrators' of the use of standards

Despite such challenges and weaknesses, non-public or private sector norming is both a natural and necessary part of risk governance in a complex society with rapid technological, cultural, and economic changes. The authorities alone are not adequately equipped, with either resources or expertise, to cover all aspects of safety management and standardization needs. Therefore, interaction between public and non-public norms is necessary. As illustrated by offshore risk regulations, such a networked form of multi-level governance is being structured at national, regional (EU), and global levels.

The role of regulators in this context could be described as 'orchestrating'. They will ensure that different actors and institutions interact in a way that in all things helps to ensure public purposes. However, as shown by Engen in Chapter 15 in this volume on tripartite cooperation on NORSOK standards, authorities face some challenges when they perform this role. Triangular cooperation, as in Norway but absent in the US, entails in itself a complex form of orchestration, by the fact that the regulators themselves are participants but also have the responsibility to have the final say as to what is actually going to be legally sufficient. At the same time, strong competing interests are involved, and there may be uncertainty and disagreement about the knowledge base on which assessments and decisions are based. The actors must manoeuvre in a landscape where both neutrality and professionally motivated decision-making are sought but, at the same time, different interests must be heeded. Different forms of 'politicization' can occur when parties bring different interests into decision-making. This can again have consequences for the norms' legitimacy and effectiveness, especially if the results are not perceived to have sufficient academic or empirical support. In a democratic society, transparency in case preparation and decisions must ensure that such politicization takes place in a legitimate manner, so that the various stakeholders can participate in current processes. This again raises questions about how and to what degree the authorities will participate actively in standardization processes that occur outside the public governance institutions.

Towards a global faceless regime

Standardization as a phenomenon in itself, and as a regulatory instrument, does not have a coherent and unified knowledge base, either nationally or internationally. Concepts, processes for development, documentation, and follow-up of standards may be quite precise and conscious within different sectors of society. However, as a pervasive instrument in a democratic society, standardization does not build on a thoughtful and overarching idea, developing into a global faceless regime (Gustafsson, 2016).

It is important to investigate who are the stakeholders and who should be included in the standardization process. The examples from offshore regulation show that the development of standards in different practices may be in the process of replacing specific requirements given directly through legislation. There are many good reasons why this can be sensible. However, there is reason to problematize this in light of the requirements for participation in governance processes that we usually want to have in a democracy.

Traditional standardization processes have been driven by experts and stakeholders, based on their own needs. The major challenge is therefore to link standardization to collective interests and democratic processes. A global management system, where standards and standardization processes play an increasingly influential role, especially with regard to public safety, can be described as a regime without a face, without a centre, or a periphery. In such regimes, it is difficult to find actors who can be held responsible and accountable for the consequences arising from the use and misuse of standards (Verbruggen, 2018). This may result in normative governance taking place without public awareness, without necessarily taking collective interests into consideration, and where special interests can play an important role. Industrial actors participate in standardization efforts based on a desire to influence technical and other standards, thus enhancing and protecting their own market segments and promoting their own interests (Mattli and Büthe, 2003).

In the same way, professional interests and academic preferences will affect the development of standards, as in the case of SDO certification standards. Confidentiality about certification is a challenge to the standardization regime. When an SDO certification programme has confidentiality vis-à-vis its customers, and an accreditation body has confidentiality vis-à-vis the certification bodies, a certificate could be like a *black box*. Key actors who can help ensure the professional content of the certification can therefore be excluded from important information. The confidentiality requirement also reduces the possibility of learning from the certified businesses and thus the necessary knowledge of both best practice and potential problems.

Conclusion

Balancing or orchestrating hard and soft regulatory approaches is a complex and demanding task. The regulator must take into account multiple factors, legislative and administrative values and norms, the roles and responsibilities of the industry, and the polycentricism of risk governance. Furthermore, regulatory practice is influenced by stakeholder perceptions of risk, which are often of a qualitative nature; the available resources; the power relations among stakeholders and interest groups; as well by the legislative and administrative cultures.

Industry needs predictable frameworks, rules, and regulations to vindicate that its activities and modes of operation fall within societally acceptable norms. The enforcement of regulations that incorporate consensus standards could make activities more predictable and safer. However, the enforcement of rules

imposed by the regulator has some obvious limitations when the industry could be locked into compliance with 'one-size-fits-all' rules, or where safety is trapped into rules that are made more prescriptive by the adoption of technically detailed standards, thereby limiting flexibility and the ability to deal with unique conditions on a case-by-case basis, innovation, and adaption to new technologies (Bieder and Bourrier, 2013). That could also enhance a reactive mindset, based on hindsight, reducing awareness of unexpected events and hazards.

On the contrary, co-regulation or enforced self-regulation, based on performance and functional rules, that enable flexibility, necessitates more permissive legal requirements that do not hamper the ability to choose the best solution in each case, based on industrial standards and best practices. This implies arenas and means for cooperation, confidence, and trust between the regulator and the regulated. Furthermore, such an approach requires mature industrial actors, with high levels of competence, motivation, and resources, in order to keep technical and industrial standards updated. In this case, the regulator, to a certain degree, gives up detailed regulatory control and presumes that the actors are willing and able to collaborate in a continuous development of legal standards. This approach is a challenge for the regulator, as it combines the roles of overseer and controller of compliance with roles as mentor and facilitator to bring about an optimal approach to each regulated activity.

The soft-regulation approach may fail if the main aim of the legislation is to define stable norms that can be controlled and enacted by the authorities in an unambiguous way. It is important that the regulator has a trustworthy role, in order to facilitate a system of learning and improvement within the industries, as well as for the regulator. Finally, the analysed cases provide arguments that support a strengthening of co-regulation and enforced self-regulation, under conditions that foster trust among the parties and the inclusion of stakeholders.

Notes

1 In law and government, *de jure* describes practices that are legally recognized, regardless of whether the practice exists in reality. In contrast, de facto ('in fact') describes situations that exist in reality, even if not legally recognized (https://en.wikipedia.org/wiki/De_jure).
2 See www.iso.org/standards.html.
3 See www.oecd.org/env/ehs/chemical-accidents/Guiding-principles-chemical-accident.pdf.
4 See www.ihs.com/products/industry-standards/organizations/api/index.aspx.
5 'API plans citizen rallies in opposition to energy, drilling reforms,' *Environment Reporter*, 41 ER 1900 (August 2, 2010); also see Baram (2010); and *Environment Reporter*, 41 ER 1899 (August 20, 2010).
6 See the PSA website, available at: www.ptil.no/framework-hse/category403.html (Section 15; Sound health, safety and environment culture).
7 See Bang and Thuestad (2014, pp. 258–259) for a short description of the programmes.

References

Ayres, I. and Braithwaite, J. (1992). *Responsive regulation*. Oxford: Oxford University Press.

Baldwin, J. and Cave, M. (2012). *Understanding regulation*. Oxford: Oxford University Press.

Bang, P. and Thuestad, O. (2014). Government-enforced self-regulation. The Norwegian case. In P. H. Lindøe, M. Baram, and O. Renn, eds. *Risk governance of offshore oil and gas operations*. New York: Cambridge University Press, pp. 243–273.

Baram, M. (2010). Big oil fought off new safety rules before rig disaster. Available at: www.Huffingtonpost.com, 26 April.

Baram, M. (2014). The US regulatory regime for preventing major accidents in offshore operations. In P. H. Lindøe, M. Baram, and O. Renn, eds. *Risk governance of offshore oil and gas operations*. New York: Cambridge University Press, pp. 154–187.

Baram, M. and Lindøe, P. (2014). Modes of risk regulation. In P. H. Lindøe, M. Baram, and O. Renn, eds. *Risk governance of offshore oil and gas operations*. New York: Cambridge University Press, pp. 34–55.

Bieder, C. and Bourrier, M. (2013). *Trapping safety into rules. How desirable or avoidable is proceduralization?* Farnham: Ashgate.

Braut, G. S. and Lindøe, P. H. (2010). Risk regulation in the North Sea: A common law perspective on Norwegian legislation. *Safety Science Monitor*, 1, pp. 1–9.

Brunsson, N. and Jacobsson, B. (2000). *A world of standards*. Oxford: Oxford University Press.

Carlisle, K. and Gruber, R. (2017). Polycentric systems of governance: A theoretical model for the commons. *Policy Studies Journal*. [online] Available at: https://onlinelibrary.wiley.com/doi/abs/10.1111/psj.12212.

Edwards, P. N., Jackson, S. J., Chalmers, M. K., *et al*. (2013). *Knowledge infrastructures: Intellectual frameworks and research challenges*. Ann Arbor, MI: Deep Blue. [online]. Available at: http://hdl.handle.net/2027.42/9/552.

Engen, O. A., Lindøe, P. H., and Hansen, K. (2017). Power, trust and robustness: The politicization of HSE in the Norwegian petroleum regime. *Policy and Practice in Health and Safety*, 15(2), pp. 145–159.

