DOCTORAL THESIS

# Securing Digital Government: Towards Governance Mechanisms for E-state Resilience

Isabel Skierka-Canton

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY
TALLINN 2023

TALLINN UNIVERSITY OF TECHNOLOGY
DOCTORAL THESIS
40/2023

# Securing Digital Government: Towards Governance Mechanisms for E-state Resilience

ISABEL SKIERKA-CANTON

TAL TECH PRESS

TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Ragnar Nurkse Department of Innovation and Governance

This dissertation was accepted for the defence of the degree Doctoral Studies in Public Administration 03/08/2023

**Supervisor**: Prof. Dr. Ringa Raudla
School of Business and Governance
Ragnar Nurkse Department of Innovation and Governance
Tallinn University of Technology
Tallinn, Estonia

**Co-supervisors**: Dr. Dr. Robert Krimmer
Dr. Krimmer Consulting OÜ
Tallinn, Estonia

Prof. Dr. Peter Parycek
Department for E-Governance and Administration
Universität für Weiterbildung Krems
(Danube University Krems)
Krems, Austria

**Opponents**: Prof. Dr. Hans Jochen Scholl
Information School
University of Washington
Seattle, WA, United States

Prof. Dr. Gabriela Viale Pereira
Department for E-Governance and Administration
Universität für Weiterbildung Krems
(Danube University Krems)
Krems, Austria

**Defence of the thesis**: 27/09/2023, Tallinn

**Declaration:**
Hereby I declare that this doctoral thesis, my original investigation and achievement, submitted for the doctoral degree at Tallinn University of Technology has not been submitted for doctoral or equivalent academic degree.

Isabel Skierka-Canton

signature

European Union
European Regional
Development Fund

Investing
in your future

ISSN 2585-6898 (publication)
ISBN 978-9916-80-016-4 (publication)
ISSN 2585-6901 (PDF)
ISBN 978-9916-80-017-1 (PDF)
Printed by Koopia Niini & Rauam

TALLINNA TEHNIKAÜLIKOOL
DOKTORITÖÖ
40/2023

# Digitaalse valitsuse turvalisus: Valitsemismehhanismid e-riigi vastupidavuse tagamiseks

ISABEL  SKIERKA-CANTON

TALTECH KIRJASTUS

# Contents

# List of Publications

The dissertation is based on the following original publications:

I. **Skierka, Isabel**. (2023). When Shutdown is No Option: Identifying the Notion of the Digital Government Continuity Paradox in Estonia's eID Crisis. *Government Information Quarterly*, *40*(1). https://doi.org/10.1016/j.giq.2022.101781 (**1.1**)

II. Schallbruch, Martin, & **Skierka, Isabel**. (2018). Cybersecurity in Germany. Springer Briefs in Cybersecurity. *Springer*. https://doi.org/10.1007/978-3-319-90014-8 (**2.1**)

III. Drott, Laura, Jochum, Lukas, Lange, Frederik, **Skierka, Isabel**, Vach, Jonas, van Asselt, Marjolein B. A. (2013). Accountability and risk governance: a scenario-informed reflection on European regulation of GMOs. *Journal of Risk Research*, *16*(9). https://doi.org/10.1080/13669877.2012.743161 (**1.1**)

IV. **Skierka, Isabel**. (2018). The governance of safety and security in connected healthcare in Europe. *Living in the Internet of Things: Cybersecurity of the IoT – 28–29 March 2018. London: Institute of Electrical and Electronics Engineers (IEEE)*, 1−12. https://doi.org/10.1049/cp.2018.0002 (**3.1**)

V. Maurer, Tim, **Skierka, Isabel**, Morgus, Robert, Hohmann, Mirko. (2015). Technological sovereignty: Missing the point? *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace; Tallinn, Estonia; 26–29 May 2015.* IEEE Xplore: IEEE, 53−68. https://doi.org/10.1109/CYCON.2015.7158468 (**3.1**)

Appendix:

VI. **Skierka, Isabel**. (2021). Messung, Prüfung und Nachweis von IT-Sicherheit [IT security measurement, evaluation, and proof]. In Gerrit Hornung & Martin Schallbruch (Eds.), *Handbuch IT-Sicherheitsrecht* [Handbook IT Security Law] (pp. 154−180). Nomos Verlag. (**3.1**)

# Author's Contribution to the Publications

The author's **contributions** to the publications in this thesis are as follows:

I. The author of this thesis is the **sole contributor** to this article.

II. The author of this thesis **contributed 50%** to the publication. She solely developed and wrote the introduction section 1 and section 3 on cybersecurity strategy. She co-developed and co-wrote section 2 on the "German view" on cybersecurity and section 5 on future trends and challenges. She also participated in the publishing process and further dissemination after publication.

III. The author **contributed 20%** to the article. She co-developed the study's theoretical framework, scenario design and case study. She then co-wrote the theoretical framework and methodology and participated in the publishing process and further dissemination after publication.

IV. The author of this thesis is the **sole contributor** to this article. She also participated in the publishing process and further dissemination after publication and presented the paper at the 2018 IET conference.

V. The author of this thesis **contributed 25%** to this article. She co-developed and co-wrote the background section about the technological sovereignty discourse, co-collected the data through desk research and a focus group, and co-wrote parts of the analysis section. She also participated in the publishing process and further dissemination after publication. She presented the paper at the 2015 CyCon conference in Tallinn, Estonia.

VI. The author of this thesis is the **sole contributor** to this book chapter.

# 1 Introduction: Scope and aim of the thesis

This dissertation examines the development of governance mechanisms for the digital state's resilience against adverse cyber events.[1] It aims to contribute to the emerging literature at the intersection of digital government (DG), cyber security, and resilience.

Almost all governments today employ digital tools for their operations, service provision or citizen engagement. The use of information and communication technologies (ICTs) in DG has many benefits, such as enhancing the internal efficiency of government improving the quality of service delivery and increasing public participation (e.g. MacLean & Titah, 2022; Dwivedi et al., 2016; Rana et al., 2015; Gil-García & Pardo, 2005). Yet, the interconnectedness of these same technologies makes them inherently vulnerable to adverse cyber events, which affect the confidentiality, integrity, and/or availability of IT systems, information, services, and processes (Austin, 2020; Romanosky, 2016; Rose & Miller, 2020, pp. 253–254). Real-world incidents and the COVID-19 pandemic have exposed the rising dependence on and simultaneous vulnerability of DG structures and services (Beduschi, 2021).

Questions about securing DG and its core functions have become more relevant than ever (Janowski, 2015; ENISA, 2020b; Krimmer et al., 2015; Stevens, 2018). This is especially true for states with highly digitized democratic infrastructures like e-voting (Krimmer et al., 2007, 2015; Parycek et al., 2017).

Hence, digital states and their government systems are increasingly exposed to **cyber risks** (Caldarulo et al., 2022; Norris et al., 2019; Romanosky, 2016, p. 124). Cyber risk, or information security risk, is a key concept of this thesis, which it defines as "the potential that threats will exploit vulnerabilities" of information asset(s) and thereby cause harm to an organization (ISO/IEC 27005, 2011) or other entities like individuals or a nation. Cyber risks embody the complexity, transboundary nature, and uncertainty of contemporary security challenges (Kjærgaard Christensen & Liebetrau, 2019; Lagadec, 2009; Perrow, 1999). They are uncertain in scope and scale, have an unprecedented speed of expansion and a high degree of diffusion. Therefore, this thesis understands cyber risks as what public policy scholars have labelled "wicked problems" (Lægreid & Rykkja, 2015, p. 476; Rittel & Webber, 1974).

Uncertainty related to the probability and impact of IT security incidents makes assessments of cyber risks particularly challenging (Eggers & Le Blanc, 2021, p. 4; NIST, 2012, p. 13; Strupczewski, 2021, p. 5). Their occurrence and timing are unpredictable, as they depend on often unknown and highly dynamic threats and vulnerabilities (ibid.). Adverse impacts can occur in both material forms, such as loss of physical or financial assets, and immaterial forms, such as harm to reputation or legitimacy. In interconnected IT infrastructures, cyber incidents can additionally cause cascading effects across technical, geographical, or functional borders (Agrafiotis et al., 2018, pp. 8–13; Dunn Cavelty, 2005, p. 259; Schneier, 2018), resulting in crises.

The cyber security challenges grow every year, with the predicted cost of cybercrime to hit 8 trillion USD in 2023 (eSentire, 2022). Digital infrastructures of governments have become particularly vulnerable to cyber-attacks throughout the past years (Caldarulo et al., 2022; Norris et al., 2019; Romanosky, 2016, p. 124). One of the most imminent

[1] Following NIST (Cichonski et al., 2021), a cyber event is "any observable occurrence in a system or network". Adverse cyber events are "events with a negative consequence". Examples include "system crashes, packet floods, unauthori[s]ed use of system privileges, unauthori[s]ed access to sensitive data, and execution of malware that destroys data" (Cichonski et al., 2021, p. 15).

cases is the Russian war of aggression against Ukraine, which is accompanied by cyber attacks against the Ukrainian government and critical infrastructures (Google TAG et al., 2023). Other cases of smaller scale in peace-time environments also abound. For example, in 2022, cyber ransomware attacks[2] significantly compromised the functioning of Albanian (Hay Newman, 2022), Montenegrin (Reuters, 2022), and Costa Rican (Burgess, 2022) government institutions and websites. Albania weighed invoking NATO's Article 5 collective defence clause over the cyber attack against its government, which cyber security experts attributed to Iran (Miller, 2022). Costa Rica declared a state of national emergency following the ransomware attack (Burgess, 2022). Local governments are also regularly affected by ransomware attacks, which interrupt their ability to provide public services to their citizens (Chokshi, Niraj, 2019; Spiegel, 2022a, 2022b).

Earlier examples of cyber threats to critical public infrastructures include the global NotPetya worm in 2017 (Greenberg, 2018), attacks against elections in the United States in 2016 and in France in 2017 (Crootoft, 2018; Willsher & Henley, 2017), attacks against the Ukrainian power grid in 2015 (Greenberg, 2019), or the distributed denial of service (DDoS) attacks against Estonian government websites and institutions in 2007 (Lesk, 2007; Ottis, 2008). Moreover, large-scale digital vulnerabilities can generate severe risks for public IT infrastructures, such as the so-called "Return of the Coppersmith Attack"–vulnerability in computer chips implemented into millions of Estonian, Slovakian, and Spanish eID cards, and trusted platform modules distributed in computers worldwide (**I**, Nemec et al., 2017) or the "Log4j" vulnerability in the widely used Java library (CISA, 2022).

In response to the inevitability of cyber incidents, states and international organizations have identified **"cyber resilience"** as a policy priority (European Commission, 2020, pp. 29–34; G7 Presidency, 2022, p. 7; World Economic Forum, 2018). But how and through which **mechanisms** do governments and other non-governmental actors **govern** these risks and achieve greater cyber resilience? An exploration of this research topic requires an understanding of the key concepts of cyber resilience and governance mechanisms, which this thesis defines in the following two sub-sections. It then elaborates on the research gap concerning cyber security in DG, which this thesis aims to address, in the third sub-section. The final sub-section presents this thesis' main and sub- research questions.

## 1.1 Cyber resilience

Over the past decade, "resilience" and "cyber resilience" have gained increasing prominence in policy discourse concerned with critical infrastructure protection (Bygrave, 2022, p. 28; Rose & Miller, 2020, pp. 253–254). Resilience is the capacity of a social system (e.g. an organization, city, or society) "to proactively adapt to and recover from disturbances that are perceived within the system to fall outside the range of normal and expected disturbances" (Boin et al., 2010, p. 9). **Cyber resilience** is still an evolving concept. It implies the realization that insecurity in digital societies is inescapable and adverse cyber events are inevitable as a part of societies' normal operation (Björck et al., 2015, p. 311). A widely used definitions of cyber resilience, which the thesis adopts as a basis, is "the ability to continuously deliver the intended outcome despite adverse cyber events" (Björck et al., 2015, p. 312). Cyber resilience goes beyond

[2] In ransomware attacks, malicious actors encrypt critical files and demand a ransom from the victim to decrypt them. Definition provided by NIST (2021).

robustness – a system's ability to continue delivering its service despite adverse events – in that it is able to recover and resume operations afterwards (Rose & Miller, 2020, p. 254).[3] Resilience of information infrastructures[4] requires redundancy and resourcefulness of those infrastructures' physical/tangible (i.e. ICTs) and less tangible (social/relational knowledge-related assets) elements (Scholl & Patin, 2014). In synthesis, this thesis understands a system's resilience as its ability to recover and adapt its functions before, during or following adverse events, not just to resist (Kott & Linkov, 2021, p. 80). Adjustments can be proactive (meaning anticipatory) or reactive (meaning in response) to a vulnerability or incident. Moreover, by focusing on governance mechanisms, the thesis considers both tangible and intangible elements of cyber resilience (see Section 3).

The thesis distinguishes between different stages of cyber resilience along a system's (administration, organization, society) ability to anticipate, monitor, respond to, and adapt to adverse cyber events (see Section 4). As to *what* is supposed to be resilient, this thesis focuses on the state's DG, including its digital systems and infrastructures, and the functions it performs. Throughout the thesis and in the title, the author also refers to this understanding of the state's DG as the "e-state" or "digital state".

Although the literature on cyber resilience is quickly emerging, it still lacks empirical qualitative studies of specific cases of organizational or national cyber resilience.[5] This thesis aims to address this gap by making a theoretically founded and empirically informed contribution to the research on cyber resilience governance mechanisms in DG. It thereby also draws on concepts from the resilience and crisis management literature (among others: Boin et al., 2016; Christensen, Lægreid, et al., 2016; Hollnagel, 2017; McConnell, 2011; Pearson & Clair, 1998; Perrow, 1999).

## 1.2 Governance mechanisms

The question of how and with what mechanisms governments can protect the security and maintain the resilience of their DG systems and operations is highly relevant for the future of the e-state. There is a broad consensus in cyber security literature and policy that the state cannot steer cyber security and resilience efforts by itself (e.g. Carr, 2016; Dunn Cavelty & Egloff, 2019; Kjærgaard Christensen & Liebetrau, 2019; Simon & De Goede, 2015; Tanczer et al., 2018). Due to the complex and transboundary nature of cyber risks, their management requires governance among diverse actors, including governments, infrastructure owners and operators, IT manufacturers, and end users across organizational borders, levels of authority, and sectors (ibid.).

Therefore, the second key concept of the thesis is that of governance mechanisms. **Governance** itself is a very broad term, which has steadily gained popularity since the 1980s and 1990s and is now widespread in academic, policy, and practitioner circles.

[3] Cyber resilience is strongly related to cyber security. Cyber security in terms of information security, refers to the "protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability" (CSRC, 2023). As Bygrave (2022) points out, cyber resilience and security are more related than the (relatively sparse) literature or policy entrepreneurs have acknowledged so far. Section 6 further illustrates this argument from a security engineering and legal perspective.

[4] Information infrastructures are not equal to IT infrastructures but rely on them to a great extent (Scholl & Patin, 2014, pp.32-33). Therefore, they are relevant in the context of cyber resilience.

[5] Exceptions are Groenendaal & Helsloot (2021, p. 440) or Kleij & Leukfeldt (2019) for a quantitative study.

Several definitions and approaches to governance have emerged[6], with the future development of a comprehensive theory of governance seeming "neither likely nor desirable" (Ansell & Torfing, 2022, p. 29). However, there seems to be a baseline agreement that governance refers to the creation of structure or order as a result of the interaction of a multiplicity of governing actors, which influence each other (Kooiman & van Vliet, 1993, p. 64; Stoker, 2018, p. 15). We can broadly distinguish between three different strands in the literature (see: Ansell & Torfing, 2022, p. 3; Bevir, 2011; Homburg, 2004; Klijn & Koppenjan, 2016, pp. 4–9; Peters, 2014, p. 302) which understand governance as

- institutions and procedures of traditional, state-centric forms of governance;
- self-organized processes in civil society;
- and/or networked forms of governance.

This thesis follows Peters' (2014) perspective that the state plays a central role in governance but that a debate focusing on actors alone has limitations. Rather, the important question is *how* actors work together to constitute governance. We therefore adopt the notion of *interactive governance*, in which the state and a plurality of other actors from society interact in order to provide steering of the economy and society (Torfing, 2012, p. 14). The author is particularly interested in the *mechanisms* of interaction developed to reach the goal(s) of governance (Peters, 2014, p. 302), which, in this thesis, is cyber resilience of the e-state. With explicit regard to (cyber) risk, the author draws on insights from the field of risk governance, which aims to regulate, reduce or control risk problems under conditions of uncertainty and ambiguity (Renn & Klinke, 2022, p. 264). This thesis further elaborates on the concept of governance mechanisms in a proposed taxonomy in Chapter 3.

## 1.3 The governance of cyber resilience in digital government

Despite their growing practical relevance for DG, resilience and cyber security remain under-investigated areas in the DG field. This results from the author's survey of the Digital Government Reference Library (DGRL, version 18.5) (Scholl, 2022) for publications that contribute to an empirical and theoretical understanding of cyber security in DG. Early DG articles laid important groundwork for research on cyber security in DG but remain at a conceptual level (Irvine, 2005; Luna-Reyes & Gil-García, 2003) or focus on specific phenomena, such as DG websites' security (Zhao & Zhao, 2010), or trustworthiness of DG technologies (Bélanger & Carter, 2008) but do not address concrete mechanisms of national cyber security, resilience or risk governance.

A large number of more recent publications on cyber security in the DG field include conceptual studies on critical information infrastructure protection policy for developing countries (Brechbuhl et al., 2010), approaches to cyber conflict (Austin & Sharma, 2020; Demchak, 2020; Foote et al., 2020; Whyte et al., 2020), country-specific cyber security strategies or risk management methods (Romaniuk & Manjikian, 2020; Viet et al., 2020; Zhang et al., 2018), sector-specific risk management (e.g. Baggott & Santos, 2020), or guidelines for effective cyber security communication framing (de Bruijn & Janssen, 2017).

[6] The 2011 SAGE Handbook of Governance (Bevir, 2011), for example, mentions 11 different approaches as "theories of governance". Similarly, the 2022 Handbook on Theories of Governance (Ansell & Torfing, 2022) mentions 11 theoretical modes of analysis for governance and 13 forms of governance.

Other areas in the literature focus on important but narrow issues, such as cyber security training and exercises at the local government level (i.e. Caldarulo et al., 2022; Gedris et al., 2021; Pike, 2021; White, 2012), methods for cyber risk management in smart city contexts (Andrade et al., 2021), or information-sharing among government organizations and European organizations (Ruohonen et al., 2016).

Despite the valuable contributions of these publications, the DG literature lacks methodologically rigorous and empirically founded studies that explain how and with which mechanisms states manage cyber resilience of their DG (see also: Caldarulo et al., 2022, p. 1). Resilience more generally is even less explored in the DG literature and has been mostly studied in the context of disaster management, sustainability, or smart cities (e.g. Andrade et al., 2021; Jasmine Yoo Jung et al., 2018; Lau et al., 2018; Sharma & Singh, 2016). Only few studies focus on the cyber security aspect of the topic (Gisladottir et al., 2017; Austin & Sharma, 2020; Klasa et al., 2020; Linkov et al., 2019; Venkatachalam et al., 2021), with the more conceptually sound studies on cyber resilience emerging from organizational studies (Björck et al., 2015, p. 2; Groenendaal & Helsloot, 2021; Rose & Miller, 2020).

## 1.4 Research questions and outline of the thesis

Given the lack of research that examines concrete mechanisms of cyber security and resilience in the DG context, this dissertation aims to address that gap and contribute empirically and conceptually founded research to this emerging field. It examines the following overarching research question:

**How can an administration develop governance mechanisms which enhance cyber resilience of the e-state?**

It attempts to answer this question by looking at the following sub-questions:

1. How does a country's national cyber security architecture impact its approach to cyber resilience?
2. How can an administration manage and overcome a large-scale cyber crisis affecting a critical DG system?
3. How can an administration govern IT systems' security in safety-relevant infrastructures?

In addressing the first sub-question – the impact of the national cyber security organisation on a state's resilience – the thesis addresses the contextual dimension of cyber security and resilience. It outlines the structures of Germany's and Estonia's cyber security architectures, based on publications **I** and **II**. The findings illustrate how formal and informal rules and norms create institutional paths along which (cyber security) governance models evolve. Germany's and Estonia's broader institutional contexts and organizational arrangements significantly differ in terms of size, administrative structures, and culture, among others. Those institutional mechanisms significantly impact interactive governance in terms of coordination and cooperation of actors. Thereby, the thesis demonstrates the importance of the institutional context for the formation of cyber resilience structures and practices.

The second sub-question – how to overcome a cyber crisis in a critical DG system – is the subject of Article **I**, which presents an in-depth case study of Estonia's 2017 eID crisis. It reveals that the criticality and wide adoption of a DG system impacts a government’s decision on whether and how to uphold the continuity of a DG during a cyber crisis. The article further identifies several mechanisms of successful crisis governance in the case of Estonia’s eID crisis, including the administration’s technology management capacity, its networked cooperation competence, the governance networks’ collaboration capital, their risk management capacity, and their ability to engage in legitimacy building through communication. This thesis additionally relates these results to other cases of severe cyber incidents.

Publications **III**, **IV**, **V**, and **VI** address the third sub-topic – the governance of IT systems security – which deals with the proactive side of cyber resilience. Article **III** examines one particular risk governance mechanism, notably accountability. The article is an example of the author’s earliest work on risk governance and safety, which informed later analyses of security and safety in subsequent publications. While the article focuses on food safety, the conclusions about EU risk governance processes and accountability mechanisms are revelatory for the other safety- and security-relevant topics studied in this thesis. **IV**’s case study of the perhaps most safety-critical Internet of Things (IoT) environment – the digital health sector – illuminates the challenges IT security risks pose to established EU safety governance and regulatory mechanisms. Its results can be transferred to other safety-critical sectors, as the discussion in chapter six of this thesis shows. The thesis considers the findings in light of the EU’s current legal cyber security framework overhaul. Publication **VI** from the appendix provides further details on evaluating the IT security of interconnected devices and systems under current German and European regulatory regimes. Article **V** about the notion of “technological sovereignty” examines how the transatlantic political crisis caused by the Snowden revelations from 2013 influenced the European discourse on IT system security governance.

This thesis is organized as follows. Chapter 2 presents an overview of the methodology applied in the articles. Chapter 3 provides operational definitions of cyber resilience and governance mechanisms that the thesis uses to analyse the research questions. It then presents the thesis’ inductively derived taxonomy of cyber resilience governance mechanisms. Chapter 4 addresses the national cyber security organisation's implications on DG resilience, mainly drawing on publications **I** and **II**. Chapter 5 focuses on national cyber resilience and crisis management in DG by answering the second sub-question. This section mainly draws upon research published in Articles **I** and **II**. Chapter 6 discusses the third sub-question about the convergence of security and safety in ubiquitously interconnected infrastructures through a discussion of Articles **III**, **IV**, **V**, and **VI**. The concluding Chapter 7 summarizes the findings and outlines avenues for further research.

## 2 Methodology

Below, this section outlines the research strategies and methods employed to research governance mechanisms for cyber resilience. First, it describes the publications' research strategies. Second, it elaborates on the methods of data collection and analysis which the publications used to analyse different governance mechanisms of cyber resilience.

Table 1 gives an overview of the research strategies, data collection methods, and corresponding research questions. The subsequent paragraphs provide additional details on how these methods have been applied in the publications.

***Table 1:*** *Overview of methodological approaches used in each publication*

| Article | Level of analysis | Research strategy | Data collection methods | Research questions |
|---|---|---|---|---|
| **I** | Process (crisis) | Case study (single exploratory, index and critical) | Desk research<br>Interviews | How did Estonia manage a large-scale cyber risk and crisis that threatened to unsettle its DG infrastructures?<br>Which factors and mechanisms can explain the overcoming of such risk and crisis? |
| **II** | Country | Case study (single descriptive, phenomenon of interest)<br>Action research | Desk research<br>Focus groups | How have German cyber security policy, strategy, and organization evolved, and why? |
| **III** | EU+ Process (product approval) | Case study (single explanatory, critical)<br>Scenario | Desk research<br>Interviews | Who can be held accountable under the complex system of supranational risk governance regarding GMO authorization, should uncertain risks materialize, and why? |
| **IV** | EU + Sector | Case study (single exploratory, critical) | Desk research<br>Focus group<br>Interviews | How do the security and safety of medical IoT devices converge, and which implications does this process have for EU safety governance mechanisms? |

| | | | | |
|---|---|---|---|---|
| **V** | Concept | Qualitative mapping / taxonomy | Desk research<br>Focus group | Which technical and non-technical proposals for “technological sovereignty” did European officials make in the wake of the Snowden revelations, and what are their implications for data security? |
| **VI** | EU+ Country | Legal (and technical) analysis<br>Action research | Desk research<br>Focus groups | How can we measure, evaluate, and prove IT security of products, services, and organizations in the EU and Germany? What are the opportunities and obstacles of current legal and technical approaches? |

## 2.1 Research strategy

The articles comprising the thesis represent different qualitative research strategies. The case study has been the core research strategy (**I, II, III, IV**). Several of the publications draw on applied legal, technical, and policy analyses (**II, V, VI**).

The author chose the **case study research strategy** for most publications, as this approach allows to tackle the research problems within their real-world context (Walsham, 1993; Yin, 2018, p. 15). As outlined above, cyber resilience phenomena require an analysis of developments and events within their technical, organizational, and strategic contexts. Case-study-based approaches are common in IS and DG research (Gil-Garcia et al., 2018; Van Der Blonk, 2003), as well as in cyber security (Groenendaal & Helsloot, 2021; Rid, 2013; Zetter, 2014) and crisis research (Boin, 2005; Deverell, 2010; Lalonde, 2007). The study of single cases allowed the author to provide thick descriptions and propose directions for further research in areas that have only scarcely been explored to date (Lune & Berg, 2017, p. 172; Yin, 2018, p. 18).

The case studies have been conducted at different levels – at a process (**I, III**), a country (**II**) or EU (**III, IV**), and sector (**IV**) level, including combinations of those categories. The case selection criteria for the publications constituting the thesis are as follows.

Article **I** is an exploratory single case study of a national cyber crisis management process. It is hypothesis-generating, insofar as it aims to identify possible causes of the crisis outcome. The case is both an index and a critical case, as is further detailed in the article’s methodology section (Gerring & Cojocaru, 2016, pp. 398–399; Patton, 2015, p. 414; Yin, 2018, p. 49).

Publication **II** is a single case study of the evolution of cyber security policy in Germany. It follows an applied research approach with a descriptive policy analysis character. The publication is part of a series of monographs examining several countries’ cyber security policies and specific cyber security issues in depth. The case selection was driven by the peculiarity of German society’s strong stance on data privacy and security as well as the country’s federalist political system. Moreover, while it scores well in international cyber security indices Germany lags behind the EU average in DG. These aspects make

Germany stand out in comparison to other Western countries regarding their cyber security policy evolutions. It merits an in-depth study and analysis as an example of a phenomenon of interest (Patton, 2015, p. 412).

The food product approval process in Article **III** constitutes a typical case of a GMO product which allowed for testing hypotheses garnered from the risk governance literature (Patton, 2015, pp. 402–403). Hence, the article constitutes an explanatory single case study. While **III** focuses on food safety, the article's conclusions about EU risk governance processes and accountability mechanisms reveal important analytical insights regarding accountability of risk governance for cyber security and safety-related policy processes.

Article **IV** presents a study of a critical case for the evaluation of the EU's product safety regime, notably medical device security, in the context of digitization. It also follows an applied policy research focus. IV's conclusions about the convergence of safety and security also offer more general insights on EU cyber security policy.

Publications **I, II, III,** and **IV** present single case studies. This overall thesis offers a cross-case synthesis, which goes beyond the discussion of the cases' individual features and makes a conceptual contribution to the topic of cyber resilience governance from multiple angles (see: Yin, 2018, pp. 194–200), as sub-section 2.2. further explains.

In addition to the case study strategy, publications **II** and **VI** use **action research strategies** (Lune & Berg, 2017, p. 138). The author had the opportunity to work with German governmental and non-governmental stakeholders within four applied research projects over a period of three years. She thereby was an embedded expert in her research and included the knowledge from the experience and interactions with relevant experts and stakeholders. The projects aimed to analyse German cyber security policy, security evaluation practices, and digital identity policy evolution and make recommendations to project partners and policymakers on how they could be improved.

Due to the interdisciplinary character of the topics examined, the publications combine approaches from political science, law, and information technology studies. Publication **VI** constitutes an analysis of the legal framework and technical methods for IT security evaluation and certification. Article **V** also constitutes a policy analysis study, based on a qualitative mapping of decision-makers' proposals to enhance "technological sovereignty" in Europe in the post-Snowden era. Hence, **II, V,** and **VI** have a more applied focus and constitute descriptive policy or legal analyses. Their target audiences are policymakers, communities of practice, and the broader public.

## 2.2 Data collection and analysis approaches

The publications make use of several data collection methods: desk research (all **I-VI**), qualitative interviews (**I, III, IV**), and focus groups (**II, IV, V, VI**). Among the approaches to data analysis, this thesis focuses on content analysis and theory development (**I**), theory testing (**III**), policy analysis (**II, IV, V**), and legal analysis (**VI**).

Desk research for each study encompassed the collection of practice-oriented documents (e.g. policy documents, newspaper articles, legislation, parliamentary documentation) as well as scientific articles. For **I**, the author additionally collected eID transaction data from the Estonian certificate authority. In addition, the author conducted semi-structured qualitative interviews with stakeholders for several articles (**I, III, IV**). For the writing of the more practice-oriented publications (**II, IV, V, VI**) the author collected data through several focus groups with policy stakeholders and researchers between 2017 and 2020.[7] By triangulating multiple types of data from different sources, the author aimed to ensure an increased validity of the studies (Miles et al., 2014, p. 262).

Concerning data analysis approaches, **I** uses a content analysis and theory development approach (Eisenhardt, 1989) for (cyber) risk and crisis management in national governance networks – a topic on which there has been little prior research. As part of the content analysis, the author qualitatively coded the data from interviews, government documents, media reports, and other research reports with thematic and pattern coding techniques (Miles et al., 2014, pp. 69–103; Saldaña, 2013). The article's annex provides an overview of the structured data analysis. Publication **II** mostly relies on the descriptive analysis of document and focus group data. The case study in **III** employs a congruence testing approach (George & Bennett, 2005, p. 126) based on a policy scenario design to refine causal hypotheses about accountability in safety risk governance garnered from the risk governance literature (Patton, 2015, pp. 402–403). The authors applied a deductive coding technique to the interviews. Articles **IV–VI** rely on descriptive policy and legal analysis techniques.

As mentioned above, this thesis offers a synthesis of findings about cyber resilience governance across cases and topics. Based on this synthesis, it inductively develops constructs for cyber resilience governance mechanisms in Section 3. The development process encompassed an analysis of the literature on governance, mechanisms and cyber resilience, and combined those notions with the conceptual and empirical findings from publications **I**–**VI**. In that process, the author sharpened and further developed the constructs she had identified in others' and her own prior publications. The constructs serve as the foundation for a taxonomy of cyber resilience governance, which this thesis proposes in the following section.

A qualitative research approach which mainly relies on case studies has limitations. Case studies, particularly single case studies, cannot produce statistically generalizable patterns. Yet, such studies do provide the basis for analytical generalization (George & Bennett, 2005; Schofield, 2011; Yin, 2018). In this sense, the goal of the case studies in this thesis is to expand and further generalize existing theoretical and practical insights and not to extrapolate probabilities in the sense of statistical generalization (Yin, 2018, p. 21). The taxonomy proposed in the following section should be seen as an attempt to further expand the analytical findings of the publications' case studies. Its constructs, too, should be seen as proposing further avenues for analysis that the concluding section elaborates on.

Moreover, the author applied several measures to strengthen the validity and reliability of this research. First, she aimed to bolster internal validity by ensuring data triangulation. Second, the research process of each publication was founded on a comprehensive review of the literature and, where applicable, legal, and technical documentation. The author conducted constant comparisons of data and emerging theory considering the academic literature and her familiarization with the cases (Dubois & Gadde, 2002, p. 558; Eisenhardt, 1989, pp. 544–545; Miles et al., 2014).

[7] The focus groups took place at ESMT Berlin, Germany.

# 3 Cyber resilience governance mechanisms

This section first outlines how the thesis and its publications operationalize cyber resilience and governance mechanisms. It then outlines the author's proposal for a taxonomy of cyber resilience governance mechanisms. The taxonomy serves as the framework of analysis and presentation of the publications' results in the subsequent chapters.

## 3.1 Operationalizing cyber resilience

To operationalize the concept of cyber resilience outlined in Section 1.1, this thesis understands it as a cyclical *process* of proactive and reactive measures, rather than a static condition. Organizations can adjust their functions prior to, during or following adverse cyber events, like incidents or crises. Most adjustments are made in a reactive manner, responding to feedback. Proactive adjustments are anticipatory and imply that the system changes to meet future demands that are expected (Groenendaal & Helsloot, 2021, p. 440).

Following the few social science studies explicitly dealing with cyber resilience (Groenendaal & Helsloot, 2021, p. 439; van der Kleij & Leukfeldt, 2019), the author uses Hollnagel's (2017) conceptualization of an organization's "resilient performance" as an analytical lens. It encompasses the potentials to *anticipate, monitor, respond* and *learn*, illustrated in Figure 1. These categories resemble those of practical frameworks, like the US National Institute of Standards and Technology's (NIST). It defines cyber resilience as "the ability to *anticipate, withstand, recover from*, and *adapt* to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources[8]" (Ross et al., 2021, p. 1, emphasis added).

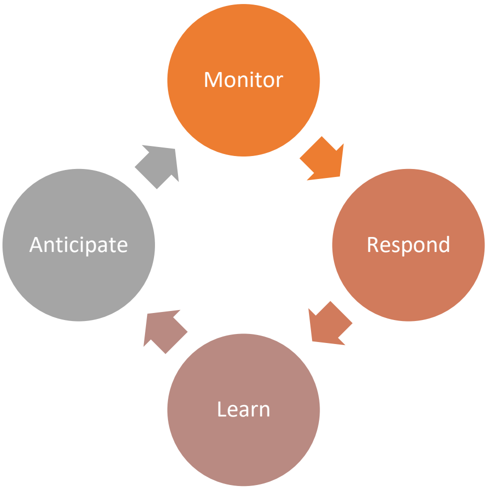


***Figure 1**: Stages of cyber resilience, based on Hollnagel (2017) (Source: author)*

[8] NIST defines a cyber resource as "an information resource which creates, stores, processes, manages, transmits, or disposes of information in electronic form and that can be accessed via a network or using networking methods."

The ability to **anticipate** means being able to "anticipate developments further into the future, such as potential disruptions, novel demands or constraints, new opportunities or changing operating conditions" (Hollnagel, 2017, p. 41). Anticipating goes beyond simply monitoring, planning, or assessing risks. It focuses more on thinking and imagining an inherently uncertain future (ibid.).

A second proactive element is the ability to **monitor**, which refers to "knowing what to look for" or being able to detect changes in the organization's internal and external environment (Hollnagel, 2017, p. 40). Monitoring, taking into account anticipation, can enable actors to make sense in situations of adversity or crisis (Boin et al., 2016; Trimintzios et al., 2015)

The ability to **respond** encompasses "knowing what to do or being able to respond to regular and irregular changes, disturbances and opportunities by activating prepared actions, by adjusting the current way of functioning or by inventing" new modes of operating (Hollnagel, 2017, p. 40). In the context of interactive governance, cooperation among actors and coordination of responses are important foundations for the abilities to monitor and respond to adversity (e.g. Boin & Bynander, 2015; Christensen, Danielsen, et al., 2016).

The ability to **learn** means "knowing what has happened or being able to learn (the right lessons) from experience." It encompasses single-loop learning from specific experiences and double-loop learning, which enables the modification of goals and objectives (Hollnagel, 2017, p. 41). Various factors can influence post-crisis policy learning, including acknowledgement of failure or analytical tractability of policy problems (Raudla et al., 2019).

Table 2 provides an overview of resilience potentials with a non-exhaustive list of examples for policy and operational instruments to implement those in the context of cyber resilience in Europe.

***Table 2:** Stages of resilience process with examples for instruments in Europe*

| | **Description** | **Instruments (non-exhaustive)** |
|---|---|---|
| **Anticipate** | Anticipate uncertain future events | - Scenario-building or forecasting in "Think Tank" or similar body (Hollnagel, 2017, p. 41), Organizations that might have the ability to engage in such activities: intelligence agencies; national / European strategy units or think tanks; NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE); EU cyber security agency ENISA |
| **Monitor** | Monitoring, detection, and analysis of changes, adverse cyber events, and threats in organization's internal and external environment | - Information (i.e. cyber threat intelligence (CTI)) collection, exchange, analysis, e.g. through Computer Incident Response Teams (CSIRTs), incentivized through shared norms or regulation (i.e. EU NIS Directives and GDPR[9])<br>- Risk awareness campaigns<br>- Training and education for public officials and critical infrastructure operator staff |
| **Respond** | Cyber incident or crisis response and recovery | - (Activation of) incident response and recovery plans<br>- EU, NATO, or national crisis exercises<br>- Operational risk, incident, and crisis management<br>- Organizational arrangements: operational cyber security agencies; CSIRTs; incident response networks; EU cyber crisis liaison organization network (EU-CyCLONe); police, law enforcement, intelligence agencies to counter cyber crime and espionage |
| **Learn** | Lesson-drawing from specific experiences, adjusting goals and objectives | - Evaluation: Post-incident / post-exercise / policy evaluation<br>- Lesson-drawing processes<br>- Adaptation of policies, structures, processes |

The following sub-sections complement this practical understanding of cyber resilience with a better understanding of categories of governance mechanisms for cyber resilience.

[9] Including *Network Information Security (NIS) Directive* (EU) 2016/1148 and its updated version, the *NIS 2 Directive* (EU) 2022/2555, and the *General Data Protection Regulation* (EU) 2016/679 (GDPR). The NIS Directives establish mandatory requirements for operators of critical and other important infrastructures and services to conduct risk assessments and report severe cyber incidents to national cyber security authorities, amongst others. NIS 1 already requires Member States to establish a national cyber security authority and a *Computer Security Incident Response Team (CSIRT)*, also called Computer Emergency Response Team (CERTs), and an EU-wide network of CSIRTs.

## 3.2 Conceptualizations of governance mechanisms

The ambition of this thesis is to propose the outlines of governance mechanisms for cyber resilience in DG. It thereby aims to lay the foundation of a taxonomy of cyber resilience governance mechanisms. As mentioned above, governance is understood as an interactive process in which the state and other actors provide steering (Torfing, 2012, p. 14) of DG and cyber resilience.

To conceptualize *mechanisms*, the author begins with Hedström & Swedberg's (1996, p. 290) broader social sciences definition of mechanisms as "theoretical constructs that provide hypothetical links between observable events". Thereby, mechanisms provide the fine-grained explanation between a cause or input and an effect or output (Hedström & Swedberg, 1996, p. 299). Reiss (2007, p. 166) points out that the term "mechanism" generally refers to the structure or process at an underlying layer, which is responsible for an event or phenomenon which we can observe at the empirical level. The mechanism – the structure or process at the underlying layer – does not necessarily have to be observable.

In the governance literature, various conceptualizations of mechanisms exist, without there being a consensus on one clear definition. The new institutional economics literature distinguishes between three broad models of coordination, each of which can be seen to illuminate different governance mechanisms: *hierarchies, markets,* and *networks* (Frances et al., 1991; Williamson, 1996). In a study mapping the cyber security institutional landscape, Kuerbis and Badiei (2017) apply these mechanisms to analyse how hierarchical, market, and networked governance structures produce and govern cyber security. These concepts prove useful as starting points to observe general cyber security governance mechanisms at play. Since this thesis focuses on public administrations, hierarchy and network structures, more than the market structures, inform our analysis of mechanisms. Even when those structures are not explicit, they can be influential as "shadows" in different governance arrangements (Peters, 2019).

In the context of the coordination of partnerships between public and private or non-profit actors, the governance literature identifies three concrete governance mechanisms, which are useful in our analysis: *structures*, *processes*, and the *actions and perceptions* of individual actors (Cheng, 2019, pp. 191–192). As Cheng (2019) shows, the operationalization of these mechanisms is possible based on various concepts from the institutionalist and network governance literature.

*Structures* for interorganizational cooperation can thus be understood in terms of different network governance models (Provan & Kenis, 2008) and / or formal and informal rules about collective decision-making (Ostrom, 1990 in Cheng, 2019, p. 192). Regarding rules, Papenfuß and Schmidt's (2021) distinction among types of "instrumental" governance mechanisms in the context of self-regulation are helpful. A "hard" governance mechanism, such as a law, is formally binding and mandatory. A "soft" governance mechanism, such as self-regulation, is not formally binding and more flexible in its application. Whereas legislators generally control the monitoring and sanctioning of hard mechanisms like law and standards, soft mechanisms can be developed by legislators but also multiactor groups (Papenfuß & Schmidt, 2021, p. 1118). The *processes* Cheng (2019, p. 192) mentions in the specific context of cooperation in interorganizational partnerships entail trust-building, leadership-building, and conflict resolution. *Actions and perceptions* of partnership participants relate to their different institutional logics and orientations, which in turn shape their expectations and, ultimately, the structures and processes of collaboration. (Cheng, 2019, pp. 192–193).

Structures and processes are also mechanisms which risk scholars refer to in their understanding of *risk governance* as the "institutional *structures* and the policy *processes* that instruct and confine collective activities of individuals, groups, and societies" under conditions of uncertainty and ambiguity, and whose aim it is "to regulate, reduce or control risk problems" (Renn & Klinke, 2022, p. 264). It can be argued that this understanding is relevant regarding the governance of complex and uncertain cyber risks.

Taken together, the conceptualizations of governance mechanisms this sub-section outlined provide some foundational concepts, which the analysis can apply to cyber resilience. *Structures, processes*, and *actions* seem useful as categories for mechanisms of governance, including in the context of risk governance. *Hierarchies, markets,* and *networks* allow to conceptualize models of cooperation between actors, whereas markets are less relevant for this thesis' focus on state-centric interactive governance than the other two mechanisms.

At the same time, the concepts show that a framework or taxonomy of governance mechanisms for the issues this thesis examines – cyber resilience and DG – is still lacking. Mainly, they do not integrate dimensions relating to the interactions between actors and technology. Therefore, this thesis aims to develop such a taxonomy, which it outlines in the subsequent section.

## 3.3 A proposed taxonomy for cyber resilience governance mechanisms

In the absence of a framework to rely on, this thesis' author inductively developed constructs for cyber resilience governance mechanisms in the DG context. She proceeded by considering concepts from the categories outlined above, as well as from the literature on governance networks (Klijn & Koppenjan, 2016; Provan & Kenis, 2008). The author then compared and combined them with the conceptual and empirical findings from the thesis' publications **I**–**VI**.

Below and illustrated in Table 3, this thesis proposes the outlines of a taxonomy of cyber resilience governance mechanisms in DG. The taxonomy should be seen as a work in progress, which shall serve as a basis for further research and development by future studies in this field. The author developed three categories of governance mechanisms at three different levels illustrated in the middle column: institutions, networked interactions, and operations. She breaks down the different mechanisms for each level in the right column. They are not isolated from each other but also frequently interact, illustrated by the dashed lines and arrows. Those mechanisms play a role in the different dimensions of resilience, in terms of what is supposed to be resilient, in the left column. Based on Duit (2016), the thesis refers to the resilience of the e-state regarding its structures – in terms of its public administrative and political structures necessary to fulfil DG functions – and the resilience of its *functions*, like providing digital public services or implementing democratic processes.

***Table 3:*** *Outline of a proposed taxonomy for cyber resilience governance mechanisms in the e-state (Source: author)*

**Governance mechanisms for Cyber Resilience in DG**

| **Dimension of resilience** | **Level of governance** | **Mechanisms** |
|---|---|---|
| ***Structural resilience***<br>*Ability to maintain, adapt administrative structures and organization to adverse events* | **Institutional** | • Formal rules – laws and regulations, administrative rules, standards (**II**, **III**, **IV**, **VI**)<br>• Informal rules – social norms, shared expectations (**I**)<br>• Organizational structures (**II**) |
| ***Functional resilience***<br>*Ability to maintain control of technological systems + dependent DG functions* | **Interactive** | • (Trusted) relations in governance networks (**I**, **II**)<br>• Institutional memory (**I**, **II**)<br>• Meaning-making (**I**, **V**)<br>• Accountability (**III**) |
| | **Operational** | • Technology management – ability to access, evaluate, control, modify technology (**I**, **IV**, **V**, **VI**)<br>• Integrative risk management (**I**, **IV**, **V**, **VI**)<br>• Capabilities – deployment of resources (financial, expertise / personnel) using organizational processes (**I**, **II**, **IV**) |

__Institutional level:__ At the institutional level, governance mechanisms occur in and through institutions, which we define as formal and informal rules and procedures “that structure social interaction by constraining and enabling actors’ behaviour” (Helmke & Levitsky, 2004, p. 727; March & Olsen, 1984; North, 1990). Formal institutions consist of **formal rules** and the monitoring and enforcement mechanisms required to sustain or underpin them (Bell, 2002, p. 2). In the context of DG, they can encompass state institutions like bureaucracies or courts, state-enforced rules like constitutions, laws, regulations, as well as non-state-enforced standards and other official rules. In all publications **I**–**VI**, we point to formal institutions like political systems, laws, and regulations as governance mechanisms, which enable or constrain actors’ resilience to adverse cyber events. One example is the federalist political system in Germany, which structures the interactions of authorities and private companies in cyber security governance. Another mechanism comprises cyber security laws and regulations like the EU’s cyber security legislation or Germany’s and Estonia’s cyber security laws, which set mandatory incident reporting requirements for critical infrastructure operators or requirements for IT software security, among others. They also encompass ‘softer’ formal governance mechanisms (Papenfuß & Schmidt, 2021, p. 1118) like IT security standards developed by multi-actor groups, as **IV** shows.

**Informal institutions** are "**socially shared rules**, usually unwritten, that are created, communicated, and enforced outside officially sanctioned channels" (Helmke & Levitsky, 2004, p. 727, emphasis added). These can take the form of socially shared expectations, norms, or codes of conducts (Helmke & Levitsky, 2004, p. 727; North, 1990, p. 36). The author highlights the influence of such informal rules in **I** with respect to the strong shared social norms of Estonia's public-private cyber security networks to protect the country's digital society against cyber threats. Adherence to those norms and the cooperation emerging from those makes up what even Estonian government authorities in official documents refer to as Estonia's "collective brain" (RIA, 2017, p. 4). In **IV**, the author observes such informal rules regarding the IT security and safety engineering communities' different approaches to assess and manage risks.

Other institutional governance mechanisms are **organizational structures**. Organizational arrangements are institutions like the formal and informal mechanisms outlined above, albeit more specific and less broad in scope. Hence, organizations are nested within and shaped by institutional arrangements and rules like legislation or federalism (Bell, 2002, p. 2; North, 1990, p. 396). **I** and **II** focus on how organizational structures in Germany's or Estonia's cyber security architecture shape organizations' and the administrations' general ability to respond to cyber incidents and crises. In Section 4, the author adopts Cheng's (2019, p. 192) and others' (Boeke, 2018; Boin et al., 2014a) proposal to conceive of these structures in terms of models of network governance for interorganizational collaboration, such as shared-governance networks, lead-organization-governed networks, and networks governed by a network administrative organization (NAO) (Provan & Kenis, 2008). *Shared-governance networks* are governed by formal and informal interactions of the network members (participants) themselves. There is no separate governance entity. This form reveals shadows of the market mechanisms evoked by Frances et al. (1992). *Lead-organization networks* constitute centralized structures governed through one or few lead organizations with asymmetrical powers. They coordinate activities or can "impose control on network elements to enhance coherence of the system and maintain efficiency" (Boin et al., 2014b, pp. 423–424). Hence, they feature elements of hierarchical governance. The *NAO structure* is a network in which a separate administrative entity is set up to govern network activities. That "network administrative organization" takes on key governance activities while leaving others to network members (Provan & Kenis, 2008, p. 8). Arguably, these models are ideal types. In practice, networks might feature characteristics of different forms of networks at the same time.

Different strands of institutional theory can further illuminate why and how institutions remain stable or change (Koning, 2016). Historical institutionalists explain continuity by previously established institutional rules and structures, which constrain possible courses of action and result in path dependencies (e.g. Steinmo et al., 1992; Thelen, 1999). Ideational institutionalists point to the role of institutions' legitimacy and them being seen as "appropriate" in their persistence (March & Olsen, 1984). It focuses on the role of ideas, attitudes, and beliefs in institutional continuity and change. Rational choice institutionalists emphasize how institutions shape actors' preferences and provide incentives for specific kinds of behaviour, which actors believe maximizes their utility. Institutional continuity can be explained by the high transaction costs of changing institutions (e.g. Weyland, 2008).

While institutionalism has focused on explaining the continuity of institutions, it also offers insight into why and how institutions can change. Change can occur because of exogenous factors, such as a crisis (Mahoney, 2000), large-scale developments in society and the economy, other institutions, and technological innovation, among others (Koning, 2016). Yet, as Koning (2016, pp. 653–659) observes, every theory also offers insights into endogenous reasons for change, such as positive or negative feedback loops, actors' changes of ideas as a result of learning, or rule application, among others. Chapter 4 takes up these aspects regarding their potential to explain changes in national cyber security governance.

**Interactive level:** Another category of governance mechanisms, which the author identified in her publications (particularly **I, II, III**) and the governance literature (e.g. Cheng, 2019; Klijn & Koppenjan, 2016; Peters, 2019; Torfing, 2012), relates to **interactive processes** between actors. These actors – individuals, groups, organizations, administrations – have their own perceptions, interests, and resulting strategies, which shape their interactions. In the context of cyber security, interactions in governance networks play a particularly important role regarding coordination and an administration's or other actors' ability to steer cyber resilience.

Governance mechanisms that influence cooperation include the building of **trusted relations** among actors in **governance networks**. **I** shows how the prior cultivation of strong relationships and trust ties between actors in Estonia's DG and cyber security collaborative networks enhanced their "networked cooperation capacity" to solve a national cyber crisis.

**Institutional memory development** is another crucial interactive governance mechanism the author identified. Drawing on work from Pollitt (2009) and Linde (2009), memories can be understood as "representations of the past", in the form of knowledge and narratives which actors in organizations or other settings, share and communicate (Corbett et al., 2020, p. 4). When these narratives are embedded in institutional processes like policy development and implementation, they become institutionalized (Corbett et al., 2020, p. 4). It can be argued that this also holds in the case of crisis management processes. Hardt (2017, p. 123) shows that institutional memory is a key mechanism in crisis management, which influences actors' capacity to collaborate. In that sense, this thesis understands institutional memory as socially constructed and something that can be actively developed, for example through policy documents or practical exercises. **I** empirically shows how the development of institutional memory in existing digital governance networks and through cyber crisis exercises enhanced Estonian cyber crisis managers' capacity to collaborate. Section 5 of this thesis also illustrates how the lack of such institutional memory can diminish cooperation capacity.

Communication of cyber security risks both within governance networks and vis-à-vis external stakeholders and the public is another important aspect of cyber resilience governance. As de Bruijn and Janssen (2017) argue, the right framing strategy is an indispensable communication practice to raise awareness for cyber security risks. Based on the empirical findings in publications **I** and **III**, this thesis determines **meaning-making** (Boin et al., 2016, pp. 78–82; Trimintzios et al., 2015) as a crucial governance mechanism of cyber resilience governance. Meaning-making encompasses communication and framing of an issue and/or the provision of a convincing narrative of what is happening and what needs to be done, e.g. during a cyber crisis (ibid.; **I**). **V** illustrates how the framing of cyber espionage risk can lead to policy proposals aiming to change internet infrastructures. **I** shows how effective meaning-making can contribute to building support among the public for decision-makers' actions, and thereby strengthen procedural legitimacy (Schmidt, 2013).

Another related procedural interactive mechanism is that of **accountability** in terms of an actor-forum relationship (Bovens, 2007) as illustrated in **III** in the context of the EU food safety regime. Rendering account for cyber incident or crisis management by explaining in a public forum what was done to manage the incident ex-ante and ex-post is another mechanism to strengthen procedural legitimacy (Boin et al., 2016, p. 102; Magetti, 2010, p. 4).

**Operational level:** The operational level comprises mechanisms of an operational and technical nature, which are indispensable in the context of DG and cyber security. A key mechanism the author identified in several publications (**I, II, IV, V**) is **technology management**. The technological resilience of IT systems – their ability to recover and resume operations after an adverse event – is a foundation for overall DG resilience. Administrations and governance networks can and need to manage resilience through different instruments, ranging from risk management and testing procedures to setting procurement requirements and enacting security legislation. **IV** outlines the interplay between institutional (laws, standards) and operational mechanisms in the management of security and safety of critical IoT devices. An important foundation for administrations to exercise technology management is their ability to access, evaluate, control, and modify technology they build into their infrastructures. Since security is highly dynamic and threats constantly evolve, the ability to install software updates, for example, is crucial. Maintaining the resilience of DG technology requires transparency, evaluation, and constant monitoring and adaptation of IT systems by qualified personnel. **I** shows how the Estonian government's technology management capacity enabled it to manage a major DG vulnerability. In **IV** and **VI**, the author argues that these principles need to be enshrined in IT security legislation. These aspects also play into broader political debates about digital or technological "sovereignty", as **V** shows.

Second, **comprehensive risk management** procedures for IT security of products and organizations that integrate security, safety, and privacy aspects of technologies are crucial at all stages of cyber resilience. **IV** and **VI** outline the necessity for integrative management of risk of software and "cyberphysical" IoT systems, and in organizations more generally. **I** demonstrates the importance of comprehensive risk management during a cyber crisis in DG, breaking down the different steps and actors' perceptions throughout the process in its Annex.

Finally, the deployment of **capabilities** will have a significant impact on DG cyber resilience. Following Amit and Schoemaker (1993, p. 35), this thesis refers to capability as an organization's capacity to deploy resources, mostly in combination with each other, and using organizational processes, to effect a desired objective. Resources can be financial or physical assets, know-how, human capital, etc. (ibid.), and technology. Hence, capability goes beyond the combination of resources, such as technology and manpower, but is a "distinctive and superior way of allocating resources" (Kusumasari et al., 2010, p. 440). They always play an implicit role in explaining the success of crisis management (**I**), shortcomings in national cyber security policy implementation (**II**), or the operational management of IT security and safety (**IV**), among others.

**Interaction between levels:** The different governance mechanisms do not operate in isolation from each other. Institutional, interactive, and operational mechanisms are often at play in combination and shape and influence each other as the following sections show.[10] For example, institutional formal and informal rules and norms and organizational structures shape actors' perceptions, strategies, and behaviours, and interactions between actors, as well as the accountability of decision-making and cyber security governance processes. Capabilities, risk management and technology management capacity evolve within the constraints of the broader institutional and organizational context. Vice-versa, they might, over time, shape interactions and ideas, beliefs, social norms or even lead to the adaptation of formal rules. Similarly, interactive mechanisms will influence both formal and informal institutions and organizational structures, as well as operational technology management capacity, risk management, and capability deployment.

## 3.4 Outline of the taxonomy's application in the thesis

The preceding section proposed constructs for cyber resilience governance mechanisms at three different levels – the institutional, interactive, and operational levels. The thesis proposes that those mechanisms influence both the resilience of administrative structures and functions of digital states in the face of adverse cyber events. Figure 2 illustrates the different dimensions of cyber resilience that the thesis addresses in the following sections. Below, Section 4 mainly focuses on a country's mechanisms for cyber resilience at the institutional (laws, (in)formal rules, organizational structures, social norms) and interactive levels (networks and cooperation) in the context of its broader cyber security architecture. Section 5 addresses interactive and operational mechanisms for managing an actual cyber crisis in DG. Section 6 outlines institutional and operational mechanisms of governing IT systems security in safety-critical IoT infrastructures in the EU and Germany. Importantly, each section and the conclusion show how the mechanisms at different levels mutually influence and shape each other.

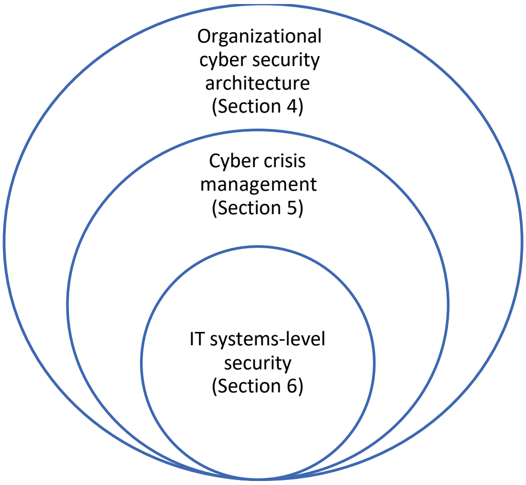

Organizational cyber security architecture (Section 4)
Cyber crisis management (Section 5)
IT systems-level security (Section 6)

***Figure 2:*** *Dimensions of national cyber resilience the thesis addresses*

[10] In addition, this argument relies on studies from the institutionalist (e.g. Bell, 2002; Koning, 2016; Lowndes, 1996; March & Olsen, 2004; North, 1990) and information systems (IS) (e.g. Fountain, 2001; Symons, 1991; Weerakkody et al., 2016) literatures, which have explored interactions between institutions, actors, and technology, and how they shape each other, in more detail.