Gilad, S. (2010). It runs in the family: Meta-regulation and its siblings. *Regulation & Governance*, 4, pp. 485–506.

Gustafsson, I. (2016). Organisering av standarder, certifiering och ackreditering som en global styringsregim. PhD dissertation, Gøteborgs University.

Hollnagel, E., Pariés, J. Woods, D. D., and Wreathall, J. (2011). *Resilience engineering in practice: A guidebook*. Farnham: Ashgate.

Hopkins, A. (2011). Risk-management and rule compliance: Decision-making in hazardous industries. *Safety Science*, 49(2), pp. 110–120.

Hovden, J. (2004). Public policy and administration in a vulnerable society: Regulatory reforms initiated by a Norwegian commission. *Journal of Risk Research*, 7(6), pp. 629–641.

Karlsen, J. E. and Lindøe, P. H. (2006). The Nordic model at a turning point? *Policy and Practice in Health and Safety*, 4, pp. 17–30.

Kringen, J. (2009). Culture and control. Regulation of risk in the Norwegian petroleum industry. PhD thesis, University of Oslo.

Lindøe, P. H. (2017). Risk regulation and resilience in offshore oil and gas production. In A. Herwig and M. Simoncini, eds. *Law and the management of disasters*. London: Routledge, pp. 105–123.

Lindøe, P. H. and Olsen, O. E. (2009). Conflicting goals and mixed roles in risk regulation: A case study of the Norwegian Petroleum Directorate. *Journal of Risk Research*, 12(3–4), pp. 1–15.

Lindøe, P. H., Baram, M., and Renn, O. (eds). (2014). *Risk governance of offshore oil and gas operations*. New York: Cambridge University Press.

Lindøe, P. H., Baram, M., and Paterson, J. (2013). Robust offshore risk regulation: An assessment of US, UK and Norwegian approaches. In G. E. Marchant, K. W. Abbott, and B. Allenby, eds. *Innovative governance model for emerging technologies*. Cheltenham: Edward Elgar Publishing.

Lytton, T. (2018). Technical standards in health and safety regulation. In J. Contreras, ed. *Cambridge handbook of technical standards law*. New York: Cambridge University Press.

Mattli, W. and Büthe, T. (2003). Setting international standards. *World Politics*, 56, pp. 1–42.

Mendelson, N. (2015). Taking public access to the law seriously: The problem of private control over the availability of federal standards. *Environmental Law Reporter*, 45, pp. 10776–10782.

National Academies of Science, Engineering and Medicine (2016). *Strengthening the safety culture of the offshore oil and gas industry. Special report no. 321.* Washington, DC: The National Academic Press, pp. 117–119.

Paulsen, G., with Andersen, H., Collet, J. P., and Stensrud, I. T. (2014). *Building trust. The history of DNV.* Oslo: Dynamo Forlag.

Rasmussen, J. and Svedung, I. (2000). *Proactive risk management in a dynamic society*. Karlstad: Swedish Rescue Services Agency.

RIMS (2011). *An overview of widely used risk management standards and guidelines*. Dallas, TX: Risk and Insurance Management Society.

Scalia, E. (2017). The value of public participation in rulemaking. *The Regulatory Review*, University of Pennsylvania. [online]. Available at: www.theregreview.org/2017/09/25/scalia-public-participation-rulemaking/

Short, J. L. and Toffel, M. W. (2010). Making self-regulation more than merely symbolic: The critical role of the legal environment. *Administrative Science Quarterly*, 55, pp. 361–396.

Sinclair, D. (1997). Self-regulation versus command and control? Beyond false dichotomies. *Law & Policy*, 19(4), pp. 529–559.

Verbruggen, P. (2018). *Tort liability for standards development in the United States and European Union.* Working Paper 12/2018. Tilburg: Tilburg University, Institute for Private Law. [online]. Available at www.ssrn.com/link/Tilburg-Private-Law.html

Verkuil, P. (2007). *Outsourcing sovereignty*. New York: Cambridge University Press.

Vinnem, J. E. (2010) Risk indicators for major hazards on offshore installations. *Safety Science*, 48, pp. 770–787.

Zwesloot, G. (2000). Development and debates on OHS system standardization and certification. In K. Frick, P. L. Jensen, M. Quinlan, and T. Wilthagen, eds. *Systematic occupational health and safety management: Perspectives on an international development.* Oxford: Pergamon, pp. 391–412.

15 Consensus and conflicts

Tripartite model and standardization in the Norwegian petroleum industry

Ole Andreas Engen

Introduction

The main aim of this book is to analyse the role of standardization in risk governance. Risk governance refers to a complex of coordinating, steering, and regulatory processes conducted for collective decision-making. The concept of risk governance comprises a broad picture of risk and looks particularly at risk-related decision-making when a range of actors is involved. Such a shift towards more inclusive governance has manifested itself in the tripartite risk regulation regime in Norway. In order to explore how risk governance produces and distributes standards, this chapter addresses how the tripartite cooperation within the Norwegian oil industry is reflected in the standardization work, through the development and designing of the so-called NORSOK standards. The Nordic cooperation model appears on many levels in Norwegian society, for example, in wage negotiation; bipartite cooperation at company level; the state's contribution to research and development, district, and business policy, etc. (Bundum, Forseth, and Kvande, 2015). In the safety field, it has significance through the tripartite institutions, where authorities, companies, and unions together contribute to the regulatory development. This work basically takes place in formal arenas, where the stakeholders meet, discuss, and eventually reach consensus on how standards should be designed and developed.

Hence, this chapter is not about standards themselves but addresses institutional and organizational processes related to the development of standards.[1] In this book, standards are defined as rules that classify objects or actors; rules that that describe organizational behaviour, design, and processes; or rules that include the plans and documentation of organizations and institutions (see Olsen, Chapter 1 and Juhl, Chapter 2, in this volume). We will concentrate on standards concerning organizational behaviour, design, and processes. The development of such standards usually takes place under certain 'rules of the game', where the involved and committed participants agree on what is allowed/what is not allowed during the time of the game. Such 'game rules' are formal and informal, with the participants striving to comply within the boundaries of the rules. Accordingly, the development of standards is an institutional process, where stakeholders express what they want from the standard development

process, which standards to use, how to disseminate them, and decide who should have access. In short, standard development is a negotiation process, in which power and politics are exercised in institutional arenas, which are perceived to be legitimate by the participants involved (Brunsson and Jacobsson, 2000).

The tripartite model is an institutional construction that refers to what Powell and de Maggio (1991) define as an 'organizational field'. Within 'organizational fields', a set of heterogeneous actors with different preferences participate and adjust to a set of common rules and norms. Hence, an 'organizational field' is an organizational unit where common goals and unity can be established (Brunsson and Jacobsson, 2000). Using the tripartite construction in the standardization work may therefore be interpreted as an attempt to institutionalize standardization, provide legitimacy, and anchor the standards among the stakeholders.

In the following, we introduce the concepts, 'organizational fields', 'regulatory regimes', and 'the Nordic model'. This is in order to clarify how standardization and standardization processes take place in the hierarchy of norms and how they function as governance instruments in the industrial organization of the Norwegian oil industry. Second, we need to describe how standardization processes mirror the mechanism of the tripartite system. The tripartite system is not a formal organizational body but a voluntary construction, where the different parties seek to solve disagreements and conflicts. An important part of the chapter is therefore to discuss reasons for this institutionalizing process to succeed; the factors that prevent it from being successful; and the factors that have threatened to explode the tripartite collaboration in the standardization process from the inside. To illustrate these reasons, we present four cases: (1) ownership and financing; (2) the revision of Health, Safety and Environment (HSE) standard S-002; (3) the NORSOK analysis project; and (4) internationalization. The chapter explores dilemmas that occur when organizing a unified standardization process, while simultaneously balancing trust and power among stakeholders with diverging interests. The cases are based on interviews with key actors in the Sector Board, performed in April and May 2018. For more detailed descriptions on cases 2 and 3, see Jonassen (2018).

Organizational fields

The term 'organizational fields' has its origins in the 'new institutionalist' tradition in organizational theory, a school that has emphasized how organizations and their activities are interwoven in major organizational and institutional systems (DiMaggio and Powell, 1983; Powell and DiMaggio, 1991; Scott, 1998; Morgan and Sturdy, 2000). According to DiMaggio and Powell (1983, p. 148), they are 'those organizations that, in aggregate, constitute a recognized arena of institutional life: key suppliers, resource and product consumers, regulatory agencies, and other organizations that produce similar services or products'. More specifically, the institutional arena where standardization takes place is described by the following three key elements:

1 *Actors*. Organizational fields consist of a broad set of actors: in this field, companies and organizations. In this context, 'companies' refers to oil companies and suppliers. 'Organizations' refers to all collective associations of actors that become effective in specific processes, such as industry organizations, trade unions, and state actors – that is, ministries, directorates, and research institutions. In other words, the 'organizational field' is a meeting place, where political and private actors encounter one another, and where knowledge and resources are unevenly distributed. In our context, the specific meeting place will be NORSOK's cooperation on standardization.
2 *Institutions*. The 'organizational' field is rooted in a broad set of institutional frameworks, which affect and limit the actors' actions in different ways. These institutions can be described as 'cognitive, normative and regulatory structures and activities that provide stability and meaning to social behavior' (Scott, 1998, p. 133). Actors and institutions create a structure that is built up of three different elements: (a) formal rules that mainly reflect back to laws and policy guidelines; (b) informal normative guidelines, which include codes, norms, and conventions; and (c) cognitive-cultural thinking, which is related to the common beliefs and belief systems that exist in a given social field.
3 *Decisions*. One last characteristic of an 'organizational field' is that it collects a set of actors and actualizes a set of institutional guidelines concerning a particular type of decision-making process, that is, the standardization process. At the same time, it is a key aspect that the actors involved in these decisions have several roles. The players involved will mainly focus on other tasks (oil production, security work in general, policy design, trade union policy, etc.), but they enter this particular organizational field when a specific type of problem is actualized and when, as a result, a certain type of decision must be taken.