# 4 The impacts of a country's national organization of cyber security on its cyber resilience

This chapter explores sub-research question one, how a country's organization of its national cyber security architecture shapes its approach to resilience, based on **I** and **II**. It limits the analysis to the civilian and internal dimensions of cyber resilience, excluding diplomatic, intelligence, and military dimensions of cyber security.[11]

This thesis and its publications examine two countries in more detail: Germany and Estonia. Both are liberal democracies and EU member states. While Germany is Europe's most populous country with over 80 million inhabitants and a federalist political system, Estonia is a small, centralized state with 1.3 million inhabitants. In an EU-wide comparison, Germany lags behind in DG, Estonia is a DG leader (Bundesregierung, 2022, p. 44; European Commission, 2022a; European Commission et al., 2022). On cyber security, both countries score well, with Estonia ranking third and Germany 13th worldwide (out of 182 countries) and Estonia second and Germany seventh in Europe (out of 46) according to the International Telecommunication Union's (ITU's) most recent Global Cyber security Index (ITU, 2021).

Neither the thesis publications nor this section present a comparative case study of Germany's and Estonia's cyber resilience governance. Rather, the case syntheses and the contrast between the two provide insights regarding the differences of models according to which a country can organize its cyber security governance architecture and their impacts on cyber resilience. The section additionally shows how institutional mechanisms impact interactive governance in terms of coordination and cooperation of actors.

The following subsections on Germany and Estonia each outline the countries' respective institutional context, cyber security governance architecture, stages of cyber resilience, and the impacts of those mechanisms (pertaining to institutions, organizational structures, and operational mechanisms) on cyber resilience. The final sub-section provides a brief synthesis.

## 4.1 Germany's cyber security governance model

In this thesis and publications **II** and **VI**, the author chooses to focus on Germany as a unique case, which merits an in-depth study and analysis as an example of a phenomenon of interest (Patton, 2015, p. 412) for several reasons. Germany is Europe's largest economy relying on a decentralized political system. Overall, Germany's public and policymakers have attached high importance to strong data protection and security standards throughout its post-World-War-II history (Freude & Freude, 2016). Civil society and the broader public often meet DG innovations with initial data privacy and security concerns.[12] Edward Snowden's revelations about US intelligence and surveillance activities in Europe and Germany in 2013 triggered an intense public debate about cyber

[11] Studies that examine offensive and military cyber security in more detail include, among others, Austin (2020), Liebetrau (2022) , Rid (2013), Smeets (2018), Smeets & Lin (2018)

[12] One example is the German eID card. When it was initially introduced in 2010, the influential civil society organization "Chaos Computer Club" warned of its potential security risks. Today, the organization has endorsed the eID card as a highly secure digital identification method (Skierka & Parycek, 2023). Similar debates arise in the context of e-health, i.e. related to the electronic patient records, or the use of other means of digital identification, amongst others.

security and surveillance that catapulted cyber security up the political agenda (**V**). Cyber security has continued to be an acute policy issue in Germany as the country has experienced several high-profile attacks against its DG infrastructures throughout the past decade. It suffered from Russian state-sponsored espionage attacks against the German parliament's (Bundestag's) IT networks in 2015 (European Union, 2020; Guarnieri, 2015) and its government networks in 2016 and 2017 (Flade & Mascolo, 2020). In 2021, attackers from a presumably Russian state-sponsored group attempted to hack parliamentarians through phishing attacks (Spiegel, 2021). Moreover, over the past years, ransomware and other cyber attacks against local governments have intensified (Kern, 2021; Stiebel, 2022).

### 4.1.1 Germany's institutional context

Germany's cyber security governance occurs through several institutions. The country's federalist political system constitutes the broader institutional arrangement shaping cyber security governance. The central state shares power with sixteen federal states ("*Länder*"). Each federal state has its own laws and legislative competences, government, and security agencies. These, in turn, constitute a decentralized system in which political decision-makers determine DG, internal security, cyber security, and data protection policy, among others. Those decisions are embedded in the formal framework of EU and national laws and regulations. They include the NIS Directives, the GDPR, national laws like the "BSI Act", sector-specific IT security laws, and other legal guidelines, some of which **II** and **VI** outline (see: Schardt, 2021 for legal requirements for cybersecurity in German DG).

On the informal institutional side, the German administrative system follows a "Rechtsstaat" orientation with a strong Weberian administrative culture (Christensen, Danielsen, et al., 2016, p. 319). It is characterized by "hierarchical subordination, clear competencies, rule-bound and legally-organized procedures" (Jann, 2003, p. 95). As a result, official rules, and standards, as well as organizational structures, characterize interactions between public officials or in the implementation of cyber security and data protection guidelines.

### 4.1.2 Germany's organizational cyber security architecture

Organizationally, Germany's cyber security architecture is extremely complex. To a significant degree, this is a result of its decentralized political system. **II** (pp. 31–45; pp. 52–54), recent expert assessments (see testimonies in: Deutscher Bundestag, 2023) and an institutional mapping (Herpig et al., 2023) provide a comprehensive overview of the organizations involved and the complexity arising from it. In Figure 3 the author presents a simplified illustration of the main actors in Germany's public cyber security architecture. For a more detailed and interactive presentation of Germany's cyber security architecture, its actors, and their relations, the author recommends the online visualization by Herpig et al. (2023).

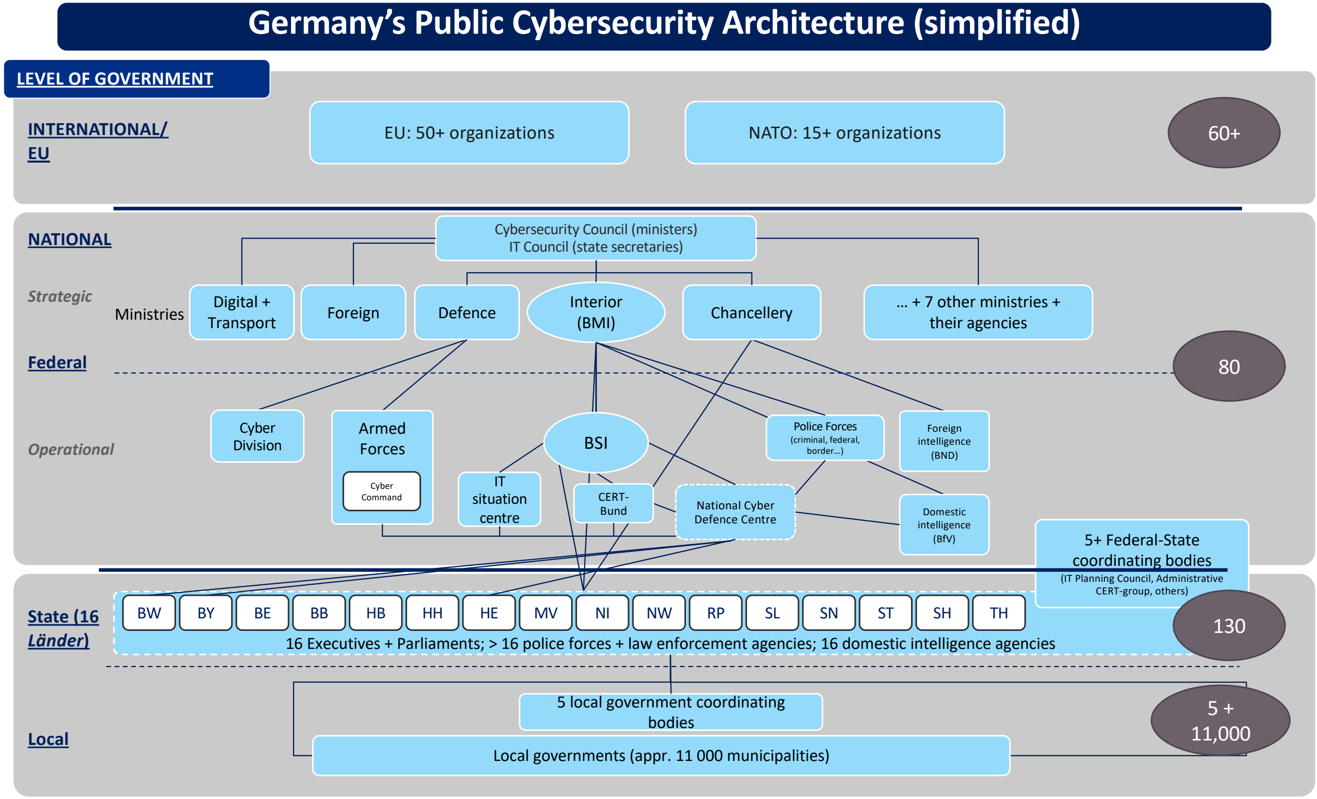

Germany's Public Cybersecurity Architecture (simplified)
LEVEL OF GOVERNMENT
INTERNATIONAL/ EU
EU: 50+ organizations
NATO: 15+ organizations
60+
NATIONAL
Cybersecurity Council (ministers)
IT Council (state secretaries)
Strategic
Ministries
Digital + Transport
Foreign
Defence
Interior (BMI)
Chancellery
… + 7 other ministries + their agencies
Federal
80
Operational
Cyber Division
Armed Forces
Cyber Command
BSI
IT situation centre
CERT-Bund
National Cyber Defence Centre
Police Forces (criminal, federal, border…)
Foreign intelligence (BND)
Domestic intelligence (BfV)
5+ Federal-State coordinating bodies
(IT Planning Council, Administrative CERT-group, others)
State (16 Länder)
BW
BY
BE
BB
HB
HH
HE
MV
NI
NW
RP
SL
SN
ST
SH
TH
16 Executives + Parliaments; > 16 police forces + law enforcement agencies; 16 domestic intelligence agencies
130
Local
5 local government coordinating bodies
Local governments (appr. 11 000 municipalities)
5 + 11,000

***Figure 3**: Overview of Germany's public cyber security architecture (numbers are only indicative values)*

At the national federal level, Germany's cyber security governance network structure resembles a *lead-organization* network, with the Federal Ministry of the Interior and Community (Bundesministerium des Innern und für Heimat, *BMI*) acting as the main strategic coordinating body for national cyber security policy and legislation, and for internal security. Under its supervision, the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, *BSI*) functions as the operational national cyber security lead organization (**II**, pp. 32–33). BSI's legal competencies, staff (currently at around 1400), and finances have increased throughout the past years and are planned to grow further in the future (BMI, 2022, p. 6). Apart from BSI, the federal and state police and intelligence agencies have important competencies in cyber security, mainly centring around countering cyber crime and espionage (**II**, pp. 31–36).

Despite the lead organization network structures at the federal level, the involvement of all additional actors at the state and local government levels with their respective competencies makes Germany's overall cyber security architecture resemble a very complex *multi-level shared governance network*. The central state structures are complemented by sixteen state governments with respective ministries, police forces, domestic intelligence offices, and prosecutors' offices responsible for specific cyber security tasks. In addition, various structures for cooperation between public and private organizations exist across these different government levels. These range from exclusive public private partnerships (PPPs) for critical infrastructure protection to broader cyber security associations for the German economy with thousands of members (**II**, pp. 41–45).

### 4.1.3 Stages of Germany's cyber resilience

Formally, Germany has set up necessary structures for proactive and reactive cyber resilience at the national federal level. Table 4 presents a summary of its organizational structures to anticipate, monitor, respond to, and learn from adverse cyber events.

***Table 4**: Organizational arrangements for cyber resilience in Germany*

| <u>Cyber resilience potentials</u> | <u>Implementation in Germany</u> |
|---|---|
| **Anticipate** | - <u>Limited</u>: strategic planning units of ministries, intelligence agencies and BSI, BSI's IT security situation assessment report. Yet, no (publicly known) distinctive cyber security forecasting / anticipatory arrangements or capabilities |
| **Monitor & Respond** | - <u>Formally advanced</u> at federal level and in most states but <u>fragmented and/or competing responsibilities</u> at horizontal (across ministries and agencies) and vertical (at different levels of government) levels can hamper effective coordination<br>- Formal rules: Constitution (decentralization of internal security, crisis management), EU legislation, e.g. NIS Directives, BSI / IT Security Acts, cyber security minimum standards and guidelines for federal and state government institutions (not mandatory for local government and national and state parliaments), a.o.<br>- Organizational arrangements<br>o Federal national: BSI (CERT-Bund, IT situation centre), BSI's Mobile Incident Response Teams (MIRTs) for CI operators and government institutions, National Cyber Defence Centre (NCAZ) coordination platform<br>o Federal-state: administrative CERT network, IT planning council, states' own decentralized cyber security organizations, some with a link to NCAZ<br>o State/local: decentralized responsibilities for state/local DG cyber security and crisis management, depend on states for resources and capabilities, which are often insufficient at the local government level<br>o Nation-wide cyber crisis exercise in 2011, next one planned for 2023 with a focus on resilience of public institutions at all levels of government (BBK, 2023)<br>o Police, law enforcement, intelligence agencies to counter cyber crime and espionage operate at federal national and state levels<br>- Plethora of PPPs for information exchange |
| **Learn** | - <u>Limited</u> – Processes aimed at building adaptive capacity through lesson-drawing, learning, and reforms, were long absent from German cyber security strategy and policy. The most recent 2021 cyber security strategy (BMI, 2021) aims to establish strategy evaluation processes involving stakeholders |

In international comparison, Germany has a mature cyber security governance architecture (ITU, 2021). The institutional context outlined in Section 4.1.1. – its federalist political system and the rules-based administrative culture – have produced a complex multi-level cyber security governance architecture. Those institutional and organizational arrangements enable administrative actors to address cyber risks at multiple levels of government according to specifically defined administrative and legal rules. However, this thesis' analysis has identified several challenges arising from respective governance mechanisms.[13]

First, the *institutional fragmentation and duplication of political and legal responsibilities* across different ministries' and (security) agencies' responsibilities at horizontal and vertical levels diminish the administration's capacity to effectively coordinate information sharing or responses to cyber incidents (see e.g. **II**, pp. 38–40; 52–54). As the literature on managing adversity and crisis points out, coordination is a foundation of resilience and effective crisis management (Boin & Bynander, 2015; Christensen, Laegreid, et al., 2016; McConnell, 2011). A lack of coordination capacity can impede the administration's potential to monitor and respond to cyber adversity. Therefore, a key strategic goal of the German government is to further consolidate Germany's public cyber security architecture, and its structures for public-private cooperation (BMI, 2022).

Second, *informal cooperation governance mechanisms* between government agencies and between private actors and government agencies do not seem strong enough to counterbalance fragmented responsibilities. Information exchange and incident response assistance follows clear inter-institutional procedures and is seldom informal. Yet, effective cyber security information sharing requires not only formal rules for cooperation but also trust between actors, which can often only be built through informal cooperation and mutual voluntary information sharing (Carr, 2016; Morgus et al., 2015; Tanczer et al., 2018). Christensen et al.'s (2016, p. 319) proposition that Germany's formalistic administrative culture may produce horizontal coordination problems likely apply to the field of cyber security governance.

Third, a culture of adhering to formal rules and procedures can increase transparency and overall *accountability* of decision-making. However, while formal accountability rules and procedures are necessary, they are not sufficient to guarantee the actual accountability of decisions (see **III**). The evaluation of past cyber incident and crisis response processes and policy more generally is an important part of accountability and learning. However, processes aimed at building adaptive capacity through lesson-drawing, learning, and reforms, were long absent from German cyber security strategy and policy (Herpig, 2021, p. 3). While the most recent 2021 cyber security strategy (BMI, 2021) aims to establish strategy evaluation processes involving stakeholders, Germany's administration's ability to engage in learning and adaptive governance remains to be assessed in the future.

Fourth, administrative organizations at the *local* political level (municipalities, including districts and cities) often lack adequate *capability* (resources and organizational processes to activate and use those) for cyber incident and crisis response[14] (Kern, 2021; Schardt, 2021, pp. 608–609; Stiebel, 2022). Due to the federalist system, local governments are to a great extent autonomously responsible for crisis management and cyber security of their own DG infrastructures. While overarching minimum security

[13] It is beyond the scope of this thesis introduction to provide an exhaustive discussion of the organizational arrangements for cyber resilience and the challenges Germany faces. In following, the author provides a summary. **II** and recent policy publications (see expert statements in: Deutscher Bundestag, 2023; Herpig et al., 2023; Kullik, 2021) provide more detailed overviews.

[14] The maturity of cyber security organizations and state / local government resources is heterogeneous among states. Some states have their own cyber security offices or cybercrime competence centres (like Baden-Württemberg, Bavaria, or Hesse), are connected to NCAZ, or simply have more cyber security resources than others.

standards exist for federal and state-level government institutions, their application is not mandatory for local governments, the administrations of the German Bundestag and state parliaments, or audit offices. As a result, the implementation of security standards remains patchy (Schardt, 2021, pp. 608–609). Since local governments are among the most vulnerable to cyber attacks (Kern, 2021), they constitute the weakest link in the country's overall cyber security landscape. An illustrative example is Germany's first officially declared cyber crisis, which resulted from a ransomware attack against the district government of Anhalt-Bitterfeld in Saxony-Anhalt in July 2021. Due to insufficient resources, the district had to request operational and administrative assistance from other local governments, the state government, and federal institutions, including a MIRT and even the federal Armed Forces (Stiebel, 2022).

### 4.1.4 Germany's public cyber security architecture and its impact on cyber resilience

Institutional path dependencies are clearly discernible in the organizational arrangements of shared responsibilities between federal national, state, and local government levels. The resulting complexity of organizational arrangements risks constraining authorities' ability to operate effectively in cases of adversity and crisis. Most political decision-makers aim to improve coordination among different actors. However, while, from a rational choice perspective, central federal level policy-makers have an interest to further consolidate responsibilities at the national level, those developments are not always in the interest of decision-makers at the state level, which can lead to competitive policy approaches. Moreover, shortcomings in the management of several past cyber incidents in DG infrastructures (and the private sector, which lies outside the direct scope of this thesis) have intensified the debate about the need for institutional change. One examples is the response to the 2015 attack against the Bundestag (Beuth et al., 2017), in which even federal authorities lacked important capability. Other examples are responses to attacks against local government infrastructures, like in Anhalt-Bitterfeld in 2021, which exposed a lack of capability and interactive governance at the local level of government. These exogenous events and policy debates might eventually lead to institutional change (Koning, 2016, pp. 654–659) through influencing decision-makers' ideas, policy approaches, and cost-benefit calculations. Moreover, the acknowledgement of past policy failure in the aftermath of severe cyber incidents might lead to lesson-drawing and learning by stakeholders, as prior research has suggested (Raudla et al., 2019, pp. 13–15). Future research could follow current and future developments to explore potential institutional change and its effects on governance mechanisms for Germany's cyber resilience.

## 4.2 Estonia's cyber security governance model

After illustrating the complex cyber security governance structures in Germany, this subsection focuses on Estonia's governance of cyber resilience. **I** provides a case study of a cyber crisis process in Estonia's DG and outlines several reasons why Estonia is a revelatory case to study in more depth.

Estonia is a small state with 1.3 million inhabitants and a central government. The country regained independence from the Soviet Union in 1991 and since then has become a world leader in DG. The country's digital government rests on two pillars: the nation-wide decentralized data infrastructure X-Road and its electronic identity (eID) scheme. Combined, they essentially create “a digital state and digital citizens” (Kattel & Mergel, 2019). As the only country worldwide, Estonia lets its citizens vote online in nation-wide elections (Krimmer et al., 2007, 2021). In the latest parliamentary elections in March 2023, 51% of votes were cast online (ERR, 2023). It is regularly among the top countries in DG rankings (European Commission, 2022a).

The security of Estonia’s IT infrastructures is a precondition for its successes in DG and the functioning of the state as such. In 2007, Estonia’s DG, bank, media, and telecommunications infrastructures suffered from a cyber-attack, which Estonian security services attributed to Russia (Czosseck et al., 2011). As a result, cyber security became a national political priority (Estonian Ministry of Defence, 2008), and Estonia was one of the first countries worldwide to adopt a national cyber security strategy in 2008 (Osula, 2015, p. 6). In 2009, the country set up a *National Cyber Defence League* and a *Data Embassy* (Robinson et al., 2019). Estonian authorities also introduced regular cyber crisis exercises. Moreover, Estonia began to push for better norms on international state behaviour in cyber space and became a norms entrepreneur in international cyber security policy discussions (Crandall & Allan, 2015). Despite claims that the online voting process was insecure (Springall et al., 2014), Estonian decision-makers have repeatedly insisted that its DG systems and political processes are secured against vulnerabilities and cyber attacks (e.g. Abel, 2014 and research interviews for I).

### 4.2.1 Estonia’s institutional context

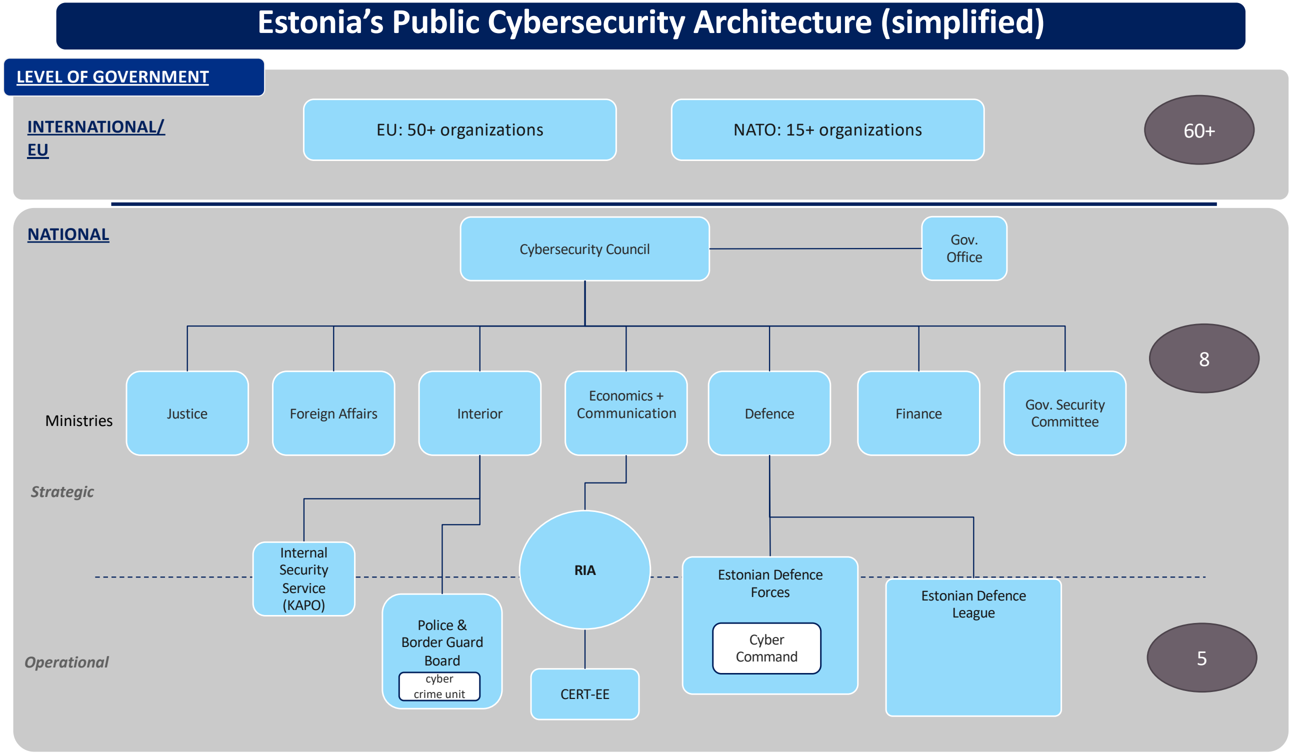
Estonia is a parliamentary republic and a unitary state. Although the country’s political system is centralized at the national vis-à-vis the regional and local levels of government, its administrative system is decentralized. Individual ministries supervising their own area of government have a strong role in the administration. They are responsible for policy formulation while implementation is the task of various agencies under the ministries’ oversight. The agencies concentrate most of the professional knowledge and operate relatively autonomously (Sarapuu, 2015, p. 61). Decentralization has several advantages, such as clearer allocation of responsibilities and accountability for policy fields and less need to spend resources on coordination. Yet, decentralization has also implied the lack of an administrative tradition of the central implementation of cross-departmental policies and tasks. Instead, horizontal cooperation has relied very much on informal networks (Sarapuu, 2015, p. 66).

Like Germany’s, Estonia’s cyber security and critical infrastructure legislation is strongly influenced by respective EU legislation and national laws, like the *Public Information Act, the Emergency Act, and the Cybersecurity Act*.

Estonia’s small size in terms of its population and government is an important factor to consider regarding its institutional structure. While formally set institutional procedures dominate large states’ systems, in small states like Estonia, “more informal and personal relationships can support institutional pursuits in developing networks both within government administrations and in external relations with stakeholders and societal partners” (Randma-Liiv & Sarapuu, 2019, p. 176). After independence, Estonia only had access to a limited number of civil service professionals and expertise. Narrow specialist skills were outsourced (Randma, 2001, pp. 42–45). In their study of Estonian collaborative governance networks, Kattel & Mergel (2019, p. 145) confirm these assumptions about small states for Estonian DG and cyber security policy, which has long relied on the cooperation of private and public sector representatives in informal governance networks. The country’s informal public-private networks underpin a *mission* *mystique* – a common belief system in the country's digital society that "strengthens networks that are driven by common values and held together by (digitally savvy) charismatic leadership" (Kattel & Mergel, 2019, p. 154). That mission mystique can also be observed in the country's "e-narrative" of a highly digitized society. It is an important informal institution that shapes interactive network mechanisms. **I** demonstrates its effects in more depth.

### 4.2.2 Estonia's organizational cyber security architecture

Compared to Germany's public cyber security governance model, Estonia's governance architecture is more centralized. While cyber security policy making and implementation is distributed among several ministries and agencies, the *Estonian Information Systems Authority* (Riigi Infosüsteemi Amet, *RIA*) fulfils a central coordinating role. It has mainly operational but also strategic tasks, like formulating Estonia's cyber security strategy. The structure is indicative of a *network administrative organization* more than a partnership network, in which RIA takes on key network governance activities, including in cyber crisis management (Boeke, 2018, p. 457). Hence, despite Estonia's otherwise decentralized administrative system, RIA acts as a network manager that introduces some centralization to the field of cyber security policy. Yet, as a government sponsored lessons-learned report about the eID crisis pointed out, responsibilities for DG and cyber security risked are unclearly allocated (Tallinna Tehnikaülikool, 2018).



Estonia's Public Cybersecurity Architecture (simplified)

LEVEL OF GOVERNMENT

INTERNATIONAL/ EU

EU: 50+ organizations

NATO: 15+ organizations

60+

NATIONAL

Cybersecurity Council

Gov. Office

Ministries

Justice

Foreign Affairs

Interior

Economics + Communication

Defence

Finance

Gov. Security Committee

8

Strategic

Internal Security Service (KAPO)

Police & Border Guard Board

cyber crime unit

RIA

CERT-EE

Estonian Defence Forces

Cyber Command

Estonian Defence League

Operational

5

***Figure 4****: Estonia's public cyber security architecture (numbers are only indicative values)*

### 4.2.3 Stages of Estonia's cyber resilience

Despite the country's small size, Estonia has implemented comprehensive cyber resilience structures and processes. "Technological resilience" of the Estonian digital society "and readiness to cope with crises" is the first of four objectives in the country's most recent cyber security strategy from 2018 (Republic of Estonia, 2021, pp. 40–44). Limited resources, both in terms of finances and manpower, remain challenges. Yet, public officials can draw on a pool of domestic and international experts through its strong digital governance networks. Analogous to sub-section 4.1.3. and Table 4, this sub-section and Table 5 provide an overview of Estonia's organizational structures for cyber resilience. Several publications from the literature (Cardash et al., 2013; Czosseck et al., 2011; Kaska et al., 2013; Kohler, 2020; Osula, 2015) and **I** provide more detailed insights.

***Table 5**: Organizational arrangements for cyber resilience in Estonia*

| Cyber resilience potentials | Implementation in Estonia |
|---|---|
| **Anticipate** | - Moderate: potential strategic units of ministries, intelligence agencies or RIA. No (publicly known) distinctive forecasting / anticipatory organizational arrangements or capabilities. Yet, Estonian government is involved in the "e-Governance academy" centre of excellence and hosts the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), which engage in analysis and anticipatory activities |
| **Monitor & Respond** | - Advanced<br>- Formal rules: EU legislation (particularly the *NIS Directives*), national Public Information Act, Emergency Act, Cybersecurity Act, a.o.<br>- Organizational arrangements<br>o RIA conducts risk analyses, serves as the reporting point for critical infrastructure operators' notification of cyber security incidents, and supervises CI operators' implementation of and enforces regulatory compliance with security measures, including through sanctions (RIA, 2023a). It also coordinates cyber incident and crisis response (I).<br>o RIA's CERT-EE monitors and handles security incidents, issues warning, supports institutions, engages in preventive cyber security activities and awareness raising (RIA, 2023b)<br>- Police, intelligence agency's units counter cyber crime and espionage<br>- Cyber Defence Unit (comprises individuals from public and private entities) supports national cyber defence (Cardash et al., 2013; Kaska et al., 2013) |
| **Learn** | - Progressing: lesson-drawing has become an objective of cyber incident / crisis management processes throughout past years. Lessons from the 2007 crisis were included in the first 2008 national cyber security strategy, 2017 lessons were published in report and included in the 2018 cyber security strategy, leading to some organizational adjustments (I) |

Beyond these formal organizational structures, Backman (2021) and this thesis' author (**I**) illustrate the strength of informal rules and cyber security governance networks at the interactive level during Estonia's management of its 2007 and 2017 cyber crises. RIA itself refers to these networks as "a 'collective brain' consisting of state and private sector data security experts acting in concert", which was able to repel the 2007 attacks "and helped to develop an action plan for the years ahead" (RIA, 2017, p. 4). The activation of those networks can help counterbalance the operational lack of resources and capability when responding to and adapting after incidents.

At the same time, the reliance on such informal modes of cooperation can raise challenges for accountability. Decision-making processes in informal networks are likely to be less transparent. Responsible parties can be less easily be identified in ex-post accountability processes than in officially documented processes.

### 4.2.4 Estonia's public cyber security architecture and its impact on cyber resilience

The Estonian case is an example of a small state with effective cyber security governance structures, which rely on a network administrative model. The national cyber security agency RIA acts as the network coordinator. Given Estonia's public administration's otherwise decentralized setup, this degree of centralization by RIA is a deviation that might merit further research.

The case also demonstrates how institutional and interactive mechanisms of governance tightly interact. In Estonia, historically grown collaborative public-private networks have persisted as a result of positive feedback loops and their legitimacy among political decision-makers. Those networks can be activated in times of severe cyber incidents and strengthen coordination (**I**). Cooperation is more informal and trust-based than in a large state with complex and a more formal administrative culture like Germany. Historical and ideational institutionalist perspectives can help further illuminate those processes.

These interactive governance mechanisms further enhance cyber security capability at the operational level. Even though resources might be scarce, Estonian decision-makers can draw on tried and tested organizational processes to combine and effectively deploy those resources through network mechanisms. Moreover, decision-makers have openly engaged in post-crisis lessons-drawing processes, specifically in the 2017 eID crisis' wake (**I**), to signal their readiness to learn. Further research could explore to what extent such processes have increased the adaptiveness of governance (Janssen & van der Voort, 2016) and cyber resilience.

## 4.3 Synthesis

This section has outlined two different national cyber security architecture models in the two EU member states Germany and Estonia. Table 6 below summarizes this section's main findings.

***Table 6:*** *Overview of the characteristics of Germany's and Estonia's national cyber security architectures*

| | **Germany** | **Estonia** |
|---|---|---|
| **Institutional context** | - Very large state (80 mio. inhabitants)<br>- Federalist system | - Small state (1.3 mio. inhabitants)<br>- Unitary political system but strong decentralization of responsibilities among ministries |
| **Formal rules** | - EU and national cyber security and critical infrastructure legislation<br>- Sectoral legislation for DG at the federal and state level<br>- Information security guidelines for federal and state government institutions (partially mandatory) | - EU and national cyber security and critical infrastructure legislation<br>- General risk management guidelines |
| **Cyber security organizational structures** | - Complex competing models:<br>o Lead organization model at federal level (BMI as policy and BSI as operational hubs)<br>o Multi-level shared governance between central and federal states (*Länder*)<br>- (Cyber) crisis management: decentralized, main authority lies with states, local governments<br>o Lack of capability during crisis, esp. local level | - Network administrative organization (NAO) model (RIA acting as hub)<br>o Unclear demarcation of responsibilities<br>- (Cyber) crisis management: NAO, RIA acting as hub<br>o Lack of capability offset by activation of public-private networks during crisis |
| **Modes of interaction** | - Hierarchical and rules-based<br>o Horizontal and state-federal coordination challenges<br>o Accountability ensured through formal procedures | - Networked and informal (strong influence of public-private governance networks)<br>o Enhanced coordination capacity<br>o Risks for transparency and accountability of decision-making |

The purpose of this section was to show how countries' institutional structures influence organizational arrangements for cyber resilience and actors' behaviour, especially their capacity to effectively coordinate. It illustrated the tight interaction between institutional and interactive governance mechanisms and indicated avenues for further research, to which Chapter 7 will return.

# 5 Cyber crisis management and resilience

This section aims to answer sub-research question two: how can an administration manage a large-scale cyber crisis affecting its DG infrastructures? On the spectrum of events of cyber adversity, a crisis lies at the outer extreme. Hence, it provides a “stress-test’” of the resilience of a system, administration, or society. Crisis management and resilience are thus closely linked (Boin et al., 2010; Boin & McConnell, 2007; Williams et al., 2017). Below, this section defines the concept of (cyber) crisis, outlines tasks of effective cyber crisis management, and presents constructs for cyber crisis governance mechanisms.

## 5.1 (Cyber) crisis and crisis management

This thesis defines crisis as a situation in which a system, organization or community experiences “a *serious threat* to the basic structures or the fundamental values and norms of a social system, which – under *time pressure* and *highly uncertain* circumstances – necessitates making crucial decisions” (Rosenthal et al., 1989, p. 10, emphasis added). Mirroring the key elements of crisis mentioned above – severe threat, urgency, and uncertainty – cyber crises are IT disruptions that “have the potential to severely limit or eliminate the functionality of key societal services or critical infrastructures, which must be dealt with urgently under conditions of deep uncertainty in order to avoid physical, financial, and/or reputational damage” (Backman, 2021, p. 435). While it is unlikely that such crises play out exclusively in the virtual realm, they will involve a cyber security dimension.

To date, only few studies (Backman, 2021; Prevezianou, 2021) have analysed the governmental management of actual cases of cyber crisis through conceptually grounded empirical case studies. The cases examined in these studies include the 2007 DDoS attacks against Estonia (Backman, 2021), the WannaCry malware’s impact on the UK’s National Health Service (NHS) in 2017 (Backman, 2021; Prevezianou, 2021), and the hack of the Democratic National Convention in the United States in 2016 (Prevezianou, 2021). **I** and this thesis build on these studies’ empirical findings and the constructs outlined below to derive underlying factors which determined the Estonian DG’s resilience during the Estonian *ROCA* crisis in 2017.

## 5.2 Tasks of crisis management

Crisis management (CM) is generally effective when a weakened or disrupted system (whether a social, organizational, or technical system) is brought back into alignment and achieves normal functioning at any stage of that process (Williams et al., 2017, p. 740). In addition, effectiveness depends on stakeholders’ perception of the crisis management outcomes’ success (Boin et al., 2018, p. 25; McConnell, 2011; Pearson & Clair, 1998).

The author discerns two constructs which determine CM performance from the literature at the intersection of crisis management and public administration. First, CM performance depends on *governance capacity*, covering the functional, operational aspects of CM, particularly *sense-making* and *coordination* capacity (Boin et al., 2014a, pp. 423–424). *Sense-making* encompasses the detection and understanding of an unfolding crisis and can be linked to the *anticipation* and *monitoring* stages of cyber resilience. *Coordination* is about making critical calls to solve dilemmas and orchestrating and implementing a coherent response (Boin et al., 2016) and can be linked to the *response* stage of cyber resilience described above. Second, it depends on *governance* *legitimacy*, which relates to the political aspects of crisis management . The CM process requires political support and trust from stakeholders and the broader public in order to be effective (Boin & Bynander, 2015; McConnell, 2011). Legitimacy is a complex concept, which generally concerns "citizens' perceptions of whether the authorities' actions are desirable, proper or appropriate within certain socially constructed systems of norms, values, and beliefs" (Jann, 2016; Lægreid & Rykkja, 2019b; Suchman, 1995). **I** distinguishes between input, output, and procedural legitimacy (Lægreid & Rykkja, 2019a; Scharpf, 1999; Schmidt, 2013).

Governance legitimacy and capacity are interrelated. An administration's legitimacy arguably influences its ability and capacity to manage a crisis. A decrease in its legitimacy or negative perceptions will likely negatively affect its ability to coordinate and implement decisions (Lægreid & Rykkja, 2019a, p. 888). In turn, crisis managers' incapacity to operationally respond to and mitigate consequences of a cyber incident for end users will decrease the crisis management's output legitimacy, and its support among the population.[15] Figure 5 below illustrates the relations between the different concepts.

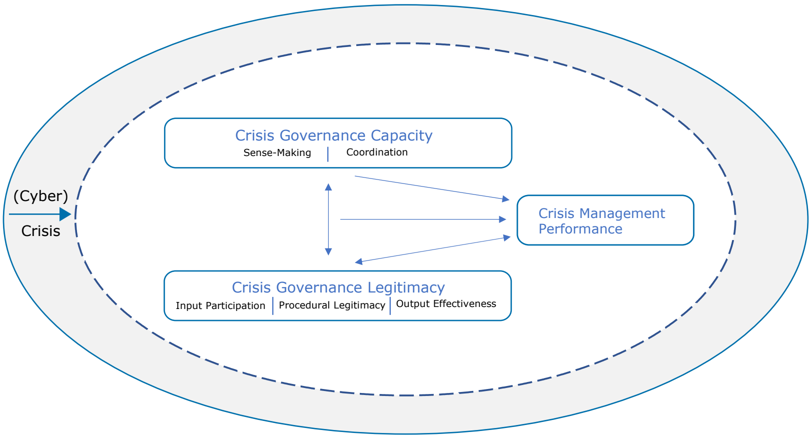


***Figure 5:*** *Author's illustration of (cyber) crisis governance capacity and legitimacy, based on the propositions put forward by Christensen et al. (2016)*

### 5.2.1 Proposal for an analytical lens: a network governance approach for cyber crisis

The dimensions of crisis governance capacity (sense-making and coordination) and legitimacy help describe the tasks crisis managers in the public sector need to tackle to effectively manage cyber crises. In **I**, the author proposes to refine those constructs towards mechanisms of cyber crisis governance that provide for resilience of affected DG systems. She proposes to examine these mechanisms through a "governance network model" approach proposed by Klijn and Koppenjan and depicted in Figure 6. Through the framework, the author analyses the modes of *interaction* of different actors involved in governance networks and the *strategies* through which they decided and implemented their decisions during the crisis process in different *rounds* of interactions. The model further considers *institutional* factors, which impact actors' behaviour and strategies (substantive and strategic factors), and network (management) structures.

[15] Claim based on arguments put forward in the disaster management and public administration literatures by e.g. Schneider (2011, pp. 60–81) or von Haldenwang (2016, p. 14).

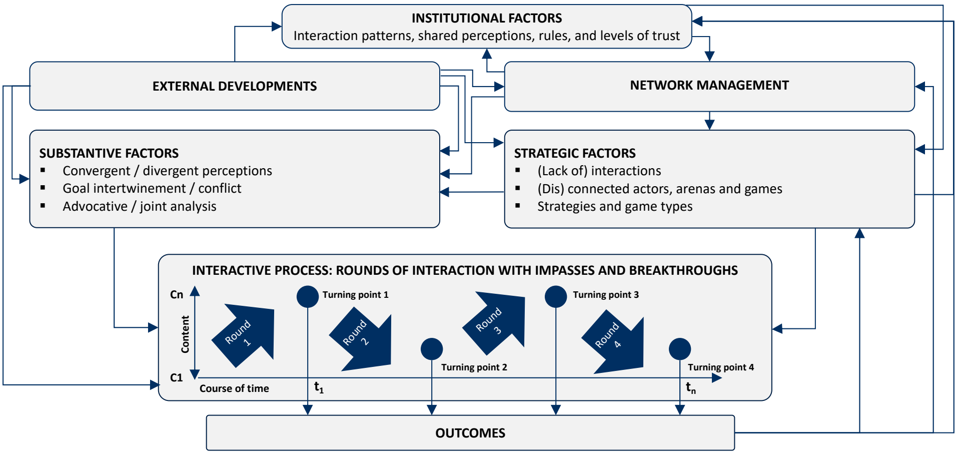

INSTITUTIONAL FACTORS
Interaction patterns, shared perceptions, rules, and levels of trust
EXTERNAL DEVELOPMENTS
NETWORK MANAGEMENT
SUBSTANTIVE FACTORS
Convergent / divergent perceptions
Goal intertwinement / conflict
Advocative / joint analysis
STRATEGIC FACTORS
(Lack of) interactions
(Dis) connected actors, arenas and games
Strategies and game types
INTERACTIVE PROCESS: ROUNDS OF INTERACTION WITH IMPASSES AND BREAKTHROUGHS
Cn
Content
C1
Course of time
Round 1
Round 2
Round 3
Round 4
Turning point 1
Turning point 2
Turning point 3
Turning point 4
t1
tn
OUTCOMES

***Figure 6:*** *Author's illustration of factors explaining governance network processes, based on the framework put forward by Klijn and Koppenjan (2016, p. 308). Source: Article* ***I***

The governance network framework can serve as the basis for operationalizing the description and explanation of actors' complex interactions in a cyber crisis management process. In its Annex, **I** proposes to analyse the following aspects to structure the case description and analysis

1) crisis management actors, their roles, and their resources
2) the arenas, issues, and tiers of cyber risk management of the crisis process
3) the rounds of the crisis process and the respective arenas, their turning points, and the state of the vulnerable DG system
4) actors' risk assessment and management strategies per round.

### 5.2.2 Constructs for cyber crisis governance mechanisms and avenues for further analysis

This thesis suggests applying the framework outlined above to analyse administrative governance networks' management of cyber crises. In **I**, the author deployed the framework in an exploratory case study of Estonian governance networks' management of the 2017 "*ROCA*" crisis. A previously unknown vulnerability, the "Return of the Coppersmith Attack" vulnerability or "ROCA", affected the chip built into nearly 800,000 Estonian eID cards, among millions of other chips and trusted platform modules worldwide. The vulnerability of such a critical DG system triggered a crisis in Estonia's DG, which the country managed over the course of several months between fall 2017 and spring 2018. The analysis generated several conceptual constructs which we propose for further refinement and testing in future case studies. These constructs constitute the foundation for the governance mechanisms at the operational and interactive levels proposed in Section 3. Figure 7 provides an overview of the constructs. Below, the section explains how the author derived them in the context of the case study and other cases of cyber crisis in DG.

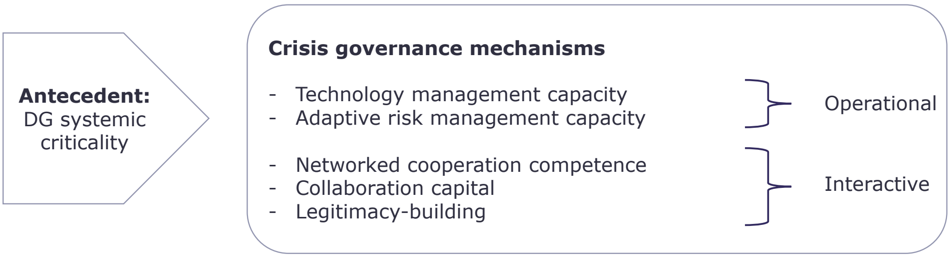

Antecedent:
DG systemic criticality
Crisis governance mechanisms
- Technology management capacity
- Adaptive risk management capacity
Operational
- Networked cooperation competence
- Collaboration capital
- Legitimacy-building
Interactive

***Figure 7**: Proposed constructs that influence cyber crisis management in DG (Source: author)*

First, the author identified the *DG's systemic criticality* as a *primary parameter* guiding crisis managers' decisions on handling an adverse cyber event affecting a DG system. She found that the degree of criticality of the DG system, in this case, Estonia's national eID system, strongly influenced government leadership's and crisis managers' perception of the cost associated with an interruption of DG services. Maintaining the (vulnerable) system's continuity became the primary goal in Estonia's ROCA crisis. The author argues that this parameter might have played out differently in a country with a less advanced DG. To strengthen that argument, she evoked the cases of Austria, Spain, and Slovakia, whose eID systems were impacted by the exact same vulnerability. Yet, those states' DG are much less developed than Estonia's, and only a fraction of their populations used their affected eID cards' identification or signature functions. Hence, the thesis proposes that a DG's maturity, which might be determined based on adoption rates or usage, will influence a government's decision whether and how to uphold DG continuity in case of a large-scale vulnerability or incident.

The cases of several other additional cyber crises affecting DG or public critical infrastructures strengthen that argument. Examples include the UK's NHS during the WannaCry incident in 2017 (Backman, 2021) or the German district Anhalt-Bitterfeld's social security system during a ransomware attack in 2021 (Stiebel, 2022). In those cases, political decision-makers' and crisis managers' primary goal was to maintain or restore the availability of the systems' critical functions – the provision of healthcare services in the UK's case, and the provision of social government services in the German case.

Scholars can also draw on the case of the hack of the Dutch Certificate Authority (CA) DigiNotar in 2011. DigiNotar was relevant for DG, as it issued Dutch government certificates, among others. Attackers breached the CA and managed to generate falsified certificates. The case evolved into a national disaster and DigiNotar had to revoke all certificates (van der Meulen, 2013, pp. 53–54). However, after their revocation, it turned out that the certificates had been more critical for Dutch commerce than the Dutch government had been aware of. The high opportunity cost of certificate revocation, for example for the delivery of imported goods in Rotterdam Harbour, became visible only after the government had initiated the revocation (van der Meulen, 2013, pp. 54–55). In this case, the DG system's criticality was greater than assumed. Awareness of the cost might have led to different CM decisions.

In addition to this finding about the primary parameter of DG systemic criticality, **I** suggests five constructs of cyber crisis governance. These can be directly related to the proposed cyber resilience governance mechanisms outlined in Section 3. At the **operational** level, the author identified the Estonian administration's *technology* *management capacity* and actors' adaptive cyber *risk management capacity* as two mechanisms to solve the ROCA crisis. Technology management capacity depended on the condition of technological infrastructures – including their robustness, redundancy and resulting technical resilience – and the ability to deploy competent experts with deep knowledge of affected systems. **I** further proposes a risk management mechanism (illustrated in the Annex) that encompasses not only technical methods but also encompasses actors' risk perceptions and goals.

In the Estonian ROCA case, the administration had access to the necessary *capabilities*, including resources like highly qualified experts and practitioners, and respective established informal processes to activate them through their collaborative network ties ("collective brain"). The lack of such capabilities in terms of resources and processes to implement operational goals can be a serious obstacle in other cyber crisis contexts. In the case of the cyber attacks against the German district Anhalt-Bitterfeld in 2021, the local state's cyber security resources were insufficient. so that the district had to request assistance from federal authorities, even the Armed Forces (Stiebel, 2022). A lack of qualified personnel and organizational processes to activate resources also posed challenges in the coping with the attack against the German Bundestag in 2015 (Beuth et al., 2017). Therefore, the author added capability deployment as an additional necessary mechanism to the operational level.

**I** further emphasizes the importance of **interactive** processes in cyber crisis governance. The author found that actors' "*networked cooperation competence*", which relied on flexible and decentralized network structures as well as actors' underlying common norms and values, enhanced sense-making and coordination capacity among actors. As Section 4 outlines, those trusted relations between public and private network members had evolved historically and could then be activated once the crisis hit. The cyber and crisis literatures have repeatedly emphasized the importance of informal trust relations (Backman, 2021; Boin et al., 2016; Carr, 2016; Morgus et al., 2015). Therefore, the author sees the *building of trusted relations* as a key interactive mechanism for cooperation in the face of adverse events.

Another mechanism the author identified at the interactive level that strengthened cooperation was actors' "*collaboration capital*", which they could draw on to remain resilient in times of cyber incidents and crisis. It emerged from the *institutional memory* (Corbett et al., 2020; Hardt, 2017) of past experiences with cyber incidents, cyber exercises, and resulting interpersonal relations. Those, in turn, shape network actors' perceptions and interactions in crisis governance processes.

Finally, *legitimacy-building* through *meaning-making* and communication was crucial to justify crisis managers' course of actions and create support for their decisions. More precisely, communication and meaning-making can strengthen the procedural legitimacy of a crisis management process. Issue framing, symbolic messaging, and the organization's credibility matter to a great degree in this process (Boin et al., 2016, 78–82). In the case of cyber risks, connecting technical issues to more deeply rooted values is crucial to enhance the effectiveness of crisis communication (de Bruijn & Janssen, 2017, p. 6).

Empirical evidence from the ROCA crisis (**I**) but also other examples, like the management of the crisis in Anhalt-Bitterfeld, Germany, suggests that post-crisis lesson-drawing processes were effective in raising awareness and strengthening ex-post *accountability*.

## 5.3 Summary

This section summarized this thesis' findings relating to the question how an administration can manage a large-scale cyber crisis affecting its DG infrastructures. Based on existing concepts and empirical findings, it presented constructs for cyber crisis governance mechanisms that the thesis included in its proposed taxonomy of cyber resilience governance mechanisms. It focused primarily on the operational and interactive levels of governance and complemented Chapter 4's analysis of institutional rules and structures.

# 6 Resilience through governance of IT systems security

This chapter aims to answer sub-research question three: how can a government manage the security of the IT systems deployed in safety-relevant infrastructures? Research on and practice of (national) cyber resilience is concerned with the different procedural stages of anticipation, monitoring, response, and learning, as the previous chapters illustrated. In this context, the security and resilience of the underlying technological systems often remains a neglected aspect. However, in our ubiquitously interconnected world, those systems' (in)security constitutes the "soft underbelly" of societal digital resilience. As a result, global cyber security policy and legislation, as well as technology providers, are increasingly concerned with finding governance solutions for global IT systems security.

This chapter addresses governance mechanisms to manage the (in)security of technology and associated risks underpinning modern societies. Thereby, it is concerned with the proactive side of cyber resilience and draws on findings from **III, IV, V,** and **VI**.

In answering the research question, this chapter does not uniquely focus on DG systems but on broader trends of IT (in)security in the digital transformation of modern societies. The state, as the guarantor of safety and security for its citizens and provider of services of general interest, like healthcare, electricity, water, and others, has a special responsibility to safeguard those services' supply. This includes the underlying infrastructures' protection from disruption and the preservation of their resilience in the face of adverse cyber events that those infrastructures and systems are increasingly exposed to. Hence, the functional dimension of cyber resilience is in the foreground of the following analysis.

This chapter is divided into two subsections. The first part summarizes findings relating to institutional structures and operational processes for governing IT security – regulation and standards, as well as risk management processes – and the related challenges for public administrations. The second part discusses the more politicized aspects of technology management capacity in the context of the EU's and Germany's quest for "digital sovereignty".

## 6.1 Challenges and mechanisms of IT security and safety governance

As our societies increasingly rely on IT systems for nearly every aspect of modern life, questions of the controllability of technology have moved from the technical spheres of IT engineering into the world of policy and politics. Focusing events like data leaks about espionage and surveillance, e.g. the Snowden revelations in 2013 (**V**), data misuse, e.g. the Cambridge Analytica scandal from 2017 (Dowling, 2022), or hacking attacks against connected "Internet of Things" (IoT) systems, like cars, or medical devices (**IV**; Schneier, 2018), catalyzed awareness for those issues. The growing body of EU legislation at the time of writing is evidence to this trend.

In digitized societies, the (in)security of IT components that make up the systems we use to identify ourselves digitally, for example, can determine whether we can digitally access DG services like digital social benefits or even vote online (**I**; Krimmer et al., 2015). In the 'smart city' context, those DG security challenges become even more pertinent (Pereira et al., 2020, p. 625). In addition, devices like household appliances and toys, or safety-critical systems such as vehicles, medical devices, and intelligent power grids are part of the IoT in a broader sense – they are directly or indirectly networked with the internet.

With the networking of physical devices in the IoT, boundaries between *safety* and *IT security* are blurring. "Integrating software components across safety-critical infrastructures carries design flaws, bugs and security concerns to these systems", which attackers take advantage of (Johnson, 2012). Resulting vulnerabilities have led to new systemic risks and negative externalities, as various types of cyber attacks in recent years have demonstrated. Malicious software can infect hundreds of thousands of computer systems worldwide in a matter of hours and can disrupt critical logistics processes and production environments (Buchanan, 2016; Snyder, 2017). Examples are the WannaCry ransomware worm and subsequently the NotPetya wiper worm from 2017. Botnets consisting of IoT devices, such as the 2016 Mirai botnet, can bring down parts of internet infrastructures through massive DDoS attacks, and hackers regularly demonstrate attacks on medical devices and vehicles (Kleinhans, 2017). At the same time, many of those newly connected devices lack even basic security. For decades, IT security had simply not been a priority for manufacturers of technology, including IT manufacturers, as they lacked economic or other incentives to secure their products against cyber attacks (Anderson & Moore, 2007). Figure 8 provides an overview of the mechanisms to govern IT systems security, which the following sub-sections address in more detail.

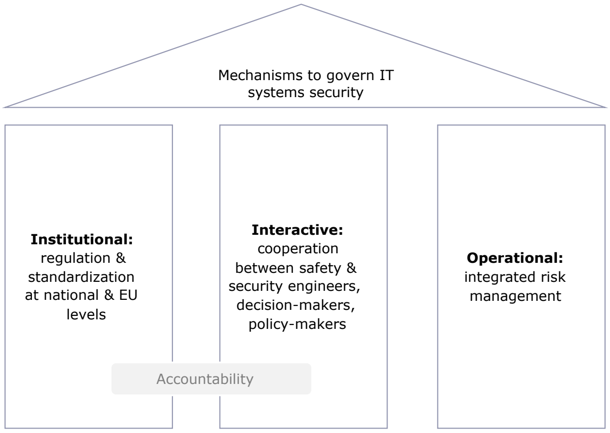

Mechanisms to govern IT systems security
**Institutional:** regulation & standardization at national & EU levels
**Interactive:** cooperation between safety & security engineers, decision-makers, policy-makers
**Operational:** integrated risk management
Accountability

***Figure 8***: *Mechanisms to govern IT systems security in safety-critical infrastructures*

### 6.1.1 Operational challenges

There are several structural security engineering challenges of an **operational** nature, which amplify the issue of IoT insecurity. First, security might compete with the *usability* and *efficiency* of IT systems. In embedded systems, security mechanisms like encryption or authentication can take up scarce computation power and memory. They can also add additional steps for end-user operation (like authenticating with multiple factors), which constrain usability (Koppel et al., 2015; Rostami et al., 2013; Sasse & Flechais, 2005).

Second, *lifecycle conflicts* are common. Software often has a much shorter lifespan than physical control systems in critical infrastructures or even connected household devices. As a result, connected devices require updates to close vulnerabilities for a longer period than software is usually supported by updates (**IV**, p. 5; (European Commission, 2022c, p. 69; Fonseca & Vieira, 2014; Yousefnezhad et al., 2020).

Third, the *patching* of security vulnerabilities is complicated. The deployment of software updates for desktop or mobile operating systems is easily feasible and scalable through end users. For devices operating in critical infrastructures, including DG infrastructures, however, the installation of updates can pose challenges (Bellovin, 2017; ICS2, 2020; Nunnikhoven, 2017). Patches usually need to be tested in their operating environment (e.g. hospitals) to prevent unforeseen interactions or malfunctions. They also need to be deployed in secure ways to avoid manipulations (**IV**, p. 5). Moreover, responsibilities for update deployment and installation within larger critical organizations need to be clear. **IV** points to this issue in the context of safety-critical medical devices in hospital or patient environments but **I** also illustrates how delicate and complicated the deployment of software updates at scale can be for DG systems.

Fourth, *proprietary and opaque software* in many IoT devices, critical and DG infrastructures diminishes the ability of end-users – whether hospitals, governments, or individuals – to control the security of the systems they use (European Commission, 2022b, p. 13). While software does not necessarily have to be open-source and free to be secure, it should at least be accessible and testable against security requirements for trusted third parties (ENISA, 2020a, p. 30; IoT Security Foundation, 2023).

Finally, as *risk management methods* for safety and IT security have evolved separately over time, methods and standards to address these risks in an integrated manner were long lacking. Safety mechanisms are mainly concerned with accidental risks originating from a system that can cause damage to the environment. Respective risk assessments traditionally rely on statistical and static methods, like the functional testing for the presence or absence of specified behaviour (**IV**; Hänninen et al., 2016; Kriaa, 2016, pp. 13–25). Yet, established safety practices fall short of addressing the cyber security threats that ensue from the growing interconnectivity of formerly isolated systems (Leverett et al., 2017).

Security, on the other hand, is concerned with risks caused by unspecified intentional behaviour of malicious threat actors. IT security risk is a function of several factors, including a threat agent and its capabilities, intent, and motivation, which exploits a vulnerability with a certain likelihood of success to cause an adverse impact (NIST, 2012). They are highly dynamic, as threats and vulnerabilities are constantly changing. Therefore, security risks of IT systems need to be constantly monitored and managed during its entire lifetime, after it has been marketed, and not only occasionally (Bryans, 2017).

### 6.1.2 Legislation, certification, and standards

Those challenges are mirrored at the **institutional level**. Technical standards and legal frameworks are yet to address these risks in an integrated manner. At the EU level, requirements for the quality and safety of products are generally defined within the framework of the "New Legislative Framework" (NLF) (which extends the "New Approach" from 1985). The NLF refers to a set of EU Directives aimed at the removal of barriers to trade and the harmonization of technical requirements to enable the free movement of goods. These lay down the essential requirements for the safety and performance of certain product groups such as machinery, toys, electrical equipment, medical devices, or construction products. For products for which there are no specific regulations, the EU General Product Safety Directive 2001/95/EC applies.

The NLF guidelines only define basic protection requirements. The technical concretization according to the "state of the art" takes place in technical standards or norms, which define the requirements and serve as a reference for certification. To prove that a product is compliant with the respective requirements, it is marked with the "CE" mark (for Communauté Européenne). Conformity assessment is carried out by the manufacturer itself (for products with a low safety risk) or by a "notified body". Notified bodies must be accredited by national accreditation bodies.

Certification resulting from conformity assessment procedures also exists for IT products, as **VI** explains in more detail. The *Common Criteria for Information Technology Security Evaluation* (CC), for example, constitute a long-established international framework for the evaluation and certification of IT security. A key task for engineers, decision-makers, and regulators is to combine different safety and security approaches to expand established practices, risk management frameworks, standards, and regulations to fit the IoT reality (**IV**; Grotto & Schallbruch, 2021; Leverett et al., 2017).

At the same time, certification has limits as a mechanism to evaluate and prove IT systems security (**VI**, pp. 179–180). Software is dynamic and requires continuous updates to close vulnerabilities or improve its functionality. Since certification is static in principle, i.e., determines compliance with requirements at a given point in time, the maintenance of products and services through updates must be handled differently. The repeated testing or re-certification of a product after each software update is not scalable because of the effort involved. These challenges must be addressed by an ICT-focused certification framework. Future testing and verification mechanisms must resolve this conflict between one-time certification and constant software development. Therefore, approaches are needed that maintain the validity of certificates over the entire product lifecycle and can map the growing complexity of technologies (Hofmann, 2023; Krcmar et al., 2018).

In an effort to respond to such challenges, the EU is in the process of adopting ever more comprehensive IT security legislation, creating an overarching legal framework for IT security (Eckhardt & Kotovskaia, 2023, p. 4). It has thereby begun to enshrine the engineering guideline of "security by design" as a "hard law" principle in primary and secondary EU legislation (Bygrave, 2022, p. 36). A first regulatory step was the adoption of the "Cybersecurity Act" (CSA)[16] in 2019, which establishes a framework for the development of certification schemes for certain ICT products, processes and services. However, certification under respective schemes is voluntary, unless specified otherwise in legislation. In 2022, the European Commission proposed the Cyber Resilience Act (CRA), which sets out horizontal cyber security requirements for most products with digital elements. It subjects manufacturers, distributors, and importers of such products to new cyber security obligations across the entire supply chain. They include, among others, IT security conformity assessments, transparency and documentation obligations, and the mandatory provision of software updates. As a horizontal framework, the CRA overlaps with the updated Network and Information Security Directive[17] and several product-specific and sectoral EU regulations, including the Radio Equipment Directive[18], the draft General Product Safety Regulation[19], as well as the Draft Artificial Intelligence Regulation[20].

In the upcoming legislative process, legislators will need to ensure that these legal acts containing provisions for IT systems security interplay in a frictionless way, avoid regulatory overlap and maintain legal certainty for market actors (Eckhardt & Kotovskaia,

[16] Regulation (EU) 2019/881

[17] Directive (EU) 2022/2555

[18] Directive 2014/53/EU

[19] COM (2021) 346 final

[20] COM/2021/206 final

2023, p. 17; Grotto & Schallbruch, 2021, p. 89). In addition, the EU Commission and member states will need to balance the CRA's measures' high complexity and resulting burdens and costs for technology manufacturers, importers and distributors, with its effectiveness in maintaining a competitive IT market.

## 6.2 The quest for "digital sovereignty"

The objective to enhance the controllability of technology of potentially insecure technological infrastructures has also resulted in debates about strengthening countries' "digital" or "technological sovereignty". These political discussions are characterized by geopolitical considerations regarding the control over technologies and impacts on states', economies', and individuals' capacity to act (Benner & Skierka, 2015; Pohle & Thiel, 2020).

Calls for promoting technological sovereignty first surfaced in Europe in the wake of the former National Security Agency (NSA) contractor Edward Snowden's revelations of US intelligence agencies' surveillance activities of European citizens, companies, and heads of state. **V** provides a comprehensive mapping of senior officials' and decision-makers' proposals between 2013 and 2015 to strengthen control over technology and prevent espionage and surveillance. The proposals included technical proposals, such as new undersea cables, localization of data storage and flows, and strengthened encryption, and policy proposals, such as the provision of better support to local industry, or better data protection laws. However, an evaluation of the technical proposals in **V** shows their limited effectiveness in strengthening individuals', companies', or states' protections against surveillance or espionage. The implementation of better encryption of data at flow would have significantly improved data security. However, most other proposals, like the restriction of internet traffic routing within the Schengen-zone, were neither feasible nor compatible with the principles of an open internet.

We can regard **V** as a snapshot of the early debate about digital or technological sovereignty and an analysis of its origins in Europe. Many of the concrete proposals did not sustain themselves over time and slowly disappeared again from the political agenda. Others were implemented. For example, to protect its DG infrastructures, the German government terminated contracts with US providers like Verizon that had provided services for the German government network, and replaced them with German providers (Deutscher Bundestag, 2017; Hathaway, 2014).

Remarkably, the quest for digital or technological sovereignty remains a key objective of European and especially German IT security policy, as evidenced by Germany's "Digital Agenda" from 2014 and its most recent cyber security strategy from 2021 (**II**, pp. 9–11; BMI, 2021).

Despite their extensive use in public discourse, to this date technological or digital sovereignty remain political expressions that serve to strengthen the case for a range of measures ranging from the promotion of privacy-preserving legislation and tools to more comprehensive support of domestic and European IT industries, e.g. through the Cloud hyper scaling project Gaia-X (Monsees & Lambach, 2022). Their meaning remains a subject of debate among experts, policy makers and practitioners (Lambach & Oppermann, 2022; Pohle & Thiel, 2020).

An interesting aspect with respect to the previous subsection is the resurgence of the notion of digital sovereignty in the context of potential and actual bans of critical infrastructure components manufactured by technology vendors deemed untrustworthy.

The case of the debate around a restriction of the participation of the Chinese technology company Huawei in the expansion of EU members' 5G mobile networks is a prime example. The author has described the case in more detail (Skierka, 2020). The EU, caught between its two main trading partners, the US and China, was facing a geopolitical challenge: how should it deal with potentially risky but effective and competitive technology provided by Chinese firms in its next generation of telecommunications networks? This challenge also had broad implications for the region's cyber resilience.

As mentioned above, purely technical mechanisms to evaluate and prove IT security of systems, like technical testing and certification, have limits. They are not suitable for assessing national security risks and insufficient for overarching risk assessments.

In the case of 5G networks, the EU adopted a comprehensive risk assessment procedure called the "5G Cyber security Toolbox" in 2020 that identifies technical and strategic measures to mitigate security risks and critical dependencies in 5G networks. The toolbox makes clear that strategic risks – in particular the "risk of interference by a third country or dependency risks" – cannot be managed through purely technical measures alone but requires additional political or regulatory measures. As a result of this debate, Germany adopted new legal rules in the 2021 IT Security Act 2.0, which require an additional evaluation of trustworthiness of components to be built into critical infrastructures (Skierka, 2020).

At the same time, such procedures will need to be designed in a way to safeguard accountability of decisions. As **III** demonstrates, respecting formal procedures in technocratic risk management processes does not necessarily translate into actual accountability. Decisions can then be politically contested. One example from Germany for such a decision is the government's BSI's issuance of an official warning against the use of Kaspersky software in 2022, after Russia had attacked Ukraine (BSI, 2022). Administrative courts confirmed the legality of the warning (*4 B 473/22*, 2022). Yet, the decision has sparked an ongoing public debate about who should decide about the risks of software and hardware in the future, and how that 'high risk' should be determined in an accountable way (Atug & Herpig, 2022; Kipker, 2022).

## 6.3 Synthesis: Mechanisms of IT systems security governance

Addressing challenges of IT systems security governance requires not only technical but also policy and governance responses at the operational and institutional levels, as we show in **IV** and **VI** (see also: Grotto & Schallbruch, 2021, pp. 79–82). Technology manufacturers and suppliers can take several measures at the operational level, such as applying security principles in the design and development phases of systems; integrating safety and security risk assessments and management; and operating vulnerability reporting programmes, among others (**IV**, pp. 7–8).

Administrations, in their role as regulator, will need to work on harmonized legal rules fostering these operational principles at the institutional level, while paying attention to keeping the market competitive. Moreover, they can design organizations and instruments to support and incentivize practices like effective standardization, cybersecurity information-sharing, awareness-raising, training, and incident response through governance mechanisms at operational, interactive, and institutional levels.

The debate about digital sovereignty and the case of the 5G network rollout illustrate how seemingly technical issues of IT systems security are becoming increasingly politicized. They further illustrate the interaction and partial conflict between cyber resilience governance mechanisms at the operational and institutional levels, and actors' or administrations' political goals.

One governance aspect that is missing from these debates is that of accountability. As **III** shows in the context of the EU's food safety regime, compliance with risk governance processes and safety regulation does not ensure accountability. Lessons from that case study can be transferred to the IT security evaluation regime of procedures, standards, and regulations. Uncertain risks resulting from IT innovation pose a particular governance challenge. Hence, decision-makers would do well to make their decisions about dealing with high-risk manufacturers or other issues of technological sovereignty understandable and their processes accountable.

# 7 Conclusion

This thesis set out to explore governance mechanisms for the digital state's resilience against adverse cyber events. Today, the performance of core government functions increasingly depends on the availability and integrity of its information infrastructures. The thesis put forth one primary research question and three sub-research questions to be answered:

**How can an administration develop governance mechanisms which enhance the cyber resilience of the e-state?**

1. How does a country's national cyber security architecture impact its approach to cyber resilience?
2. How can an administration manage and overcome a cyber crisis affecting a critical DG system on a large scale?
3. How can an administration govern the security of IT systems deployed in safety-relevant infrastructures?

The overall objective of this thesis is to contribute theoretically and empirically founded research to a yet underexplored field in academic literature at the intersection of DG, cyber security, and resilience. Thereby, it also aims to complement the predominantly practical and policy approaches that currently exist to address challenges of cyber risk to the digital state with more methodologically rigorous and in-depth analysis.

To answer these questions, this doctoral thesis relied on research contributions from six publications. The publications originate from different scholarly disciplines and address varied aspects of cyber security, DG, and resilience from technical, organizational, and institutional perspectives. An interdisciplinary angle to study the thesis topic was particularly suitable, as research on cyber resilience, particularly in the context of DG, is only emerging in the social sciences.

It takes an interactive governance approach as a point of departure for the analysis, in which the state and a plurality of other actors from society interact to provide the steering of DG and cyber security. The findings of this thesis mainly build on case study research strategies, as well as on applied legal and policy analyses.

To answer the main research question, this thesis proposes inductively derived constructs along which governments can develop governance mechanisms to enhance cyber resilience of their e-state. It identifies mechanisms at three different levels of governance – the institutional, the interactive, and the operational levels. Resilience comprises both an administration's structural resilience – its ability to maintain and adapt its administrative structures to adverse events – and its functional resilience – its ability to maintain control of technological systems and the functions depending on those. At the institutional level, governance mechanisms of cyber resilience comprise formal and informal rules, as well as organizational structures. At the interactive level, cyber resilience governance mechanisms encompass interactive processes, which influence cooperation in networks. Those include trusted relationship-building, institutional memory development, meaning-making and communication, and accountability of interaction. Key mechanisms at the operational level through which states can enhance cyber resilience, include technology management, comprehensive risk management, and the deployment of capabilities (resources and processes). Importantly, mechanisms at different levels influence and shape each other, as the publications' findings and the responses to the sub-research questions show.

The thesis proposes these constructs within an outline of a taxonomy of e-state cyber resilience governance mechanisms, which can serve as a basis for further analysis in future research. Throughout the thesis, the proposed taxonomy serves as an overarching framework that structures the replies to the sub-research questions.

To answer the first sub-research question how a country's national cyber security architecture impacts its approach to cyber resilience, the thesis explores the different ways in which Germany and Estonia organize the governance of cyber security at the national level. It concludes that the broader institutional structures and culture, and the degree of interaction and trust within governance networks influences actors' capacity to effectively coordinate their actions horizontally and vertically, as well as the effective deployment of capabilities across levels of government. Thereby, Chapter 4 illustrates the tight interaction between institutional and interactive governance mechanisms. It further highlights the potential of institutional theoretical approaches to explain institutional and organizational path dependencies – e.g. Germany's complex multi-level cyber security architecture – or actors' norms and ideas – e.g. Estonia's cyber security and DG's community shared beliefs in the governance networks' "collective brain" or Germany's formalistic administrative culture. It proposes to explore contemporary and future institutional change in both countries, particularly Germany with institutional theoretical approaches.

In its answer to the second sub-research question – how an administration can manage and overcome a cyber crisis affecting a critical DG system at large scale – the thesis draws on the authors' publications' findings and a combination from the network governance and cyber crisis literatures to identify several constructs at the operational and interactive levels explaining cyber crisis management in DG.

The thesis identifies an antecedent for decision-making in cyber crisis processes affecting DG systems, notably the DG's systemic criticality. It proposes that the degree of a DG system's criticality will greatly influence the costs that governments are willing to incur to maintain its availability during a cyber crisis. Moreover, it proposes that a country's crisis governance networks' management of cyber resilience needs to be assessed based on five interactive and operational constructs: their 1) technology management capacity, 2) networked cooperation capability, 3) collaboration capital, 4) risk management capacity, and 5) legitimacy building. Those factors feed into the taxonomy of cyber resilience governance mechanisms for further testing and development in future studies.

In addressing the third sub-research question, the thesis examines the proactive side of cyber resilience concerned with the management of the IT security of systems that underlie modern societies' infrastructures. It identifies several operational and institutional governance mechanisms in the EU and at the national level in Germany, which states use to enhance their technology management capacity. First, the EU increasingly engages in expanding its regulatory framework for the IT security of products and services. The author argues that while this endeavour is ongoing, policy-makers need to avoid the risk of fragmentation or regulatory overlap. Second, as **IV** and **VI** show, the challenges arising from the convergence of safety and security in the IoT requires not only regulatory measures, but also the promotion of standards and risk management procedures that integrate both dimensions (as well as privacy, which this thesis does not consider in depth). Third, in their quest to extend their political control over the security and trustworthiness of technologies they use, states resort to broad notions of "digital" or "technological sovereignty" (**V**). Amid this debate, the case of the restriction of

Chinese suppliers in the rollout of next-generation 5G mobile networks illustrates tensions between technical and national security approaches to manage cyber security risks. The design and implementation of risk assessments that integrate these different operational, geopolitical, and national security aspects will influence states' future cyber resilience in significant ways. At the same time, shifting risk assessment and management processes to expert committees and technocratic processes risks negatively impacting the accountability of decisions about the deployment of technologies in critical infrastructures. Here, the thesis draws on lessons from the lack of accountability of the EU governance process of uncertain food safety risks in **III**.

Overall, this thesis contributes in three ways. First, it provides a proposal for a taxonomy for governance mechanisms of cyber resilience of the e-state. This taxonomy constitutes a first step toward proposing measures that administrations – in cooperation with other stakeholders – can develop to address cyber resilience. It shall serve as a basis for further refinement of those mechanisms in research and practice. Second, the thesis contributes to the emerging literature of cyber crisis management through empirical insights on interactive governance processes during a crisis in one of the most digitized countries internationally, notably Estonia. Third, it raises several practical policy considerations related to the future design of cyber security regulation and risk assessment in the field of tension between technological security, geopolitics, and national security.

Based on the six different publications, this thesis covers a broad range of topics that each can only be partially illuminated from specific angles. As mentioned in the methodology, the case studies that this thesis relies on do not claim statistical but analytical generalizability. A cyber crisis affecting Estonia's DG will almost certainly play out very differently in France, the United States or a country from yet a different part of the world, for example. Cyber security organizations and regulation in Germany differ from those in neighbouring countries. However, the constructs and practical takeaways the author identified in her research might be useful and testable in future case studies. The taxonomy to analyse governance mechanisms, and each of the constructs and categories identified at the intersection of cyber resilience and DG, offer several avenues for further conceptual and empirical studies.

One field that future research should explore is how and to what extent institutional governance mechanisms impact institutional change in the context of national cyber resilience: How can those mechanisms lead to actual changes in the institutional structures to anticipate, monitor, respond to, and learn from cyber adversity? In particular, the roles of endogenous and exogenous factors merit more empirical in-depth analysis. The study of endogenous factors could, for example, examine how ideational changes among actors within institutions, including their beliefs and evaluation of cyber security and DG administrative structures or culture, affect those very structures over time. In a related manner, changes in the interests and strategies of powerful political actors who can have the ability to change cyber security and DG institutions could play an important role. Regarding exogenous factors, future studies could examine whether and how severe cyber incidents or crises can lead to changes in administrative cybersecurity structures or "critical junctures" (Mahoney, 2000) in established paths in administrative cyber security structures. In this context, more research is also needed on the stage of learning from cyber crises, and how this feeds back into the overall cyber resilience process.

At the time of writing, it appears that institutional change is underway in Germany's organizational cyber security architecture, resulting from several severe cyber incidents in DG at the local levels, pressures from industry and civil society stakeholders, and a higher interest in the issue among political actors, mainly at the federal level. Therefore, Germany continues to constitute a case of interest to study further. In Estonia, a comparison of institutional changes after the cyber crises from 2007, 2017, and recent incidents during the period of the Russian war against Ukraine from 2022 onwards, might yield insightful findings. The author proposes that future research should examine how a combination of historical, ideational, and rational choice institutional approaches can provide paths for further analysis and extend existing theoretical models (see: Koning, 2016).

Yet, this dissertation's findings are limited to two EU member states. Considerably more research is needed beyond the EU and also the US contexts, which much of the literature about governance and cyber security has focused on so far (Chen & Yang, 2022; Peters, 2014). Future studies could, for example, explore the governance of cyber resilience in Asia, Africa, and Latin America. Particular attention could be paid to rising powers (e.g. Brazil, China, and India) and the so-called "Swing States" in the internet governance debate (Ebert & Maurer, 2013; Maurer & Morgus, 2014).

Another fruitful area for further work is the analysis of the link between learning and adaptive governance for cyber resilience. As shown at various points throughout this thesis, learning is an essential step in the cycle of (cyber) resilience. At the same time, it is often neglected in practice – policy actors frequently lack incentives to engage in critical evaluation of their actions and subsequent reform. This thesis' research suggests that learning is likely to occur because of exogenous factors like cyber crises. More research is needed to explore the role of learning as a core value of adaptive governance (taking as a starting point, for example: Janssen & van der Voort, 2016; Kim et al., 2020; Smith & Lawrence, 2018) of cyber resilience based on empirical data.

In the context of the dynamic field of IT systems security governance and digital sovereignty, future geopolitical technology rivalries between nations will continue to influence cyber resilience governance. Additional studies will be needed that explore the impact of future developments in international relations on the EU's and states' institutional approach to govern cyber resilience. Particular attention should be paid to the blurring of boundaries between broader geopolitical trends and operational approaches to technology risk governance.

In conclusion, this thesis has proposed several constructs along which researchers and practitioners can develop governance mechanisms that enhance cyber resilience of the e-state. While it is beyond the scope of this thesis to investigate and test each one of those mechanisms comprehensively, it provides multiple starting points for avenues of future work at the intersection of DG, cyber security and resilience.

# List of Figures

# List of Tables

# References

4 B 473/22, (OVG Nordrhein-Westfalen 28 April 2022). https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=OVG%20Nordrhein-Westfalen&Datum=28.04.2022&Aktenzeichen=4%20B%20473/22

Abel, S. (2014, May 13). Government Calls Group's Criticism of National E-Voting System Unfair. *ERR*. https://news.err.ee/112524/government-calls-group-s-criticism-of-national-e-voting-system-unfair

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), 1–15. https://doi.org/10.1093/cybsec/tyy006

Amit, R., & Shoemaker, P. J. H. (1993). Strategic assets and organizational rent. *Strategic Management Journal*, *14*(1), 33–46.

Anderson, R., & Moore, T. (2007). Information Security Economics – and Beyond. In A. Menezes (Ed.), *Advances in Cryptology—CRYPTO 2007* (pp. 68–91). Springer. https://doi.org/10.1007/978-3-540-74143-5_5

Andrade, R. O., Guun Yoo, S., Tello-Oquendo, L., & Ortiz-Garcés, I. (2021). Cybersecurity, sustainability, and resilience capabilities of a smart city. In A. Vizvizi & R. Perez del Hoyo (Eds.), *Smart cities and the UN's SDG's* (pp. 181–193). Elsevier.

Ansell, C., & Torfing, J. (Eds.). (2022). *Handbook on Theories of Governance*. Edward Elgar Publishing. https://doi.org/10.4337/9781800371972

Atug, M., & Herpig, S. (2022). Kaspersky-Produktwarnung: Reine Symbolpolitik? *Tagesspiegel Background Cybersecurity*. https://background.tagesspiegel.de/cybersecurity/kaspersky-produktwarnung-reine-symbolpolitik

Austin, G. (2020). *National cyber emergencies: The return to civil defence*. Routledge.

Austin, G., & Sharma, M. (2020). From cyber resilience to civil defence: Contested concepts, elusive goals. In G. Austin (Ed.), *National cyber emergencies: The return to civil defence* (pp. 10–30). Routledge.

Backman, S. (2021). Conceptualizing Cyber Crises. *Journal of Contingencies and Crisis Management*, *29*, 429–438.

Baggott, S. S., & Santos, J. R. (2020). A Risk Analysis Framework for Cyber Security and Critical Infrastructure Protection of the US Electric Power Grid. In *Risk Analysis* (Vol. 40, Issue 9, pp. 1744–1761). https://doi.org/10.1111/risa.13511

BBK. (2023). *LÜKEX Aktuell*. Bundesamt Für Bevölkerungsschutz Und Katastrophenhilfe (BBK). https://www.bbk.bund.de/DE/Themen/Krisenmanagement/LUEKEX/Aktuell/aktuell.html

Beduschi, A. (2021). Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations. *Data & Policy*, *3*, e15. https://doi.org/10.1017/dap.2021.15

Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. In *Journal of Strategic Information Systems* (Vol. 17, Issue 2, pp. 165–176). https://doi.org/10.1016/j.jsis.2007.12.002

Bell, S. (2002). Institutionalism: Old and New. In D. Woodward, A. Parkin, & J. Summers (Eds.), *Government, Politics, Policy and Power in Australia* (7th ed.). Longman.

Bellovin, S. (2017, May 12). Patching is hard. *SM Blog, Columbia University*. https://www.cs.columbia.edu/~smb/blog/2017-05/2017-05-12.html

Benner, T., & Skierka, I. (2015). Digitale Souveränität—Begriffsdefinition. In *Handwörterbuch Internationale Politik* (Vol. 13, pp. 45–49). Verlag Barbara Budrich.

Beuth, P., Biermann, K., Klingst, M., & Stark, H. (2017, May 11). Bundestags-Hack: So wurde das deutsche Parlament ausspioniert. *Die Zeit*. https://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland

Bevir, M. (2011). *The SAGE Handbook of Governance*. SAGE Publications.

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber Resilience – Fundamentals for a Definition. In A. Rocha, A. M. Correia, S. Costanzo, & L. P. Reis (Eds.), *New Contributions in Information Systems and Technologies* (Vol. 353, pp. 311–316). Springer International Publishing. https://doi.org/10.1007/978-3-319-16486-1_31

BMI. (2021). *Cybersicherheitsstrategie für Deutschland 2021*. Bundesministerium des Innern, für Bau und Heimat. https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf;jsessionid=F8255BD5C1A027AE19A3B0D36B9F283E.1_cid340?__blob=publicationFile&v=2

BMI. (2022). *Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat*. https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.pdf?__blob=publicationFile&v=4

Boeke, S. (2018). National cyber crisis management: Different European approaches. *Governance*, *31*(3), 449–464. https://doi.org/10.1111/gove.12309

Boin, A. (2005). Disaster research and future crises: Broadening the research agenda. In *International Journal of Mass Emergencies and Disasters* (Vol. 23, Issue 3, pp. 199–214).

Boin, A., Busuioc, M., & Groenleer, M. (2014a). Building European Union capacity to manage transboundary crises: Network or lead-agency model? *Regulation & Governance*, *8*, 418–436.

Boin, A., Busuioc, M., & Groenleer, M. (2014b). Building European Union capacity to manage transboundary crises: Network or lead-agency model?: Building EU crisis management capacity. *Regulation & Governance*, *8*(4), 418–436. https://doi.org/10.1111/rego.12035

Boin, A., & Bynander, F. (2015). Explaining success and failure in crisis coordination. *Geografiska Annaler: Series A, Physical Geography*, *97*, 123–135. https://doi.org/doi:10.1111/geoa.12072

Boin, A., Comfort, L. K., & Demchak, C. C. (2010). The rise of resilience. In L. K. Comfort, A. Boin, & C. C. Demchak (Eds.), *Designing resilience: Preparing for extreme events*. University of Pittsburgh Press.

Boin, A., & 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), 50–59. https://doi.org/10.1111/j.1468-5973.2007.00504.x

Boin, A., ’t Hart, P., & Kuipers, S. (2018). The Crisis Approach. In H. Rodrigues, W. Donner, & J. Trainor (Eds.), *Handbook of Disaster Research* (2nd ed.). Springer.

Boin, A., ’t Hart, P., Stern, E., & Sundelius, B. (2016). *The politics of crisis management: Public leadership under pressure*. Cambridge University Press.

Bovens, M. (2007). Analysing and Assessing Accountability: A Conceptual Framework. *European Law Journal*, *13*(4), 447–468. https://doi.org/10.1111/j.1468-0386.2007.00378.x

Brechbuhl, H., Bruce, R., Dynes, S., & Johnson, M. E. (2010). Protecting Critical Information Infrastructure: Developing Cybersecurity Policy. In *Information Technology for Development* (Vol. 16, Issue 1, pp. 83–91).

Bryans, J. W. (2017). The Internet of Automotive Things: Vulnerabilities, risks and policy implications. *Journal of Cyber Policy*, *2*(2), 185–194. https://ideas.repec.org//a/taf/rcybxx/v2y2017i2p185-194.html

BSI. (2022, March 15). *BSI-Warnung gemäß BSIG § 7: Virenschutzsoftware des Herstellers Kaspersky*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Warnungen-nach-P7_BSIG/Archiv/2022/BSI_W-004-220315.html?nn=129284

Buchanan, B. (2016). The Life Cycles of Cyber Threats. *Survival*, *58*(1), 39–58. https://doi.org/10.1080/00396338.2016.1142093

Bundesregierung. (2022). *Digitalstrategie: Gemeinsam digitale Werte schöpfen*. https://bmdv.bund.de/SharedDocs/DE/Anlage/K/presse/063-digitalstrategie.pdf?__blob=publicationFile

Burgess, M. (2022, June 12). Conti’s Attack Against Costa Rica Sparks a New Ransomware Era. *Wired*. https://www.wired.com/story/costa-rica-ransomware-conti/

Bygrave, L. A. (2022). Cyber Resilience versus Cybersecurity as Legal Aspiration. *2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon)*, *700*, 27–43. https://doi.org/10.23919/CyCon55549.2022.9811084

Caldarulo, M., Welch, E. W., & Feeney, M. K. (2022). Determinants of cyber-incidents among small and medium US cities. *Government Information Quarterly*, *39*(3), 101703. https://doi.org/10.1016/j.giq.2022.101703

Cardash, S., Cilluffo, F., & Ottis, R. (2013). Estonia’s Cyber Defence League: A Model for the United States? *Studies in Conflict and Terrorism*, *36*(9), 777–787.

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43–62. https://doi.org/10.1111/1468-2346.12504

Chen, X., & Yang, Y. (2022). Contesting Western and Non-Western Approaches to Global Cyber Governance beyond Westlessness. *The International Spectator*, *57*(3), 1–14. https://doi.org/10.1080/03932729.2022.2101231

Cheng, Y. (Daniel). (2019). Governing Government-Nonprofit Partnerships: Linking Governance Mechanisms to Collaboration Stages. *Public Performance & Management Review*, *42*(1), 190–212. https://doi.org/10.1080/15309576.2018.1489294

Chokshi, Niraj. (2019, May 22). *Hackers Are Holding Baltimore Hostage: How They Struck and What’s Next*. The New York Times. https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html

Christensen, T., Danielsen, O. A., Lægreid, P., & Rykkja, L. H. (2016). Comparing Coordination Structures for Crisis Management in Six Countries. *Public Administration*, *94*(2), 316–332. https://doi.org/10.1111/padm.12186

Christensen, T., Laegreid, P., & Rykkja, L. H. (2016). Organizing for Crisis Management: Building Governance Capacity and Legitimacy. *Public Administration Review*, *76*(6), 887–897. https://doi.org/10.1111/puar.12558

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2021). *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology* (NIST SP 800-61r2; p. NIST SP 800-61r2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

CISA. (2022, April 8). *Emergency Directive 22-02*. https://www.cisa.gov/emergency-directive-22-02

Corbett, J., Grube, D. C., Brooke, H., & Scott, J. R. (2020). *Institutional Memory as Storytelling—How Networked Government Remembers*. Cambridge University Press.

Crandall, M., & Allan, C. (2015). Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms. *Contemporary Security Policy*, *36*(2), 346–386.

Crootoft, R. (2018). International Cybertorts: Expanding State Accountability in Cyberspace. *Cornell Law Review*, *103*(3), 565–644.

CSRC. (2023). *information security—Glossary | CSRC*. NIST Computer Security Resource Center. https://csrc.nist.gov/glossary/term/information_security

Czosseck, C., Ottis, R., & Talihärm, A.-M. (2011). Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *1*(1), 24–34.

de Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7. https://doi.org/10.1016/j.giq.2017.02.007

Demchak, C. C. (2020). Cybered conflict, hybrid war, and informatization wars. In E. Tikk & M. Kerttunen (Eds.), *Routledge handbook of international cybersecurity* (pp. 36–51). Routledge, Taylor & Francis Group.

Deutscher Bundestag. (2017). *Abschlussbericht des 1. Untersuchungsausschusses (NSA)* (Drucksache 18/12850).

Deutscher Bundestag. (2023, January 25). *Deutscher Bundestag—Anhörung zur Cybersicherheit—Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland*. Deutscher Bundestag. https://www.bundestag.de/ausschuesse/a23_digitales/Anhoerungen/928388-928388

Deverell, E. C. (2010). *Crisis-induced learning in public sector organizations*. Utrecht University.

Dowling, M.-E. (2022). Cyber information operations: Cambridge Analytica's challenge to democratic legitimacy. *Journal of Cyber Policy*, *7*(2), 230–248. https://doi.org/10.1080/23738871.2022.2081089

Dubois, A., & Gadde, L.-E. (2002). Systematic combining: An abductive approach to case research. *Journal of Business Research*, *55*(7), 553–560. https://doi.org/10.1016/S0148-2963(00)00195-8

Duit, A. (2016). Resilience Thinking: Lessons for Public Administration. *Public Administration*, *94*(2), 364–380.

Dunn Cavelty, M. (2005). The socio-political dimensions of critical information infrastructure protection. *International Journal of Critical Infrastructures*, *1*(2/3), 258–268.

Dunn Cavelty, M., & Egloff, F. J. (2019). The Politics of Cybersecurity: Balancing Different Roles of the State. *St Antony's International Review*, *15*(1), 37–57.

Dwivedi, Y. K., Sahu, G. P., Rana, N. P., Singh, M., & Chandwani, R. K. (2016). Common Services Centres (CSCs) as an approach to bridge the digital divide: Reflecting on challenges and obstacles. In *Transforming Government: People, Process and Policy* (Vol. 10, Issue 4, pp. 511–525). https://doi.org/10.1108/TG-01-2016-0006

Ebert, H., & Maurer, T. (2013). Contested Cyberspace and Rising Powers. *Third World Quarterly*, *34*(6), 1054–1074. https://www.jstor.org/stable/42002175

Eckhardt, P., & Kotovskaia, A. (2023). The EU's cybersecurity framework: The interplay between the Cyber Resilience Act and the NIS 2 Directive. *International Cybersecurity Law Review*. https://doi.org/10.1365/s43439-023-00084-z

Eggers, S., & Le Blanc, K. (2021). Survey of cyber risk analysis techniques for use in the nuclear industry. *Progress in Nuclear Energy*, *140*, 1–17. https://doi.org/10.1016/j.pnucene.2021.103908

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *The Academy of Management Review*, *14*(4), 532–555. https://www.jstor.org/stable/258557

ENISA. (2020a). *Guidelines for Securing the Internet of Things*. https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

ENISA. (2020b, September 29). *Blue OLEx 2020: The European Union Member States launch the Cyber Crisis Liaison Organisation Network (CyCLONe)*. https://www.enisa.europa.eu/news/enisa-news/blue-olex-2020-the-european-union-member-states-launch-the-cyber-crisis-liaison-organisation-network-cyclone

ERR, E. N. |. (2023, March 4). *Estonia sets new e-voting record at Riigikogu 2023 elections*. ERR. https://news.err.ee/1608904730/estonia-sets-new-e-voting-record-at-riigikogu-2023-elections

eSentire. (2022). *ESentire | 2022 Official Cybercrime Report*. https://www.esentire.com/resources/library/2022-official-cybercrime-report

Estonian Ministry of Defence. (2008). *Cyber Security Strategy*. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cyber-security-strategy/@@download_version/993354831bfc4d689c20492459f8a086/file_en

European Commission. (2020). *2020 Strategic Foresight Report: Charting the course towards a more resilient Europe*. Publications Office. https://ec.europa.eu/info/sites/default/files/strategic_foresight_report_2020_1_0.pdf

European Commission. (2022a). *Digital Economy and Society Index (DESI) 2022—Digital public services*. https://digital-strategy.ec.europa.eu/en/policies/desi-digital-public-services

European Commission. (2022b). *Impact Assessment Report 1/3 Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020* (SWD(2022) 282 final, Part 1/3).

European Commission. (2022c). *Impact Assessment Report 2/3 Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020* (SWD(2022) 282 final, Part 2/3).

European Commission, Capgemini, Sogeti, IDC, & Politecnico di Milano. (2022). *eGovernment Benchmark 2022: Synchronising digital governments : insight report.* https://data.europa.eu/doi/10.2759/488218

European Union. (2020). *Official Journal L 351I/2020—Council Decision (CFSP) 2020/1537 of 22 October 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States*. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2020:351I:FULL&from=DE

Flade, F., & Mascolo, G. (2020, May 5). Hackerangriff auf Bundestag—Haftbefehl gegen Russen. *Sueddeutsche.De*. https://www.sueddeutsche.de/politik/hack-bundestag-angriff-russland-1.4891668

Fonseca, J., & Vieira, M. (2014). A Survey on Secure Software Development Lifecycles. In *Software Design and Development: Concepts, Methodologies, Tools, and Applications* (pp. 17–33). IGI Global. https://doi.org/10.4018/978-1-4666-4301-7.ch002

Foote, C., Maness, R. C., Jensen, B., & Valeriano, B. (2020). Cyber conflict at the intersection of information operations: Cyber-enabled information operations, 2000–2016. In C. Whyte, A. T. Thrall, & B. M. Mazanec (Eds.), *Information warfare in the age of cyber conflict* (pp. 54–70). Routledge/Taylor & Francis Group.

Fountain, J. E. (2001). *Building the virtual state: Information technology and institutional change*. Brookings Institution Press.

Frances, J., Levatic, R., Mitchell, J., & Thompson, G. (1991). Introduction. In G. Thompson & Open University (Eds.), *Markets, hierarchies, and networks: The coordination of social life* (pp. 1–20). Sage Publications.

Freude, A. C. H., & Freude, T. (2016). *Echoes of History: Understanding German Data Protection* (Newpolitik, pp. 85–91). Bertelsmann Foundation. https://www.astrid-online.it/static/upload/freu/freude_newpolitik_german_policy_translated_10_2016-9.pdf

G7 Presidency. (2022). *Joint Declaration by the G7 Digital Ministers on cyber resilience of digital infrastructure in response to the Russian war against Ukraine*.

Gedris, K., Bowman, K., Neupane, A., Hughes, A., Bonsignore, E., West, R., Balzotti, J., & Hansen, D. (2021). Simulating municipal cybersecurity incidents: Recommendations from expert interviews. In *Proceedings of the 54th Hawaii International Conference on System Sciences (HICSS-54)* (pp. 2036–2045). University of Hawai'i at Manoa. https://doi.org/10.24251/HICSS.2021.249

George, A. L., & Bennett, A. (2005). *Case studies and theory development in the social sciences*. MIT Press.

Gerring, J., & Cojocaru, L. (2016). Selecting Cases for Intensive Analysis: A Diversity of Goals and Methods. *Sociological Methods & Research*, *45*(3), 392–423.

Gil-Garcia, J. R., Dawes, S. S., & Pardo, T. A. (2018). Digital government and public management research: Finding the crossroads. In *Public Management Review* (Vol. 20, Issue 5, pp. 633–646). https://doi.org/10.1080/14719037.2017.1327181

Gil-García, J. R., & Pardo, T. A. (2005). E-government success factors: Mapping practical tools to theoretical foundations. In *Government Information Quarterly* (Vol. 22, Issue 2, pp. 187–216). https://doi.org/10.1016/j.giq.2005.02.001

Gisladottir, V., Ganin, A. A., Keisler, J. M., Kepner, J., & Linkov, I. (2017). Resilience of Cyber Systems with Over- and Underregulation. *Risk Analysis*, *37*(9), 1644–1651. https://doi.org/10.1111/risa.12729

Google TAG, Mandiant, & Google Trust & Safety. (2023). *Fog of War—How the Ukraine Conflict Transformed the Cyber Threat Landscape*. https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

Greenberg, A. (2019). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers* (First edition.). Doubleday.

Greenberg, A. (2018, August 22). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *WIRED*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Groenendaal, J., & Helsloot, I. (2021). Cyber resilience during the COVID-19 pandemic crisis: A case study. *Journal of Contingencies and Crisis Management*, *29*(4), 439–444. https://doi.org/10.1111/1468-5973.12360

Grotto, A. J., & Schallbruch, M. (2021). Cybersecurity and the risk governance triangle: Cybersecurity governance from a comparative U.S.–German perspective. *International Cybersecurity Law Review*, *2*(1), 77–92. https://doi.org/10.1365/s43439-021-00016-9

Guarnieri, C. (2015, June 19). *Digital Attack on German Parliament: Investigative Report on the Hack of the Left Party Infrastructure in Bundestag*. Netzpolitik.Org. https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/

Hänninen, K., Hansson, H., Thane, H., & Saadatmand, M. (2016). Inadequate Risk Analysis Might Jeopardize The Functional Safety of Modern Systems. *Västeras*.

Hardt, H. (2017). How NATO remembers: Explaining institutional memory in NATO crisis management. *European Security*, *26*(1), 120–148. https://doi.org/10.1080/09662839.2016.1263944

Hathaway, M. (2014). Connected choices: How the internet is challenging sovereign decisions. *American Foreign Policy Interests*, *36*(5), 300–313.

Hay Newman, L. (2022, August 4). An Attack on Albanian Government Suggests New Iranian Aggression. *WIRED*. https://www.wired.com/story/iran-cyberattack-albania/

Hedström, P., & Swedberg, R. (1996). Social Mechanisms. *Acta Sociologica*, *39*(3), 281–308.

Helmke, G., & Levitsky, S. (2004). Informal Institutions and Comparative Politics: A Research Agenda. *Perspectives on Politics*, *2*(04), 725–740. https://doi.org/10.1017/S1537592704040472

Herpig, S. (2021). *Sachverständigenstellungnahme von Dr. Sven Herpig, Leiter für Internationale Cybersicherheitspolitik bei der Stiftung Neue Verantwortung e. V., für die Sitzung des Bundestagsausschusses für Inneres und Heimat am 01.03.2021 zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit Informationstechnischer Systeme – BT-Drucksache 19/26106*. Deutscher Bundestag. https://www.bundestag.de/resource/blob/824770/b6ab111086e6417ab4c3fccb4d5a6846/A-Drs-19-4-741-B-data.pdf

Herpig, S., Rupp, C., Dutke, F., & Beigel, R. (2023). *Deutschlands staatliche Cybersicherheits-architektur*. https://www.stiftung-nv.de/de/publikation/deutschlands-staatliche-cybersicherheitsarchitektur

Hofmann, J. M. (2023). *Dynamische Zertifizierung*. Nomos Verlag. https://www.nomos-shop.de/nomos/titel/dynamische-zertifizierung-id-73727/

Hollnagel, E. (2017). *Safety-II in practice: Developing the resilience potentials* (1st ed.). Routledge.

Homburg, V. (2004). E-government and NPM: A perfect marriage? *Proceedings of the 6th International Conference on Electronic Commerce - ICEC '04*, 547. https://doi.org/10.1145/1052220.1052289

ICS2. (2020, December 15). *Patch Management in IT and OT Environments*. (ISC)$^2$ Blog. https://blog.isc2.org/isc2_blog/2020/12/patch-management-in-it-and-ot-environments.html

IoT Security Foundation. (2023). *Software Bills of Materials for IoT and OT devices—An introduction to the use of SBOMs in the procurement and maintenance of connected devices* (Release 1.1.0). https://www.open-access.bcu.ac.uk/14250/1/RELEASE-2022-02-19-IoTSF-SBOM-whitepaper-v1-1-0.pdf

Irvine, C. E. (2005). Cybersecurity Considerations for Information Systems. In G. D. Garson (Ed.), *Public Administration and Public Policy: A Comprehensive Publication Program* (2nd ed., Vol. 111, pp. 203–218). Taylor & Francis.

ISO/IEC 27005. (2011). *Information technology—Security techniques—Information security risk management*.

ITU. (2021). *Global Cybersecurity Index 2020.* International Telecommunication Union - Development Sector. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Jann, W. (2003). State, administration and governance in Germany: Competing traditions and dominant narratives. *Public Administration*, *81*(1), 95–118. https://doi.org/10.1111/1467-9299.00338

Jann, W. (2016). Accountability, Performance and Legitimacy. In T. Christensen and P. Lægreid (Ed.), *The Routledge Handbook on Accountability and Welfare State Reforms in Europe*. Routledge.

Janowski, T. (2015). Digital government evolution: From transformation to contextualization. *Government Information Quarterly*, *32*(2), 221–236.

Janssen, M., & van der Voort, H. (2016). Adaptive governance: Towards a stable, accountable and responsive government. *Government Information Quarterly*, *33*(1), 1–5. https://doi.org/10.1016/j.giq.2016.02.003

Jasmine Yoo Jung, H., Narae, K., Sangwon, L., & Jang Hyun, K. (2018). Community disaster resilience and social solidarity on social media: A semantic network analysis of the Sewol ferry disaster. *Information Research*, *23*(3), 1–18.

Johnson, C. (2012). CyberSafety: CyberSecurity and Safety-Critical Software Engineering. In C. Dale & T. Anderson (Eds.), *Achieving Systems Safety* (pp. 85–95). Springer. https://doi.org/10.1007/978-1-4471-2494-8_8

Kaska, K., Osula, A.-M., & Stinissen, J. (2013). *The Cyber Defence Unit of the Estonian Defence League: Legal, Policy and Organisational Analysis* (pp. 1–45). NATO CCDCOE. https://ccdcoe.org/library/publications/the-cyber-defence-unit-of-the-estonian-defence-league-legal-policy-and-organisational-analysis/

Kattel, R., & Mergel, I. (2019). Estonia's Digital Transformation: Mission Mystique and the Hiding Hand. In M. E. Compton & P. 't Hart (Eds.), *Great Policy Successes* (pp. 143–160). Oxford University Press.

Kern, E. (2021). *Cyberangriffe auf deutsche Kommunen im Jahr 2021* (BIGS Essenz). Brandenburgisches Institut für Gesellschaft und Sicherheit. https://www.bigs-potsdam.org/app/uploads/2022/04/2022_BIGS-Essenz-Nr.19-WEB.pdf

Kim, M.-H., Cho, W., Choi, H., & Hur, J.-Y. (2020). Assessing the South Korean Model of Emergency Management during the COVID-19 Pandemic. *Asian Studies Review*, *44*(4), 567–578. https://doi.org/10.1080/10357823.2020.1779658

Kipker, D.-K. (2022, April 8). *BSI warnt vor Kaspersky: Eine echte 'Sicherheitslücke'?* Legal Tribune Online. https://www.lto.de/recht/kanzleien-unternehmen/k/kaspersky-ovg-nrw-warnung-bsi-gute-chanchen-sicherheitsluecke-bewertung/

Kjærgaard Christensen, K., & Liebetrau, T. (2019). A new role for 'the public'? Exploring cyber security controversies in the case of WannaCry, Intelligence and National Security. *Intelligence and National Security*, *34*(3), 395–408. https://doi.org/10.1080/02684527.2019.1553704

Klasa, K., Birge, H., Hossain, K., Kirchner, S., Palma-Oliviera, J., Merad, M., Silverstein, R. S., Stepien, A., & Saumya, P. (2020). Challenges in Establishing Legal Frameworks and Governance Options That Promote Arctic Cyber Resilience. In B. D. Trump, K. Hossain, & I. Linkov (Eds.), *Cybersecurity and resilience in the arctic* (pp. 321–360). IOS Press.

Kleinhans, J.-P. (2017). *Internet of Insecure Things*. Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/internet_of_insecure_things.pdf

Klijn, E. H., & Koppenjan, J. (2016). *Governance Networks in the Public Sector*. Routledge.

Kohler, K. (2020). *Estonia's National Cybersecurity and Cyberdefense Posture*. Center for Security Studies (CSS), ETH Zürich.

Koning, E. A. (2016). The three institutionalisms and institutional dynamics: Understanding endogenous and exogenous change. *Journal of Public Policy*, *36*(4), 639–664. https://doi.org/10.1017/S0143814X15000240

Kooiman, J., & van Vliet, M. (1993). Governance and Public Management. In Eliassen, K. & Kooiman, J. (Eds.), *Managing Public Organisations* (2nd ed.). SAGE.

Koppel, R., Smith, S., Blythe, J., & Kothari, V. (2015). Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient? *Studies in Health Technology and Informatics*, *208*.

Kott, A., & Linkov, I. (2021). To Improve Cyber Resilience, Measure It. *Computer*, *54*(2), 80–85. https://doi.org/10.1109/MC.2020.3038411

Krcmar, H., Eckert, C., Roßnagel, A., Sunyaev, A., & Wiesche, M. (Eds.). (2018). *Management sicherer Cloud-Services*. Springer Fachmedien. https://doi.org/10.1007/978-3-658-19579-3

Kriaa, S. (2016, March 11). *Joint safety and security modeling for risk assessment in cyber physical systems*. https://www.semanticscholar.org/paper/Joint-safety-and-security-modeling-for-risk-in-Kriaa/e8f933df99b04d4a92e742e05eae9010b9cf7e69

Krimmer, R., Duenas-Cid, D., & Krivonosova, I. (2021). New methodology for calculating cost-efficiency of different ways of voting:is internet voting cheaper? *Public Money & Management*, *41*(1), 17–26. https://doi.org/10.1080/09540962.2020.1732027

Krimmer, R., Rincon, A. M., & Nielsen, M. M. (2015). *Governance of Cyber-Security in Internet-Based Elections*. 1st Interdisciplinary Cyber Research Workshop, Tallinn, Estonia.

Krimmer, R., Triessnig, S., & Volkamer, M. (2007). The Development of Remote E-Voting Around the World: A Review of Roads and Directions. In A. Alkassar & M. Volkamer (Eds.), *Proceedings of the 1st International Conference on E-Voting and Identity (VoteID 2007)* (Vol. 4896, pp. 1–15). Springer.

Kuerbis, B., & Badiei, F. (2017). Mapping the cybersecurity institutional landscape. *Digital Policy, Regulation and Governance*, *19*(6), 466–492. https://doi.org/10.1108/DPRG-05-2017-0024

Kullik, J. (2021). *Deutschlands Cybersicherheitsstrategie im nächsten Jahrzehnt* (BAKS-Arbeitspapiere, pp. 1–5). Bundesakademie für Sicherheitspolitik. https://www.baks.bund.de/sites/baks010/files/arbeitspapier_sicherheitspolitik_2021_2.pdf

Kusumasari, B., Alam, Q., & Siddiqui, K. (2010). Resource capability for local government in managing disaster. *Disaster Prevention and Management: An International Journal*, *19*(4), 438–451. https://doi.org/10.1108/09653561011070367

Lægreid, P., & Rykkja, L. H. (2015). Organizing for “wicked problems” – analyzing coordination arrangements in two policy areas. *International Journal of Public Sector Management*, *28*(6), 475–493. https://doi.org/10.1108/IJPSM-01-2015-0009

Lægreid, P., & Rykkja, L. H. (2019a). Organizing for Societal Security and Crisis Management: Governance Capacity and Legitimacy. In P. Lægreid & L. H. Rykkja (Eds.), *Societal Security and Crisis Management—Governance Capacity and Legitimacy* (pp. 1–23). Palgrave Macmillan.

Lægreid, P., & Rykkja, L. H. (2019b). *Societal Security and Crisis Management—Governance Capacity and Legitimacy*. Palgrave Macmillan.

Lagadec, P. (2009). A New Cosmology of Risks and Crises: Time for a Radical Shift in Paradigm and Practice. *Review of Policy Research*, *26*(4), 473–486.

Lalonde, C. (2007). The Potential Contribution of the Field of Organizational Development to Crisis Management. *Journal of Contingencies and Crisis Management*, *15*(2), 95–104.

Lambach, D., & Oppermann, K. (2022). Narratives of digital sovereignty in German political discourse. *Governance*. https://doi.org/10.1111/gove.12690

Lau, E. T., Chai, K. K., Chen, Y., & Loo, J. (2018). Efficient Economic and Resilience-Based Optimization for Disaster Recovery Management of Critical Infrastructures. In *Energies* (Vol. 11, Issue 12, pp. 1–20). https://doi.org/10.3390/en11123418

Lesk, M. (2007). *The new front line: Estonia under cyberassault. Security & Privacy, ieee, 5(4), 76–79.* (IEEE, Ed.; Vol. 5, pp. 76–79).

Leverett, E., Clayton, R., & Anderson, R. (2017). *Standardisation and Certification of the `Internet of Things'*. 6th Annual Workshop on the Economics of Information Security (WEIS).

Liebetrau, T. (2022). Organizing cyber capability across military and intelligence entities: Collaboration, separation, or centralization. *Policy Design and Practice*, 1–15. https://doi.org/10.1080/25741292.2022.2127551

Linde, C. (2009). *Working the Past: Narrative and Institutional Memory.* Oxford University Press.

Linkov, I., Roslycky, L., & Trump, B. D. (2019). *Resilience of hybrid threats: Security and integrity for the digital world*. IOS Press.

Lowndes, V. (1996). Varieties of New Institutionalism: A Critical Appraisal. *Public Administration*, *74*(2), 181–197. https://doi.org/10.1111/j.1467-9299.1996.tb00865.x

Luna-Reyes, L. F., & Gil-García, J. R. (2003). E-Government Security, Privacy and Information Access: Some Policy and Organizational Trade-offs. In *International Conference on Public Participation and Information Technologies 2003 (ICPPIT03)* (pp. 1–4).

Lune, H., & Berg, B. L. (2017). *Qualitative Research Methods for the Social Sciences* (9th ed.). Pearson.

MacLean, D., & Titah, R. (2022). A systematic literature review of empirical research on the impacts of e-government: A public value perspective. In *Public Administration Review* (Vol. 82, Issue 1, pp. 23–38). https://doi.org/10.1111/puar.13413

Magetti, M. (2010). Legitimacy and Accountability of Independent Regulatory Agencies: A Critical Review. *Living Reviews in Democracy*, *2*, 1–9.

Mahoney, J. (2000). Path Dependence in Historical Sociology. *Theory and Society*, *29*(4), 507–548.

March, J. G., & Olsen, J. P. (1984). The New Institutionalism: Organizational Factors in Political Life. *American Political Science Review*, *78*, 734–749.

March, J. G., & Olsen, J. P. (2004). The logic of appropriateness. *ARENA Working Papers, WP 04/09*. https://www.sv.uio.no/arena/english/research/publications/arena-working-papers/2001-2010/2004/wp04_9.pdf

Maurer, T., & Morgus, R. (2014). *Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate*. CIGI; Chatham House. https://www.cigionline.org/publications/tipping-scale-analysis-global-swing-states-internet-governance-debate/

McConnell, A. (2011). Success? Failure? Something in-between? A framework for evaluating crisis management. *Policy and Society*, *30*(2), 63–76.

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative Data Analysis: A Methods Sourcebook* (3rd ed.). SAGE Publications.

Miller, M. (2022, October 5). *Albania weighed invoking NATO's Article 5 over Iranian cyberattack*. POLITICO. https://www.politico.com/news/2022/10/05/why-albania-chose-not-to-pull-the-nato-trigger-after-cyberattack-00060347

Monsees, L., & Lambach, D. (2022). Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity. *European Security*, *31*(3), 377–394. https://doi.org/10.1080/09662839.2022.2101883

Morgus, R., Skierka, I., Hohmann, M., & Maurer, T. (2015). *National CSIRTs and their role in computer security incident response*.

Nemec, M., Sys, M., Svenda, P., Klinec, D., & Matyas, V. (2017). *The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli*. ACM CCS 17 Proceedings, Dallas, Texas, United States.

NIST. (2012). *SP 800-30: Guide for conducting risk assessments, Rev. 1*. National Institute of Standards and Technology, U.S. Department of Commerce.

NIST. (2021, September 27). *Ransomware*. Information Technology Laboratory. https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware

Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2019). Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity. In *Public Administration Review* (Vol. 79, Issue 6, pp. 895–904). https://doi.org/10.1111/puar.13028

North, D. C. (1990). *Institutions, institutional change, and economic performance*. Cambridge University Press.

Nunnikhoven, M. (2017, May 15). WannaCry & the reality of patching. *Trend Micro Blog*. https://vulners.com/trendmicroblog/TRENDMICROBLOG:90481B7D0C6FD15C950712E718E29E3A

Osula, A.-M. (2015). *National Cyber Security Organisation: Estonia*. NATO CCDCOE.

Ottis, R. (2008). Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective. *Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth*, 163–168.

Papenfuß, U., & Schmidt, C. A. (2021). Understanding self-regulation for political control and policymaking: Effects of governance mechanisms on accountability. *Governance*, *34*(4), 1115–1141. https://doi.org/10.1111/gove.12549

Parycek, P., Sachs, M., Virkar, S., Krimmer, R., Krimmer, R., Volkamer, M., Braun Binder, N., Kersting, N., & Pereira, O. (2017). *Voting in E-Participation: A Set of Requirements to Support Accountability and Trust by Electoral Committees*. Second International Joint Conference, E-Vote-ID 2017, Bregenz, Austria.

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (Fourth edition). SAGE Publications Inc.

Pearson, C. M., & Clair, J. A. (1998). Reframing Crisis Management. *Academy of Management Review*, 59–76.

Pereira, G. V., Wimmer, M., & Ronzhyn, A. (2020). Research needs for disruptive technologies in smart cities. In Y. Charalabidis, M. A. Cunha, & D. Sarantis (Eds.), *13th International Conference on Theory and Practice of Electronic Governance (ICEGOV 2020)* (pp. 620–627). Association for Computing Machinery. https://doi.org/10.1145/3428502.3428594

Perrow, C. (1999). *Normal Accidents: Living with High-Risk Technologies*. Basic Books.

Peters, B. G. (2014). Is governance for everybody? *Policy and Society*, *33*(4), 301–306. https://doi.org/10.1016/j.polsoc.2014.10.005

Peters, B. G. (2019). Governing in the shadows. *Journal of Chinese Governance*, *4*(2), 108–122. https://doi.org/10.1080/23812346.2019.1596057

Pike, R. (2021). Enhancing cybersecurity capability in local governments through competency-based education. In *Proceedings of the 54th Hawaii International Conference on System Sciences (HICSS-54)* (pp. 2019–2025). https://doi.org/10.24251/HICSS.2021.247

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1532

Pollitt, C. (2009). Bureaucracies remember, post-bureaucratic organizations forget? *Public Administration*, *87*(2), 198–218.

Prevezianou, M. F. (2021). Beyond Ones and Zeros: Conceptualizing Cyber Crises. *Risk, Hazards & Crisis in Public Policy*, *12*(1), 51–72. https://doi.org/10.1002/rhc3.12204

Provan, K. G., & Kenis, P. (2008). Modes of Network Governance: Structure, Management, and Effectiveness. *Journal of Public Administration Research and Theory*, *18*(2), 229–252. https://doi.org/10.1093/jopart/mum015

Rana, N. P., Dwivedi, Y. K., & Williams, M. D. (2015). Evaluating the validity of IS success models for the electronic government research: An empirical test and integrated model. In Irma (Ed.), *Public Affairs and Administration: Concepts, Methodologies, Tools, and Applications* (Vol. 4, pp. 1965–1986). IGI Global. https://doi.org/10.4018/978-1-4666-8358-7.ch101

Randma, T. (2001). A small civil service in transition: The case of Estonia. *Public Administration and Development*, *21*(1), 41–51.