The organizational field designed here for analysing the standardization work is thus part of the institutional framework that constitutes the Norwegian model and the Norwegian regulatory regime. Accordingly, the chapter seeks to show how the organizational field as it appears in the tripartite arena, where work is being developed for regulatory development and security, is being applied to NORSOK's work on standardization. This implies that the same actors, interests, conflict lines, and alliances tend to overlap in the areas where the tripartite construction occurs or in the Norwegian oil industry in general.

Risk regulation and internationalization

High-risk regulatory regimes have been in the forefront in developing regulations based on function, purpose and goals (Gilad, 2010; Short and Toffel, 2010; Hopkins, 2011). Such a regime rests on the assumption that the involved parties have a common interest in maintaining the system, and that the conflicts of interest that may arise will naturally be solved without threatening the foundation

of the trust between the involved parties. How much power each of the involved agents actually possesses will vary, depending on many variables (e.g. context, risk perception, severity of incidents). The new era of free trade and globalization causes constant reorganization in industries trying to seize opportunities and increase competitiveness. High-risk industry today therefore is undergoing major changes, due to downsizing and mergers, which inevitable affect and challenge the safety level of the industry.

Principles of enforced self-regulation (functional regulations) rely on the capability of the industry to manage its own risks according to accepted norms and standards. However, such processes are vulnerable, due to the comprehensive, frequent, and multifaceted patterns of interaction among government, operators/suppliers, and labour unions. Functional risk regulation requires a balance of power and mutual trust among the intervening actors. Function-based regulation thus needs some form of discretionary criteria – 'legal standards' – that link functional requirements in the law to industrial standards.

Legal standards refer to norms and practices existing alongside the law that change over time, such as the consequences of new technology, organizational procedures, and historical and social contexts. Legal standards tie the unchanging word of law to the ever-changing implementation of the norms and ideas embedded in that law. The use of legal standards aims to achieve an appropriate level of regulation in highly dynamic industries and to ensure the safety and quality in key areas of society in changing circumstances (see Lindøe and Baram, Chapter 14, in this volume; Haugland, 2015).

Consistent application of a function-based regime requires a comprehensive and systematic review of how the various provisions are understood and how the appropriate standards should be used in order to meet the requirements. Procedures must stipulate relationships between laws, regulations, and technical/professional standards. For the regulatory authorities and inspectors, this can be a demanding and comprehensive system to update, and it requires that the standards keep pace with global requirements (Bieder and Bourrier, 2013). There is an inherent tension between following comprehensive guidelines and best practice and the desire to require industry to continually innovate and implement any new expertise and scientific knowledge that may improve safety. Risk regulation with stakeholder involvement requires a balance of power between state control and industrial degrees of freedom. A function-based regulatory system is, from such a perspective, flexible, adaptable, and expedient regarding globalization processes (Coglianese, 2010, 2019). On the other hand, if the power balance deteriorates, the system may become ineffective with respect to both innovation and safety.

The Nordic model

This book emphasizes how risk governance is embedded in everyday social and institutional practices and how it supports or challenges Nordic values, such as democratic participation, equal opportunities, personal freedom, etc. In terms of risk regulation and governance, 'the Nordic model' refers to a high degree of

formalized industrial relations. This implies a centralized regulatory structure within the national government but, at the same time, a trinity of cooperation among employers, employees, and the government, concerning economic policy, exchange of information, and consultation. In Norway, this model of industrial organization also supported a national system for the collective negotiations between employers and employees and, moreover, contributed to the maturation of the oil companies, according to the formal and informal rules of the Norwegian setting. Unlike in the United Kingdom and the United States, in Norway, the working conditions offshore were subjected to the same legal framework as working conditions onshore. The Environmental Act in 1977 gave employees in Norway extended privileges in general and became a powerful instrument for offshore workers in terms of influencing security and safety regulations. A safety deputy, for instance, had the same power as the platform manager to stop the production stream if there was any suspicion of technical or organizational irregularities that could increase the risk of undesirable incidents (Hernes, 2006; Engen *et al.,* 2013).

'The Nordic model' refers to institutional frameworks organizing and regulating negotiations, wealth distribution, and conflict resolution. Conflicts between parties are solved through extensive laws and systems of agreements. Historically speaking, the Nordic model implied that employers supported unions and their professional activities to a certain degree. Moreover, employers have been forced several times to de-emphasize short-term profit goals to advance longer-term managerial objectives. The success of this policy may be explained by the strength of the unions in national and local political processes. From this perspective, we may say that the Nordic model has functioned as a stabilizing factor in Norwegian politics and society. It has formed and shaped the political strategies, concerning how to balance a growing resource economy with other economic sectors, how to find a balance between the public and private sector, and, finally, how to consider challenges created by the fact that oil is a non-renewable and exhaustible resource (Engen, 2014).

In terms of safety, 'the Nordic model' is embodied in the tripartite collaboration, involving employer, employees, and the government. A common feature within the tripartite system is the in-house use of an occupational health and safety organization that offers three different collaborating structures. First, safety committees provide opportunities for employer and employees to meet and discuss important issues. Second, there are independent and autonomous safety representatives, such as safety deputies, and, third, there are a number of experts on occupational health and safety, who may be called upon in disputes, either as an in-house service or as external expert consultants. Hence, safety and an optimal working environment constitute one of the cornerstones of the model.

A system based on trust

The Norwegian regime provides an illustration of the role of trust within the tripartite system. In the balance of power between the authorities, industry, and

unions, the legal framework seldom provides a clear-cut threshold for acceptable risk and regulatory compliance. Kringen (2014) points to reputational concerns and a compliance-friendly regulatory incentive structure as the reason for a lack of sharp confrontations over legal issues and very few lawsuits. Enforcement strategies with legal alternatives regarding industrial response strategies rely on functional trust for the best results. The regulator may also escalate enforcement and sanctions along the trust–distrust dimension. Rosness and Forseth (2014) use a narrative of the tripartite collaboration with periods of erosion, conflicts, negotiations, joint action, and subsequent revitalization to emphasize that all stakeholders as a whole have to work to ensure trust and reputation.

Within the two-fold 'system logics', the regulator must trust the companies and their ability to develop robust and resilient systems and procedures for safe work, both for themselves and their suppliers. Further down the value chain, oil companies must trust contractors, subcontractors, and employees to perform their work according to agreed rules and standards of quality and safety. Trade unions have to trust that companies and merchants have established the right supervisory and control chains.

In a study of safety culture on an oil platform, Tharaldsen (2011) discusses how trust and distrust can occur in functional and dysfunctional features through a variety of possible combinations, as presented in Figure 15.1. Based on realistic precautions, trust may be functional (1), but too much confidence may lead to a dysfunctional relationship when there is naïveté and blind trust (2). On the other hand, distrust may be functional when the relationship contains realistic precautions (3), while dysfunctional distrust may occur in rigid control strategies (4).

In the process of value-creation, professionals are interrelated, and dependency can be denoted as *trust-chains* (Grimen, 2009). A high degree of trust promotes the flow and quality of information and reduces complexity and transaction costs (Luhmann, 2017; see also Virta, Chapter 8, in this volume). Confi-

<table>
<tr><td></td><td colspan="2">Trust</td><td></td></tr>
<tr><td rowspan="2">Functional</td><td>1

Trust based on realistic precautions</td><td>2

Naïve and blind trust</td><td rowspan="2">Dysfunctional</td></tr>
<tr><td>3

Distrust, based on realistic precautions</td><td>4

Distrust based on detailed surveillance and control</td></tr>
<tr><td></td><td colspan="2">Distrust</td><td></td></tr>
</table>

Figure 15.1 Trust model.

Source: Adapted from Tharaldsen (2011).

dence and trust among actors create positive expectations about others' intentions and behaviour in the chain and reduce complexity, but they also introduce vulnerability. As Figure 15.1 illustrates, too much confidence may turn into naïveté, while too much distrust may end up in rigid control strategies (see also Figure 14.4, in Chapter 14).