Randma-Liiv, T., & Sarapuu, K. (2019). Public Governance in small states: From paradoxes to research agenda. In A. Massey (Ed.), *A Research Agenda for Public Administration* (pp. 162–179). Edward Elgar Publishing.

Raudla, R., Juuse, E., & Cepilovs, A. (2019). Policy learning from crisis in financial regulation and supervision: Comparative analysis of Estonia, Latvia and Sweden. *Journal of Baltic Studies*, *50*(4), 495–514. https://doi.org/10.1080/01629778.2019.1632911

Reiss, J. (2007). Do We Need Mechanisms in the Social Sciences? *Philosophy of the Social Sciences*, *37*(2), 163–184. https://doi.org/10.1177/0048393107299686

Renn, O., & Klinke, A. (2022). Risk Governance. In C. Ansell & J. Torfing (Eds.), *Handbook on Theories of Governance* (pp. 264–277). Edward Elgar Publishing. https://doi.org/10.4337/9781800371972

Republic of Estonia. (2021). *Cybersecurity Strategy 2019-2022*.

Reuters. (2022, September 1). Montenegro blames criminal gang for cyber attacks on government. *Reuters*. https://www.reuters.com/world/europe/montenegro-blames-criminal-gang-cyber-attacks-government-2022-08-31/

RIA. (2017). *Annual Cybersecurity Assessment 2017*. https://ria.ee/media/1508/download

RIA. (2023a). *IT baseline security system ISKE*. https://ria.ee/en/cyber-security/management-state-information-security-measures/it-baseline-security-system-iske

RIA. (2023b). *Monitoring cyberspace and impeding incidents*. https://www.ria.ee/en/cyber-security/handling-cyber-incidents-cert-ee/monitoring-cyberspace-and-impeding-incidents

Rid, T. (2013). *Cyber War Will Not Take Place*. Oxford University Press.

Rittel, H. W., & Webber, M. M. (1974). Wicked problems. *Man-Made Futures*, *26*(1), 272–280.

Robinson, N., Kask, L., & Krimmer, R. (2019). The Estonian Data Embassy and the Applicability of the Vienna Convention: An Exploratory Analysis. *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance*, 391–396. https://doi.org/10.1145/3326365.3326417

Romaniuk, S. N., & Manjikian, M. (2020). *Routledge companion to global cyber-security strategy*. Routledge.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, tyw001. https://doi.org/10.1093/cybsec/tyw001

Rose, A. Z., & Miller, N. (2020). Measurment of cyber resilience from an economic perspective. In R. T. Brigantic, A. M. Waterworth, & S. Chatterjee (Eds.), *Applied risk analysis for guiding homeland security policy and decisions* (pp. 193–209). John Wiley & Sons, Inc.

Rosenthal, U., Charles, M. T., & ’t Hart, P. (1989). *Coping with crises: The management of disasters, riots, and terrorism*. C.C. Thomas.

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach* (NIST SP 800-160v2r1; p. NIST SP 800-160v2r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2r1

Rostami, M., Burleson, W., Koushanfar, F., & Jules, A. (2013). *Balancing security and utility in medical devices?* The 50th Preneel, On the (in)security of the latest generation implantable Annual Design Automation Conference, Austin, TX.

Ruohonen, J., Hyrynsalmi, S., & Leppänen, V. (2016). An outlook on the institutional evolution of the European Union cyber security apparatus. In *Government Information Quarterly* (Vol. 33, Issue 4, pp. 746–756). https://doi.org/10.1016/j.giq.2016.10.003

Saldaña, J. (2013). *The coding manual for qualitative researchers* (2nd ed). SAGE.

Sarapuu, K. (2015). Post-Communist Development of Administrative Structure in Estonia: From Fragmentation to Segmentation. *Transylvanian Review of Adminsitrative Sciences*, *Special Issue*, 54–73.

Sasse, M. A., & Flechais, I. (2005). Why Do We Need It? How Do We Get It? In L. Cranor & Garfinkel (Eds.), *Security and Usability: Designing secure systems that people can use* (pp. 13–30). O'Reilly.

Schardt, M. (2021). § 25 Öffentliche Verwaltung. In G. Hornung & M. Schallbruch (Eds.), *Handbuch IT-Sicherheitsrecht* (1st ed., pp. 595–619). Nomos.

Scharpf, F. W. (1999). *Governing in Europe: Effective and Democratic?* Oxford University Press.

Schmidt, V. A. (2013). Democracy and Legitimacy in the European Union Revisited: Input, Output, and Throughput. *Political Studies*, *61*(1), 2–22.

Schneider, S. K. (2011). *Dealing with Disaster: Public Management in Crisis Situations*. M. E. Sharpe.

Schneier, B. (2018). *Click here to kill everybody: Security and survival in a hyper-connected world* (First edition.). W.W. Norton & Company.

Schofield, J. W. (2011). Increasing the Generalizability of Qualitative Research. In A. M. Huberman & M. B. Miles (Eds.), *The Qualitative Researcher's Companion* (pp. 171–203). SAGE Publications.

Scholl, H. J. (2022). *The Digital Government Reference Library (DGRL). Version 18.5*. http://faculty.washington.edu/jscholl/dgrl/

Scholl, H. J., & Patin, B. J. (2014). Resilient information infrastructures: Criticality and role in responding to catastrophic incidents. In *Transforming Government: People, Process and Policy* (Vol. 8, Issue 1, pp. 28–48). https://doi.org/10.1108/TG-12-2012-0015

Sharma, D., & Singh, S. (2016). Instituting environmental sustainability and climate resilience into the governance process: Exploring the potential of new urban development schemes in India. In *International Area Studies Review* (Vol. 19, Issue 1, pp. 90–103). https://doi.org/10.1177/2233865916632942

Simon, S., & De Goede, M. (2015). Cybersecurity, Bureaucratic Vitalism and European Emergency. *Theory, Culture & Society*, *32*(2), 79–106. https://doi.org/10.1177/0263276414560415

Skierka, I. (2020). *Die 5G Debatte: Ein Test für die digitale Souveränität Europas*. KAS Analysen und Argumente. https://www.jstor.org/stable/pdf/resrep25286.pdf?acceptTC=true&coverpage=false&addFooter=false

Skierka, I., & Parycek, P. (2023). Einwurf–Kann Deutschland seine eID noch retten? *HMD Praxis Der Wirtschaftsinformatik*, *60*(2), 255–260. https://doi.org/10.1365/s40702-023-00958-0

Smeets, M. (2018). The Strategic Promise of Offensive Cyber Operations. *Strategic Studies Quarterly*, *12*(3), 90–113. https://www.jstor.org/stable/26481911

Smeets, M., & Lin, H. S. (2018). Offensive cyber capabilities: To what ends? *2018 10th International Conference on Cyber Conflict (CyCon)*, 55–72. https://doi.org/10.23919/CYCON.2018.8405010

Smith, K., & Lawrence, G. (2018). From disaster management to adaptive governance? Governance challenges to achieving resilient food systems in Australia. *Journal of Environmental Policy & Planning*, *20*(3), 387–401. https://doi.org/10.1080/1523908X.2018.1432344

Snyder, C. (2017). *Too Connected To Fail—How Attackers Can Disrupt the Global Internet, Why It Matters, And What We Can Do About It*. Belfer Center for Science and International Affairs.

Spiegel. (2021, March 26). Hack gegen Abgeordnete: Russische Gruppe »Ghostwriter« attackiert offenbar Parlamentarier. *Der Spiegel*. https://www.spiegel.de/politik/deutschland/russischer-hack-erneute-attacke-hack-auf-bundestag-sieben-abgeordnete-betroffen-a-75e1adbe-4462-4e30-bd94-96796aed6b8a

Spiegel. (2022a, October 28). Ransomware: Cyberangriff auf Anhalt-Bitterfeld gravierender als bislang bekannt. *Der Spiegel*. https://www.spiegel.de/netzwelt/ransomware-cyberangriff-auf-anhalt-bitterfeld-gravierender-als-bislang-bekannt-a-d538f846-1926-484d-b8d6-19554ad8c4c5

Spiegel. (2022b, December 31). Potsdam schaltet nach möglicher Cyberattacke seine Internetserver ab—Verwaltung offline—DER SPIEGEL. *Der Spiegel*. https://www.spiegel.de/netzwelt/potsdam-schaltet-nach-moeglicher-cyberattacke-seine-internetserver-ab-verwaltung-offline-a-5703d9d1-dff1-4a63-9c5d-6a0005ee632d

Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., & Halderman, A. (2014). Security Analysis of the Estonian Internet Voting System. *Proceedings of the 2014 ACM SIGSAC Conference of Computer and Communications Security*, 703–715.

Steinmo, S., Thelen, K., & Longstreth, F. (Eds.). (1992). *Structuring Politics: Historical Institutionalism in Comparative Analysis*. Cambridge University Press. https://doi.org/10.1017/CBO9780511528125

Stevens, T. (2018). Global Cybersecurity: New Directions in Theory and Methods. *Politics and Governance*, *6*(2), 1–4. https://doi.org/10.17645/pag.v6i2.1569

Stiebel, B. (2022, July 6). „Es ist unsere verdammte Pflicht“. *Tagesspiegel Background Cybersecurity*. https://background.tagesspiegel.de/cybersecurity/es-ist-unsere-verdammte-pflicht

Stoker, G. (2018). Governance as theory: Five propositions. *International Social Science Journal*, *68*(227–228), 15–24. https://doi.org/10.1111/issj.12189

Strupczewski, G. (2021). Defining cyber risk. *Safety Science*, *135*, 1–10. https://doi.org/10.1016/j.ssci.2020.105143

Suchman, M. C. (1995). Managing Legitimacy: Strategic and Institutional Approaches. *Academy of Management Review*, *20*(3), 571–610.

Symons, V. J. (1991). A review of information systems evaluation: Content, context and process. *European Journal of Information Systems*, *1*(3), 205–212.

Tallinna Tehnikaülikool. (2018). *ID-kaardi kaasuse õppetunnid*.

Tanczer, L. M., Brass, I., & Carr, M. (2018). CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy. *Global Policy*, *9*(S3), 60–66. https://doi.org/10.1111/1758-5899.12625

Thelen, K. (1999). Historical Institutionalism in Comparative Politics. *Annual Review of Political Science*, *2*, 369–404.

Torfing, J. (2012). *Interactive governance: Advancing the paradigm*. Oxford University Press.

Trimintzios, P., Holfeldt, R., Koraeus, M., Uckan, B., Gavrila, R., & Makrodimitris, G. (2015). *ENISA Report on Cyber Crisis Cooperation and Management: Comparative study on the cyber crisis management and the general crisis management*. https://data.europa.eu/doi/10.2824/34669

Van Der Blonk, H. (2003). Writing case studies in information systems research. *Journal of Information Technology*, *18*(1), 45–52. https://doi.org/10.1080/0268396031000077440

van der Kleij, R., & Leukfeldt, E. R. (2019). Cyber resilient behavior: Integrating human behavioral models and resilience engineering capabilities into cyber security. *Advances in Human Factors in Cybersecurity, Proceedings of the AHFE 2019 International Conference on Human Factors in Cybersecurity, July 24-28, 2019, Washington D.C., USA*, 16–27.

van der Meulen, N. (2013). DigiNotar: Dissecting the First Dutch Digital Disaster. *Journal of Strategic Security*, *6*(2), 46–58. https://doi.org/10.5038/1944-0472.6.2.4

Venkatachalam, N., O’Connor, P., & Palekar, S. (2021). Cyber security and cyber resilience for the Australian e-health records: A blockchain solution. In K. Sandhu (Ed.), *Handbook of research on advancing cybersecurity for digital transformation* (pp. 61–78). IGI Global.

Viet, H. L., Van, O. P., & Ngoc, H. N. (2020). Information Security Risk Management by a Holistic Approach: A Case Study for Vietnamese e-Government. In *International Journal of Computer Science and Network Security* (Vol. 20, Issue 6, pp. 72–82).

von Haldenwang, C. (2016). Measuring legitimacy: New trends, old shortcomings? *Discussion Paper*.

Walsham, J. (1993). *Interpreting Information Systems in Organizations*. John Wiley & Sons.

Weerakkody, V., Omar, A., El-Haddadeh, R., & Al-Busaidy, M. (2016). Digitally-enabled service transformation in the public sector: The lure of institutional pressure and strategic response towards change. In *Government Information Quarterly* (Vol. 33, Issue 4, pp. 658–668). https://doi.org/10.1016/j.giq.2016.06.006

Weyland, K. (2008). Toward a New Theory of Institutional Change. *World Politics*, *60*(2), 281–314.

White, G. B. (2012). A Grassroots Cyber Security Program to Protect the Nation. In *Proceedings of the 45th Hawaii International Conference on System Sciences (HICSS-45)* (pp. 2330–2337). IEEE. http://www.computer.org/csdl/proceedings/hicss/2012/4525/00/4525c330-abs.html

Whyte, C., Thrall, A. T., & Mazanec, B. M. (2020). Introduction. In C. Whyte, A. T. Thrall, & B. M. Mazanec (Eds.), *Information warfare in the age of cyber conflict* (pp. 1–12). Routledge/Taylor & Francis Group.

Williams, T. A., Gruber, D. A., Sutcliffe, K. M., Shepherd, D. A., & Zhao, E. Y. (2017). Organizational Response to Adversity: Fusing Crisis Management and Resilience Research Streams. *Academy of Management Annals*, *11*(2), 733–769. https://doi.org/10.5465/annals.2015.0134

Williamson, O. E. (1996). *The mechanisms of governance*. Oxford University Press.

Willsher, K., & Henley, J. (2017, May 6). Emmanuel Macron's campaign hacked on eve of French election. *The Guardian*. https://www.theguardian.com/world/2017/may/06/emmanuel-macron-targeted-by-hackers-on-eve-of-french-election

World Economic Forum. (2018). *Cyber Resilience: Playbook for Public-Private Collaboration*.

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (Sixth Edition). SAGE Publications.

Yousefnezhad, N., Malhi, A., & Främling, K. (2020). Security in product lifecycle of IoT devices: A survey. *Journal of Network and Computer Applications*, *171*, 102779. https://doi.org/10.1016/j.jnca.2020.102779

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon* (First Edition.). Crown Publishers.

Zhang, H., Tang, Z., & Jayakar, K. (2018). A socio-technical analysis of China's cybersecurity policy: Towards delivering trusted e-government services. In *Telecommunications Policy* (Vol. 42, Issue 5, pp. 409–420). https://doi.org/10.1016/j.telpol.2018.02.004

Zhao, J. J., & Zhao, S. (2010). Opportunities and threats: A security assessment of state e-government websites. *Government Information Quarterly*, *27*(1), 49–56.

## Acknowledgements

One of the most important insights of my PhD journey is that academic research and writing is not possible without the constant support of and exchange with colleagues, mentors, and friends – especially as a part-time student – which I would like to acknowledge in the following paragraphs.

First of all, I would like to express my deepest gratitude to my supervisor, Prof. Dr. Dr. Robert Krimmer, for his guidance and mentorship throughout this entire PhD degree. His feedback and encouragement consistently supported me through the challenging academic writing and peer-review process. His academic experience and problem-solving oriented way of working, as well as our countless conversations about digital government, have always helped me balance the academic and real-world aspirations of my PhD degree.

I would also like to express my deep appreciation to my supervisor Prof. Dr. Ringa Raudla for her guidance and support through consistent feedback on my publications and the thesis introduction from the early stages until and especially during the final months. I could always count on substantive and constructive comments – especially regarding theoretical and methodological questions – and on finding inspiration in her academic work.

I also could not have undertaken this journey without my supervisor Prof. Dr. Peter Parycek. He is the reason I started my degree as an external student at the Ragnar Nurkse Department of Innovation of Governance, advising me to reach out to Prof. Robert Krimmer when I approached him in spring 2018 with my very rough ideas for a thesis. I am particularly thankful for our conversations and professional collaborations on issues of digital government and identity management beyond the PhD degree.

I am thankful to my co-authors, in particular Martin Schallbruch, who I also had the pleasure of collaborating with as my senior colleague for five years at the Digital Society Institute (DSI) at the European School of Management and Technology (ESMT) Berlin. I am grateful for his mentorship both in my research and professional endeavours.

My gratitude further extends to the Ragnar Nurkse Department of Innovation and Governance (RND). Although I was an external PhD student, I always felt welcome and supported and am proud to call myself an RND graduate after defending this thesis. It has been a pleasure to regularly participate in the PhD research seminar and the summer retreats, from which multiple iterations of my articles and thesis greatly benefitted. In particular, I would like to thank the director, Prof. Dr. Erkki Karo, and – again – the head of the PhD programme, Prof. Dr. Ringa Raudla, for supporting and encouraging the PhD students wherever possible. I am also particularly grateful to Dr. Amirouche Moktefi and Dr. Veiko Lember for providing extensive feedback on the earlier version of this thesis in the pre-defense, and for carefully reading my drafts and providing constructive criticism regarding the logic of my argumentation. I would also like to thank all fellow former and current PhD students for their support, especially Iuliia, Maarja, Nick, Shobhit, Alexis, Jaanus, and many more. I am lucky to have met you during my stays in Tallinn.

I would like to thank the RND and general TalTech staff for always being responsive and helpful when navigating administrative university matters: this is to Piret Kähr, Maria Edur, and Mirjam Piik in particular.

I would like to thank my academic colleagues from the digital government research community around the world who were kind and patient enough to read and help improving my manuscripts – among them, Prof. Dr. Vincent Homburg in particular.

Thanks also go to my employer, the DSI at ESMT Berlin, for providing me with the opportunity to work on thematically related projects in my professional life. DSI Director Heli Tiirmaa-Klaar has played a special role in my PhD studies' final year as an experienced advisor and role model. I am also particularly grateful to my past and current colleagues at DSI – Prof. Dr. Christoph Thiel, Dr. Henning Lahmann, and Lilly Schmidt for fruitful professional collaborations, inspiring conversations and continuous support and mentorship. I would also like to thank the TÜV NORD Group and Dr. Dirk Stenkamp who supported the beginnings of my PhD research through a professional project grant.

I would further like to acknowledge the people I met on this journey through countless professional conferences, workshops, projects, and summer schools, which I attended throughout the past five years across Europe and the United States. Special thanks go to the colleagues from Stiftung Neue Verantwortung and the wider German cyber security policy community. The conversations with you were always a source of inspiration for me.

Most of all, I would like to thank my family, for letting me follow this path. I want to thank my parents Annette and Volker. My passion for getting to the bottom of issues comes from them. I further want to thank my parents, my sister Antonia, and most of all my husband Thomas for always being by my side, supporting me, and taking away the burden from my shoulders, allowing me to focus on the PhD. Lastly, I would like to thank my little son Timothée for bringing so much joy to Thomas' and my life and for leaving me some spare time to finalize this thesis.

# Abstract

## Securing Digital Government: Towards governance mechanisms for e-state resilience

The growing threat of cyber incidents in public IT infrastructures has made questions about securing digital government (DG) and its core functions – the ‘e-state’ – more relevant than ever. Governments need to deploy strategies for managing respective risks and crises. This thesis seeks to explore and explain administrations’ cyber security governance in DG to achieve greater cyber resilience.

Based on contributions from six original research publications, this thesis brings empirical and theoretical insights into our understanding of cyber resilience of DG. It thereby aims to contribute to the DG and cyber security literatures, which to date lack methodologically rigorous and empirically founded studies that explain how and with which mechanisms states manage cyber resilience of their e-state. Thereby, it also aims to complement the predominantly practical and policy approaches that currently exist to address challenges of cyber risk to the e-state with more theoretically informed and in-depth analysis.

To explore this topic, the thesis examines one primary research question and three sub-research questions:

How can an administration develop governance mechanisms which enhance the cyber resilience of the e-state?

1. How does a country’s national cyber security architecture impact its approach to cyber resilience?
2. How can an administration manage and overcome a cyber crisis affecting a critical DG system at large scale?
3. How can an administration govern the security of IT systems deployed in safety-relevant infrastructures?

The dissertation answers these questions through a qualitative research approach based on a synthesis of case studies, action research, and applied legal and policy research. The research findings identify three stages at which administrations can develop governance mechanisms: at the levels of institutions, interactive networks, and operations. At the institutional level, governance mechanisms of cyber resilience comprise formal and informal rules, as well as organizational structures. At the interactive level, cyber resilience governance mechanisms encompass interactive processes, which strongly influence cooperation in networks. Those include trusted relationship building, institutional memory development, meaning-making and communication, and accountability of interactions. Key mechanisms at the operational level through which states can enhance cyber resilience include technology management, integrated risk management, and the deployment of capabilities, which encompass both resources and processes. The thesis inductively derives and proposes these constructs as an outline of a taxonomy of e-state cyber resilience governance mechanisms to be refined in future research and analysis.

In its exploration of the sub-research questions, the thesis illustrates the tight interaction between mechanisms at those different governance levels. In its analysis of the impact of national cyber security architectures on cyber resilience, it concludes that the broader institutional structures and culture, and the degree of interaction and trust within governance networks, influences actors’ capacity to effectively coordinate their

actions horizontally and vertically, as well as the effective deployment of capabilities across levels of government.

In its examination of cyber crisis management in DG, this thesis suggests that the degree of a DG system's criticality will greatly influence the costs that administrations are willing to incur to maintain its availability during a cyber crisis. It further highlights five constructs which appear decisive for successful cyber crisis management in DG: the crisis governance networks' 1) technology management capacity, 2) networked cooperation capability, 3) collaboration capital, 4) risk management capacity, and 5) legitimacy building. Those factors feed into the taxonomy of cyber resilience governance mechanisms for further testing and development in future studies.

The thesis' analysis of the proactive side of cyber resilience is concerned with the management of the IT security of systems that underlie modern societies' infrastructures. It raises several practical policy considerations related to the future design of cyber security policy and regulation: 1) the need to avoid EU regulatory fragmentation and overlap in growing horizontal and vertical cyber security legislation; 2) ways to integrate IT security, safety, and privacy into standards and practices of IT security risk assessments; and 3) the challenges for political decision-makers to deal with the growing tension between technological security, geopolitics, and national security in the context of IT systems security.

In synthesis, this thesis proposes several constructs along which researchers and practitioners can test and further develop and refine the proposed governance mechanisms to enhance cyber resilience of the e-state. The dissertation provides multiple starting points for avenues of future work at the intersection of DG, cyber security and resilience. Respective research fields could benefit from drawing on insights from the public administration literature, particularly institutionalism, policy-learning, and adaptive governance, to study how cyber resilience can be more sustainably embedded in administrative structures and processes.

# Lühikokkuvõte

## Digitaalse valitsuse kindlustamine: juhtimismehhanismid e-riigi vastupanuvõimekuseks

Info- ja kommunikatsioonitehnoloogiate laialdane kasutamine e-valitsuses on muutnud valitsused oma olemuselt haavatavaks ebasoodsate kübersündmuste suhtes, mis mõjutavad IT-süsteemide, teabe, teenuste ja protsesside konfidentsiaalsust, terviklikkust ja/või kättesaadavust. Seetõttu on küsimused e-valitsuse ja selle põhifunktsioonide – nn e-riigi – turvalisuse kohta isegi siis, kui küberintsidentide esinemine on vältimatu, muutunud aktuaalsemaks kui kunagi varem. Selle doktoritöö eesmärk on uurida ja selgitada haldusasutuste küberriskide juhtimist, et parandada kübervastupidavust. Ühes sellega on eesmärgiks kõrvaldada teadusuuringute lünk e-valitsemise kirjanduses, kus puuduvad metodoloogiliselt ranged ja empiiriliselt põhjendatud uuringud, mis selgitaksid, kuidas ja milliste mehhanismidega riigid oma e-riigi kübervastupidavust haldavad.

Tuginedes kuue originaalse teaduspublikatsiooni kaastööle, annab see doktoritöö empiirilise ja teoreetilise ülevaate meie arusaamast e-valitsemise kübervastupidavuse kohta. Lisaks, täiendaks see olemasolevaid valdavalt praktilisi ja poliitilisi lähenemisviise küberriskiga seotud väljakutsete lahendamiseks metoodiliselt rangema ja põhjalikuma analüüsiga.

Selle teema uurimiseks käsitletakse doktoritöös ühte esmast uurimisküsimust ja kolme alamuuringu küsimust:

Kuidas saaks avaliku halduse asutus välja töötada juhtimismehhanisme, mis suurendavad e-riigi kübervastupidavust?

1. Kuidas mõjutab riiklik küberturvalisuse arhitektuur riigi lähenemist kübervastupidavusele?
2. Kuidas saab riik juhtida ja ületada küberkriisi, mis mõjutab ulatuslikult kriitilist e-valitsuse süsteemi?
3. Kuidas saab riik juhtida IT-süsteemide julgeolekut, mida kasutatakse turvalisusega seotud infrastruktuurides?

Doktoritöö annab neile küsimustele vastused kasutades kvalitatiivseid uurimismeetodeid: juhtumiuuringud, tegevusuuringud ning rakenduslikud õigus- ja poliitikauuringud. Uurimistulemused määravad kindlaks kolm tasandit, mille põhjal haldusasutused saavad juhtimismehhanisme välja töötada: institutsiooniline, interaktiivsete võrgustike ning operatiivne tasand. Doktoritöö tuletab need mehhanismid induktiivselt ja esitab need e-riigi kübervastupidavuse juhtimismehhanismide taksonoomia raames, mis võiks olla aluseks edasisele analüüsile tulevastes uuringutes. Institutsioonilisel tasandil hõlmavad kübervastupidavuse juhtimismehhanismid nii ametlikke ja mitteametlikke reegleid kui ka organisatsioonilisi struktuure. Interaktiivsel tasandil hõlmavad kübervastupidavuse juhtimismehhanismid interaktiivseid protsesse, mis mõjutavad koostööd võrgustikes. Nende hulka kuuluvad usaldusväärsete suhete loomine, institutsioonilise mälu arendamine, tähenduse kujundamine ja suhtlemine ning koostöö vastutus. Peamised operatiivtasandi mehhanismid, mille kaudu riigid saavad kübervastupidavust suurendada, hõlmavad tehnoloogia juhtimist, kõikehõlmavat riskijuhtimist ja võimete (ressursside ja protsesside) kasutuselevõttu.

Otsides alamuuringu küsimustele vastuseid, illustreerib doktoritöö mainitud mehhanismide tihedat koostoimet erinevatel juhtimistasanditel. Selles jõutakse järeldusele, et laiemad institutsioonilised struktuurid ja kultuurid ning suhtluse ja

usalduse määr juhtimisvõrgustikes mõjutavad osalejate suutlikkust tõhusalt koordineerida oma tegevust nii horisontaalselt, vertikaalselt, kui ka võimete tõhusat rakendamist valitsustasanditel.

Uurides küberkriiside haldamist e-valitsuses, on leitud viiteid sellele, et e-valitsemise süsteemi kriitilisuse aste mõjutab suuresti kulusid, mida valitsused on nõus kandma selle toimetuleku säilitamiseks küberkriisi ajal. Lisaks tuuakse välja viis mehhanismi, mis näivad eduka küberkriisijuhtimise jaoks e-valitsustes otsustava tähtsusega: kriisijuhtimise võrgustike 1) tehnoloogiahaldusvõime, 2) võrgustatud koostöövõime, 3) koostöökapital, 4) riskijuhtimise suutlikkus ja 5) legitiimsuse suurendamine. Need tegurid on kübervastupidavuse juhtimismehhanismide taksonoomiat, mis võiks olla aluseks edasiseks testimiseks ja arendamiseks tulevastes uuringutes.

Doktoritöö kübervastupidavuse ennatliku poole analüüs käsitleb kaasaegsete ühiskondade infrastruktuuride aluseks olevate IT-süsteemide turvalisuse juhtimist. See tõstatab mitmeid praktilisi poliitilisi kaalutlusi, mis on seotud tulevase küberjulgeolekupoliitika ja -regulatsiooni ülesehitusega: 1) vajadus vältida EL-i regulatsiooni killustumist ja kattumist uutes horisontaalsetes ja vertikaalsetes küberjulgeolekualastes õigusaktides; 2) viise, kuidas integreerida IT julgeolek, turvalisus ja privaatsus IT julgeolekuriskide hindamise standarditesse ja praktikatesse; ja 3) lahendusi poliitiliste otsustajate väljakutsetele, mis on seotud tehnoloogilise julgeoleku, riikliku julgeoleku ja geopoliitika vahel kasvavavate pingetega IT-süsteemide turvalisuse kontekstis.

Käesolevas doktoritöös pakutakse välja mitmeid mehhanisme, mille abil teadlased ja praktikud saavad katsetada ning edasi arendada ja viimistleda kavandatud juhtimismehhanisme, et suurendada e-riigi kübervastupidavust. Doktoritöö pakub mitmeid lähtekohti tulevasteks uuringuteks e-valitsemise, küberturvalisuse ja -vastupidavuse ristumiskohas. Vastavad uurimisvaldkonnad saaksid kasu avaliku halduse valdkonna kirjandusest, eelkõige institutsionalismi, poliitika loomise ja kohaneva valitsemise teemade, et uurida, kuidas kübervastupidavust saaks jätkusuutlikumalt haldusstruktuuridesse ja protsessidesse kinnistada.

# Appendix - Publications

**Publication I**

Skierka, Isabel. (2023). When Shutdown is No Option: Identifying the Notion of the Digital Government Continuity Paradox in Estonia’s eID Crisis. *Government Information Quarterly*, *40*(1). (1.1.).

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

# When shutdown is no option: Identifying the notion of the digital government continuity paradox in Estonia's eID crisis

Isabel Skierka [a,b,*]

[a] ESMT Berlin, Schlossplatz 1, 10178 Berlin, Germany
[b] Ragnar Nurkse Department of Innovation and Governance, Tallinn University of Technology, Akadeemia tee 3, 12618 Tallinn, Estonia

ARTICLE INFO

*Keywords:*
Digital government
Cyber risk
Cyber crisis management
Network governance
Resilience
Electronic identity
Estonia

ABSTRACT

States must increasingly manage cybersecurity threats and disruptions in their digital government infrastructures. However, the digital government literature lacks a systematic, more rigorous understanding of how states respond to such risks and crises and what factors can explain these responses. This article addresses this research gap by identifying explanatory mechanisms of cyber risk and crisis governance in a critical and, to date, unique case: the Estonian government's management of the 'ROCA' vulnerability, which rendered two-thirds of its national electronic identity cards vulnerable to a major security risk. The case provides one of few examples in which a digitally highly advanced state publicly dealt with a large-scale cyber risk at the heart of its digital government. Estonia overcame the crisis without constraining the affected infrastructures' functionality, while other countries did not. The article examines a seeming paradox of 'digital government continuity': Crisis managers can not afford to shut down widely adopted, yet vulnerable, digital systems. However, the vulnerable systems' continued operation contributes to their resilience. The article identifies five constructs that help explain digital government resilience: 1) technology management, 2) networked cooperation, 3) collaboration capital, 4) risk management capacity, and 5) legitimacy building.

## 1. Introduction

The growing threat of cyber incidents in public IT infrastructures requires governments to deploy strategies for managing respective risks and crises. Cyber-attacks have become an integral part of criminal, intelligence, and military operations (e.g. Austin, 2020; CSIS, 2020; Greenberg, 2019; Rid, 2013; Schmitt, 2017; Zetter, 2014). Digital infrastructures of governments are increasingly vulnerable (Caldarulo, Welch, & Feeney, 2022; Norris, Mateczun, Joshi, & Finin, 2019; Romanosky, 2016, p. 124). Not least, real-world incidents and the COVID-19 pandemic have exposed the rising dependence on and simultaneous vulnerability of digital government (DG) structures and services (Beduschi, 2021; Pandey & Pal, 2020). As a result, cyber resilience has emerged as a policy priority for states internationally (European Commission, 2022; G7 Presidency, 2022).

Against this backdrop, the article explores governments' handling of cyber risks and resulting crises in critical DG infrastructures. We understand cyber crises as situations in which IT disruptions have "the potential to severely limit or eliminate the functionality of key societal services or critical infrastructure, which must be dealt with urgently under conditions of deep uncertainty to avoid physical, financial, and/or reputational damage" (Backman, 2021, p. 432). The study adopts a holistic perspective on cyber crisis management (CM), including technical, organizational, and institutional aspects.

Despite its high practical relevance, cyber risk, CM, and resilience in DG remains an under-investigated area. Research on cybersecurity and incident management has mainly originated from computer science and adjacent technical disciplines (Dunn Cavelty, 2018, pp. 24–26). Over the past decade, a growing number of publications in DG research has addressed cybersecurity in the DG context (e.g. de Bruijn & Janssen, 2017; Irvine, 2005; Luna-Reyes & Gil-Garcia, 2003; Romaniuk & Manjikian, 2020; Viet, Van, & Ngoc, 2020; Zhang, Tang, & Jayakar, 2018; Zhao, Zhao, & S., 2010). However, only few studies explore aspects of cyber risk and CM in DG, such as cybersecurity incident management and exercises at the local government level (e.g. Caldarulo et al., 2022; Gedris et al., 2021; Norris et al., 2019; Pike, 2021; White, 2012), methods for cyber risk management in smart city contexts (Andrade, Guun Yoo, Tello-Oquendo, & Ortiz-Garcés, 2021), or cyber threat information sharing among governmental organizations and across the EU (e.g. Lanzendorfer, 2020; Ruohonen, Hyrynsalmi, & Leppänen, 2016).

[*] Corresponding author at: ESMT Berlin, Schlossplatz 1, 10178 Berlin, Germany.
*E-mail address:* isabel.skierka@esmt.org.

https://doi.org/10.1016/j.giq.2022.101781
Received 2 September 2021; Received in revised form 6 November 2022; Accepted 6 November 2022
Available online 9 December 2022

Remarkably, DG research lacks rigorous, empirically founded studies exploring the mechanisms of national cyber risk and CM (see also: Caldarulo et al., 2022, p. 1).

In crisis research, cybersecurity has only recently attracted growing attention (Kuipers & Welsh, 2017, p. 9). Publications studying the phenomenon of cyber crises address national governance structures and capabilities (Austin, 2020; Boeke, 2018; Collier, 2017; Garn, Kieseberg, Schreiber, & Simos, 2021), CM tasks (Berg & Kuipers, 2022; Prevezianou, 2021; Schrijvers, Prins, & Passchier, 2021) or practical exercises (Bahuguna, Bisht, & Pande, 2019; Østby & Katt, 2020; Østby & Kowalski, 2020; Simola & Lehto, 2020; Simon & De Goede, 2015; Smeets, 2022). Only few studies empirically examine mechanisms of cyber CM or resilience in a real-life crisis context (Backman, 2021; van der Meulen, 2013; Groenendaal & Helsloot, 2021).

This paper sets out to address this research gap and analyses national cyber CM through an in-depth study of Estonia's eID crisis. A leader in DG, Estonia is known for its successful defence against the first (publicly known) large-scale distributed denial of service (DDoS) attacks against government and banking websites in 2007. In 2017, it handled a large-scale cyber risk, emerging from the 'ROCA' vulnerability in two-thirds of the country's electronic identity (eID) cards (Lips, Pappel, Tsap, & Draheim, 2018; Valtna-Dvořák et al., 2021). This critical case allows us to understand how a highly advanced DG can overcome a cyber crisis endangering its infrastructures while keeping its digital society working.

The eID is an indispensable pillar of Estonia's digital society. All public and most private digital services rely on it, and almost 60% of the population uses the eID for digital service authentication and signing at least once per year (RIA, 2022). Its failure would have dramatic consequences for Estonia's "e-state"[1] and large parts of society: the eID system is 'too big to fail'.

Yet, despite the severe threat to the foundation of Estonia's digital state, the country managed to overcome ROCA without significantly constraining any of the eID or other DG systems' functions. Other countries, i.e. Austria, Slovakia, and Spain, whose e-signature or eID systems suffered from the same vulnerability, decided to revoke all vulnerable certificates and rendered affected cards unusable (ENISA, 2017; Meyer, 2017; The Slovak Spectator, 2017). That contrast points to the empirical puzzle of how Estonia managed to maintain the full functionality of its DG in the face of a large-scale cyber risk while other countries did not.

Our resulting research questions are:

- How did Estonia manage a large-scale cyber risk and a crisis that threatened to unsettle its DG infrastructures?
- Which factors and mechanisms can explain the overcoming of such risk and crisis?

This article presents a thick description of the Estonian response and attempts to provide a rigorous and interdisciplinary explanation of the event's occurrence. Our study aims to develop explanatory concepts that make our case's cyber risk and CM mechanisms comprehensible. While empirically grounded, our paper seeks to contribute to theoretical discussions at the nexus of DG and cybersecurity governance.

The study claims analytical generalisability in terms of rigorous discussion of explanatory variables and causal mechanisms but no statistical generalisability (see the methodology section for a more elaborate discussion) (George & Bennett, 2005; Schofield, 2011; Yin, 2018).

First, the study outlines a priori conceptual constructs from the different literatures in Section 2, followed by the research methodology in section 3. Section 4 presents the context and case description. Section 5 develops explanatory patterns for our case study considering the a priori conceptual constructs. The concluding section 6 discusses our theoretical and practical contributions in the context of the broader research literature. An annex presents a structured overview of the case and the article's data.

## 2. Conceptual approaches for exploring national cyber risk and crisis management

This article examines an administration's success in managing a severe cyber risk and resulting crisis in DG infrastructures without constraining the functionality of those infrastructures. Our problem analysis requires an understanding of different perspectives. Therefore, this section outlines several a priori conceptual constructs from the cybersecurity, public administration, and CM disciplines for our case study: (1) cyber risk, crisis, and resilience, (2) governance network theory, and (3) crisis governance capacity and legitimacy.

### *2.1. Cyber risk, crisis, and resilience*

Cybersecurity threats embody the complexity, transboundary nature, and uncertainty of contemporary security challenges like few others (Kjærgaard Christensen & Liebetrau, 2019; Lagadec, 2009; Perrow, 1999). From a technical perspective, a 'cyber' or information security risk is "the potential that threats will exploit vulnerabilities" of information asset(s) and thereby cause harm to an organization or other entities like individuals or a nation (ISO/IEC 27005, 2011). It is a function of (i) the adverse *impacts* that would arise if the circumstance or event occurs; and (ii) the *likelihood* of occurrence (NIST, 2012, p. 6).

*Uncertainty* related to the likelihood and impact of cyber incidents renders the assessment of cyber risks challenging (Eggers & Le Blanc, 2021, p. 4; NIST, 2012, p. 13; Strupczewski, 2021, p. 5). Their occurrence and timing are likely unpredictable, as they depend on often unknown and highly dynamic threats and vulnerabilities (ibid.). Adverse impacts can occur in material forms, such as loss of physical or financial assets, and immaterial forms, such as harm to reputation or legitimacy. Incidents in interconnected IT infrastructures can have cascading effects across technical, geographical, or functional borders (Agrafiotis, Nurse, Goldsmith, Creese, & Upton, 2018, pp. 8–13; Dunn Cavelty, 2005, p. 259; Schneier, 2018) and escalate into crises.

In our analysis, we pay specific attention to risk and CM effectiveness as an outcome. Risk management can be considered effective when risk is reduced to a level risk managers consider acceptable in the organizational or national context. CM is generally effective when a weakened or disrupted system (whether a social, organizational, or technical system) is brought back into alignment and achieves normal functioning at any stage of that process (Williams, Gruber, Sutcliffe, Shepherd, & Zhao, 2017, p. 740). In addition, effectiveness depends on stakeholders' belief that the successful outcomes of short-term and long-term impacts of crises outweigh the failure outcomes (Boin, Hart, Stern, & Sundelius, 2016, p. 25; McConnell, 2011; Pearson & Clair, 1998, pp. 60–61). As Williams et al. (2017, p. 742) note, effective CM is closely linked to *resilience*. We understand resilience as the capacity of a social system, like a society, "to proactively adapt to and recover from disturbances that are perceived within the system to fall outside the range of normal and expected disturbance" (Boin, Comfort and Demchak, 2010, p.9).

### *2.2. Governance networks and wicked problems*

Cyber risks and crises constitute *wicked problems* which combine complexity, ambiguity, and uncertainty (Lægreid & Rykkja, 2015, p. 476). Due to their complex and transboundary nature, their management requires governance among a diverse network of actors, which include governments, infrastructure operators, IT manufacturers, and end users across organizational borders, levels of authority, and sectors (Dunn Cavelty, 2005; Kjærgaard Christensen & Liebetrau, 2019; Lehto &

[1] Following official Estonian documents and language used in the Estonian media, we refer to the entirety of Estonia's digital government as the 'e-state'. The Estonian government often refers to the country as '*E*-Estonia' in marketing campaigns.

Limnéll, 2020; Simola & Lehto, 2020; Simon & De Goede, 2015, p. 88).

The 'governance network model' proposed by Klijn and Koppenjan (2016, p. 14) and depicted in Fig. 1 helps examine the governance of wicked cybersecurity-related problems in *networks,* which are "more or less stable patterns of social relations between mutually dependent actors" that cluster around a policy problem. It analyses the modes of *interaction* of different actors involved in governance networks and the *strategies* and *mechanisms* through which they decide and implement their decisions during a problem-solving process. Governance processes are *games* or "series of interactions between actors that focus on influencing problem formulations, solutions, and procedures regarding an approach to a specific policy issue" (van Bueren, Klijn, & Koppenjan, 2003, p. 195). Interactions occur in *arenas*, which are places or institutional settings of interaction, which may be formal organizational arrangements and bodies or informal settings like meetings (Ostrom, 1986 in: Klijn & Koppenjan, 2016, p. 82). Games develop in different *rounds*, during which actors explore problems and solutions. Each round ends and begins with a *turning point* defined by a crucial event or decision changing the course of events. Interactions – including breakthroughs or impasses – in the games can be explained by *substantive factors* such as actors' perceptions and interests and *strategic factors* like actors' strategies. Behind these substantive and strategic factors lie *institutional* factors, which impact actors' behaviour and network structures. We understand institutions as formal and informal rules, norms, and "standard operating procedures" which constrain and enable actors (March & Olsen, 1984). Relatedly, *network management* – the "strategies focused on improvement of the cooperation of the actors" in the games – can influence governance processes (van Bueren et al., 2003, p. 197). Such factors at the levels of network actors and their interactions can explain the *outcomes* of such "games".

Network governance usually "needs a long time and the involvement of many independent stakeholders who have to agree with each other" (Janssen & van der Voort, 2016, p. 1). This study applies the framework to a crisis that lasted only several months, thereby exploring its potential to explain short-term interactions in crisis.

### 2.3. Governance capacity and governance legitimacy

Since we examine how a state managed a national crisis triggered by a technical vulnerability, we additionally consider conceptual constructs from the crisis and public administration literature.

Approaches studying the national or supranational management of technologically complex crises argue that CM performance depends on crisis governance *capacity* and *legitimacy* (Boin, Busuioc, & Groenleer, 2014; Christensen, Lægreid, & Rykkja, 2016). Governance capacity comprises CM's functional and operational aspects, particularly *sense-making* and *coordination* capacity (Boin et al., 2014, pp. 423–424). *Sense-making* encompasses the detection and understanding of an unfolding crisis. It depends on crisis managers' capacity to access, exchange, and analyze information at the technical, operational, and political levels to build a strategic picture of the situation (Boin et al., 2016, pp. 23–45). *Coordination capacity* is about orchestrating and implementing a coherent response (Boin & Bynander, 2015, p. 124).

Governance *legitimacy* concerns CM's political aspects and concerns "citizens' assessment and acceptance of government actions in crises" (Christensen et al., 2016, p. 889). It "may be related to politics, participatory quality and support for political parties (input); to processes within the administrative apparatus (throughput); or to policies, means and measures (output)" (ibid; Scharpf, 1999, pp. 7–21; Schmidt, 2013, pp. 14–19). Arguably, crisis managers' communication and the public's support for political institutions also influences the legitimacy of national CM (Boin & Lodge, 2016, p. 293; Helsloot & Groenendaal, 2017; Easton, 1965, in: Stark, 2010, p. 4).

### 2.4. Application of conceptual constructs to the case analysis

The concepts outlined in this section serve as a priori constructs which guide our case analysis. The governance network framework constitutes the basis for operationalizing the description and explanation of actors' complex interactions in the CM process. The following section outlines the study's research methodology and the constructs' application in more detail.

## 3. Research methodology

We selected a case study research strategy to explain how actors in Estonia's national governance networks managed a cyber crisis successfully and why. The case study approach is particularly well-suited for the analysis as it allows for in-depth investigation of a phenomenon when "the boundaries between phenomenon and context may not

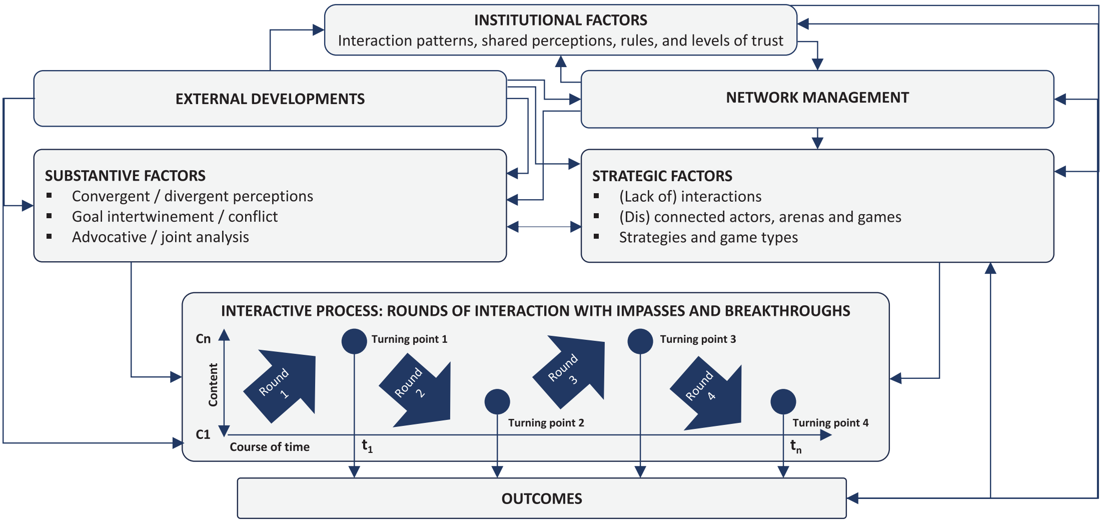

INSTITUTIONAL FACTORS
Interaction patterns, shared perceptions, rules, and levels of trust
EXTERNAL DEVELOPMENTS
NETWORK MANAGEMENT
SUBSTANTIVE FACTORS
Convergent / divergent perceptions
Goal intertwinement / conflict
Advocative / joint analysis
STRATEGIC FACTORS
(Lack of) interactions
(Dis) connected actors, arenas and games
Strategies and game types
INTERACTIVE PROCESS: ROUNDS OF INTERACTION WITH IMPASSES AND BREAKTHROUGHS
Cn
Content
C1
Round 1
Turning point 1
Round 2
Turning point 2
Round 3
Turning point 3
Round 4
Turning point 4
Course of time
t1
tn
OUTCOMES

**Fig. 1.** Factors explaining governance network processes, adopted in a slightly modified version from Klijn and Koppenjan (2016, p. 308)" about here.

be clearly evident" (Yin, 2018, p. 15). Blurring boundaries between context and process is a pronounced characteristic of crises (Deverell, 2010, p. 67; Roux-Dufort, 2007, p. 112). Moreover, it allows us to use a thick description to understand the phenomenon's complexity under investigation. Following the case study research design allowed us to engage in theory development (Eisenhardt, 1989) in (cyber) risk and CM in national governance networks, for which there has been little prior research.

We focus on this single case for several reasons. (1) The Estonian response to ROCA is a historically unique *index* case (Gerring & Cojocaru, 2016, pp. 398–399). Compared to other cyber crises, like the Estonian 2007 DDoS attacks, the impact of the NotPetya worm on the national health system in the United Kingdom in 2017, or cyber-attacks against critical energy infrastructure (Backman, 2021; Greenberg, 2019), ROCA threatened the core of a country's DG infrastructure at a society-wide scale. Even the severe and perhaps more similar 2011 hack of the 'Diginotar' certificate authority in the Netherlands did not affect the Netherlands' DG to a comparable extent (van der Meulen, 2013). (2) Estonia is one of a small number of states which can claim to run a *proper* DG (Solvak et al., 2019, p. 39) and uses electronic voting since the early 2000s (Krimmer, Triessnig and Volkamer, 2007). In this context, the Estonian eID crisis is the first and, until now, only case which offers insight into how decision-makers managed cybersecurity risks in a country with an advanced DG. Hence, the case is *critical* for understanding cyber risk governance in DG (Yin, 2018, p. 49). (3) The case has a *signalling effect* for other countries that will need to prepare for similar incidents in the future. An expert discussion in a forum sponsored by the US government in the spring of 2021 referred to Estonia as a "time machine," which allows us to "look into the future" of DG and eID management (US Forum on Cyber Resilience, 2021). Therefore, we believe that information from this case can inform the analysis of challenges and governance strategies in other cases. (4) Finally, the case is very *well-documented*. Media articles, post-crisis reports, and empirical studies provided a good basis for data analysis.

We aim to ensure increased reliability of the study by triangulating multiple data types from different sources (Miles, Huberman, & Saldaña, 2014). The data analyzed for the study encompasses relevant academic literature, official documents issued by public institutions and private companies, media reports, eID transaction data, as well as data from 25 semi-structured qualitative interviews with 22 key stakeholders, which we conducted in multiple phases between 2018 and 2022 (see Table 1, Annex). Reflection interviews with three key interviewees in 2022 allowed us to integrate their considerations of the case in the context of the current state of cybersecurity nearly five years after the ROCA crisis and to validate our findings. The numbers of eID transactions in Tables 5 and 6 (Annex) are based on data provided to the authors by SK ID Solutions. The eID transaction data constitute approximate information about the actual transaction and were used to analyze general trends only.

Our study takes into consideration results from an Estonian government-commissioned report of the case (Tehnikaülikool, 2018), two conference papers relying on the Tallinna Tehnikaülikool report's set of interview data (Lips et al., 2018; Valtna-Dvořák et al., 2021), and a computer science thesis on Estonian eID security (Parsovs, 2021). Those empirical studies and a semiotic analysis of the political and media discourse during the crisis (Ventsel & Madisson, 2019), constitute additional data points for this article. Our study distinguishes itself from these prior studies in that it forms an in-depth explanatory and theoretically founded analysis of the case and is based on independently collected data.

A priori constructs gathered from the literature shaped our initial research design. We adopted a theory development and content analysis research approach (Eisenhardt, 1989; Lune & Berg, 2017, pp. 181–200). In that process, we continually moved back and forth between data sources and analysis (Dubois & Gadde, 2002, p. 554; Eisenhardt, 1989, p. 546). We then collected and qualitatively coded the data from interviews, government documents, media reports, and other research reports with thematic and pattern coding techniques (Miles et al., 2014, pp. 69–103; Saldaña, 2013).

We used Klijn and Koppenjan's (2016) governance network framework to structure our case study along rounds, arenas, actors, and interactions in the CM process. The Annex' Tables 2 to 7 present the structuration of our data along this framework. Subsequently, we generated explanatory patterns for our case based on the identified categories emerging from our data analysis (Galunic & Eisenhardt, 2001; Yin, 2018, pp. 179–181). We related the patterns with the a priori conceptual constructs outlined in Section 2, refined them, and discussed them in the context of related literature (Eisenhardt, 1989, p. 541). We suggest several explanatory factors for large-scale cyber risk and CM in DG, which may be tested and refined in future studies. We aim to consolidate internal validity by ensuring data triangulation, constant comparison of data and emerging theory in light of the academic literature and the authors' familiarization with the case (Dubois & Gadde, 2002, p. 558; Eisenhardt, 1989, pp. 544–545; Miles et al., 2014).

An important limitation of a single case study research strategy is that it cannot produce generalizable statistical patterns. Hence, our analysis of a single national cyber crisis in one small and highly digitized state cannot generate externally valid statements on effective crisis governance in other countries worldwide. Yet, it can provide the basis for analytical generalization (George & Bennett, 2005; Miles et al., 2014; Schofield, 2011; Yin, 2018). In this sense, this case study's goal is to expand and further generalize existing concepts and theories, not to extrapolate probabilities in the sense of statistical generalization or to serve design purposes (Yin, 2018, p. 21). Our study avails itself as a starting point for further research, including validation and discussion of the study's findings on national cyber risk and CM in DG.

## 4. The 2017 ROCA eID crisis in Estonia

This section describes the case of Estonia's 2017 ROCA crisis. It first explains the case's context by focusing on Estonia's governance network structures and its eID management system (eIDMS). Subsequently, it describes the ROCA vulnerability at the origin of the crisis. The last subsection and Tables 3 to 6 in the Annex present the CM process structured along categories of the network governance framework introduced in Section 2.

### 4.1. Governance networks in Estonia

Estonia is an international leader in DG (Kitsing, 2011). It has ranked among the top three to eight countries in recent United Nations e-government development rankings (United Nations, 2020, 2022) and first for digital public services provision in the EU (DESI, 2021).

The eID card is a pillar of Estonia's DG and its internationally unique e-voting process (Kalvet, 2007; Krimmer, Triessnig, & Volkamer, 2007, p. 5; Martens, 2010). An institutional cornerstone of Estonia's e-state is the country's self-managed public-private networks and their governance of digital policy issues, ranging from public data sharing to cyber defence (Kattel & Mergel, 2019, p. 145). They emerged in the early 1990s when Estonia began to build its e-state in the wake of its independence from the Soviet Union. The country's small size and the resulting limited personnel and expertise in the public sector led the government to rely on experts from the private sector or academia to participate in policy-making (Randma, 2001, p. 46). According to Kattel and Mergel (2019, p. 154), the country's informal public-private networks underpin a *mission mystique* that "strengthens networks that are driven by common values and held together by (digitally savvy) charismatic leadership." It consists of an underlying common belief system and a mobilizing and supportive culture that produce a shared sense of identity among network actors (Goodsell, 2011, p. 479), which is tied to the country's 'e-narrative' of a highly digitized society (Drechsler, 2018).

Estonia's governance networks already played an essential role in managing Estonia's first cyber crisis in 2007, when experts from the public and private sectors joined forces to defend against the DDoS attacks (Landler & Markoff, 2007; Lesk, 2007; Ottis, 2008). The civilian cybersecurity agency, the Estonian Information System Authority (RIA), echoes this argument in a 2017 report where it states that "a 'collective brain' consisting of state and private sector data security experts acting in concert was able to repel the attempted attacks and helped to develop an action plan for the years ahead – one we have been able to follow to this day" (RIA, 2017, p. 4).

Indeed, Estonia has long focused on strengthening its cybersecurity capabilities (Drechsler, 2018; ITU, 2021). Since the 2007 attacks, Estonia has conducted regular national security and cyber crisis exercises, including multinational cyber exercises within NATO and EU structures (Kohler, 2020). The Estonian Defence Forces have been hosting the technical environment of NATO's 'Locked Shield' cyber exercise since 2013 (Smeets, 2022, p. 14). Since 2008, Estonia has been home to the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), an international military organization to promote research, training, and exercises on cybersecurity.

### 4.2. Estonia's eIDMS

A public-private governance network has managed Estonia's eID system since its emergence in the early 2000s (Martens, 2010; Republic of Estonia, 2018). Technologically, it is based on a public key infrastructure (PKI). Smartcards were the central tokens during the ROCA crisis for the Estonian eID. A card held two 2048-bit RSA keys with corresponding X.509 public-key certificates to provide the cryptographic functionality for authentication and the qualified electronic signature function. The two private keys were each securely protected on the card by unique user PINs. A mobile version of the eID card, "Mobile-ID," also existed. The solution is based on a secure mobile SIM card, which the user has to request from an Estonian mobile phone operator. The SIM card stores private keys and supports authentication and signature functions. Yet, only around 10 % of the population used Mobile-ID in 2017 (SK ID Solutions, 2018). In November 2016, the certificate authority SK and the Estonian cybersecurity firm Cybernetica introduced the "Smart-ID" software-based mobile solution for secure electronic authentication and signature. At the time of ROCA in 2017, Smart-ID was still a new solution, which did not have the same legal status as the eID card or Mobile-ID. Hence, it could only be used with private services that accepted it. In November 2018, Smart-ID was certified as a qualified electronic signature creation device (compliant with the EU's eIDAS-regulation on electronic identification and trust services) and was recognized by public sector authorities in Estonia and across the EU.

The eIDMS governance illustrated in Fig. 2 comprises four main parties cooperating in a public-private network: The Police and Border Guard Board "Politsei- ja Piirivalveamet" (PPA), the Estonian Information Systems Authority "Riigi Infosüsteemi Amet" (RIA), SK ID Solutions, and Gemalto.

Within the eIDMS, the PPA issues the eID card. It is responsible for applications, revocations of eID cards, and the suspension, revocation, or updating of certificates. The IT Development Centre (SMIT) provides IT support in ID card-related activities to the PPA. The Ministry of Interior oversees PPA.

RIA is Estonia's civilian cybersecurity authority, houses the national Computer Emergency Response Team (CERT-EE), and maintains public IT systems and the eID software. It is overseen by the Ministry of Economic Affairs and Communication "Majandus- ja Kommunikatsiooniministeerium" (MKM).

SK ID Solutions (hereafter: SK) is the eID scheme's certificate authority and administrator of the PKI. It issues certificates for national eID documents and is responsible for maintaining them throughout their lifecycle, covering their creation, activation, suspension, and revocation. As a subcontractor of SK, mobile operators deliver SIM cards with Mobile-ID functionality. Until 2018, the competent authority for supervising SK as a TSP was the Technical Surveillance Authority "Tehnilise Järelevalve Amet" (TJA). TJA did not play a significant role in the ROCA CM. In 2018, RIA assumed that function from TJA, expanding its responsibilities within the eID system.