The two partite and tripartite arenas are organizational fields composed of dichotomous issues. They consist of common interest and conflict of interest, alliance building and division, and trust and distrust. Common to all arenas, especially on the tripartite level, is the fact that the authorities play a significant role. The authorities' role is not always formal and can switch between that of passive observer to that of a more active participant. Often the authorities take the initiative to establish the arena but subsequently retire later in the process. In this chapter, it is important to underline that the action patterns that characterize one organizational field are also recognized in another. Often the same players participate and express the same interests and, accordingly, transfer the same conflict patterns from one organizational field to another. We thus can talk about a correspondence between different organizational fields, illustrated by tripartite constellations from safety forums and regulatory forums transferred to the standardization bodies in NORSOK.

Standardization in NORSOK

In 1993, the establishment of the NORSOK programme took place. Initially, the NORSOK programme had a far broader goal and mandate than standardization. The aim was to reduce the total cost of the Norwegian continental shelf by 50 per cent. The NORSOK programme mirrored the Norwegian cooperation model, with the key actors, that is, oil companies, suppliers, and the main trade union, LO (*Landsorganisasjonen*), acting as partners. The smaller and independent trade unions (later SAFE: *Sammenslutningen av Fagorganiserte i Energisektoren*), chose not to participate during the process (Engen, 2002). The task of the working group responsible for standardization was 'to prepare a set of common technical standards for oil and gas drilling and production facilities where the standards aim at significant savings in cost and time'.

The standardization effort required extended cooperation and a significant degree of common interests and legitimacy among the participants. The process could not be taken care of by one company alone or merely be an industry affair. Consistency between the participants in general and openness and broad anchoring among all actors in the oil industry had to be ensured. Accordingly, the standardization work had to be based on the tripartite model. At the same time, the work required competence from parties not included in the tripartite constellation initially and also knowledge not possessed by the tripartite members alone. Hence, other players had to be welcomed on board. The standardization processes required new resources and a clear and strong inclusion of research. All recognized that the tripartite arenas were not always appropriate for developing this kind of skill and understanding.

The first NORSOK standards were developed in cooperation with all involved parties and based on the common experience from the Norwegian Continental Shelves (NCS). The working form was 'the Norwegian cooperation model' and the standards were available to all. The standards were thus 'owned by' all actors involved in the Norwegian oil activities. This was to change after the 2000s. Accordingly, the processes concerning further standardization also changed. Today, the NORSOK standards are owned by the Norwegian Oil and Gas Association, the Federation of Norwegian Industries, and the Norwegian Shipowners' Association. A new ownership agreement was signed on April 15, 2015 that regulates the cooperation and obligations between the parties. At the same date, the NORSOK owners and Standards Norway signed a contract, which deals with how Standards Norway manages and organizes the NORSOK standards on behalf of NORSOK's owners. Roles and responsibilities are now regulated through the owners' agreement, the contract of employment, and the annual allocation letter from the owners to Standards Norway.

The Sector Board Petroleum takes care of the tripartite cooperation. There are clear links to the tripartite institutions of the oil industry and the organization of standardization processes. It is, however, of equal importance to emphasize that there are several other key actors involved, primarily from industry and from the research sector – that is, experts responsible for the technical and quality aspects of the standardization process not bound by interest constellations from the tripartite arenas. Sector-controlled oil standardization committees are appointed by Standards Norway's board of directors and are intended to ensure the relationship between Standards Norway, the owners, and users of the oil standards. Responsibilities of the Sector Board are:

- to lead standardization activity in the Norwegian oil industry, including the strategic work programme and budget;
- to contribute to securing finance;
- to help to facilitate necessary company contributions/voluntary resources;
- to allocate personnel resources;
- to approve new and revised NORSOK standards;
- to propose new, or contribute suggestions for revisions of, international standards (NORSOK analysis report).

Box 15.1 details some of the roles involved in NORSOK.

The following are represented on the Sector Board: Petroleum: Norwegian Oil and Gas (chair and three members), the Federation of Norwegian Industry (deputy chair and three members), the Norwegian Shipowners' Association (two members), Det Norske Veritas Germanischer Lloyd (DNV GL) (one member), SAFE (one member), LO (one member), Lederne (one member), Petroleum Safety Authority PSA-N (one member) and Standards Norway (one member).

Box 15.1 Roles in NORSOK

Business manager oil standardization

The business manager for oil standardization in Standards Norway leads its secretariat for the oil area. This person serves as the secretary of the Sector Board Petroleum and reports on the status and progress of its activity.

Secretariat in Standards Norway

The secretariat's job is to manage and facilitate standardization work for the oil area in Standards Norway within the specified disciplines in line with the strategy, action plans, and budgets adopted by the Sector Board Petroleum. That includes relevant international activities and the NORSOK industry standards.

Expert groups

The members and chairs of expert groups are technical specialists from the Norwegian oil industry, selected in collaboration with Standards Norway. Their job is to develop and revise the individual standards and to look after the industry's interests in the specific disciplines. Through standardization work, suppliers and clients develop a necessary sense of industry community

Source: NORSOK analysis project

Organizing the standardization work

The organization of standardization work in NORSOK follows the same principles as those of International Organization for Standardization (ISO), where different technical committees accomplish quality assurance and provide general support to ensure that the standards fulfil their purposes. ISO consists of a number of subcommittees, which in turn are responsible for different working groups. Within the ISO system, conflict of interest relates to national and industrial inequalities. In particular, national protests have emerged in recent years, causing the work in certain areas to cease, with the result that some countries have decided to withdraw from the ISO family. This demonstrates a central prerequisite for all standardization work. It depends on the stakeholders' willingness to compromise and that these compromises are achievable and consistent with the qualitative requirements set by the different expert groups. Accordingly, the work within ISO struggles because some countries have not been willing to follow its obligations, claiming separate national requirements and thus sabotaging cooperation.

In general, standardization work follows three main principles: (1) influence from expertise and research; (2) end-user orientation and stakeholder participation; and (3) representation. These principles are closely positively interrelated. Ideally, the experts should be neutral and independent, but, in practice, they

bring with them their interests and values, and sometimes also conflicts develop between different expert groups. End-user orientation and stakeholder participation attempt to ensure broad involvement from all parties. Representation contributes to ensuring that the procedures regarding selected standardization alternatives follow democratic principles, that the individual groups feel properly heard and recognized, and that the processes are adequately rooted and legitimized.

The NORSOK standards have embraced all the above-mentioned organizational principles, in particular the involvement aspect basically because of the tripartite participation in the Sector Board but also because NORSOK historically was based on the Nordic model. In recent years, however, the employee side claims that these traits have become less clear – because of the commercialization of the NORSOK standards and the reduction of tripartite influence on the Sector Board.

Standardization work in practice: four cases

The standardization work in NORSOK is no different from the corresponding organization and processes in, for example, ISO and European Committee for Standardization (CEN). This is, as underlined above, reason to assert that the representation principle and end-user orientation, particularly emphasized as tripartite cooperation, is so strongly reflected in the Sector Board. This is what we refer to as 'transfer of an organizational field' – where the norms and rules of tripartite are recreated – in the work on NORSOK standards. Most of the standards have a technical character with the aim of maintaining quality and competitiveness in development and operation. Risk management and HSE, represented with their own standards (Z-013 and S-002), however, attract attention from the involved parties and are considered of high importance.

Hence, HSE has been the subject of several conflicts in the Sector Board, where the parties have different views about the content of the standards and how to organize the processes. The way in which the stakeholder participation proceeds affects the degree of anchorage and legitimacy in the standardization processes. In the following section, we will briefly present four cases that show how the tripartite relationships generate tensions in the organizational field of the tripartite model and illustrate how trust and power relations reveal themselves in the standardization processes. The three areas are: (1) ownership and financing; (2) the revision of HSE standard S-002; and (3) the NORSOK analysis project. The fourth topic concerns internationalization, that is, how the NORSOK standards relate to international standards, and how some standardization organizations operate in order to conquer industrial positions.

Ownership and financing

At the outset, all NORSOK standards were freely available and could be downloaded and distributed by everyone. This changed in 2015. After a decision by the Sector Board, the NORSOK standards had to be purchased and therefore

were subject to copyright. Most standards became commercialized, which means that a company must have some form of subscription in order to apply. The decision was passed against the vote of one of the trade unions, SAFE.

The decision to commercialize the standards did not happen without debate. Some representatives from the industry believed that many of their members could benefit from free standards. For many small companies, payment services would mean additional burdensome costs. Several on the employers' side were sympathetic to such arguments, but the fact that the standards were copied and sold internationally, and that the authorities refused to subsidize further development of the standards, led to the employer, the PSA-N, and Standards Norway voting together in favour of introducing payment services.

A payment system was first introduced for standards without the HSE label. At the outset, the workers' side was sceptical, and, for a while, it was a matter of even greater disagreement. However, a compromise proposal that suggested that union and safety deputies in companies could gain free access to all NORSOK standards solved almost all the conflicting issues. The Sector Board also stipulated that all employee representatives should have access to all standards a company subscribed to. Such a solution had probably been the case all along, but the decision of the Sector Board clarified it. Notwithstanding, payment for the standards meant a significant increase in revenue. The majority of the union representatives voted therefore together with those in the Sector Board who were concerned about how to strengthen the financial muscles of NORSOK and to intensify the progress of the revision of the standards.

One union representative, SAFE, claimed that this was a violation of the ideal goals of the NORSOK cooperation, in particular, and of tripartite cooperation of standardization, in general. The union argued that payment services reduced the power and influence of the employee side. Actually, the union claimed that ownership gave the employers a kind of copyright to the standards and that unions actually could be criminally liable if they shared information about standards with others.

The revision of HSE standard S-002

The example of the payment system illustrates opposition in the Sector Board, where only one of the members from the employee side stood alone. In other words, there was nearly consensus among all the other members. Other processes were more complicated and revealed how power, trust, and interests interplayed in a complex mix. The process associated with NORSOK standard S-002 on Working Environment is a good illustration. We will thus go systematically through this narrative to confirm the value-laden and politicized character of this particular standardization body – characteristics that largely apply to standardization bodies in general (Brunsson, Rasche, and Seidl, 2012).

The revision of NORSOK S-002 started in autumn 2013; the PSA-N and the trade unions were active participants in the audit work, that is, as participants in working groups and in an expert group. In 2016, the first revised draft was subjected to consultation, which initiated a number of comments.

In order to assist the expert group to evaluate the many consultation comments, the Sector Board appointed a reference group, consisting of PSA-N, employers, and employees' representatives. The mission of the reference group was to evaluate, sort out, and systematize the comments. After a considerable effort, it was possible to deliver a consensus proposal for a new revised NORSOK S-002. Only SAFE dissented. The submission of a revised NORSOK S-002 to the Sector Board for approval took place in the autumn of 2017.

As the PSA-N had participated in the reference group, it was thus surprising to the employers' side that the PSA-N, with one day's notice before the meeting at which approval should take place, made a claim that the revised NORSOK S-002 was of poor quality, which also implied that the PSA-N would refrain from approving the standard. The Sector Board therefore decided to call for an extraordinary meeting, at which the PSA-N had to explain why they had reached such a conclusion.

Consequently, the Sector Board decided to set up another tripartite group to assess the new comments from PSA-N and the unions and from others who might have additional comments in the aftermath. It is worth noticing that the NORSOK owners were always in a position to push through the approval of the standard through a majority decision in the Sector Board. The NORSOK owners claim, however, that they chose to abstain from such an option and, instead, chose dialogue as a way out of the conflict.

Seemingly, the dialogue strategy succeeded, and, in March 2018, the submission of another revised draft took place. This draft had the PSA-N's support, while the union, SAFE, still dissented. According to the employers' side, there was great surprise when the largest union, LO, now declared that they could only approve the new proposal if new revisions of the standard commenced immediately. This requirement created a major debate in the Sector Board. In particular, the Norwegian Shipowners' Association responded strongly by referring to how every standard revision led to increased compliance cost.

It is, however, the Expert Group which suggests and proposes new revisions, based on its assessments. As a solution, it was decided in the Sector Board that the draft should be assessed by the Expert Group during 2018 and that the Expert Group should evaluate LO's audit requirements. Hence, the approval of revised NORSOK S-002 passed in the Sector Board meeting in March 2018 and, eventually, the publication of NORSOK S-002 – revision 4 could take place.

Why so much reluctance regarding the proposal for the new S-002? The reason was primarily disagreement about the text in the sketches and, as mentioned, different perceptions as to whether the proposal for the new S-002 was sufficiently consistent with the regulations in general. The task of the individual members of the Sector Board is, after all, to try to influence each case and disagree where and when the standard proposals are considered to cross the interests of the individual participating organizations. In addition, the revision process was challenging to lead. It took a disproportionately long time and was eventually affected by low oil prices and companies' need for cost reductions. This substantially changed the conditions. And even though there are two separate

issues, the process associated with the NORSOK analysis project may also have negatively influenced the cooperation climate in the Sector Board.

NORSOK analysis project

The aim of the NORSOK analysis project was to update the NORSOK owners on the portfolio of the standards. According to the NORSOK owners, it appeared that the work on NORSOK standards in the period 2008–2014 had lost momentum. In the same period, the world oil price reached an all-time high level, which reduced attention to the continuous development of cost-effective organizational and technical solutions. The NORSOK analysis project delivered its report in December 2016. Besides the evaluation of NORSOK standards, the report also contained a critical discussion of both the working procedures in the Sector Board and the tripartite influence in general.

At the same time, the petroleum companies and companies among the service industry had implemented a number of specific, inappropriate, and unnecessarily complicated requirements (Austnes-Underhaug *et al*. 2011). Accordingly, the main goal became to revitalize the purpose of the original NORSOK work, namely, how to reduce costs. The initiative for the NORSOK analysis project came from Norwegian Oil and Gas Association, which brought along the other NORSOK owners, the Norwegian Shipowners' Association and the Federation of Norwegian Industries. Neither the authorities nor the unions received an invitation to participate. According to the Norwegian Oil and Gas Association, the reason was a need to 'clean up your own house, and therefore [it was] not appropriate to have all the parties involved in the process'. To further quote one of the NORSOK owners, 'They constantly updated the Sector Board, anyway.'

Despite apparently legitimate arguments, the overriding concern of the tripartite institution was perceived as a demonstration that the employers' side and the industry wanted stronger governance and control of NORSOK standards. This is also confirmed in the final report, especially in the discussion about the government's role in the Sector Board. Here the employers' side does not hide the fact that they want to clarify the role of the authorities, but what they explicitly mean by 'such kind of clarification' is not expressed further.

Internationalization

As mentioned above, there are a number of standards in the global oil arena. One of the main official objectives of the NORSOK owners is to increase the use of NORSOK standards, particularly where Norwegian companies are involved. However, and as indicated above, there has also been increasing interest in the NORSOK standards among international players, an interest which has also actualized the competitive relationship between ISO, NORSOK, CEN, and American Petroleum Institute (API) standards. Today, Standards Norway develops standards in most areas of society, apart from the telecommunications and electronics council. Standards Norway is Norway's member of the European

standardization organization, CEN, and the international standardization organization, ISO. As the Norwegian member, Standards Norway is obliged to determine and publish CEN and ISO standards as a Norwegian standard, in accordance with CEN and ISO administrative directives.

However, in recent years, the relationship between API and ISO has deteriorated, officially due to the embargo against Iran and Russia. The long cooperation between ISO and API has broken down, and it has been reported informally that API is operating as an aggressive commercial actor, supporting American firms and interests exclusively, trying to outnumber other standards (see also Lindøe and Baram, Chapter 14, in this volume).

According to Standards Norway, this is serious situation for two reasons; first, the Norwegian and the international oil industries have experienced a number of mergers among the great international supplier companies. An important part of such a positioning has been increased collaboration with the oil companies associated with the American Petroleum Institute (API) to design a new set of technology standards. The aim has been to find cheap standard solutions that can be mass-produced. It may sound like a natural adaptation to a new era of lower oil prices, but experience with corresponding standardization processes indicates that the specifications are tailored to the capabilities of the companies that are designing them. API has also launched an aggressive strategy to establish its standards as dominant in all offshore markets globally. The interpretation of API's retirement from the International Standard Institute, ISO, is thus American protectionism, combined with global ambitions.

National industry standards, such as NORSOK, cover the identified gap between international standards and the Norwegian requirements, where these are the most appropriate. Consequently, the development and maintenance of NORSOK standards are intended to expand and maintain the Norwegian industry's competitiveness nationally and internationally, while allowing it to pursue its operations safely and acceptably. But what happens if the companies feel threatened to choose standards more compatible with API? An aggressive API will thus threaten the international competitiveness of the Norwegian-based supply industry and undermine tripartite collaboration in NORSOK.

The strengths of the Norwegian regulatory regimes are vigorous stakeholder involvement and adopted capability-building between the industry and the regulatory body. The tripartite system is tailor-made to ensure large stakeholder involvement in safety discussions. However, there are vulnerabilities in such a function- and trust-based regime, where, for instance, global political and economic issues can easily weaken trust between the parties and undermine cooperation. Similarly, the win-win principles between safety and the economy during economically difficult times are challenging to maintain. When continuously confronted with global challenges, small economies may have to adjust to safety regulations and standardizations that are less adaptable to national styles and traditions, thereby inevitably being forced to change and harmonize their regulatory regimes.

Trust and power

The standardization processes mirror all other tripartite arenas. Our cases illustrate a functional but vulnerable and complex system, consisting of trust and power relations and inconsistent processes, characterized by consensus orientation and conflicts.