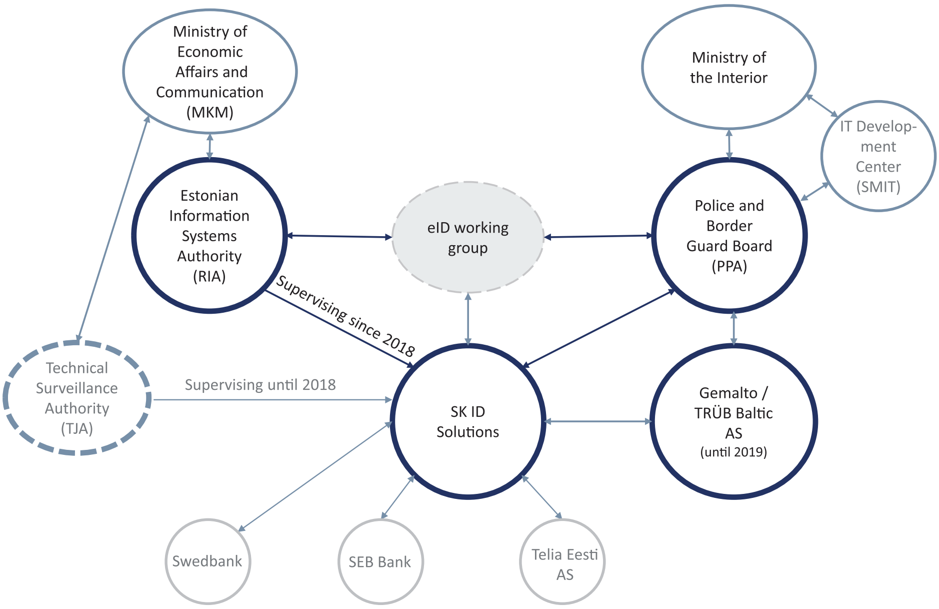

Ministry of Economic Affairs and Communication (MKM)
Ministry of the Interior
IT Development Center (SMIT)
Estonian Information Systems Authority (RIA)
eID working group
Police and Border Guard Board (PPA)
Supervising since 2018
Technical Surveillance Authority (TJA)
Supervising until 2018
SK ID Solutions
Gemalto / TRÜB Baltic AS (until 2019)
Swedbank
SEB Bank
Telia Eesti AS

**Fig. 2.** Estonia's eIDMS.

The firm Gemalto was Estonia's eID card manufacturer from 2002 until 2018 as a subcontractor of the PPA. It supplied the smart card and personalized it through its subsidiary TRÜB Baltic AS. It also issued the eID certificates under a contract with SK. Infineon Technology AG supplied the eID card's chip.

The PPA, RIA, and SK met regularly in the setting of an "eIdentity Working Group" (Interviewees 16, 21; Martens, 2010, p. 222). However, a clear formal demarcation of responsibilities did not exist at the time of the crisis (Tehnikaülikool, 2018). Beyond the formal members outlined above, the broader eID ecosystem includes many other actors. These actors comprise service providers integrating eID card and Mobile-ID solutions, academic institutions with technical expertise, and technology firms, such as the cybersecurity firm 'Cybernetica,' which has a close working relationship with RIA and serves as the government's 'crypto think tank' (Interviewee 12). In cases with technical infrastructure changes, all services using the eID must also implement changes at their end.

### 4.3. The ROCA vulnerability

The Estonian eID crisis began on 30 August 2017 and lasted until spring 2018. It originated in the so-called "Return of the Coppersmith Attack" (ROCA) vulnerability (CVE-2017-15,361). ROCA emerged from a cryptographic key generation optimization mechanism integrated into a chip from the manufacturer Infineon technologies, which a research team from Masaryk University discovered (Nemec, Sys, Svenda, Klinec, & Matyas, 2017). The chip was built into millions of identity cards, signature devices, and trusted platform modules worldwide (Goodin, 2017), including all Estonian eID cards issued after 16 October 2014. As a result, two-thirds, or around 760,000, of Estonia's national eID cards were vulnerable to ROCA. Since the Estonian eID scheme nearly exclusively relied on the eID card, the vulnerability had a severe potential impact. The successful exploitation of this security vulnerability could have enabled a third party to calculate the RSA private key of an eID cardholder with only the knowledge of the corresponding RSA public key with much less computational complexity than should have been possible (Nemec et al., 2017, p.11). The required computing power's initially estimated cost was around USD 80000 (RIA, 2018, p. 1), although cryptography experts later estimated the costs were as low as USD 25000 or less (Bernstein & Lange, 2017). Even one single exploitation could have called into question the identification, authentication, and signing operations with the affected cards (Nemec et al., 2017).

Although ROCA also affected signature cards in Austria and eID cards in Spain and Slovakia, those events did not evolve into crises. In Austria, only 30,000 out of around 8.8 million Austrian citizens held an e-signature card at the time. Only a few thousand certificates issued by one trust service provider (TSP) were affected by ROCA (Interviewee 6). The TSP revoked the certificates in June 2017 (ENISA, 2017) (Interviewee 6). Slovakia, where only around 300,000 out of 2.5 million ID cards contained e-signature certificates, and only 30% of DG services required an electronic signature, revoked affected certificates in late October 2017 (Ministry of the Interior of the Slovak Republic, 2017; The Slovak Spectator, 2017). The Spanish government, where less than 1 % of citizens used the eID card for public service engagement, decided to revoke the certificates of 17 million eID cards in November 2017 (El Diario in: Meyer, 2017). Due to the low eID user numbers in those countries, there was no visible effect (Lips et al., 2018, p. 7). Those states' DG is much less developed than Estonia's, and only a fraction of their populations used the cards' identification or signature functions.

### 4.4. The Estonian eID crisis management process

This sub-section outlines the crisis process' major developments. Following Klijn and Koppenjan's (2016) network governance approach, Tables 2 through 5 in the Annex present a more detailed overview of the CM process.

Within Estonia's governance networks, various autonomous yet interdependent *actors* are involved in different *roles* in the CM process, which Table 2 (Annex) illustrates. Their actions and strategies influenced the course and outcomes of social interaction processes.

The interactions during the CM process took place in six *arenas* illustrated in Table 3 (Annex). The ROCA crisis process developed in several rounds of interactions between actors in overlapping arenas, which Table 4 (Annex) shows. A short version of Table 4 is included below for a better overview.

The crisis process began on 30 August 2017. After ROCA's disclosure to CERT-EE, the Estonian government immediately involved essential stakeholders in a national crisis response effort and set up strategic, technical-legal, and communication crisis working groups (WGs). The government publicly announced the vulnerability at a press conference on 5 September 2017. The eID's operations were upheld, including online voting during municipal council elections in mid-October. On 25 October 2017, the government released an update to patch vulnerable certificates, which users could install remotely or physically in service points. After the publication of ROCA details in a research paper on 30 October 2017 (Nemec et al., 2017), the government suspended all remaining vulnerable certificates. The update process continued until 1 April 2018, when the crisis officially ended.

Table 4 illustrates the CM process' *rounds* and *turning points*. The column "*arenas*" indicates which arenas converged in which rounds. Below is a simplified version.

As eID transaction numbers in Tables 4 and 5 (Annex) show, total transactions did not significantly decrease, which indicates no significant loss of confidence in the eID. Table 5 further shows that the use of the Smart-ID increased at the expense of eID card usage during the crisis.

*Simplified version of Table 4 "Rounds in the Estonian ROCA crisis management process."*

| | Actions in rounds | Arenas |
|---|---|---|
| Turning point | ROCA discovery and disclosure to the manufacturer in January / February 2017 | |
| Round 1: Vulnerability Disclosure Failures | ROCA disclosure to the manufacturer (late January 2017), later Gemalto (May 2017), formal incident notification by ENISA (June 2017). | AR5, AR6: IT Security, EU |
| Turning point | ROCA vulnerability disclosure to CERT-EE on 30 August 2017 | |
| Round 2: Estonia's crisis response organization | ROCA disclosure to CERT-EE (30 August 2017), subsequent political crisis roundtable, and operational (strategic, technical-legal, communications) crisis working groups. | AR1, AR2, AR3: Political strategic CM, Operational CM, eID management |
| Turning point | Press conference on 5 September 2017 | |
| Round 3: Public vulnerability announcement | Emergency press conference by Prime Minister and Director Generals of RIA and the PPA (5 September 2017), continuity of eID services was upheld. | AR1, AR2, AR4: Political strategic CM, eID management, eID end user |
| Turning point | Municipal election from 5 to 11 October 2017 | |
| Round 4: Online elections | Despite political challenges, online voting remained possible during municipal council elections scheduled from 5 to 11 October 2017, the Supreme Court rejected a legal appeal. | AR1, AR5: Political strategic CM, IT security |
| Turning point | Patch deployment on 25 October 2017 | |

(continued on next page)

(*continued*)

| | Actions in rounds | Arenas |
|---|---|---|
| Round 5: Patch deployment | RIA and the PPA deployed the technical vulnerability patch, which users could install remotely or in physical service points, on 25 October 2017. | AR2, AR4: Operational CM, eID end user |
| Turning point | Publication of researchers' paper with ROCA details on 30 October 2017 | |
| Round 6: Emergency suspension of certificates | The university researchers published their paper with ROCA details on 30 October. Estonian authorities suspended all remaining vulnerable certificates on 3 November 2017. PPA and Gemalto engaged in legal proceedings. | AR1, AR2, AR5: Political strategic CM, Operational CM, IT security |
| Turning point | Authorities revoked certificates of all non-updated eID cards on 1 April 2018 | |
| Round 7: Operational crisis termination | The government terminated the crisis by revoking the remaining vulnerable certificates on 1 April 2018. RIA held an international 'lessons learned' conference and commissioned a post-crisis report. | AR1, AR3, AR5, AR6: Political strategic CM, eID management, IT security, EU |
| Turning point | Conference Report Publication on 9 May 2018 | |
| Round 8: Post-crisis blame games | The legal liability dispute between the PPA and Gemalto ended with a compromise agreement in February 2021. | AR 1: Political strategic CM |
| Turning point | Settlement of legal liability dispute on 6 February 2021 | |

### 4.5. *Crisis outcomes*

This section described the Estonian management of its ROCA crisis and its context. Following Klijn and Koppenjan's (2016) network governance framework, it gave an overview of the crisis process' key actors, arenas, rounds of interaction, as well as actors' risk perceptions and response strategies.

The case provides an example of somewhat effective cyber CM and resilience in DG. CM effectiveness consisted of bringing the disrupted eID system back into alignment and normal functioning (Williams et al., 2017, p. 740). By the end of the crisis in the spring of 2018, the Estonian government had successfully mitigated the risk. Estonia's DG proved *resilient*: overall, the e-state could absorb ROCA's disturbance and remain functional.

Based on this this section's and the Annex' structured case description, the subsequenet section aims to build explanatory patterns for Estonia's resilience in the face of ROCA.

## 5. Explanatory patterns for Estonia's crisis response

Estonia managed to keep its DG fully operational despite a significant security vulnerability in its eID system. How did it govern a large-scale risk in an essential DG infrastructure? We found an antecedent of system criticality and five patterns that enabled Estonia to overcome the crisis and ensure DG continuity.

We identified the Estonian DG's systemic criticality as a primary parameter guiding the government's decision on handling the crisis. The actual and perceived value of the eID for Estonia's DG determined crisis managers' perspectives on the crisis outcome and their resolve to keep the systems up and running even in a vulnerable state. An eID shutdown could have jeopardized the survival of e-Estonia in terms of citizens' trust in the system, its international reputation and the DG-leader narrative (Drechsler, 2018), which it had crafted for decades. Metaphorically, 'operating on the open heart' of DG was necessary to save it.

We call this phenomenon the *DG continuity paradox*: Intuitively, one might assume that a vulnerable DG system must be shut down or immediately repaired to avoid damage to the larger digital state ecosystem and its users. Yet, as a system passes the threshold of 'systemic criticality' for the wider DG ecosystem, it needs to continue running, even in a vulnerable state. Such decision aims to guarantee business continuity, or in our case, DG continuity.

While the antecedent explains crisis managers' initial decisions, the DG's resilience depended on several interdependent mechanisms. In the first place, ensuring the robustness of technological infrastructure was a foundation for Estonian crisis managers' capacity to act, as Pattern 1 explains. The institutional context described in Pattern 2 enabled cross-organizational collaboration among governance network actors, which enhanced sense-making and coordination during the crisis. Actors' ability to quickly orient themselves, collaborate, and improvise within their crisis response rested on their shared institutional memory explained in pattern 3. In the CM process, the actors' adaptive ad hoc cyber risk management, presented in Pattern 4, determined their capacity to decide and implement an adequate response. In addition, crisis communication and meaning-making during the crisis, described in Pattern 5, were essential to ensure broader support for and legitimacy of the CM governance process and outcomes.

The first pattern, Estonia's eID system's *technological robustness*, relied on prior IT design choices. The system's primary reliance on the smartcard as a singular technical eID means, first, predisposed the country to high technical risk. Nonetheless, the system proved redundant due to three main factors. First, the Estonian eID platform allowed migration to the alternative non-vulnerable ECC algorithm. Due to select experts' skills and detailed knowledge of the eID technical environment, the WGs were able to recognize that possibility quickly. Moreover, the possibility for eIDMS actors to revoke all vulnerable certificates provided a 'kill switch' option to mitigate damage in the event of exploitation. Finally, the new and, at that time, little-used Smart-ID seems to have provided a limited technical alternative to citizens. As eID transaction data (Table 5, Annex) illustrates, the ROCA crisis might have catalyzed the breakthrough of Smart-ID as a dominant means of identification in Estonia. It now serves as an authentication tool for state services (SK ID Solutions, 2019) and represents a state-of-the-art solution for digital authentication comparable to other easy-to-use mobile identification solutions. The post-crisis integration of the Smart-ID in the larger eIDMS increases eID redundancy and makes Estonia more resilient against future similar vulnerabilities.

The second CM pattern at the institutional level involved governance networks' *cross-organizational cooperation* through respective structures, underlying shared norms, and active network management. From the beginning of the crisis response in round 2 (Table 4), the government activated pre-existing cross-organizational governance networks. Those network members' shared sense of identity, common goal to protect Estonia's digital society, and their *mission mystique* (see Section 4.1.) were important underlying socio-cultural institutions. "Everyone (of the WG members) held the attitude 'if not me, then who?' – there was an extremely high sense of responsibility among crisis managers", which is "not necessarily characteristic of bureaucratic institutions," as one interviewee recounted (Interviewee 20). Those structures and shared norms facilitated swift cooperation across different crisis response arenas (such as the strategic political CM, operational CM, and eID management arenas mentioned in Table 4).

RIA facilitated cross-organizational cooperation as the de facto crisis network manager. It coordinated information sharing and response decisions between different arenas and their respective actors, including the operational and strategic CM, eID management, and IT security arenas (Interviewees 1, 2, 7, 13, 15, 20). As a WG member recounted: "We did not directly interact with political officials; we coordinated everything with RIA." (Interviewee 2). "No ministry, government, or other institution but RIA was the crisis manager … RIA engaged different parties, and everybody looked at them [for guidance]" (Interviewee 1).

The cross-organizational cooperation resulting from these institutions and RIA's role enabled an adaptive crisis response across institutional boundaries, gradually enhancing the administration's sense-making and coordination capacity.

Overall, the administration prioritized speed and flexibility of informal communication and decision-making processes – output effectiveness – over more time-consuming formal processes of institutional accountability and input legitimacy. No formal Emergency Act procedures were activated. Legality and accountability of CM decisions rested on the WG's legal assessments and the National Election Committee's and Supreme Court's decisions to allow online voting with the vulnerable cards (round 4, Table 4). An analysis of the legal case concluded that initial decisions to keep eID certificates functional did not breach national or European (eIDAS) legal requirements but likely neglected security requirements laid down in the eIDAS regulation and EIT-SETA for trust service providers (TSPs) (Parsovs, 2020, p. 467). Hence, deficits in throughput legitimacy and accountability of decisions during the CM were offset by increased output effectiveness.

A third pattern emerges from crisis managers' *institutional memory*. Many operational crisis managers had trained together in crisis exercises or were involved in the defence against the 2007 DDoS attacks. The resulting knowledge had been preserved through interpersonal relations and narratives of past experiences. As one interviewee said: The success of cyber CM in Estonia relied on "knowing the people, not so much about knowing the structures. It is about personal ties. You know whether you've solved things together, then you know the person, you know whom to call and what they can do and how you can cooperate" (Interviewee 21). Familiarity and interpersonal trust among network actors enhanced their ability to quickly collaborate and improvise during the crisis without much need for hierarchical directions (Interviewees 7, 13, 16, 20).

A particularly prominent narrative remains that of Estonia's 'collective brain.' As stated earlier, the 'collective brain' concept refers to a community of IT and cybersecurity experts deeply embedded in Estonia's public-private governance networks. The community's origins date back to the 1980s. It is managed by RIA, which acts as the community "gatekeeper" and organizes regular events. As one expert states: "They are basically cyberpunks [who] have practiced together … for a long time" (Interviewee 3). Community members embrace the "hacker ethic" – what counts are members' skills and knowledge rather than hierarchy or status. Rather than being committed to upholding the e-state, they aim to "serve Estonian society." Responding to large-scale cyber risks to Estonia, like the 2007 DDoS attacks or ROCA, is "a societal kind of obligation rather than obligation towards the e-state" for them (Interviewee 3). Hence, Estonia's institutional memory consisting of governance network actors' collective knowledge and learned experience shaped actors' collaborative strategies throughout the ROCA crisis.

A fourth pattern of resilience emerges from the *ad hoc assessment and management of ROCA's risk* throughout the crisis response. Unlike other similarly affected and less digitized countries, Estonia chose to *accept* instead of *avoiding* ROCA's threat to its eID system. As explained previously, an important reason for this decision was the eID's systemic criticality for decision-makers and the government's determination to uphold DG continuity. The opportunity cost of a precautionary approach, i.e., eliminating the risk by revoking two-thirds of all eID card certificates, was not acceptable. As one of Estonia's governance networks' core members argues, it was relatively easy to eliminate the technical risk: "you can just recall all the certificates, and all the eID just goes away. And (…) technically, nothing happens from that point onwards, everything is secured. However, the impact that incident could have potentially had on the trust relationship that underpins everything the digital government does – this was extremely scary" (Interviewee 3). Crisis managers chose to maintain eID functionality not *despite* Estonia's dependence on its advanced DG but *because* of it.

Understanding this choice and cyber risk assessment and management throughout the crisis requires a more detailed approach to risk than the one outlined in Section 2. We therefore followed the NIST cyber risk framework and differentiated between the risk factors threat (T), vulnerability (V), likelihood (L), and adverse impact (I) (NIST, 2012, pp. 8–12) (illustrated in Fig. 3, Annex).

Table 7 in the Annex details key decision-makers' *risk assessment, risk severity perceptions,* and *responses*. It illustrates how Estonian decision-makers might have assessed and responded to the risk in each round. The perceived risk severity among crucial actors throughout the crisis response never exceeded a moderate level. ROCA's exploitation's *impact (I)* would have been high, even if only one ID card had been affected. It could have significantly damaged trust and the reputation of the eID and the larger e-state. ROCA's *vulnerability (V)* severity depended on its exposure and ease of exploitation, i.e., how much information was publicly accessible and which security controls, like the patch, were in place. Theoretically, a range of possible adversarial *threat sources (T)* with various capabilities and levels of intent existed, such as skilled hackers with financial motivations or foreign intelligence agencies aiming to create political unrest or mistrust. Government leadership actors publicly claimed an attack was unlikely since it would have required strong cryptography expertise and computing power costing 80,000 US Dollars per card. However, technical experts from the CM WGs were confident that threat actors would exploit the risk once ROCA details were public. One WG member, for example, emphasized that "if information [about ROCA] was released and everybody knew how to use the vulnerability, we were 100% sure that it will be used (…) The Estonian eID ecosystem is large enough to definitely find a person to attack for a meaningful amount of money (…) Even if it's one or eight million, you can build a scenario where that pays off." (Interviewee 1). Another technical WG member stated: "The attack cost was a little bit downplayed… I think in order not to create panic. But it was, I would say, cheap compared to the resources available [to hackers]. There are a lot of attackers who can afford this expense" (Interviewee 2). Moreover, a TSP like SK would face legal and business obligations to protect its users against any possible attack.

The decisive factor in the risk assessment was the threat occurrence *likelihood (L)*. Following initial days of information gathering and sense-making, political actors' and experts' perceptions and strategies converged toward the conclusion that L was low if details about ROCA remained unpublished and likely inaccessible to potential attackers. In addition, the eIDMS actors had a backup list of all vulnerable certificates and a "special release script" that could be run quickly when the vulnerability was exploited. That backup plan allowed crisis managers "to stay in this limbo position" (Interviewee 1) and further reduced the likelihood of damage. The low probability and fallback option were decisive in its ability to keep the eID up and running until the researchers published their paper on 30 October (round 6).

Throughout the decision-making process, crisis leadership relied on their experts' skills and experience with cyber risk management. As one WG member stated, politicians "were smart enough to trust the experts…[and] didn't try to decide on their own without taking the inconvenient opinion of experts into account" (Interviewee 2).

A fifth pattern emerged from the Estonian crisis leadership's *meaning-making and communication* to create legitimacy for its crisis response. In an "us vs. them" logic, the government's narrative differentiated between the Estonian nation and foreign actors, against which Estonia had to protect its e-state. Our data (Table 3, Annex) shows that the dependence on foreign actors, mainly Gemalto, was a crucial issue in the strategic political CM. In Estonian crisis managers' view, Estonia was left alone, having to deal with ROCA as a small state with limited resources and personnel, not being able to count on support from the international IT corporations it depended on (Interviewees 3, 7; Tehnikaülikool, 2018, p. 53). After ROCA's risk was mainly in check, Estonian officials began publicly blaming Gemalto for its non-disclosure of the vulnerability and their alleged, resulting responsibility in the crisis in November 2017 (round 6, Table 4) (Ventsel & Madisson, 2019, p. 132). The dispute culminated in the government pressing legal charges against the company, which led to a court procedure settled in February 2021 (ERR News, 2017; Parsovs, 2021, pp. 138–140; Pau, 2018).

The external enemy narrative might have created internal cohesion by converging actors' perceptions and strategies. Domestic network convergence is evident by overlapping issues and actors in various arenas, notably the strategic CM, operational CM, and the eID management arenas, and those arenas' convergence in multiple rounds (see rounds 2, 3, 5, 6 in Table 4).

The international conference "The Lessons We Learned" on 9 May 2018 and its presentation of the ROCA management further served to frame Estonia's image as a resilient global DG leader (RIA, 2018).

Crisis managers' transparency regarding the ROCA risk was remarkable and rather untypical compared to prior handling of eID security risks in Estonia (Parsovs, 2021, pp. 118–153) and beyond Estonia. One reason might have been that officials did not want to jeopardize public trust if somebody exposed the flaw's cover-up (Interviewees 3, 13, 15; Raag, 2018). Joint upfront communication additionally enabled the government to engage in meaning-making and control the narrative throughout the crisis. For example, the risk's framing as 'theoretical' (Vahtla, 2017a) justified decisions to keep eID systems and services operational.

Despite journalists' and some opposition politicians' considerable concerns expressed in the media (Ventsel & Madisson, 2019), the public seemed to continue trusting the eID, as the usage rates from Tables 4 and 5 indicate. Meaning-making practices served to underpin claims for throughput legitimacy by fostering public and stakeholder support for the administration's crisis governance (Interviewees 3, 7, 13, 20; Kund, 2017).

Additionally, transparent communication lowered the likelihood of an incident going undetected and could serve as an additional risk management instrument. It might have prepared eID end users for the possibility of an incident and thereby reduced the risk of a sudden loss of trust among the Estonian public.

## 6. Concluding discussion

This paper explores Estonia's management of a large-scale cyber risk to its DG and attempts to explain the overcoming of the resulting crisis. In this section, we discuss and sharpen our a priori conceptual constructs considering the explanatory patterns and the relevant literature.

We found a crucial parameter in crisis decision-making to be the systemic criticality of Estonia's DG and the eID as its key pillar. It strongly influenced government leadership's and crisis managers' perception of the cost associated with an interruption of DG services. Maintaining *DG continuity* with a vulnerable eID system became the primary goal, made possible by constant adaptive risk monitoring and management. This parameter might have played out differently in a country with a less advanced DG. Indeed, the revocation of certificates in Austria, Spain, and Slovakia, whose DGs were much less developed at the time, supports this assumption. In the case of DigiNotar's 2011 certificate hack, the certificates issued by DigiNotar were more critical for the Dutch economy than the Dutch government had been aware of. The high opportunity cost of certificate revocation, for example for the delivery of imported goods in Rotterdam Harbour, became visible only after the government had initiated the revocation of certificates (van der Meulen, 2013, pp.54-55).

We can therefore suggest that, in our case, the maturity of a country's DG and a society's resulting dependence on it impacted a government's decision on whether and how to uphold DG continuity in case of large-scale vulnerability. When DG maturity is significant, e.g., in terms of DG adoption or average use of services, crisis managers might have a different viewpoint regarding a shutdown. DG adoption and usage seem to be critical factors that matter for cybersecurity assessments. Further research should explore the significance of DG maturity for cyber risk management decisions and how the threshold can be determined beyond which DG impairment is no option anymore.

In addition to this finding, a discussion of the patterns allows us to refine the conceptual constructs and elaborate on this study's theoretical contributions to the study of cyber CM in DG. At the *context* level, the technological infrastructure robustness and the institutional structures and norms enabling cross-organizational cooperation enhanced Estonian crisis governance capacity. As explained in the previous section, technical robustness and the eIDMS network's experts' competence helped Estonian actors to keep technology operational and win time to make sense of the crisis. An analysis of the DigiNotar indicates similar takeaways. A combination of technical and organizational shortcomings led to the DigiNotar case evolving into a crisis. They included the lack of technological redundancy in the form of backup certificates, missing risk awareness, and poor security audit practices, among others (van der Meulen, 2013, p. 55). For a refined construct, we suggest that an administration's '*technology management capacity*' depending on the condition of technological infrastructures and the ability to deploy competent experts with deep knowledge of affected systems, is decisive for DG resilience.

At the institutional level, existing public-private network structures and their common norms and goals strengthened Estonian actors' crisis coordination capacity. We refer to this construct as '*networked cooperation competence.*' Our observations support previous case studies' findings, which link at least partially decentralized and flexible organizational structures to enhanced CM effectiveness (Boin & Bynander, 2015; Faraj & Xiao, 2006; Groenendaal & Helsloot, 2020). Backman (2021) specifically points to the benefits of private-public networks in Estonia and the UK in resolving national cyber crises. We can also relate the construct to adaptive modes of governance, which are flexible, and encompass efforts to mobilize internal and external capabilities, thereby "improv[ing] the speed of decision-making" (Janssen & van der Voort, 2016, p. 4).

In contrast, the role of networks' underlying common norms and actors' shared identity, has so far been only implicitly explored in the crisis literature (Faraj & Xiao, 2006). In Estonia, the shared mission to protect Estonian society helped activate sustained cooperation before and during the crisis. Further research should be undertaken to investigate the interplay of structures and actors' norms and perceptions in cyber crises. Sociological and ideational institutionalist theories might provide avenues for further analysis (Koning, 2015; March & Olsen, 1984).

The aspect of institutional memory illuminated the central role of shared knowledge, enshrined in narratives and practices, in shaping Estonian actors' perceptions and resulting interactions during the ROCA crisis. We argue that this 'memory' of past experiences and interactions created '*collaboration capital*,' which actors could draw on in the crisis. Narratives of the past, in our case, the 2007 DDoS attacks, exercises, and interpersonal relations, became embedded in processes and were thereby 'institutionalized' (Corbett, Grube, Lovell, & James Scott, 2020, p. 4). The 'collective brain,' activated during the ROCA crisis, is a good example. They constitute an informal and dynamic form of institutional memory emphasized by Hardt's (2017, p. 124) study of institutional memory in NATO crisis management.

With pattern four, adaptive cyber risk management, we developed our initial construct of cyber risk into *risk management capacity* as an essential element of cyber crisis governance. In the Estonian ROCA case, a formal risk framework based on NIST standards helped trace the structure of the risk decision process throughout the crisis. Beyond such formal guidelines, however, our analysis revealed the strong impact of actors' risk perceptions and goals on resulting practices. Multiple studies from the DG and technical cybersecurity literature suggest technical methods for cyber risk assessment and management in DG or critical infrastructures (Baggott & Santos, 2020; Viet et al., 2020). However, a more constructivist approach to cyber risk management is lacking. In future studies, we suggest engaging more with constructivist perspectives on cyber risk (Hansen & Nissenbaum, 2009).

Finally, meaning-making and transparent risk communication served to justify the government's course of action and create support for its decisions. This finding confirms previous studies' claims that meaning-making in terms of framing and symbolic messaging are central leadership tasks to gain public support during (flash) crises (Boin et al., 2016, pp. 78–82; Helsloot & Groenendaal, 2017, p. 352). The Estonian crisis communication further features several strategies for evidence-based messaging in cybersecurity (de Bruijn & Janssen, 2017), including the non-exacerbation of the risk, the singling out of villains – in this case, the foreign card manufacturer – and highlighting the heroes – Estonian crisis managers. Due to the deep embeddedness of DG in Estonian society, a connection to the public's values was relatively simple in our case. We can further propose that Estonians' general support for the e-state probably offered a reservoir of goodwill from which political actors could draw credit in times of crisis, bolstering overall legitimacy (Easton, 1965, in (Stark, 2010, p. 4). Based on these findings, we refine our construct to *legitimacy building*.

In conclusion, this article provides an in-depth study of managing a large-scale cyber risk and the ensuing crisis in Estonia's DG. Our final contribution is the proposal of a framework's outlines to study how governments handle cyber crises. We suggest explaining cyber CM in DG in our case through a network governance lens, which considers the interactions of different networks' actors and their perceptions and strategies. Our case showed that the DG infrastructure's (perceived) systemic criticality for the country's state and society determined whether the administration would prioritize DG continuity over risk avoidance by shutting down vulnerable systems. In addition, we found that the country's resilience needed to be assessed based on five constructs: the crisis governance networks' 1) technology management capacity, 2) networked cooperation capability, 3) collaboration capital, 4) risk management capacity, and 5) legitimacy building.

Thus, our approach aims to substantiate the underlying mechanisms and their interrelationships that explain (successful) cyber CM and resilience and thereby seeks to complement existing work on CM and resilience (Backman, 2021; Berg & Kuipers, 2022; Boin et al., 2016; Boin & van Eeten, 2013; Christensen et al., 2016).

The Estonian case poses a unique opportunity to observe a DG system's resilience. Certainly, no examination of one cyber crisis in one highly digitized country can produce generalizations about national cyber risk and crisis management worldwide. Nonetheless, the 'digital continuity paradox' identified in our study and the different mechanisms of resilience employed show how even one of the world's DG leaders accepted a cybersecurity risk to keep its DG running, not despite its advanced DG, but because of it.

## Research data for this article

Due to the sensitive nature of the questions asked in this study, interview partners were assured raw data would remain confidential and would not be shared. The processed data is accessible in the Annex' Tables.

## Author statement

The author confirms sole responsibility for the following: study conception and design, data collection, analysis and interpretation of results, and manuscript preparation.

## Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Acknowledgements

I would like to thank Robert Krimmer for his exceptional support with this article. I would further like to thank Vincent Homburg, Arnis Parsovs and Mihkel Solvak and my three anonymous reviewers for their valuable recommendations, which led to substantial improvements of earlier versions of this article. The article benefitted from discussing several iterations of the article from inception to final version in TalTech's Ragnar Nurkse Department's research seminar. I am grateful to SK ID Solutions for providing data, including on eID usage, for the analysis. Further thanks go to my interview partners for their knowledge and reflections on the case. Finally, I would like to thank Heli Tiirmaa-Klaar for general support and providing the organizational context that allowed me to write this article. The EU's Erasmus staff mobility funding was greatly accepted for a research stay in Estonia. The research for this paper was partly supported by the ECePS ERA Chair grant No 857622.

## Appendix A. Supplementary data

The Annex, which structures and evaluates the case data along the categories mentioned in the article in the form of Tables can be found online at https://doi.org/10.1016/j.giq.2022.101781.

## References

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity, 4*(1), 1–15. https://doi.org/10.1093/cybsec/tyy006

Andrade, R. O., Guun Yoo, S., Tello-Oquendo, L., & Ortiz-Garcés, I. (2021). Cybersecurity, sustainability, and resilience capabilities of a smart city. In A. Vizvizi, & R. Perez del Hoyo (Eds.), *Smart cities and the UN's SDG's* (pp. 181–193). Walthum: Elsevier.

Austin, G. (2020). *National cyber emergencies: The return to civil defence*. Abingdon, Oxon; New York: Routledge.

Backman, S. (2021). Conceptualizing cyber crises. *Journal of Contingencies and Crisis Management, 29*, 429–438.

Baggott, S. S., & Santos, J. R. (2020). A risk analysis framework for cyber security and critical infrastructure protection of the US electric power grid. *Risk Analysis, 40*(9), 1744–1761. https://doi.org/10.1111/risa.13511

Bahuguna, A., Bisht, R. K., & Pande, J. (2019). Don't wanna cry: A cyber crisis table top exercise for assessing the preparedness against eminent threats. *International Journal of Engineering and Advanced Technology, 9*(1), 3705–3710. https://doi.org/10.35940/ijeat.A9893.109119

Beduschi, A. (2021). Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations. *Data & Policy, 3*, Article e15. https://doi.org/10.1017/dap.2021.15

Berg, B., & Kuipers, S. L. (2022). Vulnerabilities and cyberspace: A new kind of crisis. In *Oxford Research Encyclopedia Of Politics. Oxford*.

Bernstein, D. J., & Lange, T. (2017). Reconstructing ROCA. Retrieved 30.07.2020, from https://blog.cr.yp.to/20171105-infineon.html.

Boeke, S. (2018). National cyber crisis management: Different European approaches. *Governance-an International Journal of Policy Administration and Institutions, 31*(3), 449–464. https://doi.org/10.1111/gove.12309

Boin, A., Busuioc, M., & Groenleer, M. (2014). Building European Union capacity to manage transboundary crises: Network or lead-agency model? *Regulation & Governance, 8*, 418–436.

Boin, A., & Bynander, F. (2015). Explaining success and failure in crisis coordination. *Geografiska Annaler: Series A, Physical Geography, 97*, 123–135. https://doi.org/10.1111/geoa.12072

Boin, A., Comfort, L. K., & Demchak, C. C. (2010). The rise of resilience. In L. K. Comfort, A. Boin, & C. C. Demchak (Eds.), *Designing resilience: Preparing for extreme events*. Pittsburgh, PA: University of Pittsburgh Press.

Boin, A., Hart, P., Stern, E., & Sundelius, B. (2016). *The politics of crisis management: Public leadership under pressure*. Cambridge, UK ; New York: Cambridge University Press.

Boin, A., & Lodge, M. (2016). Designing resilient institutions for transboundary crisis management: A time for public administration. *Public Administration, 94*(2), 289–298.

Boin, A., & van Eeten, M. J. G. (2013). The resilient organization. *Public Management Review, 15*(3), 429–445.

de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly, 34*(1), 1–7.

van Bueren, E., Klijn, E. H., & Koppenjan, J. F. M. (2003). Dealing with wicked problems in networks: Analyzing an environmental debate from a network perspective. *Journal of Public Administration Research and Theory, 13*(2), 193–212.

Caldarulo, M., Welch, E. W., & Feeney, M. K. (2022). Determinants of cyber-incidents among small and medium US cities. *Government Information Quarterly, 101703*. https://doi.org/10.1016/j.giq.2022.101703

Christensen, T., Lægreid, P., & Rykkja, L. H. (2016). Organizing for crisis management: Building governance capacity and legitimacy. *Public Administration Review, 76*(6), 887–897.

Collier, J. (2017). Strategies of cyber crisis management: Lessons from the approaches of Estonia and the United Kingdom. *Ethics and Policies for Cyber Operations: A Nato Cooperative Cyber Defence Centre of Excellence Initiative, 124*, 187–212. https://doi.org/10.1007/978-3-319-45300-2_11

Corbett, Jack, Grube, Dennis C., Lovell, Heather, & James Scott, Rodney (2020). *Institutional Memory as Storytelling - How Networked Government Remembers*. Cambridge, UK ; New York: Cambridge University Press.

CSIS. (2020). Significant Cyber Incidents. Retrieved 10.03.2021, from Strategic Technologies Program https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.

DESI. (2021). Digital Economy and Society Index Report 2021 — Digital Public Services. Retrieved 14.04.2022, from https://ec.europa.eu/newsroom/dae/redirection/document/80553.

Deverell, E. (2010). *Crisis-induced learning in public sector organizations. (DPhil)*. Utrecht University, Elanders Svergie (Retrieved).

Drechsler, W. (2018). Pathfinder: E-Estonia and the β-version. *JeDEM e-journal of Democracy*, 1–22.

Dubois, A., & Gadde, L. E. (2002). Systematic combining: An abductive approach to case research. *Journal of Business Research, 55*(7), 553–560. https://doi.org/10.1016/S0148-2963(00)00195-8

Dunn Cavelty, M. (2005). The socio-political dimensions of critical information infrastructure protection. *International Journal of Critical Infrastructures, 1*(2/3), 258–268.

Dunn Cavelty, M. (2018). Cybersecurity research meets science and technology studies. *Politics and Governance, 6*(2). https://doi.org/10.17645/pag.v6i2.1385

Easton, D. (1965). *A Systems Analysis of Political Life*. New York: Wiley.

Eggers, S., & Le Blanc, K. (2021). Survey of cyber risk analysis techniques for use in the nuclear industry. *Progress in Nuclear Energy, 140*, 1–17. https://doi.org/10.1016/j.pnucene.2021.103908

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review, 14*(4), 532–550.

ENISA. (2017). Incident report ID 163484 Austria. Retrieved January 25, 2020, from https://cybersec.ee/storage/Incident-report-ID-163484-Austria.pdf.

European Commission. (2022). Keynote speech by Vice-President Schinas at the Munich Cyber Security Conference (MCSC) 2022 [Press release]. Retrieved 14.04.2022, from https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_1163.

Faraj, S., & Xiao, Y. (2006). Coordination in fast-response organizations. *Management Science, 52*, 1155–1169.

Galunic, D. C., & Eisenhardt, K. M. (2001). Architectural innovation and modular corporate forms. *The Academy of Management Journal, 44*(6), 1229–1249. https://doi.org/10.2307/3069398

Garn, B., Kieseberg, K., Schreiber, D., & Simos, D. E. (2021). *Cyber crises and disaster preparation in Austria: A survey of research projects* (pp. 109–121). Springer International Publishing.

Gedris, K., Bowman, K., Neupane, A., Hughes, A., Bonsignore, E., West, R., … Hansen, D. (2021). Simulating municipal cybersecurity incidents: Recommendations from expert interviews. In *Paper presented at the proceedings of the 54th Hawaii international conference on system sciences (HICSS-54), Maui, HI, USA*.

George, A. L., & Bennett, A. (2005). *Case studies and theory development in the social sciences*. Cambridge, Mass.: MIT Press.

Gerring, J., & Cojocaru, L. (2016). Selecting cases for intensive analysis: A diversity of goals and methods. *Sociological Methods & Research, 45*(3), 392–423.

Goodin, D. (2017). Millions of high-security crypto keys crippled by newly discovered flaw. *Ars technica*. Retrieved 26.11.2020, from https://arstechnica.com/information-technology/2017/10/crypto-failure-cripples-millions-of-high-security-keys-750k-estonian-ids/.

Goodsell, C. T. (2011). Mission mystique: Strength at the institutional center. *The American Review of Public Administration, 41*(5), 475–494.

Greenberg, A. (2019). *Sandworm : A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers* (1st ed.). New York: Doubleday.

Groenendaal, J., & Helsloot, I. (2020). Organisational resilience: Shifting from planning-driven business continuity management to anticipated improvisation. *Journal of Business Continuity & Emergency Planning, 14*(2), 102–109.

Groenendaal, Jelle, & Helsloot, Ira (2021). Cyber Resilience during the COVID-19 Pandemic Crisis: A Case Study. *Journal of Contingencies and Crisis Management, 29*(4), 439–444. https://doi.org/10.1111/1468-5973.12360

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly, 53*(4), 1155–1175.

Hardt, H. (2017). How NATO remembers: Explaining institutional memory in NATO crisis management. *European Security, 26*(1), 120–148. https://doi.org/10.1080/09662839.2016.1263944

Helsloot, I., & Groenendaal, J. (2017). It's meaning making, stupid! Success of public leadership during flash crises. *Journal of Contingencies and Crisis Management, 25*(4), 350–353. https://doi.org/10.1111/1468-5973.12166

Irvine, C. E. (2005). Cybersecurity considerations for information systems. In G. D. Garson (Ed.) (2nd ed.,*, Vol. 111. Public administration and public policy: A comprehensive publication program* (pp. 203–218). Boca Raton: Taylor & Francis.

ISO/IEC 27005. (2011). *Information technology — Security techniques — Information security risk management. In (Vol. ISO/IEC 27005:2011)*.

ITU. (2021). Global Cybersecurity Index 2020. Retrieved 17.09.2022, from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

Janssen, M., & van der Voort, H. (2016). Adaptive governance: Towards a stable, accountable and responsive government. *Government Information Quarterly, 33*(1), 1–5. https://doi.org/10.1016/j.giq.2016.02.003

Kalvet, T. (2007). *The Estonian information society development since the 1990s. PRAXIS Working Paper(29)*.

Kattel, R., & Mergel, I. (2019). Estonia's digital transformation: Mission mystique and the hiding hand. In M. E. Compton, & P. Hart (Eds.), *Great policy successes* (pp. 143–160). Oxford: Oxford University Press.

Kitsing, M. (2011). Success without strategy: E-government development in Estonia. *Policy & Internet, 3*(1), 1–21.

Kjærgaard Christensen, K., & Liebetrau, T. (2019). A new role for 'the public'? Exploring cyber security controversies in the case of WannaCry, intelligence and national security. *Intelligence and National Security, 34*(3), 395–408. https://doi.org/10.1080/02684527.2019.1553704

Klijn, E. H., & Koppenjan, J. (2016). *Governance networks in the public sector*. Abingdon, Oxon New York, NY: Routledge.

Kohler, K. (2020). Estonia's National Cybersecurity and Cyberdefense posture. In *Cyberdefense report* (p. 22). Zurich, Switzerland: Center for Security Studies (CSS), ETH Zürich.

Koning, E. A. (2015). The three institutionalisms and institutional dynamics: Understanding endogenous and exogenous change. *Journal of Public Policy, 36*(4), 639–664.

Krimmer, R., Triessnig, S., & Volkamer, M. (2007). The development of remote E-voting around the world: A review of roads and directions. In A. Alkassar, & M. Volkamer (Eds.)*, Vol. 4896. Proceedings of the 1st international conference on E-voting and identity (VoteID 2007)* (pp. 1–15). Springer.

Kuipers, S., & Welsh, N. H. (2017). Taxonomy of the crisis and disaster literature: Themes and types in 34 years of research. *Risk, Hazards & Crisis in Public Policy, 8*(4), 272–283.

Kund, O. (2017). ID-card tip from Czech scientists. *Postimees*. Retrieved 02.03.2021, from https://news.postimees.ee/4236857/id-card-tip-from-czech-scientists.

Lægreid, P., & Rykkja, L. H. (2015). Organizing for "wicked problems" – Analyzing coordination arrangements in two policy areas. *International Journal of Public Sector Management, 28*(6), 475–493. https://doi.org/10.1108/IJPSM-01-2015-0009

Lagadec, P. (2009). A new cosmology of risks and crises: Time for a radical shift in paradigm and practice. *Review of Policy Research, 26*(4), 473–486.

Landler, M., & Markoff, J. (2007). Digital fears emerge after data siege in Estonia. *The New York Times*. Retrieved 30.05.2020, from https://www.nytimes.com/2007/05/29/technology/29estonia.html.

Lanzendorfer, Q. E. (2020). Information sharing challenges in government cybersecurity organizations. *International Journal of Cyber Research and Education (IJCRE), 2*(1), 32–39. https://doi.org/10.4018/IJCRE.2020010103

Lehto, M., & Limnéll, J. (2020). Strategic leadership in cyber security, case Finland. *Information Security Journal: A Global Perspective, 1-10*. https://doi.org/10.1080/19393555.2020.1813851

Lesk, M. (2007). The new front line: Estonia under cyberassault. Security & Privacy. *IEEE, 5*(4), 76–79 (Paper presented at the Security & Privacy).

Lips, S., Pappel, I., Tsap, V., & Draheim, D. (2018). Key factors in coping with large-scale security vulnerabilities in the eID field. In *Paper presented at the electronic government and the information systems perspective. EGOVIS 2018*.

Luna-Reyes, L. F., & Gil-Garcia, J. R. (2003). E-Government Security, Privacy and Information Access: Some Policy and Organizational Trade-offs (M. I. o. T. a. t. R. C. o. I. T. a. P. Democracy, Trans.). In *International Conference on Public Participation and Information Technologies 2003 (ICPPIT03)* (pp. 1–4) (Cambridge, MA).

Lune, H., & Berg, B. L. (2017). *Qualitative research methods for the social sciences* (9th ed.). Essex: Pearson.

March, J., & Olsen, J. (1984). The new institutionalism: organizational factors in political life. *American Political Science Review, 78*, 734–749.

Martens, T. (2010). Electronic identity management in Estonia between market and state governance. *Identity in the Information Society, 3*(1), 213–233.

McConnell, A. (2011). Success? Failure? Something in-between? A framework for evaluating crisis management. *Policy and Society, 30*(2), 63–76.

van der Meulen, N. (2013). DigiNotar: Dissecting the first Dutch digital disaster. *Journal of Strategic Security, 6*(2), 46–58. https://doi.org/10.5038/1944-0472.6.2.4

Meyer, D. (2017). ID card security: Spain is facing chaos over chip crypto flaws. *ZDnet*. Retrieved 01.03.2020, from https://www.zdnet.com/article/id-card-security-spain-is-facing-chaos-over-chip-crypto-flaws/.

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). Los Angeles, London, New Delhi, Singapore, Washington DC: SAGE Publications.

Ministry of the Interior of the Slovak Republic. (2017). It will temporarily not be possible to use a qualified electronic signature on an ID card for electronic signing (Translated) [Press release]. Retrieved 22.10.2022, from https://www.minv.sk/?tlacove-spravy&sprava=na-elektronicke-podpisovanie-docasne-nebude-mozne-vyuzit-kvalifikovany-elektronicky-podpis-na-obcianskom-preukaze.

Nemec, M., Sys, M., Svenda, P., Klinec, D., & Matyas, V. (2017). The return of Coppersmith's attack: Practical factorization of widely used RSA moduli. In *Paper presented at the ACM CCS 17 proceedings, Dallas, Texas, United States*.

NIST. (2012). *SP 800-30: Guide for conducting risk assessments, Rev. 1*. National Institute of Standards and Technology, U.S. Department of Commerce.

Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2019). Cyberattacks at the grass roots: American local governments and the need for high levels of cybersecurity. *Public Administration Review, 79*(6), 895–904. https://doi.org/10.1111/puar.13028

Østby, G., & Katt, B. (2020). Cyber crisis management roles – A municipality responsibility case study. In *Paper presented at the IFIP Advances in Information and Communication Technology. Conference Paper*. retrieved from https://www.scopus.

com/inward/record.uri?eid=2-s2.0-85086252395&doi=10.1007%2f978-3-030-48939-7_15&partnerID=40&md5=7a739bd203219acb1c4e38d9623dc3fc.

Østby, G., & Kowalski, S. J. (2020). Preparing for cyber crisis management exercises. In *, Vol. 12197. Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)* (pp. 279–290). LNAI.

Ostrom, E. (1986). A method for institutional analysis. In F. X. Kaufmann, G. Majone, & V. Ostrom (Eds.), *Guidance, Control and Evaluation in the Public Sector: The Bielefeld Interdisciplinary Project* (pp. 459–479). Berlin: Walter de Gruyter.

Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. In *Proceedings of the 7th European conference on information warfare and security, Plymouth* (pp. 163–168).

Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *International Journal of Information Management, 55*, Article 102171. https://doi.org/10.1016/j.ijinfomgt.2020.102171

Parsovs, A. (2020). Solving the Estonian ID card crisis: The legal issues. In *Paper presented at the proceedings of the 17th ISCRAM conference*. VA, USA: Blacksburg.

Parsovs, A. (2021). *Estonian electronic identity card and its security challenges. (Doctor of Philosophy)*. University of Tartu. Retrieved 01.07.2021, from https://dspace.ut.ee/handle/10062/71481.

Pau, A. (2018). Cyber-lollygagging cost the state millions. *Postimees*. Retrieved 12.06.2021, from https://news.postimees.ee/6383968/cyber-lollygagging-cost-the-state-millions.

Pearson, C. M., & Clair, J. A. (1998). Reframing crisis management. *Academy of Management Review*, 59–76.

Perrow, C. (1999). *Normal accidents: Living with high-risk technologies*. New York: Basic Books.

Pike, R. (2021). Enhancing cybersecurity capability in local governments through competency-based education. In *Paper presented at the proceedings of the 54th Hawaii international conference on system sciences (HICSS-54), Kauai, Hawaii*.

G7 Presidency. (2022). Joint declaration by the G7 digital ministers on cyber resilience of digital infrastructure in response to the Russian war against Ukraine Accessed today, 07.12.2022, Retrieved, from https://bmdv.bund.de/SharedDocs/DE/Anlage/K/g7-praesidentschaft-joint-declaration.pdf?_blob=publicationFile.

Prevezianou, M. F. (2021). Beyond ones and Zeros: Conceptualizing cyber crises. *Risk, Hazards & Crisis in Public Policy, 12*(1), 51–72. https://doi.org/10.1002/rhc3.12204

Raag, I. (2018). *The will of the people is upheld. 3 briefings & 2 lessons on the ID card saga*. EDASI.org (Retrieved).

Randma, T. (2001). A small civil service in transition: The case of Estonia. *Public Administration and Development, 21*(1), 41–51.

Republic of Estonia. (2018). Notification form for Electronic Identity Scheme under Article 9 (5) of Regulation (EU) No. 910/2014. Retrieved 01.10.2020, from https://ec.europa.eu/cefdigital/wiki/download/attachments/62885749/EE%20eID%20LoA%20mapping%20-%20ID%20card.pdf.

RIA. (2017). *Annual Cybersecurity Assessment. 2017*.

RIA. (2018). ROCA Vulnerability and eID: Lessons Learned. Retrieved 10.05.2021, from https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf.

RIA. (2022). *Means of eID | Estonian information system authority*. Means of eID.

Rid, T. (2013). *Cyber war will not take place*. Oxford: Oxford University Press.

Romaniuk, S. N., & Manjikian, M. (Eds.). (2020). *Routledge companion to global cyber-security strategy*. New York: Routledge.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

Roux-Dufort, C. (2007). Is crisis management (only) a Management of Exceptions? *Journal of Contingencies and Crisis Management, 15*(2), 105–114.

Ruohonen, J., Hyrynsalmi, S., & Leppänen, V. (2016). An outlook on the institutional evolution of the European Union cyber security apparatus. *Government Information Quarterly, 33*(4), 746–756. https://doi.org/10.1016/j.giq.2016.10.003

Saldaña, J. (2013). *The coding manual for qualitative researchers* (2nd ed.). London, Thousand Oaks, New Delhi, Singapore: SAGE Publications.

Scharpf, F. W. (1999). *Governing in Europe: Effective and democratic?* Oxford: Oxford University Press.

Schmidt, V. A. (2013). Democracy and legitimacy in the European Union revisited: Input, output, and throughput. *Political Studies, 61*(1), 2–22.

Schmitt, M. (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations* (2 ed.). Cambridge: Cambridge University Press.

Schneier, B. (2018). *Click here to kill everybody : Security and survival in a hyper-connected world* (1st ed.). New York ; London: W.W. Norton & Company.

Schofield, J. W. (2011). Increasing the generalizability of qualitative research. In A. M. Huberman, & M. B. Miles (Eds.), *The qualitative Researcher's companion* (pp. 171–203). Thousand Oaks: SAGE Publications.

Schrijvers, E., Prins, C., & Passchier, R. (2021). *Preparing for digital disruption*. Springer Cham.

Simola, J., & Lehto, M. (2020). National cyber threat prevention mechanism as a part of the E-EWS. In *Paper presented at the ICCWS 2020*.

Simon, S., & De Goede, M. (2015). Cybersecurity, bureaucratic vitalism and European emergency. *Theory, Culture & Society, 32*(2), 79–106. https://doi.org/10.1177/0263276414560415

SK ID Solutions. (2018). History - 2017. Retrieved 30.10.2020, from https://www.skidsolutions.eu/en/about/history/year-2017/.

SK ID Solutions. (2019). The Information System Authority will adopt Smart-ID for state services [Press release]. Retrieved 15.01.2022, from https://www.skidsolutions.eu/en/News/the-information-system-authority-will-adopt-smart-id-for-state-services.

Smeets, M. (2022). The role of military cyber exercises: A case study of locked shields. In *Paper presented at the 2022 14th international conference on cyber conflict: Keep moving! (CyCon)*.

Solvak, M., Unt, T., Rozgonjuk, D., Võrk, A., Veskimäe, M., & Vassil, K. (2019). E-governance diffusion: Population level e-service adoption rates and usage patterns. *Telematics and Informatics, 36*, 39–54. https://doi.org/10.1016/j.tele.2018.11.005

Stark, A. (2010). Legislatures, legitimacy and crises: The relationship between representation and crisis management. *Journal of Contingencies and Crisis Management, 18*(1), 2–13.

Strupczewski, G. (2021). Defining cyber risk. *Safety Science, 135*, 1–10. https://doi.org/10.1016/j.ssci.2020.105143

Tehnikaülikool, T. (2018). ID-kaardi kaasuse õppetunnid. Retrieved 25.11.2019, from https://www.ria.ee/sites/default/files/content-editors/EID/id-kaardi_oppetunnid.pdf.

The Slovak Spectator. (2017). E-ID cards have serious problem. *The Slovak Spectator*. Retrieved 15.04.2021, from https://spectator.sme.sk/c/20674746/e-id-cards-have-serious-problem.html.

United Nations. (2020). *UN E-Government Survey 2020*. Retrieved on 14.04.2022 from https://publicadministration.un.org/egovkb/en-us/Data-Center.

United Nations. (2022). *UN E-Government Survey 2022*. Retrieved on 14.04.2022 from https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2022.

US Forum on Cyber Resilience. (2021). In F. Schneider (Ed.), *Winter 2021–meeting of the forum on cyber resilience: Resilient public Services in the U.S. – Lessons and insights from Estonia. Time machine or alternate universe?*. The National Academies of Sciences, Engineering, Medicine.

Vahtla, A. (2017a). *EKRE challenges electoral committee's decision to allow e-voting. ERR News*. Retrieved 02.03.2020, from https://news.err.ee/617916/ekre-challenges-electoral-committee-s-decision-to-allow-e-voting.

Valtna-Dvořák, A., Lips, S., Tsap, V., Ottis, R., Priisalu, J., & Draheim, D. (2021). *Vulnerability of state-provided electronic identification: The case of ROCA in Estonia. Paper presented at the 10th international conference, EGOVIS 2021*.

Ventsel, A., & Madisson, M.-L. (2019). Semiotics of threats: Discourse on the vulnerability of the Estonian identity card. *Sign Systems Studies, 47*(1/2), 126–151. https://doi.org/10.12697/SSS.2019.47.1-2.05

Viet, H. L., Van, O. P., & Ngoc, H. N. (2020). Information security risk management by a holistic approach: A case study for Vietnamese e-government. *International Journal of Computer Science and Network Security, 20*(6), 72–82.

White, G. B. (2012). A grassroots cyber security program to protect the nation. In *Paper presented at the proceedings of the 45th Hawaii international conference on system sciences (HICSS-45), Maui, HI, USA*.

Williams, T. A., Gruber, D. A., Sutcliffe, K. M., Shepherd, D. A., & Zhao, E. Y. (2017). Organizational response to adversity: Fusing crisis management and resilience research streams. *Academy of Management Annals, 11*(2), 733–769. https://doi.org/10.5465/annals.2015.0134

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Thousand Oaks, California: SAGE Publications.

Zetter, K. (2014). *Countdown to zero day : Stuxnet and the launch of the world's first digital weapon* (1st ed.). New York: Crown Publishers.

Zhang, H., Tang, Z., & Jayakar, K. (2018). A socio-technical analysis of China's cybersecurity policy: Towards delivering trusted e-government services. *Telecommunications Policy, 42*(5), 409–420. https://doi.org/10.1016/j.telpol.2018.02.004

Zhao, J. J., Zhao, Y., & S.. (2010). Opportunities and threats: A security assessment of state e-government websites. *Government Information Quarterly, 27*(1), 49–56.

Isabel Skierka is a program lead for technology politics and a researcher with the Digital Society Institute at ESMT Berlin. She is finalizing her PhD at the Ragnar Nurkse School of Innovation and Governance at Tallinn University of Technology in Estonia. Previously she was a research associate with the Global Public Policy Institute (GPPi) in Berlin, a Carlo Schmid Fellow at NATO, a Bluebook Trainee at the European Commission's DG Connect, and a visiting researcher at the Institute of Computer Science of the Free University of Berlin. Isabel holds an MA from the War Studies Department of King's College London and a BA in European studies from Maastricht University.