The employers' side does not want to be dominated by state actors and, to some extent, is striving to release the standardization work from other regulatory developments – among others to be able independently to evaluate the cost-benefit aspects of all standards – including HSE standards. The PSA-N argues for involvement in the standardization work, based on its competence and responsibility as the supreme quality controller of the regulatory framework. Such arguments are supported by the unions and Standards Norway and, eventually, also accepted by the industry. The authorities have thus consolidated their role concerning the development of the NORSOK standards, as they increased the number of representatives on the Sector Board and secured a number of representatives in the working groups.

At the same time, the employers warn about the danger of mixing roles, because representatives of the working groups also meet each other in the inspection context. In some cases, it may be tempting to use the inspection role strategically when discussing individual standards. On the other hand, the government's task is to ensure that the standards are designed to be in line with the regulations. It is thus important to emphasize that, in principle, the industry is responsible for the quality of industry standards. The PSA-N's role is to contribute to the design, so that the authorities can refer to them in accordance with general regulations and guidelines.

NORSOK standards related to HSE create the most turmoil on the Sector Board. The HSE discussions challenge tripartite cooperation and clearly mirror the interests of employers and employees as they are expressed in the Safety Forum and in the Regulatory Forum. The transfer of the tripartite model to new contexts does not change the basic conflict lines – which explains why some of the employers probably want a reduction in the tripartite institution's influence in the standardization work.

Role mixing occurs in all the other tripartite arenas in the oil industry. On several occasions, the employers' side has pointed out that relations between union representatives and the PSA-N are too close. On the other hand, there are several cases where the employees' side claims that the PSA-N is not listening to them. The PSA-N has a challenging role when facilitating a well-functioning tripartite partnership, in which they must navigate between the requirements of employers and employees, simultaneously exercising the role of authority. The task of government is to establish dialogue with the different parties, to both set the leeway and develop the rules. In such contexts, the authorities must balance on a thin line when developing trust relationships, on the one hand, and exercising legitimate power, on the other (Engen *et al.,* 2013; see also Figure 14.4, Chapter 14).

Politicization and competitiveness

The main aim of this chapter is to reveal the dilemma of successfully maintaining a unifying process of standardization, while simultaneously upholding legitimacy and balancing power and trust between powerful stakeholders with diverging interests. This implies discussing how different legitimacy considerations are taken into account when establishing a normative basis, for example, through participation and user involvement in the design of the standards, and, furthermore, to discuss professional/legal/political legitimacy problems that may arise on the path from democratic processes and resolutions to concrete solutions and outcomes. The function-based regulations in the oil sector provide considerable leeway for the relevant players of the regime. This leeway opens up choice between multiple solutions and thus introduces different interpretations of what is the best solution.

Politicization, in the sense that the various relevant actors seek to secure their interests, is thus a natural part of the regime and the basis for its dynamics and functionality. Ideally, standard development should be a harmonious and exclusively professionally based process, where conflicts of interest and alliance-building are absent. In practice, however, there is significant evidence of value conflicts occurring in all standardization bodies – even where the committees consist exclusively of independent experts (Brunsson, Rasche, and Seidl, 2012). When, in this chapter, we emphasize the organization of NORSOK standards in an organizational field, it is to pinpoint how participation and user involvement express themselves and challenge the regulatory regime's general requirements of responsibility, legitimacy, and effectiveness.

Compliance in a function-based regulatory regime rests on a number of assumptions, not least trust between those who design the regulations (authorities) and industry partners on the employees' and employers' sides. Trust is a positive variable. Trust refers to those whom the actors rely on and whether those they thereafter interact with will act in an expected manner. Trust reduces the need for complicated control functions and enhances efficiency (see Figure 15.1). Extensive use of functional regulations, however, also opens up vulnerability, especially when trust relationships are accommodated in different contexts. Trust is difficult to transfer.

Standardization work is complicated, requires knowledge and skills, and provides power to those who possess the knowledge of the standards and standard processes. If you do not master the processes, this may turn into dysfunctional distrust towards those who possess the knowledge. In this way, the imbalance between power and trust increases when the knowledgeable and resourceful gain influence on behalf of those who lack the knowledge and resources. Because the employees' side experiences lack of knowledge and lack of resources, they often express reduced confidence regarding the standardization processes and the way standards are included as a part of the hierarchy of the norms. The case of payment services is a relevant example, with the unions claiming that they have limited resources to buy standards and that the system thus excludes them from participating.

All the examples show how individual cases easily threaten trust between the parties. In particular, the S-002 process has challenged the relationship between the employee side and the authorities, on the one hand, and the employers' side, on the other. The employers' side perceived lack of approval from the PSA-N as an exercise of power and control and suspected that the authorities were consciously delaying the approval procedures. The PSA-N, in turn, claimed to do their job as a 'quality assurance' within the rules of the game in a comprehensive regulatory framework. Either way, declaring that the counterpart has hidden agendas is to declare mistrust of the actor concerned.

The tripartite model opens the way for 'politicization'. 'Politicization' refers to organizational fields, where one strives for neutrality, but where professionally motivated decision-making processes are rife with political content. This happens because different groups that have different interests in the field also have the power to secure their interests and actually use this power in the decision-making processes. Politicization is not a problem in itself, but it impacts the legitimacy and effectiveness of the standards and the standardization process. Politicization becomes problematic when decisions become 'random and populistic' interventions, instead of decisions based on knowledge and normative reasons. However, politicization also arises when the individual parties seek power to secure their roles and positions. The authorities' demands for increased representation and voting rights in the Sector Board can be interpreted as politicization, although the argument is to ensure that the standards are of sufficient quality – that is, the authorities take overall responsibility for the regulations, while simultaneously ensuring tripartite cooperation (Engen, Lindøe, and Hansen, 2017).

Consequently, there is reason to assert that the regulated regime's functional nature provides autonomy for both the employers' side and the employees' side. For the employers' side, the advantage is the ability to determine the standards and thus link them to international standards. The employees' side has a strong interest in having an influence on standardization work itself, through participation in the Sector Board. The use of power by the different groups to secure their (particular) interests in this organizational field represents a kind of politicization that is challenging, mainly because it confronts the consensus-based decision-making process. The organization of NORSOK through tripartite participation has thus given the employees' side more power than other countries' regulatory regimes and standardization organizations would have given them.

Conclusion

This chapter describes the tripartite institution in the field of safety within the Norwegian oil industry as an organizational field, and how this particular organizational field is maintained in the standardization field. The NORSOK standards show a representative organizational field, in which interests, resources, power, and counter-power occur, and where the balance of power between the players determines the outcome. In NORSOK, the relations between the authorities,

the employers' side, and the employees' side determine the outcome, and it appears that sections of the employees' side in this context, as in the other tripartite arenas, consider the processes as being dominated by the employers' side.

The authorities' appearance partly compensates for such domination by acting as a facilitator for tripartite cooperation in this arena. The authorities, however, need to emphasize the industries' responsibility for standard development, while the standards simultaneously must be in such a condition that the authorities can refer to and include them in their guidelines. Also, within the standardization work, the general dilemma of functional regulation arises: how to make the industry responsible, while at the same time ensuring that the industry always selects best practices within the given leeway.

The NORSOK standards began as a minor part of the NORSOK programme in the 1990s and gradually developed into a separate organization under Standards Norway. The reason was the need for professionalization of the standard work involving professional 'players', not least technical experts and industrial actors, who had standardization as their main occupation. In this process, tripartite cooperation also became an integral part of the organization.

Nevertheless, there seems to be a desire among parts of industry and from the employers' side to free the standardization work from tripartite cooperation and from regulatory development in general. The purpose then is to reduce the politicization processes characterizing tripartite cooperation and increase the employers' influence in Norwegian standardization work. This does not apply, however, to the employers' side in general. The official standpoint is that tripartite cooperation also has a legitimate position in the standardization field, but, at the same time, it is important to prevent politicization from hampering the competitiveness and internationalization of the industry in general.

Note

1 During the drafting of the chapter, in April and May 2018, the author conducted interviews and correspondence with several key players affiliated with the Sector Board Petroleum in Standards Norway. Thanks to all informants. Thank you also to Ragnar Rosness (Sintef), Jacob Kringen (DSB), Tone Therese Linge (UiS) and anonymous referees for useful comments on an earlier draft. The analysis, interpretations, and conclusions are the sole responsibility of the author.

References

Austnes-Underhaug, R., Cayeux, E., Engen, O.A.H., Gressgård, L., Hansen, K. (2011). Læring av hendelser. En studie av bakenforliggende årsaker til hendelser på Gullfaks C og av Statoils læringsevne [Learning of events. A study of the underlying causes of incidents on Gullfaks C and Statoil's learning ability]. *IRIS-rapport* 156. Stavanger: IRIS.

Bieder, C. and Bourrier, M. (2013). *Trapping safety into rules. How desirable or avoidable is proceduralization?* Farnham: Ashgate.

Brunsson, N. and Jacobsson, B. (2000). *A world of standards*. Oxford: Oxford University Press.