# ANNEX

## 1. List of Interviewees

***Table 1***: *List of interviewees*

| Interviewee position | Interview date(s) | Involved in crisis process |
|---|---|---|
| Former RIA official | May 2018 &<br>September 2022 | No |
| Former MEAC government official | August 2018 | No |
| Former RIA official | February 2019 | Yes |
| Government official | February 2019 | Yes |
| Former RIA official | May 2019 | Yes |
| RIA official | May 2019 | Yes |
| Former RIA leading official | February 2019 | No |
| Former PBGB official | October 2019 | Yes |
| Former RIA official | November 2020 | Yes |
| Former PBGB official | March 2021 | Yes |
| Former Estonian cyber diplomat | March 2022 | No |
| Communications expert | February 2019 | Yes |
| Decision-maker at SK ID solutions | May 2018 &<br>September 2022 | Yes |
| Former Gemalto representative | May 2018 | Yes |
| Expert at Estonian cybersecurity firm | May 2018 &<br>September 2022 | Yes |
| Cybersecurity researcher | February 2019 | No |
| eID expert | February 2019 | No |
| Expert at Estonian cybersecurity firm | February 2019 | Yes |
| Legal expert | February 2019 | Yes |
| University researcher and government consultant, Austria | February 2019 | No |
| ENISA official | September 2019 | No |
| Cybersecurity researcher, Czech Republic | October 2019 | Yes |

## 2. Actors, roles and resources

Within Estonia's governance networks, a variety of autonomous yet interdependent **actors** are involved in different **roles** in the crisis management process, which Table 2 illustrates. Through their actions and strategies, they influence the course and outcomes of social interaction processes. We distinguish between core actors of Estonia's eIDMS and other actors. The division of **resources** among actors makes them dependent upon one another. In our case, we pay particular attention to *competencies* in terms of the formal or juridical authority to take decisions, *IT competence* both in terms of expertise and skills, and the capacity to give or withhold *political legitimacy* to the crisis management process.

***Table 2:*** *Actors, their roles, and their resources in the Estonian ROCA crisis management process*

| **Key actor (selection)** | **Role** | **Resources** |
|---|---|---|
| **eIDMS actors** | | |
| RIA (public) – A.1 | Civilian cybersecurity authority, houses CERT-EE, maintains public IT systems and the eID software. Overseen by the MKM. | - *Competencies*: formal authority for civilian cybersecurity and eID software.<br>- *IT competence*: very strong IT, eID expertise and skills. |
| PPA (public) – A.2 | Issues eID card, responsible for applications, revocations of eID card and suspension, revocation or updating of certificates.<br>Exception: diplomatic ID card, which is issued by the Ministry of Foreign Affairs.<br>Overseen by the Ministry of Interior. The IT Development Centre (SMIT) is responsible for providing IT support in ID card related activities to the PPA. | - *Competencies*: formal authority to issue, revoke ID cards and suspend, revoke or update certificates.<br>- *IT competence*: average IT expertise and skills. |

| | | |
|---|---|---|
| SK ID Solutions (private) – A.3 | Trust service provider. eID scheme’s certificate authority and administrator of the PKI. Issues certificates for national ID documents and is responsible for maintaining them throughout their lifecycle, covering their creation, activation, suspension, and revocation.<br>As a subcontractor of SK, mobile operators deliver SIM cards with Mobile-ID functionality. | - *Competencies*: formal authority to manage Estonia’s PKI, as a contractor to PBGB.<br>- *IT competence*: very strong IT, eID expertise and skills. |
| Gemalto (in form of TRÜB Baltic AS, which was the subsidiary in Estonia) (private) – A.4 | eID card manufacturer from 2002 until 2018 as a subcontractor of the PPA. Supplied the smart card and personalized it (through subcontractor). Issued ID certificates under a contract with SK. Infineon Technology AG supplied the eID card's chip. | - *IT competence*: very strong eID expertise and skills. |
| **Other actors in crisis process** | | |
| Estonian government leadership / Prime Minister (public) – A.5 | The government leadership active in the crisis management process comprises actors with executive functions, including the Prime Minister and his Office. | - *Competencies*: strong formal authority to take decisions.<br>- *IT competence*: ‘average Estonian end user’ literacy<br>- *Political legitimacy*: strong capacity to give or withhold legitimacy to the crisis management process. |
| Legal and technical experts in the crisis working groups (public / private / academic) – A.6 | The crisis working groups comprised between 10 and 20 experts each at its core. Experts were public officials from RIA, other participating agencies, experts from private firms like SK, Cybernetica, from NATO CCDCoE, and from academia. | - *IT competence*: very strong IT expertise and skills (some members). |
| University research team (academic) – A.7 | The research team from Masaryk University discovered ROCA and provided scientific knowledge (Nemec, Sys, Svenda, Klinec, & Matyas, 2017). | - *IT competence*: very strong IT expertise and skills. |
| Opposition party (Conservative People’s Party EKRE) (public) – A.8 | At the time of the crisis, EKRE was in the opposition. It was part of the Estonian government only after the ROCA crisis from March 2019 to February 2021. EKRE had a sceptical position toward online voting. | - *Political legitimacy*: limited capacity to give or withhold legitimacy to the crisis management processes. |
| eID end users – A.9 | Comprises all eID card users in Estonia and abroad who use their cards to access and execute online services. | - *Political legitimacy*: strong capacity to give or withhold legitimacy to the crisis management processes. |

## 3. Arenas, issues, and tiers of risk management

The interactions during the crisis management process took place in six **arenas** illustrated in Table 3: the *political strategic crisis management arena*, which comprises political and strategic discussions and interactions, the *operational crisis management arena*, which comprises operational discussions and interactions, the *eID management arena*, which comprises eIDMS management issues, the *eID end user arena*, which comprises issues and interactions relevant for eID end users, the *IT security arena*, which comprises technical IT security issues, and the *EU arena*, which comprises political and operational interactions and discussions among EU partners. In each arena, actors discuss different, often overlapping, **issues**. The arenas can be further clustered into three different **tiers** of risk management. Following the NIST risk management framework, we distinguish between the *strategic* risk management level at Tier 1, the *operational* process risk management level at Tier 2, and the *technical* information systems level at Tier 3 (NIST, 2012, p. 9). Some arenas run across different tiers.

***Table 3:*** *Arenas in the Estonian ROCA crisis management process*

| **Arena** | **AR1: Political strategic crisis management (CM) arena** | **AR2: Operational crisis management (CM) arena** | **AR3: eID management arena** | **AR4: eID end user arena** | **AR5: IT security arena** | **AR6: EU arena** |
|---|---|---|---|---|---|---|
| **Actors** | A.5 Government leadership (Prime Minister, RIA Director, PPA Director)<br>A.8 Political opposition party, and Media | A.6 Technical, legal and communications experts in crisis WGs | A.1-A.4 eIDMS network actors | A.5 Government leadership, A.9 eID card users, and Media | A.1 RIA, A.3 SK, A.4 Gemalto, A.7 Masaryk University research team, and cybersecurity firm Cybernetica | ENISA, EU member states' technical competent authorities and CERTs |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Issues** | I.1: Opportunity cost of pre-emptive eID shut-down v. continuity of eID functions<br>I.2: Trust in the eID and the e-state<br>I.3: Dependence on foreign technology suppliers<br>I.4: IT security risk assessment and mitigation | I.5: Operational crisis management coordination<br>I.4: IT security risk assessment and mitigation | I.1: Opportunity cost of pre-emptive eID shut-down v. continuity of eID functions<br>I.3: Dependence on foreign technology suppliers<br>I.4: IT security risk assessment and mitigation | I.2: Trust in the eID and the e-state<br>I.4: IT security risk assessment and mitigation<br>I.6: Integrity of democratic processes | I.4: IT security risk assessment and mitigation<br>I.7: Vulnerability information sharing and analysis<br>I.8: Recognition in the scientific research community | I.4: IT security risk assessment and mitigation<br>I.7: Vulnerability information sharing and analysis |
| **Tier** | Tier 1 (Strategic) | Tier 2 – 3 (Operational – Technical) | Tier 2 (Operational) | Tier 1 (Strategic) | Tier 3 (Technical) | Tier 2 – 3 (Operational – Technical) |
| **Level** | National | National | National | (Largely) national | National & EU | EU |

## 4. Rounds of the crisis management process

Table 4 illustrates the crisis management process' **rounds** and **turning points**. The column "**arenas**" indicates which arenas converged in which rounds. The column "**change in total eID transactions**" sums up transactions with the eID card, Mobile-ID, and Smart-ID during selected rounds. The reconstruction of the rounds, interactions, arenas in Table 4, as well as risk level perceptions and risk responses in Table 7, is based on qualitative data derived from media reports, official documents, interviews with key actors, and sources which have documented the detailed timeline of the crisis (Lips S., Pappel I., Tsap V., & Draheim, 2018, p. 7; Parsovs, 2021; RIA, 2018, p. 1). The numbers of eID transactions in Tables 5 and 6 are based on data provided to the authors by SK. The eID transaction data only represents approximate values and were therefore only used to analyze general trends.

***Table 4**: Rounds in the Estonian ROCA crisis management process*

| | **Actions in rounds** | **Arenas** | **Change in total eID transactions (eID card, Mobile-ID, Smart-ID)** |
|---|---|---|---|
| **Turning point** | ROCA discovery and disclosure to manufacturer in January / February 2017 | | |
| **Round 1: Vulnerability Disclosure Failures** | R1.1: The researchers **discovered ROCA in January 2017**, disclosed it to the manufacturer Infineon under responsible vulnerability disclosure rules in February 2017 (Nemec et al., 2017, p. 16; Švenda, 2018). Their publication of results was planned for 30 October 2017 at the ACM CCS computer science conference.<br>R1.2: **Infineon disclosed ROCA** to customers around May 2017, including Gemalto. However, Gemalto did not formally share the vulnerability information with the PPA or other Estonian government actors (Parsovs, 2021, p. 139; Švenda, 2018).<br>R1.3: In June 2017, **ENISA sent a formal incident notification** concerning vulnerable certificates of an Austrian TSP to all EU member states. Later, it became apparent that the notification had related to the ROCA vulnerability. Yet, due to lacking contextual information and no public information about ROCA at that point in time, the notification remained unnoticed among the large quantities of threat information reaching EU member states, including CERT-EE (Pau, 2018b). | **AR5, AR6**:<br>IT Security, EU | - |
| **Turning point** | ROCA vulnerability disclosure to CERT-EE on 30 August 2017 | | |

| | | | |
|---|---|---|---|
| **Round 2: Estonia’s crisis response organization** | R2.1: On 30 August 2017, the **researchers personally informed CERT-EE about ROCA**. Nearly 800 000 Estonian eID cards were vulnerable.<br>R2.2: ROCA triggered a **political crisis**: it posed a severe *threat* to Estonia’s e-government, its details were still highly *uncertain*, and it created *time pressure* for decision-makers to act. At the time, Estonia held the EU Council Presidency, in which it promoted digitization in Europe and advertised its own e-state’s success, which reinforced the political pressure to avoid reputational and political harm.<br>R2.3: The government assembled a political crisis roundtable of around 100 relevant stakeholders. It then set up **three crisis working groups** (WGs) responsible for (1) crisis management strategy, (2) technical and legal vulnerability management and (3) strategic communications (Lips S. et al., 2018). RIA functioned as the ‘de facto’ eID technical competence center and WG leader. Official Emergency Act procedures were not activated (Tallinna Tehnikaülikool, 2018). | **AR1, AR2, AR3**:<br>Political strategic CM,<br>Operational CM, eID management | - |
| **Turning point** | Press conference on 5 September 2017 | | |

| | | | |
|---|---|---|---|
| **Round 3: Public vulnerability announcement** | R3.1: ROCA could not be kept secret for long. On 5 September 2017, the Prime Minister held an **“emergency” press conference** with the Directors Generals of RIA and the PPA, among others (Raag, 2018 in: Parsovs, 2021, p. 133). Authorities announced the vulnerability of Estonia’s eID but declared that eID cards and access to digital services would remain functional, certificates would not be invalidated. They framed the risk as theoretical, which was “great enough to take it seriously, but not great enough to cancel the cards” (Vahtla, 2017c).<br>R3.2: Despite new details being released with updates from other vendors and testing tools, the government upheld the **continuity of eID services**. According to RIA, this information did not add any additional factors to change the “theoretical” nature of the risk calculation (Parsovs, 2021, p. 133). Regarding the question whether online voting was still secure, an “FAQ” on ROCA published on the ID.ee website on 5 September 2017 (the day of the press conference), states that online voting was “no more at risk than other services. Large-scale vote fraud [was] not conceivable due to the considerable cost and computing power necessary of generating a private key” (RIA, 2017).<br>R3.3.: Estonia, which held the EU Council Presidency, hosted the EU Digital Summit in Tallinn on 29 September 2017, which did, however, not noticeably mention the ROCA crisis. | **AR1, AR2, AR4:**<br>Political strategic CM, eID management, eID end user | Slight increase in total transactions by 5% in September compared to pre-ROCA levels, indicating no loss of trust in eID |
| **Turning point** | Municipal election from 5-11 October 2017 | | |
| **Round 4: Online elections** | R4.1: In light of public information, the **online voting mechanism** planned for Estonian municipal council elections scheduled for 5 to 11 October 2017 was put into question (BNS, 2017). Despite doubts in the government about the right way to deal with the risk of online voting, the National Electoral Committee (NEC) unanimously decided to proceed with online elections, citing the government’s and RIA’s statements that the risk was only theoretical (Kund, 2017).<br>R4.2: The **Supreme Court** rejected a legal appeal from the opposition party EKRE by reasoning that the resources needed to exploit the flaw were too great to pose a real threat to the elections (Vahtla, 2017a). That decision further **legitimized** | **AR1, AR5:**<br>Political strategic CM, IT security | Slight increase in total transactions by 5% in October compared to pre-ROCA levels, indicating no loss of trust in eID usage. During the elections, eID usage remained largely constant. |

| | | | | |
|---|---|---|---|---|
| | | **the NEC's and government's decision to let elections take place**. The elections had a high online voter turnout (31.7 percent of voters), a ten percent increase from that of the 2013 municipal elections and a 1 percent increase from 2015 parliamentary elections (Valimised, 2017). | | |
| **Turning point** | Patch deployment on 25 October 2017 | | | |
| **Round 5: Patch deployment** | R5: | A breakthrough occurred when RIA and the PPA deployed a **technical vulnerability patch** on 25 October 2017. The patch would switch the ID platform's cryptographic algorithm to an alternative NIST-standard elliptic curve cryptography (ECC) algorithm. ECC was not vulnerable to ROCA. Card holders could update their certificates either physically in PPA customer service points or remotely over the internet using software provided by the state. Limited system capacity and resulting crashes delayed the updating process during the first few days (Parsovs, 2021, pp. 136). | **AR2, AR4:**<br>Operational CM, eID end user | Constant level of total transactions between 25 October and 30 October or 3 November.<br>Most users installed the vulnerability update on their cards not right after it became available on 25 October, but on and after 2 November 2017 when certificates were suspended (see Round 6). |

| **Turning point** | Publication of researchers’ paper with ROCA details on 30 October 2017 | | |
|---|---|---|---|
| **Round 6: Emergency suspension of certificates** | R6.1: On 30 October, **the Masaryk University researcher team published their paper** at the ACM CSS conference. Due to the increased risk of vulnerability exploitation resulting from that publication, the Estonian authorities **suspended all remaining eID card certificates** with vulnerable keys on 3 November 2017 (Vahtla, 2017b). The vulnerable certificates became invalid but could still be updated. On 5 November, independent researchers demonstrated the heightened risk of ROCA-flaw exploitation at even 25 percent greater efficiency than initially assumed (Bernstein & Lange, 2017). The state launched large scale media campaigns for the eID card update on billboards, radio programs, and on TV (Parsovs, 2021, pp. 136).<br>R6.2: In mid-November 2017, it emerged that the **PPA had filed a legal claim against its contractor Gemalto** for the Estonian state’s total expenses to mitigate the ROCA vulnerability. It blamed Gemalto for not having informed the Estonian state about the vulnerability earlier in May or June 2017. Gemalto’s representative in Estonia disputed the claim and stated it had indeed informally informed the PPA. Gemalto’s representative was replaced in December 2017, the legal battle continued. In December, the PPA withdrew its letters of recommendation for Gemalto, which the firm had used when applying for tenders (ERR News, 2017; Parsovs, 2021, pp. 138-140; Pau, 2018a, 2018b; Tamm, 2018). | **AR1, AR2, AR5**:<br>Political strategic CM, Operational CM, IT security | Slight decrease in total transactions after certificate suspension in November 2017 and then continued to slightly increase again from December onwards, mirroring the effect of suspension. The number of installed eID software updates significantly increased on and after 2 November. It doubled and, for a few days in early November, tripled. This trend might indicate that the suspension gave card holders a motivation to update their cards. |
| **Turning point** | Authorities revoked certificates of all non-updated eID cards on 1 April 2018 | | |

| | | | |
|---|---|---|---|
| **Round 7: Operational crisis termination** | R7.1: The **crisis operationally ended** on 1 April 2018, when authorities revoked the certificates of all non-updated eID cards. From that day on, non-updated cards could not be updated anymore. A large majority of eID card holders had, by then, installed the patch (ERR News, 2018).<br>R7.2: In the spring of 2018, the Estonian government launched a **post-crisis evaluation** process. RIA commissioned TalTech University to study the eID crisis' lessons learned (Tallinna Tehnikaülikool, 2018) and organized an international conference with participation of ENISA and other EU member state authorities devoted to managing the Estonian eID crisis titled "The Lessons We Learned" held on May 9, 2018 in Tallinn (RIA, 2018). The event and publication discussed organizational crisis management failures but emphasized the overall success of managing the crisis. | **AR1, AR3, AR5, AR6**:<br>Political strategic CM, eID management, IT security, EU | Slight decrease in total transactions compared to previous rounds,<br>The curve of update numbers flattened between December 2017 and March 2018 and showed a last spike in late March right before certificate revocation on 1 April 2018 (Parsovs, 2021, p.137). |
| **Turning point** | Conference Report Publication on 9 May 2018 | | |
| **Round 8: Post-crisis blame games** | R8: The **legal liability dispute** between the PPA and Gemalto ended with a compromise agreement in February 2021, according to which Gemalto paid the Estonian state € 2.2 million in compensation (Wright, 2021). Gemalto's contract expired anyway in late 2018. IDEMA, which had signed a procurement contract already before the ROCA crisis in spring 2017, became the new card manufacturer. The personalization of cards is performed by the Estonian company Hansab AS (Parsovs, 2021, p. 21). | **AR 1**:<br>Political strategic CM | |
| **Turning point** | Settlement of legal liability dispute on 6 February 2021 | | |

## 5. eID transaction shares throughout the crisis process

In addition to the total change in eID transactions in Table 4, Table 5 below shows the development of the transaction share of the three different means of authentication and signature – the eID card, Mobile-ID, and Smart-ID – throughout the crisis process between August 2017 and July 2018. The eID transaction data only represents approximate values and were therefore only used to analyze general trends. The data indicates a growth push for Smart-ID at the expense of eID card usage numbers during the crisis.

Although Mobile-ID provided the same legal certainty as the eID card, users did not seem to have switched to Mobile-ID. One reason might have been that it required users to purchase a new specific SIM card with an Estonian mobile operator, which requires effort and financial expenses. In comparison, Smart-ID was easy-to-use and cheap.

***Table 5**: Transaction share of total transactions of the eID card, Mobile-ID, and Smart-ID between August 2017 and July 2018 (Source: SK ID Solutions)*

| **Month** | **Share in transactions** | | |
|---|---|---|---|
| | ***eID card*** | ***Mobile-ID*** | ***Smart-ID*** |
| Aug 17 | 71% | 22% | 7% |
| Sep 17 | 71% | 22% | 7% |
| Okt 17 | 69% | 23% | 8% |
| Nov 17 | 66% | 24% | 10% |
| Dez 17 | 65% | 24% | 11% |
| Jan 18 | 64% | 24% | 12% |
| Feb 18 | 63% | 24% | 13% |
| Mar 18 | 63% | 23% | 14% |
| Apr 18 | 62% | 23% | 15% |
| Mai 18 | 61% | 24% | 16% |
| Jun 18 | 60% | 23% | 17% |
| Jul 18 | 58% | 23% | 19% |

## 6. Actors' risk assessment and risk response strategies

Table 7 details the **risk assessment, risk level perceptions and risk responses** of key decision-makers. It illustrates how Estonian decision-makers among the key actors from Table 3 might have assessed the risk in each round, and how they responded to that risk.

Our analysis follows the NIST cyber risk framework (see NIST, 2012, Appendixes D-H). As illustrated by Figure 3, it combines:

- Threat (T), which can be divided into threat sources (assessed in terms of their capability and intent), and threat events such as adversarial cyber or physical attacks, or non-adversarial events.
- Vulnerability (V), which, in our study, is a weakness in an IT system, which can be exploited by an adversarial threat source. V is assessed in terms of its severity, including its exposure and ease of exploitation and/or severity of impacts that could result from its exploitation.
- Likelihood (L) of threat event initiation and of the threat event resulting in adverse impacts
- Impact (I) of the threat event on organizations, individuals, and the Estonian nation. Harm can occur in both material forms, such as loss of physical or financial assets, and immaterial forms, such as harm to reputation or legitimacy.

The determination of risk levels further depends on an entity's general attitude toward risk, including overall risk tolerance and tolerance for uncertainty and its weighting of risk factors, among others (NIST, 2012, p.34). The determination of risk factors is detailed in Table 6 from NIST (2012).

***Figure 3**: "Cyber Risk Assessment Factors modelled after NIST SP 800-30 Generic Risk Model with Key Factors"*

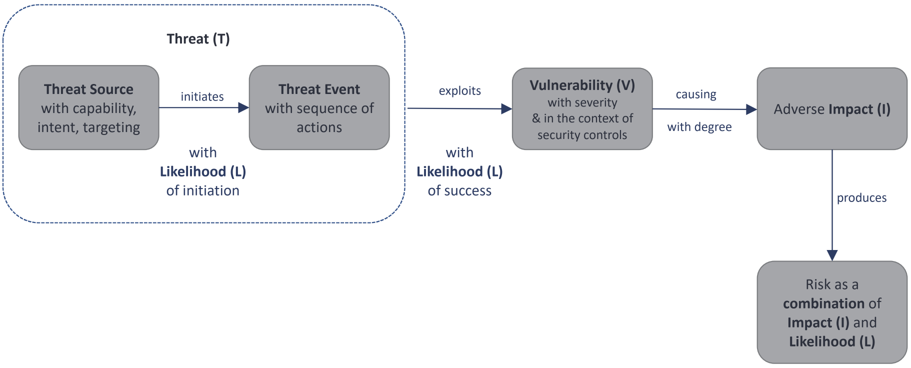

Threat (T)
Threat Source with capability, intent, targeting
initiates
Threat Event with sequence of actions
with Likelihood (L) of initiation
exploits
with Likelihood (L) of success
Vulnerability (V) with severity & in the context of security controls
causing
with degree
Adverse Impact (I)
produces
Risk as a combination of Impact (I) and Likelihood (L)

***Table 6:** "Cyber Risk Assessment Scale" (NIST, 2012, p. I-1)*

| **Likelihood** (Threat event occurs and results in adverse impact) | **Level of Impact** | | | | |
|---|---|---|---|---|---|
| | **Very Low** | **Low** | **Moderate** | **High** | **Very High** |
| **Very High** | Very Low | Low | Moderate | High | Very High |
| **High** | Very Low | Low | Moderate | High | Very High |
| **Moderate** | Very Low | Low | Moderate | Moderate | High |
| **Low** | Very Low | Low | Low | Low | Moderate |
| **Very Low** | Very Low | Very Low | Very Low | Low | Low |

In the ROCA crisis, vulnerability (V) severity varied in terms of its exposure and ease of exploitation, depending on how much information was publicly accessible and which security controls, like the update, were in place. Potential threats (T) were less specifically identifiable. Theoretically, a range of possible adversarial threat sources with a variety in levels of capability and intent existed (see NIST, 2012, p. D-3).

***Table 7:*** *Key decision-makers' risk level perceptions and risk response strategies per round*

| **Rounds** | **Key decision-makers** | **Perceived risk level of ROCA** | | **Risk management strategy** |
|---|---|---|---|---|
| **Turning point** | ROCA discovery and disclosure to manufacturer in January / February 2017 | | | |
| **Round 1: Vulnerability Disclosure Failures** | University research team (A.7),<br>Gemalto (A.4),<br>and actors involved in the supply chain like Infineon and its customers; ENISA, Austria | **V:** Moderate<br>Potentially serious impacts. V information remained undisclosed to public; controls planned but only partially implemented. | **T:** Low<br>T sources might have been motivated to exploit V but lacked information and would have required insider knowledge. | - *Risk assessment* to reduce uncertainty.<br>- *Risk mitigation* through information sharing under responsible disclosure guidelines and planning or implementation of patches. |
| | | **L:** Moderate<br>Low L of threat event occurrence, high L of threat event resulting in adverse impacts. | **I**: Moderate - High<br>Exercise of the vulnerability might have harmed operations and assets of organizations, individuals, nations. | |
| | | **Moderate** perceived risk severity (moderate likelihood, moderate impact)<br>*High degree of uncertainty* due to incomplete knowledge relating to scale and kind of affected systems worldwide, unrecognized dependencies, presence / absence of security controls, threat sources. | | |
| **Turning point** | Research Team disclosed ROCA vulnerability to CERT-EE on 30 August 2017 | | | |
| **Round 2: Estonia's organization of its crisis response** | Estonian government leadership & Prime Minister (A.5)<br>RIA (A.1)<br>PPA (A.2) | **V:** Moderate<br>Potentially severe impact. V information remained undisclosed to public, but no controls in place. | **T:** Low<br>T sources likely lacked V knowledge. | - *Risk assessment* to reduce uncertainty.<br>- *Risk mitigation* through information sharing under responsible disclosure guidelines. |
| | | **L**: Moderate<br>Low L of threat event occurrence, high L of threat event resulting in adverse impact. | **I**: High<br>Exercise of the vulnerability might significantly harm the Estonian e-state's mission, reputation and legitimacy, and result in limited loss of tangible assets. | |

| | | | | |
|---|---|---|---|---|
| | | **Moderate** perceived risk severity (moderate likelihood, high impact)<br>Still *high degree of uncertainty* due to incomplete knowledge. | | |
| **Turning point** | Press conference on 5 September 2017 | | | |
| **Round 3:**<br>**Public vulnerability announcement** | Estonian government leadership & Prime Minister (A.5)<br>RIA (A.1)<br>PPA (A.2)<br>SK ID Solutions (A.3) | **V:** Moderate<br>Potentially severe impact. basic information publicly accessible, controls planned but not implemented. | **T:** Low<br>T sources likely lacked V knowledge, publication could increase potential awareness among adversaries. | - *Risk mitigation* through restriction of access to public certificate repository and development of technical patch.<br>- Additional *risk mitigation* through *transparent communication* and publication of ROCA, which decreased the likelihood of undetected vulnerability exploitation and of a widespread loss of trust among citizens in cases of identity theft.<br>- *Risk acceptance* through keeping cards and e-services operational. Decision-makers considered the risk within state's risk tolerance to accept the vulnerability of affected eID cards while looking for a solution. |
| | | **L**: Low<br>Low L of threat event occurrence, moderate L of threat event resulting in adverse impacts. | **I**: High<br>Exercise of the vulnerability might significantly harm the Estonian e-state's mission, reputation and legitimacy, and result in limited loss of tangible assets. | |
| | | **Low** perceived risk severity (low likelihood, high impact) | | |
| **Turning point** | Municipal election takes place, 5-11 October 2017 | | | |
| **Round 4:**<br>**Online elections** | Estonian government leadership & Prime Minister (A.5)<br>RIA (A.1)<br>PPA (A.2)<br>SK ID Solutions (A.3) | **V:** Moderate<br>Potentially severe impact., basic information publicly accessible, controls planned but not implemented (s.a.). | **T:** Moderate<br>T sources lacked V detail knowledge but T with necessary motivation and/or capability to exploit V likely existed. Elections might have increased potential motivation of adversaries. | - *Risk acceptance* through keeping cards and e-services operational. Decision-makers judged shutdown of vulnerable cards and online elections to result from risk elimination and the potential ensuing loss of trust too costly. |
| | | **L**: Moderate<br>Low-moderate L of threat occurrence (slight increase with online elections); high L of threat event resulting in adverse impacts. | **I**: High<br>Exercise of the vulnerability might severely harm the Estonian e-state's mission, reputation and legitimacy, and result in limited loss of tangible assets, | |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  |  | including harm against online electoral process. |  |
|  |  | **Moderate** perceived risk severity (moderate likelihood, high impact) |  |  |
| **Turning point** | Patch deployment on 25 October 2017 |  |  |  |
| **Round 5:**<br>**Patch deployment** | RIA (A.1),<br>PPA (A.2),<br>SK ID Solutions (A.3),<br>Gemalto (A.4),<br>Estonian government leadership & Prime Minister (A.5),<br>Legal and technical experts in the crisis working groups (A.6) | V: Low-Moderate<br>Potentially serious impact for Estonian e-state, controls (patch) in course of implementation. | T: Low<br>Patch deployment increased costs and required level of capability and intent for T sources. | - *Risk mitigation* at technical and operational levels through deployment of a vulnerability patch. |
|  |  | L: Low<br>Low L of threat event occurrence, moderate L of threat event resulting in adverse impacts. | I: High<br>Exercise of the vulnerability might severely harm the Estonian e-state, but number of vulnerable cards decreased with update and trust in government to fix the vulnerability likely increased with update. |  |
|  |  | **Low** perceived risk severity (low likelihood, high impact) |  |  |
| **Turning point** | Publication of researchers' paper with ROCA details on 30 October 2017 |  |  |  |
| **Round 6:**<br>**Emergency suspension of certificates** | RIA (A.1),<br>PPA (A.2),<br>SK ID Solutions (A.3),<br>Gemalto (A.4),<br>Estonian government leadership & Prime Minister (A.5),<br>Legal and technical experts in the crisis working groups (A.6) | V: High<br>Potentially severe impact for Estonian e-state, V details and attack possibilities published, remediations still only partially installed. | T: High<br>Publication of V details and attack possibilities likely increased motivation and decreased costs and required levels of capability for adversaries. | - *Risk avoidance* through vulnerable certificates' suspension – risk exceeded the national and organizational risk tolerance.<br>- Ongoing *risk mitigation* through vulnerability patch deployment. |
|  |  | L: High<br>High L of threat event initiation due to vulnerability details' publication; high L of threat event resulting in adverse impacts. | I: High<br>Exercise of the vulnerability might severely harm the Estonian e-state, its reputation, and citizens' trust in DG services, although number of vulnerable cards decreased with update. |  |

| | | | | |
|---|---|---|---|---|
| | | **High** perceived risk severity (high likelihood, high impact) | | |
| **Turning point** | Operational ending on 31 March 2018 | | | |
| **Round 7:<br>Operational crisis termination** | RIA (A.1),<br>PPA (A.2),<br>SK ID Solutions (A.3),<br>Gemalto (A.4),<br>Estonian government leadership & Prime Minister (A.5),<br>Legal and technical experts in the crisis working groups (A.6) | **V:** Very low<br>No impact for Estonian e-state anymore, remediations installed. | **T:** Very Low<br>V was patched, threat had been eliminated. | - *Risk mitigation and elimination* through revocation of all non-updated eID cards. |
| | | **L**: Very low<br>Vulnerability remediated | **I**: Very low<br>No vulnerable cards to be exploited anymore. | |
| | | **Very low** perceived risk severity (very low likelihood, very low impact) | | |
| **Turning point** | Conference Report Publication on 9 May 2018 | | | |

## 7. References

Bernstein, D. J., & Lange, T. (2017). Reconstructing ROCA. Retrieved 30.07.2020, from https://blog.cr.yp.to/20171105-infineon.html

BNS. (2017, 05.09.2017). Estonian ID card security risk calls into question security of e-elections. *Postimees*. Retrieved 01.02.2022, from https://news.postimees.ee/4233385/estonian-id-card-security-risk-calls-into-question-security-of-e-elections

ERR News. (2017, 22.11.2017). Gemalto rep: Estonian authorities notified the ID card flaw in June. Retrieved 10.05.2021, from https://news.err.ee/644250/gemalto-rep-estonian-authorities-notified-of-id-card-flaw-in-june

ERR News. (2018, 03.04.2018). Nearly 300,000 ID card certificates not renewed by March 31 deadline. Retrieved February 10, 2021, from https://news.err.ee/693660/nearly-300-000-id-card-certificates-not-renewed-by-march-31-deadline

Kund, O. (2017, 07.09.2017). ID-card tip from Czech scientists. *Postimees*. Retrieved 02.03.2021, from https://news.postimees.ee/4236857/id-card-tip-from-czech-scientists

Lips S., Pappel I., Tsap V., & Draheim, D. (2018). *Key Factors in Coping with Large-Scale Security Vulnerabilities in the eID Field*. Paper presented at the Electronic Government and the Information Systems Perspective. EGOVIS 2018.

Nemec, M., Sys, M., Svenda, P., Klinec, D., & Matyas, V. (2017). *The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli*. Paper presented at the ACM CCS 17 Proceedings, Dallas, Texas, United States.

NIST. (2012). SP 800-30: Guide for conducting risk assessments, Rev. 1. In: National Institute of Standards and Technology, U.S. Department of Commerce.

Parsovs, A. (2021). *Estonian Electronic Identity Card and its Security Challenges.* (Doctor of Philosophy), University of Tartu, Retrieved 01.07.2021, from https://dspace.ut.ee/handle/10062/71481

Pau, A. (2018a, 06.09.2018). Cyber-lollygagging cost the state millions. *Postimees*. Retrieved 12.06.2021, from https://news.postimees.ee/6383968/cyber-lollygagging-cost-the-state-millions

Pau, A. (2018b, 08.03.2018). Gemalto and PPA are carrying tens of millions after the war. *Postimees*. Retrieved June 12, 2021, from https://tehnika.postimees.ee/4432811/gemalto-ja-eesti-politsei-veavad-kumnete-miljonite-parast-vagikaigast.

RIA. (2017). ID.ee: FAQ (Archived). Retrieved 01.02.2022, from https://web.archive.org/web/20171108223524/https://id.ee/index.php?id=38066

RIA. (2018, 09.05.2018). ROCA Vulnerability and eID: Lessons Learned. Retrieved 10.05.2021, from https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf

Švenda, P. (2018). *The goal of the research (ROCA)*. Retrieved 20.01.2022, from https://lessonslearned.publicon.ee/userfiles/RIA/lessonslearned2018/1_Petr%20Svenda%20-%20CROCS_ROCA_Tallin_20180508_finalCut.pdf

Tallinna Tehnikaülikool. (2018). *ID-kaardi kaasuse õppetunnid*. Retrieved 25.11.2019, from https://www.ria.ee/sites/default/files/content-editors/EID/id-kaardi_oppetunnid.pdf

Tamm, M. (2018, 30.08.2018). The country is looking for a compromise with the ID card manufacturer. *Delfi.ee*. Retrieved April 15, 2020, from http://www.delfi.ee/news/paevauudised/eesti/video-riik-otsib-id-kaardi-tootjaga-voimalust-kompromissiks?id=83516467

Vahtla, A. (2017a, 09.11.2017). EKRE challenges electoral committee's decision to allow e-voting. *ERR News*. Retrieved 02.03.2020, from https://news.err.ee/617916/ekre-challenges-electoral-committee-s-decision-to-allow-e-voting

Vahtla, A. (2017b, 03.11.2017). Government to suspend ID card certificates with security risk at midnight. Retrieved 01.02.2022, from https://news.err.ee/640385/government-to-suspend-id-card-certificates-with-security-risk-at-midnight

Vahtla, A. (2017c, 05.09.2017). Potential security risk could affect 750,000 Estonian ID cards. *ERR News*. Retrieved 02.03.2020, from https://news.err.ee/616732/potential-security-risk-could-affect-750-000-estonian-id-cards

Valimised. (2017). Eesti Vabariik kokku. Andmed seisuga 25.10.2017 09:43:53 (2017 Municipal Election Results). Retrieved 15.08.2021, from https://kov2017.valimised.ee/valimistulemus-vald.html

Wright, H. (2021, 06.02.2021). Gemalto, PPA reach compromise over ID-card security weakness. *ERR.ee*. Retrieved February 6, 2021, from https://news.err.ee/1608100102/gemalto-ppa-reach-compromise-over-id-card-security-weakness

**Publication II**

Schallbruch, Martin, & Skierka, Isabel. (2018). Cybersecurity in Germany. Springer Briefs in Cybersecurity. *Springer*. https://doi.org/10.1007/978-3-319-90014-8 (2.1).

# Cybersecurity in Germany

By Martin Schallbruch and Isabel Skierka

Digital Society Institute, ESMT Berlin

August 2018

# Cybersecurity in Germany – Authors' Manuscript Version

**Authors:**
Martin Schallbruch, Martin.schallbruch@esmt.org
Isabel Skierka, Isabel.skierka@esmt.org

**Abstract:** This Springer Brief provides a detailed analysis of how cybersecurity in Germany has evolved over the past decades. Once a niche topic, cybersecurity has become a top priority for the German government, the private sector and the public at large. In 2016, Germany's government presented its third cybersecurity strategy, which aims to strengthen the national cyber defence architecture, cooperation between the state and industry, and informational self-determination. For many years, Germany has followed a preventive and engineering approach to cybersecurity, which emphasises technological control of security threats in cyberspace over political, diplomatic and military approaches. Accordingly, the technically oriented Federal Office for Information Security (BSI) has played a leading role in Germany's national cybersecurity architecture. Only in 2016 did the military expand and reorganize its cyber defence capabilities. Moreover, cybersecurity is inextricably linked to data protection, which is particularly emphasised in Germany and has gained even greater public attention since Edward Snowden's revelations.

Based on official documents and their insights from many years of experience in cybersecurity policy, the two authors describe cybersecurity in Germany in the light of these German peculiarities. They explain the public perception of cybersecurity, its strong link with data protection in Germany, the evolution of Germany's cybersecurity strategies, and the current organization of cybersecurity across the government and industry. The Brief takes stock of past developments and works out the present and future gaps and priorities in Germany's cybersecurity policy and strategy, which will be decisive for Germany's political role in Europe and beyond. This includes the cybersecurity priorities formulated by the current German government which took office in the spring of 2018.

# Table of Contents

# Chapter 1: Introduction

**Abstract** With the digitisation of nearly all aspects of life, our societies increasingly depend on the resilience and security of computing and communication technologies. Hence, the protection of information technology (IT) against unauthorised access, attack, and accidental failure, has become a priority for nation-states around the world.

Throughout the past one or two decades, most countries have adopted strategies, policies and practical steps to protect the security of IT and critical infrastructures within their territory, and, by extension, their citizens. These practices are generally subsumed under the umbrella of cybersecurity.

The resulting development of various national cybersecurity perspectives and policies is covered by this dedicated Springer series. This Springer Brief provides an analysis of the evolution of cybersecurity policy in Germany over the past two and a half decades.

## *1.1 On terminology*

As a policy field, cybersecurity is still comparatively young, with most nations having started to adopt national cybersecurity policy documents and strategies only a decade ago. In fact, the very definition of the term "cybersecurity" remains unclear and the concept itself remains contested (Wagner & Vieth, 2016). Each national context will define the specific definitions and approaches to the challenges and opportunities related to it (Hathaway & Klimburg, 2012) (New America, n.d.).

Cybersecurity is closely related to concepts such as information technology (IT) security, which refers to the confidentiality, integrity, and availability of information, and information assurance, computer security, and network security. However, IT security is only one technical aspect of cybersecurity.

Cybersecurity encompasses technologies, processes, and policies that help to prevent or reduce the negative impact of events in cyberspace that can happen as the result of deliberate actions against IT by a malevolent actor (Computer Science and Telecommunications Board, 2014) (Tabansky & Ben Israel, 2015). These processes and associated practices differ across organizations and geographic regions.

The term "cybersecurity" was not used in official German government documents until the first cybersecurity strategy in 2011. Earlier documents mostly refer to "IT security" or "critical information infrastructure security", which are more technical in scope than cybersecurity. This Brief will consistently use the term "cybersecurity policy" in order to refer to the overall development of this policy area. Whenever it refers to particular documents and developments, it will use the terminology employed by policy-makers.

### *1.2 Approach*

The description and analysis of German cybersecurity policy is based on the evaluation of a variety of official documents released by German government agencies, as well as news articles and international policy documents. In addition, it draws on (so far only a small number of) academic literature and policy analyses in the field of cybersecurity, data protection, and national security more generally. The Brief further focuses on institutional arrangements and corresponding federal and state laws. It benefits from co-author's Martin Schallbruch's first-hand experience in cybersecurity policy-making in the federal government, as well as from both co-authors' experience with academic and policy research and consultancy activities in the field, most recently at the Digital Society Institute of the European School for Management and Technology Berlin.

### *1.3 Peculiarities of the German political system*

Every country's politics and political system are unique. In the post-World War II period, Germany was a divided country until 1990. Its historical past— the Nazi era and the Communist East German regime with its Stasi secret police—are ever present in politics and society. The Nazi regime systematically abused private data for the identification and persecution of Jews, homosexuals, political opponents, and other groups. East Germany functioned as a socialist dictatorship in which the Stasi ran a nationwide surveillance regime that relied on denunciation and electronic surveillance. Not least because of the lessons of this past, the German public and policy-makers attach so much importance to data protection and privacy (Freude & Freude, 2016).

Readers should take into account two additional aspects of the German political system while reading this Brief: German federalism and coalition government.

Germany's political system is based on federalism, a system of government in which power is shared between the central state (at the federal level) and federal regional states. The German federal system comprises sixteen federal states, so-called "Länder". Each state has its own government, headed by a minister president. At the national federal level, the sixteen Länder are represented by the German Federal Council (Bundesrat), which has a vital legislative role in passing new legislative initiatives, even those proposed by the federal government.

Cybersecurity is mainly dealt with as a national policy issue in Germany, although most states have some form of administrative IT security structures in place. When it comes to cyber crime and counter espionage, law enforcement agencies at the state level play an essential role. Law enforcement in Germany is constitutionally vested at the federal level and with the states, which each have their own police agencies and offices for the protection of the constitution (domestic intelligence agencies).

Finally, governments in Germany are almost always formed by party alliances, so-called coalition governments. In following, this Brief repeatedly refers to national government coalition "agreements" or "treaties". These are the political agendas which coalition parties negotiate before taking office after federal elections. The coalition treaties constitute important official documents that indicate government priorities and against which a coalition government's achievements will be evaluated. The most recent coalition treaty dates from March 2018, when the CDU, its sister party CSU, and the SPD started governing.

### *1.4 Structure*

In following, this Brief analyses public perspectives on cybersecurity, government strategies, national organizational aspects, as well as an outlook on gaps and priorities in Germany's cybersecurity policy. The remaining chapters are structured as follows:

- Chapter 2 provides an overview of the public perspective on the challenges, strategies, and instruments of cybersecurity in Germany. It illuminates the link between data protection and cybersecurity issues in the public debate, the emergence of particular political and regulatory concepts dealing with IT and cybersecurity, and the debate about "digital sovereignty" resulting from the revelations of former US National Security Agency (NSA) contractor Edward Snowden.
- Chapter 3 traces the evolution of German cybersecurity strategy throughout the past two and a half decades in historically chronological order. It describes and analyses various cybersecurity strategy and policy documents. Thereby, the chapter illustrates the increasingly comprehensive scope of German cybersecurity policy, whose emphasis has broadened from a civilian defence perspective to include international diplomatic and strategic military aspects in recent years.
- Chapter 4 explains the national organization of cybersecurity responsibilities and corresponding institutions in Germany. It focuses on cooperation and conflict between government agencies, and on public-private cooperation in cybersecurity.
- Chapter 5 presents an evaluation of current gaps in German cybersecurity policy which the government will need to address in the upcoming years. It considers six fields of action: active cyber defence, the national cybersecurity architecture, the state's handling of IT security vulnerabilities, the legal framework for IT security liability, Germany's and Europe's industrial IT security policy, and Germany's cooperation with international partners.
- Chapter 6 provides concluding remarks to this Brief.

### *1.5 References*

Computer Science and Telecommunications Board, 2014. *At the Nexus of Cybersecurity and Public Policy Some Basic Concepts and Issues,* s.l.: The National Academy of Sciences.

Freude, A. & Freude, T., 2016. *Echoes of History: Understanding German Data Protection,* s.l.: Bertelsmann Foundation.

Hathaway, M. & Klimburg, A., 2012. Preliminary Considerations: On National Cyber Security. In: *National Cyber Security Framework Manual*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, pp. 1-43.

New America, n.d. *Global Cyber Definitions Database*. [Online] Available at: http://cyberdefinitions.newamerica.org/ [Accessed 31 March 2018].

Tabansky, L. & Ben Israel, I., 2015. *Cybersecurity in Israel,* London: Springer Nature.

Wagner, B. & Vieth, K., 2016. Was macht Cyber? Epistemologie und Funktionslogik von Cyber. *Zeitschrift für Außen- und Sicherheitspolitik,* Volume 9, pp. 213-222.

# Chapter 2: The German view on cybersecurity

**Abstract** The German public perspective on the challenges, procedures, and instruments of cybersecurity follows three lines of development: First, the close link of cybersecurity with data protection and privacy issues; second, the distinct way of dealing with technical hazards by means of (regulatory and engineering) risk prevention mechanisms; and third, the debate on “digital sovereignty” that was triggered by the Snowden revelations.

**Keywords** Data Protection, Privacy, Legal Concepts, Risk Prevention, Digital Sovereignty, Snowden

## *2.1 The Public Perception of Cyber Issues*

Public attention for cybersecurity in Germany first emerged in the context of successful hacking attacks. Since the 1980s, (western) Germany has been home to a very active hacking community around the Chaos Computer Club (CCC) in Hamburg, an association founded in 1981. The CCC succeeded at an early stage in reaching a broad public with successful hacking attacks. They conducted their first notable hack in 1984 by manipulating the so-called "Btx" system, a teletext system operated by the national postal service. The CCC demonstrated how it could hack the "Hamburger Sparkasse" bank's system and steal 135,000 Deutsche Mark (former German currency unit (Oppliger, 1992, S. 18). The CCC returned the money but had successfully demonstrated the substantial risks of banks’ insecure computer systems for customers. Another hacker group associated with the CCC offered their expertise and services to the Russian intelligence service KGB from 1985 onwards. In return for payment, the group penetrated militarily relevant computer systems, including those of the American military, and provided the information to the KGB (Ammann, 1989) (Stoll, 1989).

From the very beginning, the German public perception of hacking has been ambivalent: On the one hand, successful hacks raised awareness for the risks of information technology (IT) for users, especially concerning data privacy. At the same time, hacking was considered a new form of crime and raised considerable concerns among the population. As a result, Germany was one of the first countries to make hacking a criminal offense in 1986. However, the then introduced § 202a of the penal code only criminalized the theft of data, but not the intrusion into a system under surpassing security precautions. The German parliament wanted to avoid a kind of "over-criminalization" of hacking (Lenckner & Winkelbauer, 1986, S. 488). In line with the implementation of the 2001 Cyber crime Convention of the Council of Europe into national law, Germany had to extend its criminal law. Since 2007, "mere hacking", i. e. intrusion into protected computer systems, has also been punishable by law (Schreibauer & Hessel, 2007).

Before the turn of the millennium, however, successful hacking attacks were hardly seen as significant threats. The public perception changed with the year 2000 when users became widely concerned about the availability of the computer systems in the context of the "Year 2000" or "Y2K" problem. The Y2K problem refers to a class of computer bugs related to the formatting and storage of calendar data that was projected to create havoc in computers and computer networks around the world at the beginning of the year 2000 (Y2K Bug, 2018).

In anticipation of the risk, the government assigned high priority to the preparation of computer systems for the turn of the millennium. It prepared citizens by distributing information mail to all households and set up a comprehensive crisis management plan to assure the government's ability to act in case the risk would materialize. Ultimately, few failures occurred in the transition from December 31, 1999, to January 1, 2000. What remained of the Y2K bug was an increased sensitivity for questions of computer security (Bundesministerium für Wirtschaft und Energie, 1999).

As a result, the increasingly frequent occurrence of cyber attacks triggered growing public reactions – starting with the Loveletter virus, which spread explosively via E-mail attachments in May 2000. The incident led to a first intensive debate about cybersecurity in the German Bundestag. Since the Loveletter virus exclusively affected Microsoft products, the discussion focused strongly on the question of the security relevance of a "Microsoft monoculture" (Deutscher Bundestag, 2000, S. 9541D ff.). In the wake of the incidents, the reduction of the government's, industry's, and society's dependency on Microsoft products and support for open source alternatives became a more or less vigorously pursued policy goal of the federal government.

Around the turn of the millennium, public attention concentrated on the reliability of IT. This focus shifted in the following years. The threat of cyber attacks for the confidentiality and integrity of data became more and more relevant. The traditionally high degree of attention of the German public for data protection and privacy aspects overshadowed cybersecurity issues. The media and public voices framed major hacks such as the theft of data of 17 million customers from Deutsche Telekom in 2006 foremost as data protection problems (Deutsche Welle, 2008).

### *2.2 Political and Regulatory Concepts*

The regulatory concepts for the protection of cybersecurity in Germany are closely linked to the protection of personal data. Even before the concept of "information security" emerged in the early 1980s, "data security" had been a legal obligation. Already the first Federal Data Protection Act of 1977, in Section 6, included mandatory legal responsibilities to take technical and organizational steps to protect data. Since then, this obligation applies to all companies and authorities that process personal data on computer systems. A catalogue annexed to the act provides a rough description of the measures, from which the protection goals of confidentiality and integrity of the data can already be deduced (Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung as of January 27, 1977, 1977). Until today, there are no significant differences in the ways information security and data security are technically implemented. Although data protection and IT security have different legal bases in the EU, the EU General Data Protection Regulation (EU GDPR) (GDPR EU, 2016) on the one hand and the EU Directive on Network and Information Security (NIS Directive) (NIS Directive EU, 2016) on the other, their respective technical implementation is similar.

Data security and information security laws are rooted in the regulatory concept of German technology law, which in turn originates from the environmental law but has meanwhile dispersed to a wide range of other fields of law. Following German technology law, the handling of "dangerous" technologies, i.e. systems that have potentially harmful effects on humans (and the environment), requires governmental approval, which is given only under particular (technical) conditions. This idea was transferred to the electronic data processing: Just as the operation of power plants is prohibited, unless the law and directives stipulate requirements for smoke purification and/or related requirements, data protection law prohibits the processing of personal data via IT systems, unless the systems meet specific technical data security requirements. Risks arising from the use of technology are to be reduced to such an extent through technical and organizational measures that the remaining residual risk is acceptable for humans, the environment, and society as a whole.

The definition of IT systems requirements in data protection law supplements the additional legal question of whether the data may be processed at all for a respective purpose. The systems must comply with appropriate data security measures. In this context, German (and European) data protection law typically focuses on the "state of the art" security. The idea behind this reference is to ensure that the implementation of security measures is not planned statically but is designed and updated dynamically on a long-term basis in a risk-adequate manner (Michaelis, 2016).

Given the similarity of data protection and cybersecurity in the German political debate, it is not surprising that the concept of technology law, which the data protection law already reflects, has also been adopted in the area of IT security law. The first German cybersecurity-related strategy, the 2005 National Plan for the Protection of Information Infrastructures (Bundesministerium des Innern, 2015), already focuses on the preventive protection of systems against cyber attacks. Two outstanding events were catalysts for the creation of the strategy. On the one hand, the 9/11 attacks in the United States (US) led the German government to subject Germany's security architecture under extensive scrutiny from 2002 onwards. The overhaul included - for the first time - the security of information infrastructures. In several studies, the government identified the level of protection of IT systems in Germany's most important infrastructures and recognized significant needs for improving preventive protection measures (Bundesministerium des Innern, 2004, S. 246). The second motive for the government's action was a denial of service attack on the federal government's networks in 2004, which led to considerable disruptions of digital collaboration within the government. The government networks were flooded with irrelevant e-mails. This attack considerably restricted the usual e-mail communication of the authorities (Schulze, 2006, S. 137).

Another aspect illustrating German cybersecurity policy's emphasis on technical requirements for IT systems and the technical handling of cyber attacks is the growing role of the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) throughout the past two decades. Founded as a licensing and certification authority for cryptographic systems and for eavesdropping defence purposes, the agency has meanwhile become a special police authority for all questions of IT security. Its competencies range from the investigation of IT products and the supervision of critical infrastructures to the investigation and defence of cyber attacks on governmental and critical infrastructures. With the federal cybersecurity strategy of 2011, the agency even became the lead body of the cyber defence centre, which connects all German cybersecurity authorities (Bundesministerium des Innern, 2011).

The engineering approach of the BSI, the development and use of technically secured systems, became an essential constant of German cybersecurity policy. The Federal Constitutional Court also contributed to this development. Asked about the conditions under which state authorities can use trojan software to penetrate into the computer systems of terrorist suspects, the court created a new fundamental right derived from the German constitution to guarantee the integrity and confidentiality of information technology systems, which was then also referred to as the "fundamental right to IT security" (Bundesverfassungsgericht, 2008) (Hornung, 2008). It juxtaposes the right of informational self-determination, the constitutional legal basis of German data protection, with a similarly constructed fundamental right to security of IT systems against state intervention. For each case in which governmental measures invade private ICT systems, referred to as lawful hacking, a legal basis and appropriate technical and organizational security measures are required. Lawmakers have to change a national security law to define the circumstances, under which police forces and intelligence services are entitled to lawful hacking. The constitutional court also adopted the concept of primary technical protection of IT security: in cases of considerable risks to national or individual security, the state may hack IT systems. Yet, the risks to the security of the respective IT system must be reduced by technological measures to a tolerable level.

### *2.3 Snowden and the Emerging Discussion about Technological Sovereignty*

The revelations of materials by Edward Snowden in 2013, which documented the US National Security Agency’s (NSA) and other “Five Eye” alliance intelligence agency’s surveillance activities in Europe, were particularly relevant to Germany. Virtually overnight, the revelations lifted cybersecurity from the realm of technocratic politics up onto the government's top political agenda. The German public had already historically been sensitive to data protection issues. Policymakers carefully followed the disclosures about the National Security Agency's (NSA) methods, which began with reports about the PRISM surveillance programme (Gellman & Poitras, 2013). Furthermore, it quickly became clear that German citizens, companies, and politicians were also directly affected by the NSA surveillance. The debate reached its climax with the announcement in October 2013 that the NSA had surveilled the cell phone of German Chancellor Angela Merkel. Finally, the disclosures revealed another set of facts: the German intelligence services had cooperated with and supported the NSA's electronic surveillance activities. In particular, the Foreign Intelligence Service (Bundesnachrichtendienst, BND) had collaborated closely with the NSA in monitoring international telecommunications on German territory (Rosenbach & Stark, 2014) (Deutscher Bundestag, 2017). According to German constitutional law experts, the BND practice of collecting foreign communication data infringed upon the right to private communication guaranteed by Article 10 of the German Basic Law. This right protects every person independent of her citizenship or country of residence (Bäcker, 2014) (Wetzling, 2016).

Edward Snowden's publications put German political decision-makers under pressure to provide answers to crucial questions: Do US intelligence services access German domestic digital communications? To what extent are data of German citizens protected on the servers of American companies? How safe are German companies from US industrial espionage? Are the government's communication networks and communications resources adequately secured? Are IT products and digital services from US companies still trustworthy? And above all, what can future transatlantic cooperation on cybersecurity issues look like after this loss of confidence? The reports on NSA activities acted as an accelerator for German cyber politics. In the run-up to federal elections for a new German parliament (Bundestag) in the fall of 2013, data protection and cybersecurity became critical campaign issues. Chancellor Angela Merkel quickly presented an 8-point programme for enhanced privacy protection (Bundesministerium des Innern und Bundesministerium für Wirtschaft und Energie, 2013) (Funke, 2013).

The adopted initiatives not only put intelligence cooperation with the US under scrutiny. The Federal Government also announced a speeding-up of European data protection legislation, including elevated standards for data transfer to the USA and other non-EU states. What was new in the government's official policy was the idea to strengthen the national (and European) IT industry to be able to use trustworthy products and services from Europe and to reduce their dependency on US providers (Bundesministerium des Innern und Bundesministerium für Wirtschaft und Energie, 2013, S. 6-7). A government-led roundtable on "Security Technology in the IT sector" with representatives from all levels of government, industry, and academia elaborated a wide range of measures to promote the development and use of trustworthy IT systems (Bundesministerium des Innern, 2013).

The Snowden revelations also had an impact on the programme of the newly elected federal government in autumn 2013. Never before and never since has a coalition agreement to form a German government included such a comprehensive agenda on cybersecurity. The government coalition parties agreed on the adoption of an IT security law, as well as on the strengthening of the Federal Office for Information Security's (BSI) role in cybersecurity. For the first time, Germany's coalition agreement also calls for "regaining Germany's technological sovereignty". The idea behind this call for action was to introduce technical, legal, and political measures to better protect citizens, industry, and state authorities from surveillance by foreign intelligence agencies. The deployment of trustworthy national IT security technology should provide greater protection for citizens. The coalition treaty even brought up the idea of implementing national or ‘Schengen' routing for discussion, i. e. redesigning the Internet infrastructures in such a way that data remains within Germany or Europe (CDU, CSU, & SPD, 2013, S. 148ff.).

Political decision makers’ call for regaining “technological sovereignty” in Germany and Europe subsequently developed into a broader political agenda. Apart from the 2013 coalition treaty, the German government's "Digital Agenda" of 2014 emphasised the government's plan to consider Germany's technological sovereignty in its external trade policy (Bundesregierung, 2014).

Despite their extensive use in public discourse, to this date technological or digital sovereignty remain ill-defined concepts. Instead, they are political expressions being used to justify a range of measures under the umbrella of counter-surveillance and espionage. These include the overcoming of dependencies on foreign IT components (Eckert, 2013), (Bitkom e.V., 2015), the creation of independence of own telecommunications networks from foreign servers, so that internal data traffic would not leave German jurisdiction, as well as the equipment of national intelligence agencies with better capabilities to be at eye level with foreign intelligence agencies (Schaar, 2015). As a result, the government has taken some actions to strengthen and facilitate the use of German technologies, such as research funding programmes or changes in procurement practices. In individual cases, the government terminated service contracts with

US providers and replaced them with German providers, such as the US company Verizon's services for the German government network (Hathaway, 2014, S. 302) (Deutscher Bundestag, 2017, S. 336ff.).

More recently, the term has mostly been used to refer to measures to enhance data protection and informational self-determination of individual citizens.
With the development of an IT security law, which was initiated directly at the start of the new government's work, Germany has become a European pioneer in the regulation of cybersecurity. The German law came into force in summer 2015 (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015, 2015), the corresponding EU directive followed only one year later. The boost to Germany's cybersecurity policy resulting from the Snowden revelations had a considerable impact on policy-making in the 18th parliamentary term from 2013 to 2017, even though it did not implement all agreed measures in the end (Schallbruch, Gaycken, & Skierka, 2018).

### *2.4 Combining German Data Protection and Engineering Approach with Holistic Cyber Debates*

For many years, the German discussion on cybersecurity has been limited to questions of data protection, technical and organizational security of IT systems and criminal prosecution in cyberspace. At the same time, the debate on internet policy had already been in full swing since 2005, which even led to the emergence of a new political party, the Pirate Party, which was very successful for some years (Lauer & Lobo, 2015). However, this debate had little impact on cybersecurity policy. Issues of data protection, copyright law, the blocking of illegal content on the Internet, access to metadata by security agencies or the provision of open data were far more in the focus of internet policy (including the politics of the Pirate Party) than the discussion of how Germany should defend itself, its citizens, and critical infrastructures in cyberspace. Nor did Germany develop international political visibility in the field of cybersecurity.

Although IT and cybersecurity are focus areas of digital policy as outlined in the Federal Government's Digital Agenda for the years 2014-2017, the Agenda emphasises a technical approach of data and system protection, supplemented by the expansion of law enforcement capabilities in the digital realm. Technology policy approaches to strengthening national technological sovereignty remain unclear, and the Agenda lacks a more holistic view on cybersecurity with a regard to international security, global competitiveness, and human rights (Bundesregierung, 2014).

The more extensive opening-up of cybersecurity policy did not occur until the military's late entry into the German cyber domain. For many years, the armed forces (Bundeswehr) had not developed its own cybersecurity policy. Instead, it was a contributing party within the civil cybersecurity strategies of the Interior Ministry. In 2014-2015, the Ministry of Defence started to develop its own cyber strategy. With the establishment of a Command for Cyber and Information Space (Kommando Cyber- und Informationsraum, CIR), the reorganization of the ministry and other supporting measures such as the establishment of Cybersecurity Research Resources at the University of the German Armed Forces, the military has now made a significant contribution to cybersecurity policy. The revised national defence strategy from 2016, so-called White Paper, provided the framework for the Bundeswehr's cyber command (Federal Government, 2016). The 2016 White Paper, for the first time, takes security in the global cyber and information space as a whole into account. The document outlines the Bundeswehr's contribution to the protection of this space, as well as its operational capability in cyber and information space.

The attack on the networks of the German Bundestag in summer 2015 led to an opening of cybersecurity policy debate to the public. Via an advanced persistent threat (APT) campaign, allegedly Russian intelligence services stole a tremendous amount of data from the parliament's networks. This cyber attack against the heart of the German democratic institutions led to a major change of thinking about cybersecurity. In addition to a technically-oriented cybersecurity policy focusing on data protection aspects and preventive technology management, the policy domain developed a military component and an increasingly intense discussion of active cyber defence actions.

### *2.5 Advantages and Disadvantages of German Approach – A Preliminary Balance*

Germany has developed the core of its cybersecurity policy along three strong lines: a rather engineering-motivated preventive and technology-oriented policy, a policy of protecting personal data motivated by high esteem for privacy through legal, technical and organisational measures and, last but not least, a policy formulated along extended criminal offences and the need to strengthen the security authority investigative powers against cyber crime. These three cornerstones have one point in common: they are primarily preventive and civilian. They are based on the idea of the ability to create cybersecurity through appropriate structuring of information technology systems, legal protection of people against misuse of these systems and the consistent prosecution of violations of the law.

Germany has made great progress with this approach. The legal foundations for the protection of IT critical infrastructures and digital services are an exemplary one, the Federal Office for Information Security is one of the largest and best-in-class cybersecurity authorities in the world. Since the first cybersecurity strategy in 2005, government and businesses have invested heavily in preventive cybersecurity. Cybersecurity in Germany has a solid legal and organisational foundation.

However, this approach has not yet been able to fully grasp the complexity of international cybersecurity. In regard to the unsolved basic security of information technology systems and the increase in complexity and vulnerabilities, Germany's technical and organisational measures cannot adequately protect companies and authorities. A purely defensive and preventive strategy does not help in this context. At the same time, the Snowden revelations and the subsequent efforts towards technological sovereignty, which have not been very successful so far, have shown that considerable shortcomings already exist at the level of technical security.

Finally, the increase in cyber attacks as part of a worldwide asymmetric threat situation has also made it clear to Germany, as a technology-supported export nation, that cybersecurity necessarily includes an active, military and civilian cyber defence and that capacities must be built up for this purpose.

### *2.6 References*

Ammann, T. (1989). *Hacker für Moskau. Deutsche Computer-Spione im Dienst des KGB*. Reinbek: Wunderlich.

Bäcker, M. (2014). *Erhebung, Bevorratung und Übermittlung von Telekommunikationsdaten durch die Nachrichtendienste des Bundes. Stellungnahme zur Anhö- rung des NSA-Untersuchungsausschusses*.

Bitkom e.V. (2015). *Digitale Souveränität - Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa*. Berlin.

Bundesministerium des Innern. (2004). Nach dem 11. September 2001. Maßnahmen gegen den Terror. Berlin.

Bundesministerium des Innern. (2011). *Cyber-Sicherheitsstrategie für Deutschland*. Berlin.

Bundesministerium des Innern. (09. September 2013). *Pressemitteilung 'Schutz der Privatsphäre durch vertrauenswürdige Informations- und Kommunikationstechnik'*. Abgerufen am 03. March 2018 von https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2013/09/runder_tisch.html

Bundesministerium des Innern. (2015). *Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI)*. Berlin.

Bundesministerium des Innern und Bundesministerium für Wirtschaft und Energie. (14. August 2013). *Maßnahmen für einen besseren Schutz der Privatsphäre. Fortschrittsbericht vom 14. August 2013*. Abgerufen am 03. March 2018 von https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2013/bericht2.pdf

Bundesministerium für Wirtschaft und Energie. (1999). *Das Jahr-2000-Problem in der Informationstechnik. Zweiter Fortschrittsbericht der Bundesregierung*. Berlin.

Bundesregierung. (2014). *Digitale Agenda für Deutschland* .

Bundesverfassungsgericht. (2008). *NJW*, 822.

CDU, CSU, & SPD. (2013). *Deutschlands Zukunft gestalten. Koalitionsvertrag für die 18. Legislaturperiode*. Berlin.

Deutsche Welle. (11. October 2008). *New Privacy Scandal Comes Calling at Telekom*. Abgerufen am 03. March 2018 von http://www.dw.com/en/new-privacy-scandal-comes-calling-at-telekom/a-3706182

Deutscher Bundestag. (2000). Plenarprotokoll 14/102 vom 11. Mai 2000.

Deutscher Bundestag. (2017). *Abschlussbericht des 1. Untersuchungsausschusses (NSA) vom Juni 2017, Drucksache 18/12850*. Berlin.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS directive). (2016). *OJ L* (194), 1.

Eckert, C. (23. 11 2013). Digitale Vision für Europa. *FAZ.NET*.

Federal Government. (2016). *White Paper on German Security Policy and the Future of the Bundeswehr*. Berlin.

Funke, M. (2013). Bundeskabinett: Fortschrittsbericht zum besseren Schutz der Privatsphäre. *CR*, R94.

Gellman, B., & Poitras, L. (07. June 2013). *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*. (Washington Post) Abgerufen am 31. March 2018 von https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?noredirect=on&utm_term=.7019ae7824f8

Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung as of January 27, 1977, published on February 1, 1977. Entry into force since January 1, 1978. (1977). *BGBl. I* (7), 201.

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015. (2015). *BGBl. I*, 1324.

Hathaway, M. E. (2014). Connected Choices: How the Internet Is Challenging Sovereign Decisions. *American Foreign Policy Interests, 36*(5), 300-313.

Hornung, G. (2008). Ein neues Grundrecht. Kommentierung zur BVerfG-Entscheidung. *CR*, 299.

Lauer, C., & Lobo, S. (2015). *Aufstieg und Niedergang der Piratenpartei*. Hamburg: sobooks.de.

Lenckner, T., & Winkelbauer, W. (1986). Computerkriminalität - Möglichkeiten und Grenzen des 2. WiKG. *CR*, 483-488.

Michaelis, P. (2016). Der "Stand der Technik" im Kontext regulatorischer Anforderungen. *DuD*, 45.

Oppliger, R. (1992). *Computersicherheit. Eine Einführung*. Braunschweig, Wiesbaden.

Regulation (EU) 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 (GDPR). (2016). *OJ L* (119), 1.

Rosenbach, M., & Stark, H. (2014). *Der NSA-Komplex. Edward Snowden und der Weg in die totale Überwachung*. München: DVA.

Schaar, P. (2015). Globale Überwachung und digitale Souveränität. *Zeitschrift für Außen- und Sicherheitspolitik, 8*, 447-459.

Schallbruch, M., Gaycken, S., & Skierka, I. (2018). Cybersicherheit 2018-2020: Handlungsvorschläge für CDU/CSU und SPD. *DSI Industry & Policy Recommendations (IPR) Series*(1).

Schreibauer, M., & Hessel, T. J. (2007). Das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität. *K&R*, 616-620.

Schulze, T. (2006). Bedingt abwehrbereit. Schutz kritischer Informations-Infrastrukturen in Deutschland und den USA. Wiesbaden: VS Verlag.

Stoll, C. (1989). *The Cuckoo's Egg*. New York.

Wetzling, T. (2016). *The key to intelligence reform in Germany: Strengthening the G 10-Commission's role to authorise strategic surveillance*. Berlin: Stiftung Neue Verantwortung.

*Y2K Bug*. (21. February 2018). (Encyclopedia Britannica) Abgerufen am 31. March 2018 von https://www.britannica.com/technology/Y2K-bug

# Chapter 3: The Evolution of German Cybersecurity Strategy

**Abstract** This chapter traces the evolution of German cybersecurity strategy throughout the past two and a half decades. During this period, the German approach to cybersecurity strategy has developed from a civilian preventive one to a more comprehensive one, which today includes strategic military aspects.

In following, this chapter illustrates the development of cybersecurity strategy in three phases. The first phase (1991 to 2011) marks the emergence of cybersecurity as a strategic issue in the context of critical information infrastructure protection. In the second phase (2011 to 2016), the government consolidated existing policies after adopting its first national cybersecurity strategy in 2011. The Snowden revelations in 2013 lifted cybersecurity sharply up the political agenda. In the third phase, from 2016 to early 2018, Germany adopted its second national cybersecurity strategy that outlines a comprehensive approach to cybersecurity, as well as a national defence strategy, which for the first time emphasised the strategic military dimension of cybersecurity within a hybrid warfare context. In 2017 and 2018, intensified discussions about the offensive aspects of government hacking indicated a further turn in toward a more expansive cybersecurity policy.

**Keywords** Cybersecurity strategy, Critical infrastructure protection, IT security law, Snowden, White paper on security policy

### *3.1 Introduction*

Once a niche topic in German politics, cybersecurity has become a strategic national policy issue. At the time of writing, Germany has adopted three national cybersecurity-related strategies: The National Plan for the Protection of Information Infrastructures in 2005, the first Cybersecurity Strategy for Germany in 2011, and the second Cybersecurity Strategy for Germany in 2016.

Since the emergence of the first efforts to improve IT security at the national level, cybersecurity strategy in Germany has followed a technical and preventive approach, which focuses on the protection of IT systems and the civil defence of critical (information) infrastructures. To this date, the protection of critical infrastructures (CIs) remains an essential part of German strategic efforts in the field of cybersecurity. Besides, the enhancement of counter cyber-crime and espionage capabilities, as well as human resources and research and education are vital issues emphasised throughout all German national cybersecurity strategies NCSSs.  More recently, the government began to promote the strategic and military dimensions of cybersecurity, as well as the deployment of offensive use of IT, within the 2016 cybersecurity strategy, the 2016 national defence strategy, and the 2018 coalition government treaty.

Overall, German cybersecurity policy and strategy developments are situated in an environment shaped by a changing information security threat landscape, domestic political processes, (cyber) policy developments in other states (Cavelty, Cybersecurity in Switzerland, 2014, p. 10), and “focusing events” (Kingdon, 2003), such as the Snowden revelations.

Developments in cybersecurity strategy and policy occur in five dimensions, which the analysis will continuously take into account. These dimensions each have their own emphasis and discourse followed by different government departments (Cavelty, Cybersecurity in Switzerland, 2014), (Hathaway & Klimburg, 2012):

- Technical cybersecurity: referring to the protection of computing and communication technologies from unauthorized access or attack by malware and system intrusion.
- Critical infrastructure protection and national crisis management: relating to preventive and reactive approaches to protect critical infrastructures and society as a whole from technically induced accidents, physical, and cyber attacks.
- Counter cyber crime and espionage: referring to security efforts which enable the protection of information from businesses, governments, and individuals from theft, manipulation, or sabotage by criminals or nation state actors.
- Military: referring to cyber activities encompassing the protection of the armed forces' networks, as well as the enabling of the state's own network centric warfare capabilities and strategic cyber warfare.
- International diplomatic dimension: referring to the diplomatic negotiations and efforts by governments to keep the digital realm safe and secure from threats and inter-state conflict.

### *3.2 Phase 1, 1991 – 2011: IT Security and Critical Infrastructure Protection*

As the previous chapter outlined, cybersecurity policy was strongly linked to data protection and technical or organizational aspects of IT security for many years. Germany's efforts to address IT security in a systematic manner at the federal level began shortly after German reunification in late 1990, when it adopted the law establishing the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) (BSI, 1990). With the entering into force of the law in 1991, the BSI emerged as the successor of a German foreign intelligence service's (Bundesnachrichtendienst, BND) sub-office which had been responsible for technically protecting government secrets. The newly established BSI obtained the mandate to coordinate IT security efforts among government, industry, and society in Germany and would remain at the centre of most subsequent cybersecurity policy developments (see Chapter 4).

Throughout the 1990s, public awareness for "new" asymmetric and borderless security threats, such as international crime and terrorism, as well as for the vulnerability of societies' infrastructures grew. It became clear that modern societies were dependent on essential infrastructures that increasingly relied on inherently insecure IT-systems, and thereby posed "soft targets" for criminal or terrorist adversaries (Brunner & Suter, 2008). The disruption of vital infrastructures in sectors such as information and telecommunications, energy, water, banking and finance, and others, could trigger a national security crisis. Per the official German definition, critical infrastructures (CI) are "organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences" (Federal Ministry of the Interior, 2009, S. 4).

The United States (US) was the first country to adopt CI protection (CIP) policies. In 1996, President Bill Clinton set up the US President's Commission on Critical Infrastructure Protection (PCCIP). In 1997, the commission issued a report that concluded the US needed to see CIP through a national security lens and take preventive measures, with a focus on information security (President's Commission on Critical Infrastructure Protection, 1997). Motivated by the US PCCIP, the German Federal Ministry of the Interior (BMI) initiated an inter-ministerial working group on CIs (AG KRITIS) in 1997 (Schulze, 2006, p. 155). The working group comprised ministerial representatives, a steering committee, and a permanent office at the BSI. Its mandate was to describe possible threat scenarios for German CIs, conduct a vulnerability analysis of Germany's crucial sectors, suggest countermeasures, and delineate an early-warning system (Petermann, 2011). In its (unpublished) 1999 report, the group concluded that IT security and the protection of CIs would have high relevance for German national safety and economic well-being in the future (Kurzbericht der Ressortarbeitsgruppe KRITIS - Entwurfsversion 7.95, 1999). The terrorist attacks from 11 September 2001 raised additional awareness for threats to CIs and added urgency to ongoing efforts. Moreover, they led to intensified international cooperation in the area of CIP, for example within NATO, the OECD and the G8 (Schulze, 2006, S. 267).

After a number of internal sectoral CI studies conducted by the BSI (Brunner & Suter, 2008), the government finally presented a National Plan for Information Infrastructure Protection (NPSI) in 2005 (Bundesministerium des Innern, 2015), as well as a Baseline Protection Concept for the physical protection of CIs (Bundesministerium des Innern, 2005). The focus of the NPSI were information infrastructures, which it defines as "the entirety of the IT components of an infrastructure" (Bundesministerium des Innern, 2015). Since most CIs are increasingly digitised and interconnected, critical information infrastructures (CIIs) are an essential part of CIs. The very distinction between CIs and CIIs can seldom be made anymore today (Cavelty & Suter, 2012).

The NPSI is the first IT security-related national strategy in Germany. It directly links information infrastructures to national security, mentioning "new" threats such as the deployment of malware for criminal or terrorist ends, which could lead to an outage of vital information infrastructures. Overall, it is a preventive plan. It focuses on measures to strengthen IT security of the nation's IT-dependent infrastructures along three strategic objectives:

- Prevention – adequately protecting information infrastructures
- Preparedness – responding effectively to IT security incidents
- Sustainability – enhancing German competence in IT security and setting international standards

The implementation of corresponding measures, according to the strategy, is the shared responsibility of the government, critical infrastructure operators in particular, and society as a whole. In this spirit, the NPSI announces two CIP implementation plans – a mandatory one for the federal administration ("UP Bund" or "implementation plan Bund"), and a public-private one for critical infrastructures ("UP KRITIS" or "implementation plan for critical infrastructure protection (CIP)"). The respective implementation plans entered into force in 2007 (see Chapter 4).

Moreover, the NPSI defined the newly established "IT crisis response centre" as a national command, control, and analysis centre, which has become an integral part of national crisis management (see Chapter 4). Under the strategic objective "sustainability," the NPSI established the goal to promote the development of trusted German IT products and services, particularly the encryption industry – a theme that would reappear in many following policies. Regarding the international dimension, the strategy advocates intensified cooperation with European and international partners in the field of CIP and emphasises that the government will advocate its interests in international organizations and standard-setting bodies. In the 2000s, Germany did indeed actively participate in efforts at bringing forward the European Programme for Critical Infrastructure Protection (European Commission, 2006), which led to the Directive on European Critical Infrastructures in 2008, and contributed to the EU Network Information Security Directive in 2016.

Following the establishment of the CIP implementation plans in 2007, the government adopted its first comprehensive strategy for the protection of critical infrastructures (CIP strategy) in 2009. The CIP has a wider focus than the NPSI in that it focuses on all CIs, not only information infrastructures. It defines nine CI sectors, which it divides into "technical basic infrastructures" and "socio-economic service infrastructures" (Federal Ministry of the Interior, 2009).

| Technical basic infrastructures | Socio-economic service infrastructures |
|---|---|
| Power supply | Public health; food |
| Information and communication technologies | Emergency and rescue services, disaster control and management |
| Transportation | Parliament, government, public administration, law enforcement agencies |
| (Drinking-) water supply and sewage disposal | Finance, insurance business |
|  | Media, cultural objects (including cultural heritage objects) |

The strategy emphasises the interdependencies between the different infrastructures and cascading risks resulting from potential outages. For example, a power outage would affect multiple socio-economic service infrastructures, and the breakdown of public administration and government would significantly affect the functioning of technical basic infrastructures. It re-emphasises the shared responsibility between the federal government, state (Länder) and municipal authorities, CI operators, and industry, and outlines prevention, response, and sustainability mechanisms. It announces the establishment of security partnership platforms at all government levels and emphasises the need for international cooperation, especially at the European level.

Overall, the NPSI laid the groundwork for subsequent cybersecurity policies and the NCSS in 2011. The protection of CIs would remain a core strategic objective of all cybersecurity efforts to come. Together with the more comprehensive 2009 CIP strategy, it formed an integral part of future CIP policies specifically, including an updated CIP implementation plan and council in 2014, and the 2015 IT security law. The plan's goal to promote "trusted German IT" would remain a leitmotiv within German cybersecurity strategy and gain greater traction again in the wake of the Snowden revelations. Other goals related to effective cyber prevention and defence, the enhancement of BSI's functions and competencies, and a prioritization of IT security in education, training, and research and development, would equally be taken up by following strategies.

Moreover, the NPSI outlined a "whole of nation" approach, which emphasises the shared responsibility for IT security among the government, operators of critical infrastructures, private companies, and individuals. In a fast evolving area like digital policy, the rationale behind a whole of nation approach is that "specific 'cooperation' is needed from such a great number of non-state actors that a pure legislative approach would be largely unworkable in most democracies" (Hathaway & Klimburg, 2012, p. 31). To this date, cooperation among stakeholders is a building block of German cybersecurity policy. However, that cooperation has long focused on civilian government actors, with the role of military forces being marginal, and on industry on the non-state actor side, leaving out civil society stakeholders until the second NCSS in 2016.

### *3.3 Phase 2: 2011 – 2016: Building a Civilian Cybersecurity Strategy*

#### *3.3.1 The First National Cybersecurity Strategy for Germany*

In 2011, the federal German government adopted its first national cybersecurity strategy (NCSS) (Bundesministerium des Innern, 2011). The strategy is an advancement of the 2005 NPSI and the CIP implementation plan (Kullik, 2014, p. 92).

The NCSS widens the scope of cybersecurity policy from a somewhat technical infrastructure-specific to a societal strategic issue, which includes the economic, social, and cultural interactions taking place in the digital realm (Bundesministerium des Innern, 2011). It has an explicitly civilian focus, which can be complemented by the Armed Forces' (Bundeswehr's) protection measures of their capabilities as well as other measures to make cybersecurity "a part of Germany's preventive security strategy." Like the NPSI, an overall guiding principle of the NCSS is the whole of nation approach emphasising that public and private stakeholders have to act as partners and fulfil protection tasks together (Bundesministerium des Innern, 2011, p. 4).

Cybersecurity according to the NCSS is "the desired objective of the IT security situation, in which the risk of (global) cyberspace has been reduced to an acceptable minimum." This definition applies to civilian as well as military IT systems. Cyberspace, per the strategy's definition, is "the virtual space of all IT systems linked at data level on a global scale." Hence, non-internet connected IT systems are not considered part of cyberspace (Bundesministerium des Innern, 2011, p. 14).

The NCSS's stated vision is to make a substantial contribution to a secure cyberspace, thus "maintaining and promoting economic and social prosperity in Germany" (Bundesministerium des Innern, 2011, p. 4). A national strategy would ideally translate that vision into a national action plan, a set of strategic objectives to achieve it, and guidelines on how such resources are to be applied to reach stated objectives (Luiijf, Besseling, & de Graaf, 2013, p. 4). However, the document falls short of providing a clear guide of action to achieve specific strategic objectives. As Luiijfet al. (2013, p. 13) note in their comparative analysis of the NCSS of nineteen nations, the German NCSS presents a set of strategic priority areas which other NCSS present as action lines. Indeed, the document itself refers to the ten points it outlines as "objectives and measures":

1. Protection of critical information infrastructures
2. Secure IT systems in Germany
3. Strengthening IT security in the public administration
4. National Cyber Response Centre
5. National Cybersecurity Council
6. Effective crime control also in cyberspace
7. Effective coordinated action to ensure cybersecurity in Europe and worldwide
8. Use of reliable and trustworthy information technology
9. Personnel development in federal authorities
10. Tools to respond to cyber attacks

Among these objectives and measures, the protection of CIs has been most successfully implemented by the 2015 IT security law (see 3.3.2). The measures outlined in 2., 3., 4., and 5. contribute to this strategic objective. The enhancement of secure IT systems (2.) is a recurring topic in German cybersecurity policy. Its implementation has been partially successful. As announced under the action line, the BSI has intensified its information and awareness efforts on IT security risks, and the state has provided incentives for essential security functions certified by the state, such as electronic identity proof or De-Mail. However, uptake remains very low in practice (Initiative D21, 2017). The related goal to "strengthen Germany's technological sovereignty and economic capacity" through intensified incentivization of research and development in IT security has to date not yielded any tangible results, although this agenda has been vigorously promoted after the Snowden revelations (see Chapters 1 and 5). Hence, the development of secure IT in Germany and Europe remains an ongoing issue.

While the government did establish a national cyber response centre and a national cybersecurity council, the former has not been a success (see Chapter 4). An overarching effective national cybersecurity architecture with cross-institutional cooperation mechanisms is still lacking. The related goal to develop a set of comprehensive sustainable tools to respond to cyber attacks (10.) remains very vague in the strategy. Indeed, points like this one which does not contain any concrete propositions point to the overall weakness of the strategy document, namely its lack of an outline of strategic objectives, resources, and means with which to achieve those, and ways in which to use these resources.

The lack of qualified personnel to implement the federal government's cybersecurity policies has become one of the biggest challenges in cybersecurity policy today (Schuetze, 2018) – hence, personnel development in federal authorities (9.) is still highly relevant.

The NCSS highlights the growing importance of international cooperation for the improvement of cybersecurity for the fight against cyber crime (6.) and the prevention of inter-state conflict (7.). Germany has been a signatory of the Council of Europe's Budapest Convention on Cybercrime since 2001. Bilateral and multilateral cooperation among law enforcement agencies and with the private sector remain ongoing challenges, which Germany continues to address via national public-private partnerships and collaboration with international partners, including through the European Centre for Cyber Crime. With its reference to coordinated action at the EU and international levels (7.), the NCSS for the first time strategically outlines the international fora and organizations in which Germany should be active diplomatically. Due to the borderless nature of cyberspace and uncertain spillover effects of cybersecurity risks, its promotion of international norms is an essential and ongoing priority. Hence, the strategy underlines the enforcement of international rules of conduct, standards, and norms as one of the guiding principles for the attainment of cybersecurity goals. Germany had indeed been active in the United Nations Group of Governmental Experts (UN GGE) to negotiate norms of responsible state behavior in cyberspace since its inception in 2004. In this context, the NCSS links to the EU’s Digital Agenda and promotes the establishment of “a code for state conduct in cyberspace (cyber code)" at the international level, which should be signed by as many countries as possible, and which shall include confidence-building measures.

### *3.3.2 The IT Security Law*

As mentioned above, the protection of CIIs is among the most successfully implemented objectives of the first NCSS. The 2013 government coalition treaty outlining the ruling parties CDU/CSU and SPD’s political agenda included the proposition to adopt an “IT security law” that should build on previous efforts to improve critical infrastructure protection through regulation of operators of critical infrastructures. In June 2015, the government implemented this proposition and adopted one of the first laws regulating the IT security of CIs in Europe. Discussions about IT security mechanisms for CI operators had already been ongoing at the European level for a while, and the equivalent European Network and Information Security (NIS) directive followed only one year later, in 2016. The German IT security law is, in fact, a legislative act amending the existing law establishing the BSI. It entered into force in July 2015 and is a direct continuation and a vital consolidation of previous efforts to improve CI security. Since an ever-growing share of society and its CIs rely on inherently insecure digital technologies, related cybersecurity risks increased.

Therefore, the law imposes several obligations on the operators of critical infrastructures in seven sectors (energy, health, information and telecommunication technologies, transportation, water, food, and the finance and insurance sectors). Government and public administration as well as media and culture are classified as critical infrastructures, but already regulated by other legislative acts and therefore not included into the IT security law. The law creates mandatory reporting requirements, under which CI operators need to report potential and actual significant IT security incidents to the BSI. Besides the BSI, the BKA will have a role in investigating cyberattacks against CIs in this context. Such reporting requirements had already been suggested by the EU in 2013 (Bendiek, 2013). Decision-making in the

German and other European governments saw incident information sharing as a necessary measure to ensure adequate CIP. Voluntary information sharing mechanisms had only been partially effective. CI operators and other private companies do not have a natural incentive to share incident information, which can result in reputational and financial loss as well as in potential liability claims. This is why policymakers pushed for the institutionalization of incident information sharing (Zedler, 2016, p. 39).

Moreover, CI operators need to implement mandatory minimum IT security standards which correspond to the “technical state of the art.” The respective operators within their sectors determine that "state of the art". After an elaborate coordination process between sectoral industry associations and governmental experts, the Ministry of Interior issued two regulations which further specify which critical services will be affected by the law regarding specific threshold values. The Ministry issued the respective regulations in May 2016 for the energy, water, food, and ICT sectors, and in 2017 for the health, finance and insurance, transportation, and logistics sectors. The services identified in the regulations have to implement the necessary standards and legal requirements within two years until mid-2018 and mid-2019, respectively.

### *3.3.3 The Snowden Revelations*

As the previous chapter illustrated, the revelations by Edward Snowden in 2013 constitute a “focusing event” (Kingdon, 2003) in German cybersecurity policy and intensified the public debate about data security, surveillance, and espionage. In the wake of the revelations, cybersecurity became a highly political matter. Counter-espionage and privacy became defining issues permeating official policies and strategic documents, such as the 2013 coalition government treaty or the German government’s Digital Agenda from 2014 (Bundesregierung, 2014). The once prominent calls for “technological” or “digital sovereignty” regarding enhancing control over data flows in Germany or strengthening the German IT industry never developed into a coherent strategy. Today, “digital sovereignty” is a political expression used for various measures ranging from the enhancement of data protection and informational self-determination of individual citizens to promoting the national IT industry and reducing the dependence on foreign IT components (Eckert, 2013), (Bitkom e.V., 2015).

An important consequence of the Snowden revelations was the establishment of a parliamentary inquiry committee investigating the NSA’s data collection practices, as well as German intelligence agencies’ cooperation with the NSA and other “Five Eye Alliance” intelligence services such as the British GCHQ. As mentioned in the previous chapter, the committee found that the German Foreign Intelligence Service (Bundesnachrichtendienst, BND) had closely collaborated with the NSA in monitoring international telecommunications on German territory (Rosenbach & Stark, 2014) (Deutscher Bundestag, 2017), and thereby engaged in illegal practices, according to German constitutional law experts (Bäcker, 2014) (Wetzling, 2016). In October 2016, the German parliament adopted a controversial law that expanded the agency’s surveillance powers (BND-Gesetz, 2016). On the basis of this law, the BND now has the authority to collect and process information including personal data from telecommunications networks on German territory, as long as the data stems from communications between foreigners.

### *3.4 Phase 3, 2016 – 2018: Consolidating a Comprehensive Civilian-Military Approach to Cybersecurity*

In November 2016, the German federal government adopted its second NCSS. In July of the same year, the government passed its second national defence strategy, the "White Paper on German Security Policy and the future of the Bundeswehr (Armed Forces)" (Federal Government, 2016). The White Paper for the first time specifically outlines strategic military aspects of cybersecurity.

#### *3.4.1 The 2016 White Paper on German Security Policy and the Future of the Bundeswehr*

The 2016 White Paper is the German Armed Forces' response to a rapidly globalizing, high-tech threat environment. It presents the response to threats emerging from the cyber and information domain as a major security policy challenge for Germany. The term "cyber" appears more than 70 times in the 139-page document. Cyber attacks, and other threats, such as epidemics and transnational terrorism, are part of new risks in a globalized world, in which internal and external boundaries become blurred.

Apart from cyber attacks that can cause physical damage, the White Paper mentions disinformation campaigns as a particular challenge for open and pluralistic societies, referring to them as "the use of digital communication to influence public opinion, for example through hidden attempts to sway discussions on social media and by manipulating information on news portals" (Federal Government, 2016, p. 36). Cyber attacks and disinformation campaigns are instruments of hybrid warfare, which aims to not only militarily, but also politically destabilize the opponent.

The White Paper's response to the successful prevention of hybrid threats is "whole-of-society" resilience. According to the document, resilience can only be achieved by efficiently linking relevant policy areas, including better CIP, disaster control, civil defence, and border controls, among others. International cooperation with NATO and EU allies and diplomatic measures such as confidence-building and conflict resolution mechanisms become crucial.

Concerning cyber capabilities, the White Paper declares that the defence against cyber attacks necessitates high-value defensive and offensive capacities. Following a "whole-of-government" approach, the Bundeswehr needs to cooperate with civilian actors, such as research institutions and industry, develop Bundeswehr cyber capabilities, and increase the robustness of its weapons systems. Moreover, it needs to recruit "the very best personnel by creating attractive career paths in cyber."

When the government unveiled the White Paper, the Ministry of Defence had already adopted an internal strategy that established a dedicated "cyber and information command" (CIR command) in the Bundeswehr. Chapter 4 further elaborates on the CIR command, which is operational since April 2017.

### *3.4.2 The 2016 Second National Cybersecurity Strategy, 2016*

In November 2016, the government adopted a second, updated NCSS (Bundesministerium des Innern, 2016). Compared to the first strategy, it outlines strategic objectives, means, and action items in a more coherent and structured way. This decisive character is the result of a longer and more comprehensive drafting process, as well as an advanced stage of experience with cybersecurity among decision-makers. While policy-makers had drafted the first NCSS in a quick and somewhat un-coordinated process, the second NCSS emerged from a year-long coordination process among different ministries. The Ministry of Interior led both drafting procedures but the second one was influenced by the Ministry of Defence and the Federal Foreign Office to a much greater extent than the 2011 strategy.

It outlines four areas of action:

- Safe and Self-determined Action in a Digitised Environment

This first area of action adopts a user-centric perspective to cybersecurity. Most other strategies and policies had not focused on the specific needs of individual users, but rather on society as a whole. The NCSS promotes the enhancement of digital literacy, awareness raising, secure e-identities, as well as strengthened certification and approval of ICTs and the introduction of an IT security "quality label." Such a label should make it easier for consumers and small and medium-sized enterprises to assess the security of IT products and thereby strengthen trust in IT.

The section also outlines how digital innovation across society can be designed securely. Accordingly, new policies, for example in the areas of e-health or mobility, should take into account both the economic benefits of new digital business models as well as the security of society and consumers. It advocates an evaluation of responsibilities and liability laws for vulnerable software. Moreover, the section promotes IT security by design.

As a final cross-cutting issue, the section announces new investments in various research and development initiatives and clusters. Here, the strategy can point to several existing successful research initiatives, which shows that the government has continuously invested in research and development initiatives in the field of IT.

- A Joint Effort of Government and Industry

In this area, the strategy emphasises the continued need for trusted public-private cooperation and again takes up the cooperative "whole of nation" approach already advocated in previous strategies. This action area focuses on CIP, referring to the IT security law and the CIP implementation plan, and the enhancement of counter cyber crime and espionage measures to protect German companies. It also advocates industrial policy measures to strengthen the German IT industry. The term "technological sovereignty" is notably absent from this section, but it outlines goals to promote better the development of key technologies and quality IT "made in Germany." The NCSS further proposes measures to improve cooperation with providers in the defence against cyber attacks, for example, IoT botnets. Indeed, the government has passed corresponding measures within the adoption of the EU NIS Directive implementation law in May 2017, which has extended the legal basis for Internet providers to conduct “light packet inspection” and conduct sinkholing and network blockage (Schallbruch, 2017).

- An Effective and Sustainable Cybersecurity Architecture

In this section, the strategy addresses some shortcomings in the national cybersecurity architecture and proposes measures for better coordination and the enhancement of cyber defence effectiveness (see chapter 4). It announces the further development of the national cyber response centre established in 2011 and the strengthening of onsite analysis and response capacities through so-called "Mobile Incident Response Teams" (MIRTs). It also aims to strengthen CERT structures in Germany, to better protect the federal administration, and to strengthen cooperation between federal and state level authorities for cybersecurity.

One of the section's most essential propositions is the goal to gain and develop more IT security personnel and efficiently using available resources. However, the strategy misses mentioning any concrete numbers or metrics, which leave the propositions vague.

The NCSS also announces to intensify law enforcement activities in cyberspace through the deployment of new data analysis and forensic technologies, as well as better personnel resources. Furthermore, it announces measures to better fight cyber espionage and sabotage, including the strengthening of the domestic intelligence service’s (Bundesverfassungsschutz) capabilities and an early-warning system for the foreign intelligence service BND. In addition, the section announces the establishment of a central office for IT in the security sphere (ZITiS), which will develop cyber capabilities, including hacking tools, for police agencies and domestic intelligence services. Another novel aspect in this section is the explicit reference to the military dimension of cybersecurity and the Armed Forces' 2016 White Paper.

The announcement of these capabilities has been controversially discussed. For the first time, an NCSS transparently outlines offensive capability development schemes for intelligence and police agencies. This development constitutes a departure from earlier strategies and policies, which exclusively emphasised the state's defensive capabilities and approaches.

In comparison to cybersecurity strategies and policies of other nations, however, this is not unusual. The US, France or the UK, for example, had already long endorsed offensive and defensive capabilities within their comprehensive NCSS. The growing number, complexity, and sophistication of cyber threats further contribute to the necessity of nations to outline responses, including offensive capabilities.

- The Active Positioning of Germany in European and International Cybersecurity Policy Discussions

In this NCSS, the international diplomatic dimension of cybersecurity has finally become a key strategic priority. The government proclaims that it aims to actively shape an effective European cybersecurity policy, to further advance the NATO cyber defence policy, and to actively participate in shaping cybersecurity internationally, including norms for responsible state behavior and confidence-building measures in the UN or the OSCE.

Germany has long been an active part of the UN GGE negotiations. In 2015, the German Foreign Ministry led a new round of negotiations on responsible norms for state behavior. Unfortunately, the negotiations ended without consensus, and for now, the process is on halt at the UN level. It would be in

Germany's best interest to (re-)initiate norms or confidence-building processes at the international level (see Chapter 5).

With its goal to engage in global cyber capacity building efforts, the strategy does not only promote a foreign policy, but also a development policy goal. This point underlines the importance of strengthening cybersecurity internationally in the face of borderless threats. Finally, as in previous strategies, Germany plans to enhance international cooperation in the fight against cyber crime.

### *3.4.3 Taking Stock of Past Developments for Future Cybersecurity Strategies*

Since 2005, the German government has successively expanded its cybersecurity strategy. The latest NCSS covers almost all relevant fields of action. Nevertheless, German cybersecurity policy lacks distinct strategic cornerstones and clear priorities. A national strategy should ideally identify strategic objectives (“ends”), pinpoint the resources available to reach those objectives (“means”), and provide a guide to how such resources are to be applied to reach stated objectives (“ways”) (Lindstrom & Luiijf, 2012). While the 2016 NCSS has a broader scope than the first NCSS from 2011, it constitutes a work program for respective federal government agencies rather than a strategic program. It outlines objectives and action lines but does not delineate clear responsibilities and does not allocate measurable resources for the implementation of the goals. Moreover, it lacks concrete measurable goals against which achievements can be evaluated.

The 2018 coalition government treaty outlines several fields of action for the government, which mainly complement existing lines of action in the area of research and development and the enhancement of the security of IT products (CDU/CSU & SPD, 2018). It outlines the government’s plans to expand the existing IT security law to an “IT security law 2.0”, which shall increase the responsibilities of manufacturers and providers of IT products beyond the area of critical infrastructures. It promises to enhance research and development in the field of IT security, to set up competence centres, and to make secure electronic identification and end-to-end encryption solutions more easily accessible to citizens. Besides, it aims to develop minimum IT security standards for internet connected products in cooperation with industry and introduce a quality label indicating the security level of IT products for consumers. On the institutional side, it aims to strengthen the BSI’s role in cybersecurity and to create a new cyber alliance with industry to enhance trusted cooperation between industry and public authorities.

Hence, the coalition treaty presents a range of necessary IT security measures that have the potential to increase the level of technical protection of IT in Germany. However, it almost entirely omits political questions of cybersecurity. These issues include the debated government’s expansion of offensive capabilities for government hacking purposes and discussions about active cyber defence under the umbrella term “hack backs.” This leaves a number of strategic questions unanswered, which Chapter 5 will discuss in more detail.

### *3.5 References*

Bäcker, M. (2014). *Erhebung, Bevorratung und Übermittlung von Telekommunikationsdaten durch die Nachrichtendienste des Bundes. Stellungnahme zur Anhö- rung des NSA-Untersuchungsausschusses*.

Bendiek, A. (2013). *Kritische Infrastrukturen, Cybersicherheit, Datenschutz. Die EU schlägt Pflöcke für digitale Standortpolitik ein*. Berlin: Stiftung für Wissenschaft und Politik.

Bitkom e.V. (2015). *Digitale Souveränität - Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa*. Berlin.

Brunner, E. M., & Suter, M. (2008). *International CIIP Handbook 2008/2009*. Zurich: Center for Security Studies Zurich.

BSI. (1990). BSI-Errichtungsgesetz vom 17. Dezember 1990 (BGBl. I S. 2834), zuletzt geändert durch Artikel 11 der Verordnung vom 25. November 2003 (BGBl. I S. 2304).

*Bundesgesetzblatt Teil I, Nr.67 vom 30.12.2016, Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes*. (2016, December 30). Retrieved from https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl116s3346.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl116s3346.pdf%27%5D__1523778724203

Bundesministerium des Innern. (2005). *Schutz Kritsicher Infrastrukturen - Basisschutzkonzept*. Berlin.

Bundesministerium des Innern. (2011). *Cyber-Sicherheitsstrategie für Deutschland*. Berlin.

Bundesministerium des Innern. (2015). *Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI)*. Berlin.

Bundesministerium des Innern. (2016). *Cyber-Sicherheitsstrategie für Deutschland*. Berlin.

Bundesregierung. (2014). *Digitale Agenda für Deutschland* .

Cavelty, M. D. (2014). *Cybersecurity in Switzerland*. Heidelberg and Berlin: Springer Verlag.

Cavelty, M. D., & Suter, M. (2012). The Art of CIIP Strategy: Tacking Stock of Content and Processes. In J. L. (Eds.), *Critical Information Infrastructure Protection* (pp. 15-38). Berlin, Heidelberg: Springer-Verlag.

CDU/CSU, & SPD. (2018). Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land. Koalitionsvertrag zwischen CDU/CSU und SPD, 19. Legislaturperiode. Berlin.

Deutscher Bundestag. (2017). *Abschlussbericht des 1. Untersuchungsausschusses (NSA) vom Juni 2017, Drucksache 18/12850*. Berlin.

Eckert, C. (2013, 11 23). Digitale Vision für Europa. *FAZ.NET*.

(2017). *eGovernment Monitor 2017*. Initiative D21.

European Commission. (2006). *COM(2006) 786 final - Communication from the Commission on a European Programme for Critical Infrastructure Protection*. Brussels: Commission of the European Communities.

Federal Government. (2016). *White Paper on German Security Policy and the Future of the Bundeswehr*. Berlin.

Federal Ministry of the Interior. (2009). National Plan for the Protection of Critical Infrastructures.

Hathaway, M., & Klimburg, A. (2012). Preliminary Considerations: On National Cyber Security. In A. Klimburg, *National Cyber Security Framework Manual* (pp. 1-43). Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Kingdon, J. W. (2003). *Agendas, alternatives, and public policies*. New York: Harper Collins College Publishers.

Kullik, J. (2014). *Vernetzte (Un-)Sicherheit? Eine politisch-rechtliche Analyse der deutschen Cybersicherheitspolitik*. Hamburg: Kovač.

*Kurzbericht der Ressortarbeitsgruppe KRITIS - Entwurfsversion 7.95*. (1999, December 03). Retrieved from http://userpage.fu-berlin.de/~bendrath/Kritis-12-1999.html

Lindstrom, G., & Luiijf, E. (2012). Political Aims and Policy Methods. In *National Cybersecurity Framework Manual* (pp. 44-65). Tallinn: NATO CCDCOE.

Luiijf, E., Besseling, K., & de Graaf, P. (2013). Nineteen National Cyber Security Strategies. *International Journal of Critical Infrastructure Protection, 9*(1-2), 3-31.

Petermann, T. (2011). *Was bei einem Blackout geschieht: Folgen eines langandauernden und großflächigen Stromausfalls*. edition sigma.

(1997). *President's Commission on Critical Infrastructure Protection*. Washington DC: US Government Printing Office.

Rosenbach, M., & Stark, H. (2014). *Der NSA-Komplex. Edward Snowden und der Weg in die totale Überwachung*. München: DVA.

Schallbruch, M. (2017, May 14). *IT-Sicherheit: Bundestag verabschiedet NIS-Umsetzungsgesetz*. Retrieved from CRonline: https://www.cr-online.de/blog/2017/05/14/it-sicherheit-bundestag-verabschiedet-nis-umsetzungsgesetz/

Schuetze, J. (2018). *Warum dem Staat IT-Sicherheitsexpert:innen fehlen*. Berlin: Stiftung Neue Verantwortung.

Schulze, T. (2006). Bedingt abwehrbereit. Schutz kritischer Informations-Infrastrukturen in Deutschland und den USA. Wiesbaden: VS Verlag.

Wetzling, T. (2016). *The key to intelligence reform in Germany: Strengthening the G 10-Commission's role to authorise strategic surveillance*. Berlin: Stiftung Neue Verantwortung.

Zedler, D. (2016). *Zur strategischen Planung von Cyber Security in Deutschland*. Köln: Lehrstuhl Internationale Politik, Universität zu Köln.

# Chapter 4: The organisation of cybersecurity

**Abstract** Cybersecurity as a responsibility of public institutions and as a field of cooperation between the government and the private sector is at odds with existing responsibilities. The protection of digital systems concerns a wide range of public services and organisations. In Germany, this cross-cutting nature of cybersecurity meets an already strongly subdivided structure of responsibilities for state security. Also, cybersecurity requires far greater cooperation between the state and business than traditional security policy challenges, since the majority of systems affected by cyber-attacks are not within the state's sphere of responsibility. As a result, there are various forms of public-private cooperation. These factors lead to a confusing and immature allocation of cybersecurity responsibilities.

**Keywords** Federal Office for Information Security (BSI); Law Enforcement, Intelligence Service, Cyber Command, Cyber Defence Centre, Public Private Partnerships

## *4.1 Particularities of German Law Enforcement, Intelligence, and Public Security Organisations*

In Germany's state organisation, responsibility for public security is spread across numerous different actors (Graulich, 2016) (Schönbohm, 2011, S. 71). Institutional separation rules characterise the landscape of internal security as well as sophisticated forms of cooperation rules. Two significant separations mark Germany's security architecture: the federal split between the federal and state governments and the functional split between police forces and intelligence services. The responsibility for police primarily lies with the Länder (states) with their 16 police organisations. The federal police organisations are relatively small and have limited powers. The focus of the intelligence services work is on the federal level with domestic, foreign, and military intelligence services. By comparison, Länder's domestic intelligence services are relatively modest in terms of responsibilities and resources. While intelligence services are subject to mainly executive and in the second-place parliamentary control and oversight, police authorities' prosecution activities are supervised by the judiciary. This interferes with ministerial control of the police's hazard prevention activities. Some special regulatory agencies have police-like powers for certain areas of operation. Concerning cybersecurity, the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) should be mentioned first and foremost. However, the various supervisory agencies for critical infrastructures also have security tasks that now reach into cyberspace.

At the political level, the primary responsibility for internal security lies with the interior or home affairs ministers of the federal and state governments. They are in principle responsible for police forces and intelligence services; the ministries of justice have traditionally played a lesser operational role, despite their attorneys' duties as public prosecutors, but have an important role in the further development of internal security legislation due to their responsibilities in criminal law and criminal prosecution law. The Conference of Interior Ministers of the Länder (Innenministerkonferenz, IMK) plays an important role in coordinating national security policy. The Federal Minister of the Interior (Bundesminister des

Innern, BMI) also attends the meetings. The conference and its various working groups decisively coordinate Germany's practical security policy (Hegele & Behnke, 2017).

The BSI plays a unique role. It was established in 1991 by federal law (BSI-Errichtungsgesetz, 1990). It has the overall task of promoting the security of information technology. As a result of several amendments to the law in 2009, 2015, and 2017, lawmakers successively extended the range of tasks, so that the BSI today assumes the function of a central cybersecurity authority in Germany. The BSI has neither police nor intelligence powers, but with regard to cyberspace, it fulfils both police and intelligence functions. The Office’s mission can be divided into three areas in a very simplified way: Establishing and reviewing the product and systems security, overseeing the implementation of cybersecurity measures, and operational cyber defence.

In the area of defining and testing product and system security, the BSI is initially the central accreditation and certification body for IT security in Germany. IT security certificates are only issued by BSI-accredited bodies. The BSI is also authorized to investigate the IT security of the market's products and services and may issue public warnings if a lack of IT security of products or services is detected. Wherever there is a statutory requirement for IT security in Germany, the legal provisions refer to the relevant guidelines or specifications of the BSI. Between 2013 and 2017 alone, 45 additional laws and regulations were adopted which entrusted the BSI with such tasks (Schallbruch, 2017, S. 649). Thus, the BSI has acquired a kind of "official authority" in Germany over what secure information technology is and what not. The Office's second area of responsibility concerns the supervision of the implementation of cybersecurity measures. Historically, the BSI has always carried out this task for crypto devices that protect state secrets. They have been approved by the BSI since the Office was established. This competency was successively extended, most recently by the IT security law to the entire area of critical infrastructures. The mostly private operators of the infrastructures have to protect their relevant IT systems against cyber-attacks according to the "state of the art" and have to prove this to the BSI. If the security measures are not sufficient, BSI can issue complaints and impose fines. In parallel to competencies concerning critical infrastructure security, Germany has also delegated enforcement powers for digital services (online marketplaces, search engines, and cloud services) regulated by the European Network and Information Security (NIS) Directive to the BSI (Schallbruch, 2017, S. 800). As a result, the Office can take up cybersecurity issues for almost any relevant form of technology through its investigation and warning competencies and address them by means of penalties or public notices. Thus, the BSI has an extremely high level of duty to keep an eye on the entire realm of IT security, especially since the BSI is legally obliged, at least vis-à-vis the critical infrastructures, to issue a warning without delay if relevant security evidence is available (Section 8a.2 No. 4 BSI Act). If the BSI neglects this obligation, liability claims against the state are conceivable.

The third area of responsibility of the BSI is cyber defence. Since 2009, the Office has been responsible for supporting the federal government authorities in fending off cyber-attacks. To this end, the BSI monitors the federal government's networks, investigates security incidents and takes defensive measures. However, active operations outside the federal networks are in general not permitted for the BSI. Here, the Office must cooperate with the public prosecutors' offices and police forces. Since 2015, the BSI has also been involved in the cyber defence of critical infrastructure operators. They must report cybersecurity incidents to the agency, which draws up a situation report from them and in turn helps companies to defend themselves by providing them with information. The German implementation law of the EU NIS Directive has extended this task: Due to the newly created Section 5a of the BSI Act, the Office is now also entitled to help with cyber defence at the request of a critical infrastructure operator. However, this new power is limited to the systems concerned. The BSI does not have any further (police) powers outside of these systems, e.g. within provider or telecom networks. Here the BSI has to ask the competent police department for help. All in all, however, the BSI has meanwhile assumed a central position for cybersecurity in Germany due to the multitude of new responsibilities that government and parliament assigned to the agency (Bötticher, 2015, S. 90).

The police powers in Germany are exercised primarily by the Länder with the sixteen state police forces. They form the backbone of the German police force. The federal police authorities, the Federal Police (Bundespolizei), the Federal Criminal Police Office (Bundeskriminalamt, BKA) and the Customs Investigation Bureau (Zollkriminalamt, ZKA) are only responsible for specific issues. As a rule, prosecution for cyber-attacks is a matter for the state police under the supervision of the local public prosecutor's office. Many Länder have set up so-called focal public prosecutors' offices for cyber crime, e. g. the state of Lower Saxony (Innenministerium Niedersachsen, 2011). Most Länder have also set up central units for cyber crime at their state criminal police offices, which are typically tasked by public prosecutors with cyber-related investigations. At the federal level, the Federal Criminal Police Office (BKA) is particularly important. The Federal Police is primarily a protective police force with responsibilities for border security, airports, and railway police and has only marginal duties in the area of cybersecurity. The Customs Investigation Bureau (ZKA), as the financial police in particular, also plays no significant role in cybersecurity.

The BKA has the role of a core unit of the German police, which collects and processes information on a national basis. Accordingly, the BKA publishes annual federal situation reports on cyber crime (Bundeskriminalamt, 2016). However, the Office also has its own cybersecurity powers. According to Section 4.1 No. 5 of the BKA Act, the Office is also responsible for cyber crime if attackers target the federal government or critical infrastructures. In this case, the appropriate prosecutor's office in the respective Land entrusts the BKA with the investigation. However, the investigation capabilities of the BKA in cyberspace are very limited. New investigative powers such as source telecommunications monitoring and secret access to IT systems (i.e. online searches), which the BKA received in 2017, may only be used for particular crimes. Cyber-attacks are only part of this if they are in the context of espionage. The BKA has no authority in the field of cybersecurity to prevent threats, i. e. to act in the run-up to a criminal offence. It is the state police that is in charge here.

With the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz, BfV) and the constitutional protection offices of the federal states, Germany has 17 domestic intelligence services. Besides, there is the Military Counter-Intelligence Service (Militärischer Abschirmdienst, MAD), which is, however, only responsible for activities against the German Armed Forces or those involving Bundeswehr personnel. The Federal Office for the Protection of the Constitution is mainly concerned with the investigation of right-wing and left-wing extremism, foreigners' extremism, and terrorism. However, their responsibility for counterintelligence also plays an important role in the area of cybersecurity. According to the Federal Office's observations, foreign intelligence services increasingly carry out their espionage activities digitally. According to the BfV, Germany is the target of numerous cyber espionage attacks of Russian and Chinese origin in particular, but frequently also from Iran (Bundesministerium des Innern, 2017, S. 260). In the context of cybersecurity, it is also the task of the Federal Office for the Protection (BfV) of the Constitution to collect information about attacks and attackers from open sources as well as by using intelligence resources. The Office for the Protection of the Constitution is entitled to support cyber defence. However, it has no police powers and may not carry out searches or arrests. This restriction is the result of strict segregation of police and intelligence powers. Following the experience with the secret state police of the Nazi dictatorship, the Allied forces introduced a so-called separation order as a condition for drafting the (West) German constitution after World War II. The order of 1949 has constitutional status and also limits the personal, organisational and informational cooperation between the police and the intelligence services (Fremuth, 2014).

The division of responsibilities between the federal and state constitutional protection authorities is not entirely clear. Both the BfV and the state authorities are responsible for counterintelligence. The federal office is not only responsible for coordinating the Länder offices, but also has independent powers in the case of efforts directed against the federal republic, extending beyond the area of a Land or concerning Germany's foreign affairs (Section 5.1 of the Federal Constitution Protection Act). All of these prerequisites may be present in a cyber attack. In the event of a cyber attack against a federal agency, such as the attack against the federal government's network in the winter of 2018, the competence of the federal office is obvious. The situation is different in the case of attacks against businesses, for example. When a cyber attack is detected, neither the originator nor the objective of the attack can typically be identified. Responsibilities of state and federal domestic intelligence services are widely in parallel. Accordingly, the federal and state offices must consult each other on a case-by-case basis. The federal office has no right to steer the state offices. The BfV has a specialized group for electronic attacks. Some Länder have also set up specialised organisational units in their constitutional protection agencies, such as Bavaria. With its Cyber-Alliance Centre established specifically for this purpose, the Bavarian State Office for the Protection of the Constitution is in charge of defending even against cyber-attacks against the private sector (Bayerisches Staatsministerium des Innern, 2013). Other Länder have refrained from doing so. Some states such as North Rhine-Westphalia and Bavaria have also given an authorization to secretly intrude into IT systems to the intelligence services (e. g. Section 5.2 No. 11 VSG NW (Gesetz über den Verfassungsschutz in Nordrhein-Westfalen (Verfassungsschutzgesetz Nordrhein- Westfalen, 2016) or Article 10 BayVSG (Bayerisches Verfassungsschutzgesetz (BayVSG) vom 12. Juli 2016 )). The BfV has no such right. At federal level, only the BKA is entitled to do so.

With the Federal Intelligence Service (Bundesnachrichtendienst, BND), Germany has a single foreign intelligence service, which also performs the function of a military intelligence service abroad. The Federal Chancellery steers its operations. The BND's mission is to collect a wide range of security-relevant information abroad. For this purpose, it uses standard intelligence tools, human sources (HUMINT), open sources of information (OSINT) as well as signals intelligence generated by the monitoring of electronic communications (SIGINT). The Federal Chancellery defines the specific objectives of the BND in a so-called "mission profile". The Bundestag redefined the BND's powers in 2016, not least concerning electronic cooperation with foreign intelligence services such as the NSA (Karl & Soigne, 2017). In the future, the BND will also increasingly focus on supporting cyber defence within the scope of its powers to monitor electronic communications. As part of the task called "SIGINT Support to Cyber Defence (SSCD)" by the BND, the BND collects information abroad on current or upcoming cyber-attacks, malware, etc. (Bundesnachrichtendienst, kein Datum). Active cyber defence activities such as Cyber Networks Operations (CNO) are not a task of the BND.