Brunsson, N., Rasche, A., and Seidl, D. (2012). The dynamics of standardisation: Three perspectives on standards in organisation studies. *Organisation Studies*, 33, pp. 613–632.

Bundum, B., Forseth, U., and Kvande, K. (2015). eds. *Den norske modellen. Internasjonalisering som utfordring og vitalisering* [The Norwegian model. Internationalization as a challenge and revitalization]. Oslo: Fagbokforlaget.

Coglianese, C. (2010). Management-based regulation: Implications for public policy. In: *Risk and regulatory policy: Improving the governance of risk. OECD reviews of regulatory reform*. Paris: Organisation for Economic Co-operation and Development

Coglianese, C. (2019). Optimizing regulation for an optimizing economy. Research Paper NO 18–35 ILE – Institute for Law and Economics. University of Pennsylvania.

DiMaggio, P. J. and Powell, W. (1983). The iron cage revisited. Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48, pp. 147–160.

Engen, O. A. (2002). Rhetoric and realities. The NORSOK programme and technical and organisational change in the Norwegian industrial complex. PhD thesis, University of Bergen.

Engen, O. A. (2014). Emergent risk and technologies. In P. H. Lindøe, M. Baram, and O. Renn, eds. *Risk governance of offshore oil and gas operations*. New York: Cambridge University Press.

Engen, O. A., Lindøe, P. H., and Hansen, K. (2017). Power, trust and robustness – the politicization of HSE in the Norwegian oil regime. *Policy and Practice in Health and Safety*, 15(2), pp. 145–159.

Engen, O. A. *et al*. (2013). *Tilsynsstrategi og HMS-regelverk i norsk oljevirksomhet, rapport fra regjeringsoppnevnt ekspertgrupp.* [Supervision strategy and HSE regulations in Norwegian oil business: Report from government-appointed expert group]. Oslo: Arbeids- og Sosialdepartementet.

Gilad, S. (2010). It runs in the family: Meta-regulation and its siblings. *Regulation & Governance* 4(4), pp. 485–506.

Grimen, H. (2009). *Hva er tillit?* [What is trust?]. Oslo: Universitetsforlaget.

Haugland, A. (2015). Bruk av funksjonsbasert regelverk og rettslige standarder [The use of function-based regulations and legal standards]. In P. Lindøe, J. Kringen, and G. S. Braut, eds. *Risiko og tilsyn* [Risk and inspection]. Oslo: Universitetsforlaget.

Hernes, G. (2006). *Den norske mikromodellen. Virksomhetsstyring, partssamarbeid og sosial kapital* [The Norwegian micro model. Corporate governance, cooperation and social capital]. *Fafo-notat* 2006: 25.

Hopkins, A. (2011). Risk management and rule-compliance: Decision-making in hazardous industries. *Safety Science* 49(2), pp. 110–120.

Jonassen, Ø. (2018). Utfordringer med funksjonelt regelverk og bruk av standarder I norsk petroleumsindustri? En studie av overordnet regelverk og hva som avkreves av utredning ved utvikling av de forskjellige nivåene [Challenges with functional regulations and use of standards in the Norwegian petroleum industry? A study of general regulations and what is required of investigation in the development of the different levels]. Master's thesis, University of Stavanger.

Kringen, J. (2014). Contested terrains in risk regulation. In P. H. Lindøe, M. Baram, and O. Renn, eds. *Risk governance of offshore oil and gas operations*. New York: Cambridge University Press.

Luhmann, N. (2017). *Trust and power*. Cambridge: Polity Press.

Marchant, G. E., Abbott, K. and Allenby, B. eds. (2013). *Innovative governance models for emerging technologies*. Cheltenham: Edward Elgar Publishing.

Morgan, G. and Sturdy, A. (2000). *Beyond organizational change. Structure, discourse and power in UK financial services*. Basingstoke: Palgrave Macmillan.

Powell, W. and DiMaggio, P. J. (1991). *The new institutionalism in organizational analysis*. Chicago: The University of Chicago Press.

Rosness, R. and Forseth, U. (2014). Boxing and dancing. Tripartite collaboration as an integrated part of a regulation regime. In P. H. Lindøe, M. Baram, and O. Renn, eds. *Risk governance of offshore oil and gas operations*. New York: Cambridge University Press.

Scott, W. R. (1998). Organizations: Rational, natural and open systems, *Canadian Journal of Sociology*, 29.

Short J. M. and Toffel, M. W. (2010). Making self-regulation more than merely symbolic: The critical role of the legal environment. *Administrative Science Quarterly*, 55(2010), pp. 361–396.

Tharaldsen, J. (2011). *In safety we trust – Sikkerhet, risiko og tillit i offshore oljeindustri* [In safety we trust – Safety, risk and trust in the offshore oil industry]. PhD thesis, University of Stavanger.

Further reading

Mandat for sektorleder [Mandate for sector leader].

Mandat for sektorstyret [Mandate for the sector board].

Meld. St. 12 (2017–2018). Helse, miljø og sikkerhet i oljevirksomheten [White Paper 12, 2017–2018 Health, environment and safety in the oil business]. Available at: www.regjeringen.no/no/dokumenter/meld.-st.-12-20172018/id2595598/

Prosjekt NORSOK analyse (2016). Norsk Olje og Gass [NORSOK analysis project Norwegian Oil and Gas Association]. Available at: www.norskindustri.no/contentassets/bd73caa821de492480ab6c43b3e7556a/final-report-norsok-analysis-project-29-01-2017-eng-an.pdf

Retningslinjer for utvikling og utforming av NORSOK standarder A-001 [Guidelines for the development and design of NORSOK standards A-001]. Available at: www.standard.no/en/sectors/energi-og-klima/petroleum/

Standard Norge vedtekter.[Standard Norway Articles of Association]. Standard Norge.

Stortingsmelding 17 (2002–2003). Om statlige tilsyn [White Paper 17 (2002–2003). About state supervision]. Available at: www.regjeringen.no/no/dokumenter/stmeld-nr-17-2002-2003-/id134860/

Stortingsmelding nr. 29 (2010–2011). Felles ansvar for eit godt og anstendig arbeidsliv [White Paper 29 (2010–2011). About a decent working life]. Available at: www.regjeringen.no/no/dokumenter/meld-st-29-20102011/id653071/

16 Dilemmas of standardization in risk governance

Odd Einar Olsen

Standardizing risk governance

In this book, we have presented a variety of standardization processes and applications of standards that may influence our judgements of risk and the organizing of risk governance – and, accordingly, our behaviour. They vary from regulations of international and national cooperation in risk governance and crisis management, to regulation of infrastructure and industrial sectors, as well as risk management in the activities and duties within or among organizations. Could standards provide compatible systems and thereby increased efficiency, cooperation, and coordination? Or will increased standardization only open up a landscape of new dilemmas and unintended consequences?

Although standardization of risk governance might mean many things, different chapters illustrate the growing efforts to make risks more comparable and thereby more manageable. This includes standardization for legal purposes, as well as for improved coordination between different organizational or national bodies. Compatibility goes to the core of standardization and is included in almost all contributions. But standardization could also be an instrument to dominate an industry or technology, or part of the rationalizing of public services and elements in risk governance, such as contingency planning and crisis management. General standards for risk management, such as the International Standardization Organization (ISO) standards are often used when establishing frameworks for risk governance, but standards, rules, and regulations also apply to specific sectors, specific risk problems, or methodologies applied in risk governance. Many contemporary risk problems are influenced by several actors with different interests and perceptions. The context in which risk problems are dealt with is often characterized by considerable uncertainty, ambiguity, and complexity. Hence, interpretation of the context constitutes the main challenges when using standards and guidelines in risk governance. Standards and standardization are often referred to as a panacea for governing risk in all sorts of contexts, but the utility, effects, and problems associated with their use in a constantly changing and interdependent risk landscape has gained little attention among scholars.

Standardization and standards could affect risk governance in different ways. The most important lessons drawn from the present contributions could be

condensed into three topics: (1) how standardization may affect power relations and interests; (2) how standardization may change flexibility in decision-making, communication, and cooperation; and (3) how standardization could (re)direct attention and risk perception.

Standardization, power, and interests

Controlling standards and standardization processes could be an important source of power (Brunsson and Jacobsson, 2000; Busch, 2011). For decades, a struggle to control the rules and standard setting in financial and product markets has been going on, especially between the USA and the EU (Büthe and Mattli, 2011). Governments, together with big private companies, are struggling to control, or at least influence, private standard-setting agencies. Being in a position to define standards might give certain organizations and institutions a comparative advantage and power in markets, social networks, and political processes. But struggling to maintain a successfully unifying process of standardization, while simultaneously upholding legitimacy and credibility among powerful stakeholders with divergent interests, could be a challenging exercise.

Controlling standard-setting processes in risk governance probably does not have the same economic potential as controlling standard setting in financial and product markets. Embedded in other power games, risk governance systems are influenced by the political and socio-economic context, and how safety and security are organized is a highly political issue. Safety and security have been one of the most important tasks for authorities in all organized societies. The way risk governance is organized will often reflect national traditions and values. Consequently, standardizing risk governance across national borders could easily develop into a political game. The EU is probably the biggest and most successful 'standardization project' in the world. However, developing common standards for risk governance and coordinated disaster response systems for all member states has turned out to be one of the most challenging topics the EU has tried to standardize. In this case, standards may threaten existing politics by being political.

Another aspect of the power of standards and standardization is the political risks if responsible agencies fail to handle threats and risks. Political leaders and executive managers have made their future or aborted a promising career because of decisions they made in a critical situation. In that aspect, it could be practical to replace difficult political decisions by standards as apparently neutral tools, but this could create new challenges. Widespread and acknowledged standards may reduce reflection on how appropriate such standards are in all cases. Consequently, standards may become reified and appear as independent powers, for which no one can be made accountable because of faceless institutional processes. Whereas the political is embedded in safety and security, standardization through safety and security policies and decision-making could de facto imply an intentional de-politicization of security. Attempting to confine a highly uncertain political risk by fixed procedures (standards) and approaching it

through a non-political perspective, for instance, in risk management, could hide the political aspects and reduce critics and resistance against controversial methods to increase safety and security. This is often the case in security-related issues, such as terrorism, where methods used to increase security could violate other values in society, such as the right to freedom and a private life.

Another challenge may appear when different risk logics meet. How could it be possible to compare and prioritize action based on contesting value-based risks? Some contributions highlight this political problem. The UN Guiding Principles on Business and Human Rights are standards for managing human rights risk, which are supposedly defined to mitigate corporate human rights harm. Yet the standards deploy an economic risk logic, which is focused on financial risk to the firm and thus incompatible with the human rights risk to the rights-holder. Economic logic overrules human rights logic with the impact it could have for the respect of human rights in business. In this case, standards are governing the politics.

Other challenges could arise when different expert knowledge and methodologies are confronted with initiatives to develop a standardized risk-ranking tool or when totally different risks such as environmental, safety, and security risks are combined into a common risk picture. In such cases, standardization of the risk analysis and management could appear a prerequisite for communication and cooperation between stakeholders with different interests and risk knowledge. However, standardization may take place at the expense of comparability with other societal risks. In such cases, politics may replace standards.

Using standards as guiding tools could be an easy way out of wicked political problems in risk governance and, in a way, leaves responsibility for choices to somebody or something else. But it will also produce new challenges.

Changing flexibility

The different chapters in this volume clearly show how risks appear in many disguises, and anticipated risks could often materialize as incidents or disasters in unexpected ways. The development of common risk pictures and assessments implies a common language among the stakeholders. But standards contribute to the upholding of the established pictures and ideas of the risks we are surrounded by and may reduce the awareness and capacity to handle so-called black swans (Aven, 2014). Consequently, risk governance structures need to be flexible. Even if global standards for risk governance are developed, they still need to be translated into the specific local context before they are used, which, in turn, may result in very different practices in different countries and in different companies. Standardization produces conformity and homogeneity between stakeholders, while risk governance requires diversity and heterogeneity in information, systems, and organization. Even so, standards could be useful. For example, dilemmas could appear regarding prioritization between low likelihood, high impact events and high likelihood, low impact events, as well as every possible combination in between, none of which is desirable.

Guidelines and standards may serve as a useful decision-making support by reducing flexibility in risk governance. They maybe make dilemmas more invisible, but they can never solve the dilemmas arising.

The main driving forces for the introduction of standards in risk management are intended to reduce numbers of difficult and even impossible choices or remove practicalities in governing risks. Introducing standards could make it easier to establish platforms for cooperation between institutions dealing with risk governance. But risk governance is heavily influenced by the political and socio-economic context, which differs between institutions and across countries. Standardization may also be a prerequisite for communicating the perceived problem in exact and precise ways. But standardized risk management and crisis response systems may undermine the validity of the thorough examination of contextual assumptions and reduce the importance of local knowledge and individual capacities. Standardization could make it easier to make decisions but, at the same time, make them less relevant to the actual situation.

The use of different sources of information is normally vital in risk assessments. It is possible to indicate that increased standardization of risk descriptions will probably facilitate the work of combining several sources of information in a risk assessment. But it also indicates that increasing the level of standardization might lead to a reduced motivation to conduct risk assessments. It thus appears that combining different risk information and increasing the motivation to conduct risk assessments based on standards cannot be achieved at the same time. A similar dilemma could appear if explicitly formulated rules for regulating individual and collective behaviour have to be balanced against the ability to perform one's job according to knowledge, experience, and need for improvisation. In such cases, standardization has to compromise with flexibility, in order to avoid increasing existing risks.

Directing attention

Standards are the means by which we construct realities (Busch, 2013, p. 13). They may direct our attention, defining good or bad, and affect the way in which we perceive risks. Well-known and authorized standards are rarely discussed in public or in circles outside those who formulated them and those who are expected to adapt to them. They keep the world together in a common language that reduces transaction costs between individuals, institutions, companies, and countries.

Standardization of risk governance is a necessity when different actors are supposed to cooperate and build capacity together. Standardization may therefore come to serve as a common ground for developing national and international agreements and treaties to meet threats and defined risks. But standardization may also reduce our attention to the unthinkable threats and risks it is easy to talk about but difficult to handle. A high degree of standardization may reduce comparability with other complex risks and could reduce the capacity to discover and understand new risks on the horizon. If not taken into consideration, a

comprehensive standardization of risk governance may lead to a poorer understanding of the mechanisms producing (new) transboundary risks and, consequently, to a reduced capacity to implement efficient means for mitigation and preparation. In other words, standardization of risk may create blind spots in risk governance and management, and shadow alternative solutions, making it impossible to recognize a new risk before it is too late. The consequence may be a lower capacity for efficient risk management and crisis response. An example could be the use of risk matrices, which at least to a certain degree need to be standardized; they may at the same time increase collective mindfulness of some risks, while decreasing awareness of other risks.

Standardization could make the structures and fundamental values of society less visible. When making risk assessments or designing risk management systems, semi-professional analysts often take standards for granted. They may choose standards that seems to be workable, without reflecting on their appropriateness in the given context. But we cannot blame a standard for anything illegal, even if it proves to be wrong. Organizations and individuals following an acknowledged standard could hardly be blamed, even though the outcome appears to be very poor. However, standardization could generate secondary effects that run counter to its original goal, if the focus is directed on following rules instead of creating safety and security. In this respect, standardization of risk governance might give an illusion that the level of safety and security is better than it actually is.

Preparing for the unthinkable and standardizing the response?

The temptation to standardize even the most complex risk governance systems may appear, due to an implicit idea that there is a common understanding of risks, a design of risk management systems, contingency planning, and emergency responses. But risk governance is not an exact science, and there is not only one way to design a risk governance system. The chapters also highlight how standardization of risk governance may produce new dilemmas and paradoxes. There is a saying that a crisis is best handled when it stays within existing sectorial boundaries and responsibilities and keeps to one administrative level. But how often does that happen? Even well-known societal risks, for which precedents exist, carry a high degree of uncertainty about how a given risk may materialize and the potential consequences if it does. This is the main challenge in risk governance.

'You should prepare for the unthinkable' is a well-known slogan among consultants in risk and disaster management. Some take it even further and state that the consequences of an emergency can be mitigated by thinking the unthinkable, while, at the same time, admitting that emergencies come in many forms and no two are exactly alike. These seem to be incompatible positions, and they illustrate that standardization in itself can hardly solve important problems inherent in risk governance. Risk per se cannot be standardized, but elements in

risk governance could. It will never be a question of whether to standardize or not to standardize, because efficient risk governance, as the application of principles to the identification, assessment, management, and communication of risk, is built on organizational and national cooperation. The question is: Which elements in risk governance are suitable for standardization, and how could standardization take place without reducing the necessary flexibility that is vital in risk governance (Alexander, 2009)?

The invisible standardization of risk governance, embedded in the digitalization of surveillance, analytical tools, decision-making support systems, and logistical support, has only just started. Expected developments will strengthen the need for both more political reflections and practical considerations about standardization in risk governance. Problems and dilemmas arising from standardization of risk governance will not vanish because they are made invisible.

References

Alexander, D. (2009). Principles of emergency planning: Standardisation, integration and sustainability. In U. Fra Paleo, ed. *Building safer communities: Risk governance, spatial planning and responses to natural hazards.* Amsterdam: IOS Press, pp. 162–174.

Aven, T. (2014). *Risk, surprises and black swans: Fundamental ideas and concepts in risk assessment and risk management*. London: Routledge.

Brunsson, N. and Jacobsson, B. (2000). *A world of standards*. Oxford: Oxford University Press.

Busch, L. (2013). *Standards: Recipes for reality*. Cambridge, MA: MIT Press.

Büthe, T. and Mattli, W. (2011). *The new global rulers: The privatization of regulation in the world economy*. Princeton, NJ: Princeton University Press.

Index

Page numbers in *italics* denote figures.