In the context of cybersecurity in critical infrastructures, the supervisory agencies established for each sector also have a role to play. Some infrastructure sectors are in principle subject to federal supervision, such as energy supply, telecommunications or finance, while the Länder authorities largely supervise other sectors such as health care, food supply, or transport. All sectoral supervisory authorities are usually also responsible for the proper functioning of the infrastructure sectors. With respect to cybersecurity issues, they operate alongside the BSI. The role of the supervisory authorities is more significant if they have their own sectoral statutory powers for cyber, such as in the energy supply, telecommunications, or finance sectors. The agencies operating there, such as the Bundesnetzagentur (BNetzA) for telecommunications and energy or the Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht, BAFin), receive reports of cyber-attacks in parallel with the BSI and may impose severe sanctions against companies that do not comply with their security obligations. In addition to the sectoral supervisory authorities, the Federal Government runs a Federal Office of Civil Protection and Disaster Assistance (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, BBK), which plays a coordinating role in the area of critical infrastructures and also conducts regular crisis exercises, including those in the field of cyber defence. As early as 2011, the federal and state authorities had already trained in an exercise called "LÜKEX 2011" to deal with a cyber attack. Approximately 3000 persons in various agencies, the German Armed Forces, and 45 critical infrastructure companies were involved in a table-top exercise under the direction of the National Crisis Management Group in the BMI (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2012). In 2020, another large-scale Bund-Länder cyber exercise is to take place, this time with the scenario of a cyber attack on critical infrastructures and the problem of maintaining government functions (Innenministerkonferenz, 2017, S. 24).

### *4.2 German Military's Role in the Cyber Realm*

The German Bundeswehr is a defence army and a parliamentary army. Its fields of operation are very limited by the German constitution. Also, deployments require the explicit approval of the German Bundestag. The main purpose of the Bundeswehr is to defend Germany against armed attacks from outside. Beyond defence, the military may only be deployed in narrowly defined cases, which are expressly regulated by the constitution (Marxsen, 2017). The German constitution makes a differentiation between the Bundeswehr's intervention below the threshold of deployment and explicit deployments approved by parliament. Below the threshold, the German Armed Forces can, for example, take measures to secure themselves in the cyber sector. They are, however, limited because they do not allow any interference with the legal rights of third parties, i. e. no access to computer systems outside the German armed forces' networks. Cases of cyber defence, in which the German Armed Forces provide assistance to other authorities within the framework of their powers (so-called administrative assistance), are not regarded as deployments. The Bundeswehr could, for example, support the BSI or the police forces in cyber defence activities on a selective and individual basis. However, administrative assistance is not sufficient as a legal basis for lasting institutionalised cooperation in which the military itself takes over cyber defence measures (Marxsen, 2017, S. 546).

Cyber defence operations carried out under its own responsibility and affecting third parties must, in any case, be characterised as a deployment of the German Federal Armed Forces. It needs a legal basis for this. For domestic missions, only the competence of the German Armed Forces for defence is applicable. A prerequisite for this is an armed attack on the federal territory. It must be essentially the same as a military attack, both regarding its effects and its originator, a foreign state. Other cyber-attacks fall within the competence of internal security authorities (Marxsen, 2017, S. 548). Besides, the Bundeswehr would always need parliamentary approval for cyber defence missions. No problem at all is the execution of cyber operations within the framework of foreign missions of the German Federal Armed Forces, for which a mandate of the UN, NATO, or EU exists and which the Bundestag has approved. In this context, not only conventional weapons may be used, but cyber operations may be carried out as well.

The legal framework for the deployment of the German Federal Armed Forces in cyber defence is thus considerably restricted. The Bundeswehr will only be able to fend off cyber-attacks in Germany if it can record a clearly belligerent cyber operation and obtain the approval of the Bundestag. Accordingly, the Bundeswehr has set up only tiny forces for Cyber Network Operations (CNO). They have never been deployed a single time, at least until 2015 (Bundesministerium der Verteidigung, 2015, S. 3). At the same time, however, the cyber domain has developed internationally as a central field of action for the military, without the threshold of armed attacks being typically surpassed. The Bundeswehr, too, must prepare itself for this because it has to carry out cyber operations within the framework of mandates, at least for its own security and also for the preparation of missions abroad. Therefore, the development of cyber skills is an explicit will of the German government (Bundesministerium des Innern, 2016, p. 33).

Based on this demand, in 2017 the German Armed Forces set up a "Command Cyber and Information Space (Kommando Cyber- und Informationsraum, CIR), a separate military operational area for operations in cyberspace. Some 14,000 soldiers are expected to be deployed. A large part of the posts are transferred from existing units. Only 300 additional posts are planned (Bundesministerium der Verteidigung, 2016, S. 22). The concept of the CIR command follows a comprehensive approach to combine all forces needed for the reconnaissance, operation, and management of cyberspace in one military organisational area. The mission includes the handling of communications as well as the operation of command support systems, the protection of the Bundeswehr's IT systems against attacks as well as the execution of cyber network operations within the framework of deployments. In the new structure, the Centre for Communications and the Centre for Geoinformation Systems for the Information supply, the Bundeswehr IT Centre (IT-Zentrum Bw) for system operation, the Centre for Cybersecurity of the Bundeswehr (Zentrum für Cybersicherheit der Bundeswehr, ZCSBw) for the protection of its own systems and the Centre for Cyber Operation (Zentrum für Cyber-Operationen, ZCO) for CNO are responsible (Bundesministerium der Verteidigung, 2016). The expansion of training and research activities at the

Bundeswehr University in Munich supports the further development of the Bundeswehr's cyber capabilities (Bundesministerium der Verteidigung, 2016, S. 33-35).

With the CIR command, the Bundeswehr has taken a significant organisational step towards strengthening military cybersecurity in Germany. The efficacy cannot yet be estimated. The consequences of the organisational restructuring will not be noticeable until a few years from now. Moreover, the cyber forces have not yet been significantly strengthened (Zedler, Zur strategischen Planung von cyber security in Deutschland, 2017, S. 74).

### *4.3 Cooperation and Conflict Between Agencies*

Cybersecurity is not easy to locate in the complex distribution of responsibilities among authorities with security tasks in Germany. Both the federal and state civil security authorities and the military have tasks and powers in cyberspace. They range from intelligence and investigation measures in the run-up to cyber threats (intelligence services, BSI, Bundeswehr) to the definition and control of protective measures (BSI, supervisory agencies) and the protection of own infrastructures (BSI, Bundeswehr), the concrete prevention of hazards in the event of cyber-attacks (police, BSI) up to prosecution (police) and finally the defence of Germany against war-like cyber-attacks (Bundeswehr). In many cases, it is difficult to determine which authority is responsible in an individual case, because, depending on the respective perspective, different bodies can claim responsibility.

This claim is particularly evident in the case of cyber defence, for example in the case of severe attacks against state institutions such as the federal government's computer network at the beginning of 2018. BSI is responsible for protecting the federal government's IT, including government networks. Due to the apparent allegations of espionage, the BfV is also accountable. Because the attackers targeted a federal institution, the BKA is responsible for criminal prosecution (on behalf of the attorney general). Finally, with regard to the power of protection of its own networks and capabilities, the Bundeswehr, which is at least marginally affected by the attack, also has responsibilities in this case – it also uses the attacked computer network for its own purposes. In the specific case, Länder authorities are not involved. This would be different if not the federal government but, for example, a critical infrastructure were attacked.

An explicit allocation of competence to only one authority is not possible in the system of the German security authorities. This is due to the nature of cyber-attacks. When a cyber attack is discovered, typically neither the originator of the attack nor its target can be identified. Also, in the first few days after the discovery of a possible attack, the focus is still on the containment of the attack, the analysis of the scope of the affected systems, and, if necessary, the restarting of the systems. These tasks, which are - especially if they are to be carried out in the networks of private companies - not of classical police or intelligence nature, they are most suitable for the technical focus of the BSI.

In June 2011 the federal government established a National Cyber Defence Centre (Cyber-Abwehrzentrum, Cyber-AZ). The Centre is an attempt to coordinate the multiple responsibilities of the authorities and create a joint information and exchange platform. The Cyber-AZ is a part of the BSI. It is staffed by civil servants from the BSI, the BfV, and the BBK. Liaison officers ensure the exchange with the BKA and the Federal Police. In some cases, the BND, the ZKA, and the various facilities of the

Bundeswehr also cooperate (Bötticher, 2015, S. 91) (Graulich, 2016, S. 776). Supervisory authorities from the federal government are also successively integrated, for example, the Federal Financial Supervisory Authority BAFin (Bundesanstalt für Finanzdienstleistungsaufsicht, 2018). The Cyber Defence Centre has no independent competences and powers. All powers remain with the authorities involved. Cyber-AZ only coordinates their cooperation. The Cyber-AZ was inspired by the Joint Terrorism Defence Centre (Gemeinsames Terrorismus-Abwehrzentrum, GTAZ), in which federal and state authorities from the police and the Office for the Protection of the Constitution have been working together since 2008. However, the GTAZ has a staff of 200 employees, while only 10 permanent employees work in the Cyber-AZ (Linke, 2015, S. 130). The effectiveness of the Cyber-Defence Centre is not only being called into question in the public eye. The Federal Audit Office (Bundesrechnungshof, BRH) also criticised the establishment and lack of effectiveness of the centre in 2014. It would not be in a position to pool the fragmented competencies and capabilities for cyber defence (Goetz & Leyendecker, 2014). Three years later, this finding has been confirmed by representatives of the security agencies (Zedler, 2017, S. 75), even though many cyber defence operations have been coordinated in the meantime (Bundesamt für Sicherheit in der Informationstechnik, 2016). However, the government has neither given significantly more personnel to the defence centre nor independent responsibilities and powers. Due to the constitutional situation, the latter would only be possible in Germany through a law. However, with legal regulation of the Cyber-AZ, the information cooperation between intelligence services and the police in the centre would have to be formally described in detail – concerning the separation requirement (Linke, 2015). Therefore, to avoid bureaucratic procedures, politics has so far refrained from doing so. The Cyber-AZ also has limited capacity for coordination and information exchange. Neither the private sector is represented in the Cyber-AZ, nor even the critical infrastructures. Neither are the Länder involved nor are they linked in any way. The federal government must implement the Länder participation in the future, in line with the NCSS 2016 (Bundesministerium des Innern, 2016, p. 27).

The assignment of tasks and cooperation between the federal government and the Länder in cybersecurity as a whole has not yet been clearly defined. It is true that the representatives of the Länder join the National Cybersecurity Council, which has been responsible for strategic cybersecurity issues since the 2011 national cybersecurity strategy under the leadership of the BMI. However, it has not yet achieved any notable overall effectiveness, not even in federal-state coordination. The powerful conference of interior ministers (Innenministerkonferenz) continues to dominate here (Hegele & Behnke, 2017), which periodically deals with cybersecurity issues and has set up a working group for this purpose (Innenministerkonferenz, 2017, S. 5). However, the organisational structure, which also differs widely from state to state, makes coordination considerably more difficult than in the case of police forces and intelligence services. Bavaria, for example, is the first German state to establish its own State Office for Information Security (LSI). On the one hand, it is responsible for primary Bavarian tasks such as the protection of the state's IT systems; on the other hand, it also has duties that overlap with the activities of the BSI, such as advising industry and critical infrastructures (Landesamt für Sicherheit in der Informationstechnik, kein Datum). Other Länder refrain from having own authorities and instead enter into cooperation agreements with the BSI. In addition, cooperation between the federal government and the Länder is made more difficult by the fact that, in addition to coordination within the Cybersecurity

Council and the Conference of Interior Ministers with the IT Planning Council (IT-Planungsrat), there is a third federal and state body responsible for cybersecurity issues. Its responsibility is the cooperation between the federal government and the Länder in the security of the state's IT systems (Schallbruch, 2017, S. 654).

Civil-military cooperation on cybersecurity has been optimised, at least from the military side, by setting up the CIR command. A unified organisation and the concentration of supervision of all cybersecurity issues in the Cyber and Information Technology directorate general of the Federal Ministry of Defence make military cyber defence more willing to cooperate with the civilian side (Bundesministerium der Verteidigung, 2016, S. 18). At the same time, the Ministry of Defence has always emphasised in the reorganisation process that the leadership of the Ministry of the Interior for cybersecurity should remain in place. The Bundeswehr has created the conditions for intensive civil-military cooperation in the past few years. However, shortcomings in the cybersecurity cooperation between government agencies in Germany continue to exist between the various civil authorities of the federal government and in unsettled federal-state collaboration.

### *4.4 Public-Private Cybersecurity Cooperation*

In general, cyberspace is privately owned. Major digital infrastructures such as backbone networks or critical infrastructure IT systems belong to private companies. Innovations in the cyberspace are the result of the market-driven development of private-sector products and business models. The global interconnection of the digitalized world is not driven by state actors, but by the private sector. Like almost all national cybersecurity strategies (Carr, 2016, S. 44) the German cybersecurity strategy also emphasises the need for "trusting cooperation and close exchange" between the state and industry as a prerequisite for sustainable cybersecurity (Bundesministerium des Innern, 2016, p. 21). Since 2005, various forms of cooperation between the state and industry have developed in Germany for this purpose, which more or less successfully see cybersecurity as a joint task. In some cases they are highly institutionalized, in others, they consist only of loose agreements between public and private actors.

The different approaches to public-private cooperation can be broadly broken down into four different areas, depending on the degree of commitment: (1) the joint organisation of responsibility for cybersecurity in a sector, (2) platforms and formats for exchanging operational cybersecurity information (3) cooperation formats for preventive cybersecurity, and (4) forms of cooperation for the dissemination of cybersecurity know-how to the public.

In the *first area of cooperation*, the organisation of joint responsibility between the state and the private sector, the so-called UP KRITIS is the oldest and most important partnership. It was founded in 2007 on the initiative of the federal government together with the operators of critical infrastructures in order to secure the cybersecurity of critical infrastructures. UP KRITIS stands for "Implementation Plan Critical Infrastructures" (Bundesministerium des Innern, 2007) and is an outcome of the first German cybersecurity strategy 2005, which had adopted a cooperative approach to the protection of cybersecurity critical infrastructures and provided for the necessary measures to be defined by an agreement between government and industry (Bundesministerium des Innern, 2015, p. 8). The UP KRITIS serves this purpose, but it was more than just a declaration. Besides, there was an exchange and coordination platform with initially 40 participants. These included individual infrastructure operators such as Deutsche Bahn as well as industry associations such as the German Insurance Association. BSI, BBK, and also the Bundesbank represented the public side in the UP KRITIS. BMI acted as a chair of the platform. In the meantime, the BSI has taken over the coordination and administration of the growing platform. At the beginning of 2018, it counted 540 participants (UP KRITIS-Geschäftsstelle, 2018). Initially, the motives of the government and the private sector to participate in UP KRITIS were very similar: reducing complexity. Having a lack of knowledge about the IT security of critical infrastructures, the government had a need for reliable assessments and for a certain degree of expressiveness towards the public. Given the diversity of supervisory and security authorities in the federal and state governments, companies wanted to ensure that their relations with the state would be able to meet a certain degree of reliability, which protected their business from surprises (Freiberg, 2016, S. 112).

The UP KRITIS has developed a wide variety of activities according to the mutual interest in making the other side more transparent. From the beginning, four working groups dealt with identifying cross-sector critical dependencies between infrastructures, defining crisis management processes in the event of cyber attacks, preparing joint exercises and exchanging views on EU activities and EU legislation. The UP KRITIS has produced many practical results, such as the establishment of sectoral Single Points of Contacts for the exchange of situational information or the joint implementation of the exercise LÜKEX 2011. However, it was not possible to broaden the cooperation in such a way that all critical infrastructure sectors became involved in the partnership. As a result of a detailed analysis of IT security of critical infrastructures conducted in 2012, the BMI found that the voluntary approach "did not have a nationwide impact in all security-related areas" (Bundesamt für Sicherheit in der Informationstechnik, 2017, S. 9) and presented the draft of a law. Though the government turned down the purely voluntary cooperation, the mutual trust that had developed as a result of the close collaboration in UP KRITIS also survived this strategic change. The government also made efforts to support this and incorporated key findings of the UP KRITIS into the legal regulations and the implementation of the law. An example is the provision in Section 8a.2 of the IT Security Act, according to which BSI can recognize industry standards that are drawn up by critical infrastructures operators as a fulfilment of legal obligations. Usually, the industry working groups of UP KRITIS are developing such standards (UP KRITIS-Geschäftsstelle, 2018). In addition, the working groups of UP KRITIS were closely involved in the development of the legal provisions with which the Federal Government determined which operators fall under the IT security law (Bundesministerium des Innern, 2016, S. 1).

Following this, UP KRITIS developed from a voluntary public-private partnership to a cooperation platform of state and critical infrastructures, which operates within the framework of legal regulations and supports its implementation. It also provides additional cooperation contributions that are not regulated by the legislator, such as the organisation of crisis management processes and the preparation of exercises. In 14 industry working groups and nine thematic working groups, the state and the business community are engaged in improving the cybersecurity of critical infrastructures (Bundesamt für Sicherheit in der Informationstechnik, 2017, S. 19). The cooperation is widely viewed as being beneficial by both sides

(Zedler, Zur strategischen Planung von cyber security in Deutschland, 2017, S. 77) (Bundesamt für Sicherheit in der Informationstechnik, 2017, S. 21).

Less institutionalized cooperation exists between the government and the internet providers in Germany. The collaboration between security agencies and providers is particularly important in the defence against ongoing cyber-attacks. For instance, the government regularly provides internet providers with information about systems and users affected by cyber-attacks on their networks, e. g. in the event of a case of millions of identities stolen in 2014 (Bundesamt für Sicherheit in der Informationstechnik, 2014) or the takedown of the Avalanche botnet in 2016 (Bundesamt für Sicherheit in der Informationstechnik, 2016). The close cooperation has led to the federal government's adoption of special powers for providers to defend against cyber threats in the new law on the implementation of the EU NIS Directive adopted in 2017. Section 109a of the Telecommunications Act has since permitted the blocking of users who are part of a botnet or the redirection of data traffic to so-called sinkhole servers. The state and telecoms are thus taking joint responsibility for the security of internet infrastructures.

The *second field of cooperation* between government and business is the exchange of operational information on cyber defence. The IT Security Act introduced very formal reporting obligations for the infrastructure operators that are affected by cyber-attacks. Also, various more informal exchange platforms have developed in Germany. One of these is the German Competence Centre against Cyber Crime (G4C) (German Competence Centre against Cybercrime, 2018). The BKA together with companies from the financial sector founded the association. It is inspired by the American National Cyber Forensics & Training Alliance (NCFTA). In the meantime, BSI is also involved. At a joint location in Wiesbaden, government officials and corporate employees work together to analyse and solve cyber-attacks, especially in the field of phishing.

The German Cybersecurity Organisation (Deutsche Cyber-Sicherheitsorganisation, DCSO) is pursuing an even more far-reaching cooperation approach. It was founded in the form of a private, non-profit-making company by a group of large DAX companies. Core areas are the exchange of information on vulnerabilities, exploits, attack vectors and specific attacks, the assessment of attacks as well as the joint security assessment of IT products and services. DCSO exchanges information with the BSI. BMI and BSI are represented in the company's boards (Deutsche Cyber-Sicherheitsorganisation, 2016). For the operational exchange of cybersecurity information, there are also a number of other agreements, mainly bilateral contracts and platforms between public authorities and private companies. With the NCSS 2016, the federal government announces the creation of a unified cooperation platform for this purpose (Bundesministerium des Innern, 2016, p. 25).

The *third area of cooperation* between government and industry in the field of cybersecurity is dedicated above all to the development of preventive assistance, exchange, and advice. Here, several different forms of cooperation have arisen which have similar objectives, overlapping groups of participants but slightly different priorities. The reasons for this diversity are the mostly parallel initiatives of various government agencies to establish exchange platforms for cybersecurity together with industry. At the action of the BSI, the Alliance for Cybersecurity was established in 2012. BMI and BSI together it with some trade associations jointly support it. By 2018 the association already has 2600 members, mainly individual companies, but also a large number of public authorities. Within the alliance, the members exchange non-operational cybersecurity information. The services include, for example, a monthly IT security status report provided by the BSI. Alliance participants can also submit their own materials, such as guidelines and information sheets. Expert circles and advanced training seminars complete the offer (Federal Office for Information Security, 2014).

At the initiative of the Federal Ministry of Economics and Energy (Bundesministerium für Wirtschaft und Energie, BMWi), the Task Force "IT Security in Business" was set up - at the same time as the NCSS 2011. Meanwhile renamed "Initiative IT security in Business", the primary goal of the cooperation between BMWi and business enterprises is to increase IT security in small and medium-sized enterprises. The initiative does not have a membership structure like the Alliance for Cybersecurity. It is more a funding programme that the ministry, together with experts and representatives from industry, has conceived and implemented. Results include, for example, technical tools for SMEs to check their websites, specific seminars, targeted awareness-raising activities for particular groups such as the craft trades and freelance professions, or the involvement of multipliers in cybersecurity such as tax advisors or auditors (Bundesministerium für Wirtschaft und Energie). In contrast to the Alliance for Cybersecurity, which aims at an open and comprehensive exchange of experience and information between government and business, the initiative focuses very strongly on SMEs.

Finally, it is worth mentioning the "Initiative for Business Protection" (Initiative Wirtschaftsschutz), which was founded mainly on the initiative of the BfV. Supporter of this interchange platform are the federal security agencies BfV, BKA, BND, and BSI as well as the umbrella organisations of the German business community (BDI and DIHK) and other business associations. It aims to intensify cooperation between government and industry to protect German companies against industrial espionage, sabotage and other forms of crime (Zedler, 2017, S. 76). The platform is a part of a national business protection strategy jointly presented by government and industry (Bundesministerium des Innern, 2016). However, the strategy itself has never been published. Although the BSI is cooperating, information on cybersecurity is hard to find on the platform of the "Initiative Wirtschaftsschutz", apparently to differentiate it from the Alliance for Cybersecurity. The effectiveness of this public-private partnership (PPP) for cybersecurity is currently difficult to assess.

Finally, the *fourth area of cooperation* between government and industry in Germany in the field of cybersecurity is to be noted: joint information, advice, and support for citizens concerning cyberspace threats. A not-for-profit association founded in 2006, "Deutschland sicher im Netz e. V." (DsiN) is under the patronage of the BMI. Its members are some bigger companies, mainly from the ICT industry, and a few NGOs. DsiN provides a wide range of information about security on the Internet and carries out projects to bring certain target groups to IT security, such as pupils, seniors, parents or users of certain Internet services. (Deutschland sicher im Netz e.V., 2017). There are several similar initiatives such as "Deutschland sicher im Netz", both nationwide and at the state level.

In no other field of security policy has the German state entered into so many partnerships with the private sector. In total, many thousands of public and private institutions are in some way involved in PPPs on cybersecurity. Almost every aspect of the implementation of the government's cybersecurity strategy is accompanied or supported by cooperation with industry. In the light of the linkage between public and private responsibility, there is probably no alternative. With the various PPPs, especially at federal level, however, the state also transfers its deficits in cooperation and coordination of cybersecurity to the private sector. Many of the initiatives work largely in parallel, often with similar actors. The German Armed Forces, which found its position in cyberspace very late in the game, is also seeking to be close to the world of business, for example by setting up a Cyber Innovation Hub to connect military demand with business innovation

While cooperation in the protection of critical infrastructures seems to be organized adequately by the UP KRITIS, there is still no robust exchange of operational cyber defence information between the state and industry. Neither the Alliance for Cybersecurity nor smaller entities such as G4C and DCSO adequately cover the interest of companies in quickly obtaining high-quality information from security agencies on vulnerabilities, attack vectors and cyber situation to protect themselves. There is a definite need for improvement here, especially since the amount of information accumulated by the government is steadily increasing: at BSI from mandatory reporting requirements and legally stipulated product tests, at the intelligence services from the expanded powers to investigate cyberspace.

Germany has worked very intensively on building public-private partnerships for cybersecurity but has not yet found a sustainable long-term solution.

### *4.5 References*

Bayerisches Staatsministerium des Innern. (2013, April 11). *Regierungserklärung des Bayerischen Staatsministers des Innern, Joachim Herrmann*. Retrieved March 05, 2018, from https://www.stmi.bayern.de/assets/stmi/med/reden/stm_reg-erklaerung_cybersicherheit_130411.pdf

Bayerisches Verfassungsschutzgesetz (BayVSG) vom 12. Juli 2016 . (n.d.). *GVBl. Bayern* , S. 145.

Bötticher, A. (2015). Strukturlandschaft der Inneren Sicherheit. In H.-J. Lange, & A. (. Bötticher, *Cybersicherheit* (pp. 69-102). Wiesbaden: Springer VS.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. (2012). *Auswertungsbericht LÜKEX 2011 . IT-Sicherheit in Deutschland*. Retrieved March 05, 2018, from https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Broschueren_Flyer/Luekex_11_Auswertung.pdf

Bundesamt für Sicherheit in der Informationstechnik. (2014, April 07). *Pressemitteilung 'Neuer Fall von großflächigem Identitätsdiebstahl: BSI informiert Betroffene'*. Retrieved March 06, 2018, from https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Neuer_Fall_von_Identitaetsdiebstahl_07042014.html

Bundesamt für Sicherheit in der Informationstechnik. (2016, December 01). *Pressemitteilung 'BSI ermöglicht Zerschlagung der Botnetz-Infrastruktur Avalanche'*. Retrieved March 06, 2018, from https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2016/Botnetz_Avalanche_01122016.html

Bundesamt für Sicherheit in der Informationstechnik. (2017). *Schutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS*. Retrieved March 06, 2018, from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Schutz-Kritischer-Infrastrukturen-ITSig-u-UP-KRITIS.pdf

Bundesanstalt für Finanzdienstleistungsaufsicht. (n.d.). *Presseerklärung 'BaFin arbeitet im Nationalen Cyber-Abwehrzentrum mit'*. Retrieved March 05, 2018, from https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Pressemitteilung/2017/pm_170331_cyber-abwehrzentrum.html

Bundeskriminalamt. (n.d.). *Bundeslagebild Cybercrime*. Retrieved March 05, 2018, from https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html

Bundesministerium der Verteidigung. (2015). Antwort auf die Kleine Anfrage "Elektronische Kampfführung der Bundeswehr", Drucksache 18/3963.

Bundesministerium der Verteidigung. (2016). *Abschlussbericht Aufbaustab Cyber- und Informationsraum*. Bonn.

Bundesministerium des Innern. (2007). *Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen*. Berlin.

Bundesministerium des Innern. (2015). *Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI)*. Berlin.

Bundesministerium des Innern. (2016, 04 26). *Bundessicherheitsbehörden und Verbände ziehen an einem Strang. Nationale Wirtschaftsschutzstrategie vorgestellt*. Retrieved 03 06, 2018, from https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2016/04/nationale-wirtschaftsschutzstrategie-vorgestellt.html

Bundesministerium des Innern. (2016). *Cyber-Sicherheitsstrategie für Deutschland*. Berlin.

Bundesministerium des Innern. (2016, 01 13). *Referentenentwurf des BMI - Entwurf einer Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz*. Retrieved 03 06, 2018, from https://www.bmi.bund.de/SharedDocs/downloads/DE/gesetztestexte/gesetztesentwuerfe/kritis-vo-entwurf.html

Bundesministerium des Innern. (2017). *Verfassungsschutzbericht 2016*. Berlin.

Bundesministerium für Wirtschaft und Energie. (n.d.). *Initiative IT-Sicherheit in der Wirtschaft*. Retrieved 03 06, 2018, from http://www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Navigation/root.html

Bundesnachrichtendienst. (n.d.). *Cyber-Sicherheit – Sicherung der nationalen Informationstechnik in Zeiten globaler Vernetzung*. Retrieved March 05, 2018, from http://www.bnd.bund.de/DE/Themen/Lagebeitraege/Cyber-Sicherheit/Cyber-Sicherheit_node.html

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs, 92*(1), 43-62.

Deutsche Cyber-Sicherheitsorganisation. (2016, August 19). *Deutsche Cyber-Sicherheitsorganisation unterstützt Unternehmen bei Abwehr von Gefahren aus dem Netz*. Retrieved March 06, 2018, from https://www.presseportal.de/pm/121523/3407438

Deutschland sicher im Netz e.V. (2017, 03). *Jahresbericht 2016*. Retrieved 03 06, 2018, from https://www.sicher-im-netz.de/sites/default/files/download/dsin-jahresbericht_2016_web.pdf

Federal Office for Information Security. (2014, 08 01). *Alliance for Cybersicherheit. General Information*. Retrieved 03 06, 2018, from https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/ACS_Broschuere_en.html?nn=6644222

Freiberg, M. (2016). Öffentlich-private Zusammenarbeit zum Schutz von IT-Infrastrukturen. In *Cybersicherheit* (pp. 103-120). Wiesbaden: Springer VS.

Fremuth, M. (n.d.). Wächst zusammen, was zusammengehört? Das Trennungsgebot zwischen Polizeibehörden und Nachrichtendiensten im Lichte der Reform der deutschen Sicherheitsbehörden. *AöR*, *139*, 32-79.

*German Competence Centre against Cybercrime*. (n.d.). Retrieved 03 06, 2018, from http://www.g4c-ev.org/

Gesetz über den Verfassungsschutz in Nordrhein-Westfalen (Verfassungsschutzgesetz Nordrhein-Westfalen - VSG NW -) vom 20.12.1994, zuletzt geändert durch Gesetz vom 20. September 2016. (2016). *GV.NRW*, 789.

Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik vom 17. Dezember 1990. (1990). *BGBl. I*, 2834.

Goetz, J., & Leyendecker, H. (2014, 6 7). Rechnungsprüfer halten Cyber-Abwehrzentrum für "nicht gerechtfertigt". *Süddeutsche Zeitung*.

Graulich, K. (2016). Elemente der sogenannten Neuen Sicherheitsarchitektur der Bundesrepublik. In *Festgabe für Rosemarie Will 'Worüber reden wir eigentlich?'* (pp. 738-779). Berlin.

Hegele, Y., & Behnke, N. (2017). Horizontal coordination in cooperative federalism: The purpose of ministerial conferences in Germany. *Reg. Fed. Stud.*(5), 529–548.

Innenministerium Niedersachsen. (2011). AV Schwerpunktstaatsanwaltschaften zur Bekämpfung der Kriminalität im Zusammenhang mit Informations- und Kommunikationstechnik (IuK-Kriminalität) vom 04.11.2011. *Nds. MBl.*(43), 834.

Innenministerkonferenz. (2017, 12 August). *Sammlung der freigegebenen Beschlüsse der Innenministerkonferenz am 07./08.12.2017 in Leipzig*. Retrieved March 06, 2018, from https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/2017-12-07_08/beschluesse.pdf;jsessionid=B48A17311B512333542F22CB2BBDFA56.1_cid382?__blob=publicationFile&v=3

Karl, W., & Soigne, M. (2017). Neue Rechtsgrundlagen für die Ausland-Ausland-Fernmeldeaufklärung. *NJW*, 919-925.

Landesamt für Sicherheit in der Informationstechnik. (n.d.). *Aufgaben des LSI*. Retrieved 03 06, 2018, from https://www.lsi.bayern.de/lsi/index.html

Linke, T. (2015). Rechtsfragen der Einrichtung und des Betriebs eine Nationalen Cyber-Abwehrzentrums als informelle institutionalisierte Sicherheitskooperation. *Die Öffentliche Verwaltung*, 128-139.

Marxsen, C. (2017). Verfassungsrechtliche Regeln für Cyberoperationen der Bundeswehr. *JZ*(11), 543-552.

Schallbruch, M. (2017). IT-Sicherheitsrecht – Schutz digitaler Dienste, Datenschutz und Datensicherheit. *CR*, 799-804.

Schallbruch, M. (2017). IT-Sicherheitsrecht – Schutz kritischer Infrastrukturen und staatlicher IT-Systeme. Zur Entwicklung des IT-Sicherheitsrechts in der 18. Wahlperiode (Teil 1). *CR*, 648-656.

Schönbohm, A. (2011). *Deutschlands Sicherheit: Cybercrime und Cyberwar*. MV-Verlag.

UP KRITIS-Geschäftsstelle. (2018, 01 29). *UP KRITIS-Jahresbericht 2017*. Retrieved 03 06, 2018, from https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/Jahresbericht_2017.pdf

Zedler, D. (2017). Zur strategischen Planung von cyber security in Deutschland. *Zeitschrift für Außen- und Sicherheitspolitik*(10), 67-85.

# Chapter 5: Current priorities and gaps in German national cybersecurity, future trends

**Abstract** Current German cybersecurity policy suffers from several gaps that this section examines in more detail. These gaps become apparent in international comparison and contrast with German officials' own claims that Germany's cybersecurity policy is strategically comprehensive. First, Germany has not devised a clear concept for the goal, scope, and legal framework of "active cyber defence" measures. Second, a major question remains that of the overarching institutional architecture for cybersecurity, including the responsibilities of the individual security authorities in the cyber domain and their differentiation and cooperation. Third, the debate on how the state should deal with IT security vulnerabilities is still in its infancy. Fourth, an implementation concept for the politically undisputed increase in the liability of software manufacturers for vulnerabilities in their products is lacking. Fifth, a national and European industrial policy on cybersecurity, which is widely called for under the banner of "digital sovereignty", is still largely undefined. Finally, Germany must define and assume a more comprehensive role in international efforts to maintain peace and stability in cyberspace.

**Keywords** Active cyberdefence, Cybersecurity architecture, Vulnerabilities, Digital sovereignty, Manufacturer's liability

### *5.1 Introduction*

German policy-makers still understand cybersecurity to be primarily a preventive task of technical and organizational protection of IT. The core issues of German cybersecurity policy are

- the development of secure technologies,
- the dissemination of technical know-how,
- the technical and organizational security of critical systems,
- the legal obligation to and enforcement of protective measures,
- the development of defensive capabilities and increased criminal prosecution in the field of cyber crime.

This civilian and preventive approach combines various paths of development. The strong influence of data protection with its emphasis on the legal, technical and organizational protection of systems has extended to the field of cybersecurity. The influential role of the BSI and its development towards a de-facto national cybersecurity authority has made the engineering-oriented approach to cybersecurity, which stresses the development and deployment of well-defined secure systems, the guiding principle of cybersecurity policy. Other domestic security agencies have not yet or only temporarily found a place in the "digitizing" national security architecture. Moreover, their overlapping responsibilities often lead to their engagement into turf wars and blockages. Only the Bundeswehr (German Armed Forces) has promoted a more comprehensive view of security in the "cyber" domain in its national strategy. However, due to the tight legal restrictions relating to the Bundeswehr's deployment and competencies, it also remains more focused on securing its own systems than on cyber defence at home and abroad.

Industry and private associations have largely not yet devised a consistent cybersecurity strategy. German IT security companies support the idea of strengthening their industry and IT products on the national or European level, following the loosely defined principle of "digital sovereignty". However, they lack an agenda or strategy to implement this approach. Most of the big successful internet companies originate in the US or Asia, exporting their IT security know-how and solutions to Europe.

National standalone approaches are not competitive on a broad scale. Only in the area of critical infrastructures has Germany found a consistent and consequent approach to obliging the deployment of national certified IT security products through a mix of legal obligations and public-private cooperation. This is also fully in line with the tradition of the aforementioned preventive, technical-organizational strategic approach.

In contrast to its own claim, but also in international comparison, current German cybersecurity policy has several gaps which the following section examines in more detail.

### *5.2 Legal, Technical and Practical Development of Active Cyber Defence*

Active cyber defence (ACD) has not been among German security agencies' instruments for many years. To date, no concrete actions have followed from the 2011 national cybersecurity strategy's (NCSS) announcement to create a "complete set of instruments for the defence against attacks in cyberspace" (Bundesministerium des Innern, 2011, S. 12). Instead, cyber defence in Germany followed a civilian preventive approach. On an international level, the debate about more far-reaching cyber defence actions has been ongoing for many years. There is no generally accepted term for active cyber defence (ACD). According to cybersecurity expert Lachow, "ACD can best be understood as a set of operating concepts that all involve taking the initiative and engaging the adversary in some way" (Lachow, 2013, S. 3). ACD can comprise a set of measures which the defender uses in its own IT systems, such as the redirection of traffic or deception of the attacker. Yet, ACD can also affect provider networks, through measures such as the setting up of sinkholes for data flows. It can affect third-party systems if the attacked party manipulates an attack's Command & Control (C2) servers. Finally, ACD can also involve action in the attacker's systems, including the manipulation of attack tools or deletion of data. Tactically, each of these options can make sense at certain stages of a cyber attack (Lachow, 2013, S. 1). However, the deployment of such tactics can raise legal concerns, increase operational risks (such as detection) or cause collateral damage. The latter could, for instance, occur in the form of political or diplomatic disruptions if a defending party's measures compromised servers in other countries (Reinhold & Schulze, 2017).

There are a number of scenarios in which such measures seem necessary. This could be, for example, the takedown of a botnet. The US Federal Bureau of Investigation (FBI), in cooperation with private sector partners, regularly engages in botnet takedowns. Germany has benefited from such operations without executing takedowns itself. A takedown could involve the destruction of leaked data on drop zone servers.

It could also include the disruption of C2 servers that control physical attacks, such as detonating bombs (Reinhold & Schulze, 2017, S. 6).

Germany's government has not yet developed a legal framework for ACD actions and has no authority for such far-reaching active cyber operations. ACD activities in Germany have thus to date been limited to operations carried out in cooperation with the respective providers or system operators, and in cross-border operations by means of international legal assistance. The debate on active cyber operations in reaction to attacks did not begin until 2017. Back then, the Federal Minister of the Interior announced a corresponding concept, the Federal Security Council (Bundessicherheitsrat) is said to have addressed the issue in a secret meeting (Reinhold & Schulze, 2017, S. 3), and various federal agencies offered to expand their scope of activities accordingly (Tanriverdi, 2017a) (Tanriverdi, 2017b). In Germany, the discussion about ACD is taking place under the buzzword "Hack-Back"; however, this refers to the complete spectrum of active cyber operations, not only to the infiltration of adversarial systems to defend against an ongoing cyber attack (responsive cyber defence).

While Germany continues to approach ACD measures only cautiously, cyber operations in the form of “lawful hacking” for criminal prosecution purposes have found their way into the competencies and capability development of the security agencies. This is mainly due to the increasing undermining of a key investigative tool, notably lawful interception. Due to the increase in the encryption of communications and the use of unmonitorable services such as “The Onion Router” or Tor software ("going dark"), security agencies need to find ways to access electronic communications directly on the suspect's systems.

In 2006, the parliament of North Rhine-Westphalia gave the State Office for the Protection of the Constitution the authority to secretly penetrate computer systems in order to monitor suspects. The respective law was overturned by the Federal Constitutional Court (Bundesverfassungsgericht, 2008) (Hornung, 2008).

Later, however, the law of a number of Länder (states) regulated this power for state intelligence services and the Federal Criminal Police. Ultimately, covert access to computers was allowed for law enforcement agencies in the summer of 2017 but limited to the prosecution of particularly serious crimes (Singelnstein & Derin, 2017). Government hacking for purposes of law enforcement and for certain limited intelligence purposes is successively being introduced into German security policy - and is being discussed critically, especially with regard to the handling of vulnerabilities (Herpig, 2017). In order to support police forces and intelligence services in the development of relevant methods, a new authority was established in 2017, the Central Office for Information Technology in the Security Sphere (Zentrale Stelle für Informationstechnik im Sicherheitsbereich, ZITiS). It is also supervised by the Interior Ministry. Its task is to develop techniques for lawful interception, online searches, cryptoanalysis, digital forensics and big data analyses (Bundesministerium des Innern, 2016, S. 32).

It remains to be seen how these different singular approaches of active cyber and legal hacking operations will be combined into an overall strategy. Substantial legal, technical and organisational questions remain. From a legal point of view, it is not clear whether ACD will be implemented successively as an extension of the competencies of the various security agencies, intelligence services, police forces and the BSI, or whether a holistic approach will be found. The latter seems to make sense for two reasons. First, ACD, which affects the rights of third parties, is accompanied by a significant risk of collateral damage, which has to be considered holistically. Second, all actions that have an impact outside Germany are relevant to foreign policy; their legal regulation must provide for a foreign policy cross-check, including the involvement of the Foreign Ministry. In any case, a legal regulation also requires a graduated list of measures and an increasingly strict obligation to observe a duty of care depending on the balancing of the purpose and the respective rights of third parties.

From a technical point of view, the question is how the tools for ACD are developed, who is in charge of assessing them and how they are deployed in order to minimise collateral damage. ZITiS will have an important role to play here. In addition, the involvement of internet providers in defence efforts must be even more intensive than before. Finally, it is also necessary to answer the organisational question relating to which institution shall be responsible for active cyber defence. This must be answered in the context of the cybersecurity architecture as a whole, which we will come to in the following section.

### *5.3 Cybersecurity Architecture – Roles and Responsibilities of Agencies*

German security agencies operate in absence of an overarching cybersecurity architecture. Cybersecurity responsibilities have progressively increased for almost all security agencies and several other authorities. The only significant organizational developments in the German cybersecurity landscape are the continuous strengthening of the BSI with new tasks and new personnel, the concentration of the military's capabilities in the CIR command, as well as the establishment of central units at the state level, mainly in the police force and sometimes in the intelligence service. None of these steps have solved any of the four structural problems facing the German security apparatus in cyberspace.

First, there is no clear *jurisdiction for cyber defence at the federal level*. The cyber-defence centre operates only to a very limited extent, the Bundeswehr is not responsible, and the BSI is working considerably above its capacity. A fundamental reorganization is necessary here by creating a cyber defence authority with clear jurisdiction. Second, the widening of *active cyber defence requires a defined jurisdictional competence* at the federal level. In principle, the BSI has the necessary capabilities. However, it should be excluded as a responsible authority because active operations do not suit the character of the agency’s preventive security mission. The domestic intelligence services and the police are limited to domestic activities, which means that only the Bundeswehr or the BND can carry out such operations. The decision is a political and legal question. If Germany wants to remain in line with its defensive approach, the military should be excluded. Military cyber defence operations tend to escalate conflicts. In addition, the Bundeswehr's powers under constitutional law are far more limited than those of the Foreign Intelligence Service BND.

To combine the two issues—cyber defence in Germany and the execution of active operations that can also affect foreign countries—it would be reasonable to create a new institution, a cyber defence agency that is responsible for the recognition, analysis and holistic defence of attacks with the help of the police and intelligence services in Germany and the help of the BND abroad. The military would need to be involved as well. The BSI, on the other hand, would only participate in this process insofar as insights from ongoing attacks are relevant for the establishment of protective measures by the government or critical infrastructures. In any case, a comprehensive and extensively debated amendment of the law is a prerequisite for a proper distribution of responsibilities.

The third structural problem is the *link with the Länder*. Even if under the German constitutional order, domestic security is first of all a matter for the federal states, there is no resistance to a strong federal approach to cyber defence among the Länder interior ministers. Creating cyber defence authorities 16 times over across the federal states is impossible due to the international nature of cyber defence, its closeness to military defence and the expense of developing human and technical resources. Given that the federal states are nevertheless responsible for police and intelligence services, a central institution of each of the Länder must be closely linked to the federal cyber defence agency, ideally a central unit of the state police. Local police powers, e. g. to conduct home searches or shutdown of servers, may be required for cyber-defence purposes.

Finally, a fourth structural problem still needs to be solved, the *cooperation between security agencies and the private sector*. Germany needs to create a cybersecurity operations platform that is as uniform as possible between the government and the private sector. The very inconsistent manner in which security-relevant information is exchanged between public sector authorities and companies today is not acceptable in the long term. The government cannot justify the fact that it is largely coincidental as to whether or not information that is necessary for a company's self-protection reaches it. There are many reasons why the BSI should establish such a central platform for all federal authorities, including intelligence services, police forces and a cyber defence agency. Technical parameters are at the core of an operational information exchange. Intelligence findings or police information may only be shared with third parties to a very limited extent, so that they are not suitable for a platform. The government might require the industry to become more concentrated, for example, through a joint private sector institution that brings together industries and companies with the BSI platform.

It remains to be seen whether the new federal government, which came into office in the spring of 2018, will tackle such a major structural reform of the cybersecurity architecture in Germany.

### *5.4 Towards a Governmental Vulnerability Handling Strategy*

The increased use of encryption in communication tools and web services poses a growing challenge for law enforcement agencies (LEAs) all over the world. LEAs argue they are at risk of criminals "going dark" due to the LEAs' inability to investigate criminal suspects' encrypted communication. Several countries, such as the United Kingdom and France or the US, have adopted or are debating laws to give authorities the right to interfere with cryptography. In contrast, the German federal government has so far abstained from options to weaken cryptographic security mechanisms and instead adhered to the principles of cryptography, which the Cabinet established in 1999. At the core of these principles lies the government's commitment to never ban or weaken crypto products (Bundesregierung, 1999). Indeed, the installation of backdoors into crypto products would undermine the security of IT and thereby, of its users, and would severely impair confidence in German technology products on the global market, in turn harming the German IT industry.

Therefore, Germany aims to strengthen LEAs' and intelligence agencies' capabilities to circumvent encryption through "advanced technical procedures." In this context, Germany established the aforementioned Central Authority for Information Technology in the Security Sphere (ZITiS). As pointed out above, one of its tasks is to develop tools and capacities for government hacking to gain targeted access to computer systems, interception of communication, and analysis.

Government hacking often relies on the exploitation of a vulnerability – a flaw in software or hardware which enables third parties to gain access to a system directly or via an "exploit". Vulnerabilities might be known to the manufacturer (for *n* number of days, therefore referred to as "n-days") or unknown to the manufacturer (for 0 days, therefore referred to as "0-days"). Once a third party, for example, a security researcher, discloses an 0-day to the manufacturer, the manufacturer can develop and deploy a patch which fixes the vulnerability. In general, most IT products contain a multitude of vulnerabilities, especially as the majority of IT systems become increasingly complex.

At the time of writing, the rules for government hacking in Germany are far from settled and fiercely debated (Krempl, 2017), (Herpig, 2017). Most importantly, it is unclear how security agencies will handle vulnerabilities in IT systems, which they inevitably need to exploit for their (targeted) surveillance activities. If government agencies exploit 0-day vulnerabilities in IT products without disclosing them to the products' manufacturers, the vulnerabilities will likely not receive a patch and therefore remain open for any motivated and capable malicious actor to exploit. Hence, such use of undiscovered vulnerabilities by state security agencies bears risks for the overall IT-ecosystem and society at large.

This is one reason why the German (and global) IT industry and civil society organizations resist government hacking efforts. Moreover, the exploitation of vulnerabilities in IT security products interferes with individuals' legally-guaranteed rights to the protection of the integrity and confidentiality of IT systems enshrined in a 2008 German Constitutional Court ruling (Abel & Schafer, 2009). Therefore, the intrusion of security agencies into computer systems via the exploitation of an unknown vulnerability requires appropriate and proportionate justification within the remits of the national criminal and basic law.

The CDU/CSU and SPD governing coalition will need to address a number of political, ethical, and legal challenges related to the handling of IT security vulnerabilities. The otherwise comprehensive set of cybersecurity measures outlined in the government's coalition treaty from 2018 did not include any reference to government agencies' handling of IT security vulnerabilities (CDU/CSU & SPD, 2018). Within the 19th legislative period which began in 2018, the government will need to devise a process or set of rules and parameters guiding security agencies' legal and legitimate exploitation of IT vulnerabilities.

One option would be to authorize security agencies to use known n-day vulnerabilities only. In fact, many systems remain unpatched even after vulnerabilities are known. The annual Verizon Data Breach Investigation Report has regularly concluded that most attacks against IT systems exploited well-known vulnerabilities for which patches had long been available (Verizon, 2017), (Verizon, 2015). Hence, there are chances that security agencies could still gain access to a system via known vulnerabilities. From an IT security perspective, this is a practicable and preferable solution. However, prosecutors argue that they need 0-day vulnerabilities to stay one step ahead of sophisticated criminals.

In this context, another option would be to authorize security agencies to exploit 0-day vulnerabilities, which bears significant and potentially systemic security risks. For example, the exploitation of a previously unknown vulnerability in a widely used operating system, such as Microsoft Windows, could have dramatic consequences worldwide. Accordingly, first ideas and procedures to assess possible consequences of the use of vulnerabilities by security agencies in the context of potential gains for security agencies are emerging. The US has adopted an interagency "Vulnerabilities Equities Process" in which different government stakeholders assess the tradeoff between the national security benefits of using an 0-day vulnerability and the security risks it poses to critical infrastructures and IT systems generally, were the vulnerability to be exploited by malicious actors (Government of the United States, 2017).

The US Vulnerabilities Equities Process might provide some guidance for the Germany, for example when it comes to the inclusion of multiple stakeholders with different interests. However, as (Gaycken, 2017) points out, the decision-making within such a process risks becoming a political negotiation subject to power dynamics among different government departments and stakeholders. While such dynamics can never be avoided in practice, a vulnerability equities process should follow clearly defined criteria and ensure a balance between stakeholders. The assessment should weigh the criticality of a vulnerability for individual users and systemic security of IT against the value of this vulnerability for solving crimes or national security (Gaycken, 2017). Following a precautionary approach, vulnerabilities that would have a very serious impact on human life or the economy if exploited by criminal actors should always be disclosed to the technology's manufacturer. Above all, an equity process needs to be based on a clear legal basis, follow a transparent legislative procedure, and happen under judicial oversight, none of which exists to date in Germany. While the IT industry, representatives from the judiciary, and civil society representatives cannot participate in case-by-case decision processes, the government should institute a regular dialogue about the handling of vulnerabilities with them. Moreover, the IT industry itself should transparently document their own handling of vulnerabilities in their products and support users with fixing them.

Overall, the German government will need to address the handling of both known and unknown vulnerabilities within a comprehensive set of considerations, including the cyber threat situation, the diversity or monoculture of hard- and software deployed in systems at home and abroad, and alternative ways to gain access to information within a criminal prosecution.

### *5.5 Implementing a Comprehensive IT Security Industry Policy*

One of the guiding themes of German cybersecurity strategy has been the strengthening of the German and European IT industry, with a focus on trustworthy and secure ICT products. The most recent 2016 national cybersecurity strategy (NCSS) outlines the goal to better promote the development of key technologies and quality IT "made in Germany".

Indeed, the deployment of reliable and trustworthy IT components in critical infrastructures, industry, and individual user environments is a key enabler for cybersecurity. Following the Snowden revelations, political and industry leaders in Germany and Europe called for regaining the country's and region's "technological sovereignty", including industrial policy measures to strengthen the domestic IT industry and to reduce the dependence on foreign IT components, which might contain backdoors (Gallagher, 2014).

However, as the European Network and Information Security Agency (ENISA) pointed out in 2014, "over the past 15 years Europe has lost its leading position in ICT technology. All the new global players are situated outside the EU" (ENISA, 2014). The most recent German Ministry of Economics and Energy's report on the IT security market in Germany dating from 2014 shows that domestic demand in Germany for IT security products has been met by around 22 percent of imported and the remaining share of 78 percent by domestic products (Bundesministerium für Wirtschaft und Energie, 2014). Hence, the German IT security industry, including IT services, software, and hardware, is meeting high domestic demand but its exports remain low compared to US or Chinese ICT products. Moreover, while the share of software of the German IT security market has increased to 44 percent, the share of hardware has decreased to only 4 percent (from 13 percent in 2005) in 2013. One reason for this trend might be the growing importance of software in increasingly interconnected environments and the "Internet of Things" (IoT) (KPMG, 2014).

In the field of critical infrastructures, Germany has succeeded to implement legal and technical measures obliging operators and technology manufacturers to comply with specific industrial and regulatory IT security standards (Schallbruch, 2017). However, across the broader industrial context, measures that promote the deployment of trustworthy IT are still outstanding. A number of industry and government-commissioned studies have examined means to enhance Germany's, the industry's or individuals' ability of self-determined and autonomous action in the digital realm through secure and trustworthy ICTs (Forschungszentrum Informatik, Accenture GmbH, Bitkom Research GmbH, 2017), (Diekmann, Gesa, 2015). Proposed measures include the expansion and enhancement of national key technologies, an increase of investment in research and development, the enforcement of technical guidelines and standards as part of a European certification scheme (see 5.5), leveraging the EU's public procurement mechanisms, the promotion of innovative business sectors and models, and mechanisms to improve the education of technology and IT experts (Forschungszentrum Informatik, Accenture GmbH, Bitkom Research GmbH, 2017), (Diekmann, Gesa, 2015), (KPMG, 2014).

The lack of a comprehensive national and a properly coordinated EU industry policy for the IT (security) sector constitutes a significant gap in German and European digital policy. While national investment as well as research and development programs will help promote national industrial initiatives, an internationally competitive IT industry will likely be able to emerge only at the European level. The German government will be well-advised to cooperate with its European partners, and France in particular, to promote innovative business models for EU companies producing IT and cybersecurity products and services – moving toward an IT "made in Europe" rather than a "made in Germany" approach.

First steps can be recognized in the current government's 2018 coalition treaty, which announces the establishment of a public Franco-German centre for artificial intelligence. Moreover, the treaty declares to establish a strategic industry and innovation policy to support the expansion of Industry 4.0 (CDU/CSU & SPD, 2018, p. 13). It aims to promote, in a targeted manner, digital key technologies, as well as the investment into research and development efforts to advance key technologies such as microelectronics, quantum computing, robotics, Blockchain, and others, and to continue to invest in microelectronic technologies (CDU/CSU & SPD, 2018, p. 57).

Germany should assign priority to implement such suggestions and avoid being left behind by other countries, including France, which has adopted an ambitious digital agenda under President Emmanuel Macron. Overall, the promotion of industrial and societal cybersecurity should be seen as part of a broader future-driven technology policy strategy which requires cooperation with European partners, the promotion of high security and reliability standards, and foundations to enable European companies to innovate.

### *5.6 Finding a Coherent Legal Concept for Safety and Security*

In the relatively short period between 2013 and 2017, the German government passed numerous laws on IT security. In addition, there are important provisions of European law which have become directly applicable in Germany or have been transposed into national law, such as the NIS Directive, the eIDAS regulation or the GDPR (Schallbruch, 2017). At the heart of the regulations are requirements for various types of operators of IT systems and providers of digital services to take preventive IT security measures and report security incidents to the authorities. Corresponding obligations exist for operators of critical infrastructures (Hornung, 2015) (Schallbruch, 2017), web server operators (Gerlach, 2015), providers of significant digital services such as online marketplaces, search engines, and cloud services (Schallbruch, 2017), and, in accordance with Art. 32 of the new GDPR, also for operators of systems on which personal data are processed (Schallbruch, 2017).

Although the requirements of the different legal areas differ considerably in detail, the final result is that the operators or providers must implement state-of-the-art IT security measures.

Germany has failed to achieve the politically intended tightening of the liability of IT manufacturers for the security of their products. In the common opinion of German scholars, the provisions of existing law are not sufficient to force manufacturers to maintain a minimum level of security and to act responsibly when dealing with warnings, vulnerabilities, patches and updates (Spindler, 2016). Whereas there is no suitable manufacturer responsibility for the IT products that are available on the market in Germany, a large number of special categories of products are precisely specified by government specifications as to which security measures must be taken for products. This concerns for example medical devices, smart energy meters or IT components in the infrastructure of health care. They require state approval on the basis of defined IT security standards, which are usually developed by the BSI.

The consequence is an enormous differentiation in the market for IT products. On the one hand, there is a state-regulated sector with special German IT security requirements and correspondingly high-security products, and on the other hand there is a largely unregulated sector of IT products without any IT security requirements, i.e. the consumer products. The new government, which took office in March 2018, wants to overhaul this state. The coalition agreement includes various statements on this issue. The aim is to establish minimum security standards for consumer-related products and to establish duties of care for manufacturers, such as the prompt identification and elimination of vulnerabilities. Manufacturer liability is also to be increased (CDU/CSU & SPD, 2018, S. 45, 128).

This approach is significantly different from the current considerations at the European level. For this purpose, the European Commission presented comprehensive proposals in September 2017 (European Commission, 2017). The existing national certification procedures are to be gradually replaced by a European framework. The Commission itself intends to be empowered to make certification schemes binding for product groups on the basis of preliminary work. The present draft regulation does not provide for the content of such a certification but leaves it to the individual schemes. If a European cybersecurity certification scheme has been defined for a product group, the member states should be prevented from defining their own schemes for this product group. At the same time, the Commission also wants to be able to use its implementing act to determine whether the existing national schemes lose their validity at a given time. In this way, a European regime could gradually replace national rules.

The certification itself would be executed by certification and accreditation bodies established by national law. Certificates shall be completely voluntary. Each company could then decide whether and where to apply for a European Cybersecurity Certificate. Certificates issued shall be valid for three years. The Commission proposes three different security levels (basic, substantial, high) without specifying exactly what these levels mean. This would also have to be determined on a product group-specific basis.

Overall, this proposal is a step in the right direction towards a uniform European assessment of the security of IT products. Nonetheless, the voluntary approach, which also ties in very strongly with traditional IT security certification, falls short of expectations. The Commission has not put forward any proposals on how the responsibility (and also liability) of manufacturers and service providers for the safety of their products can be increased. Their proposal does not even indicate how to overcome the current problems of safety certification – speed, cost, low "lifetime". The speed of the certification processes is significantly slower than the speed of technical innovation. The costs of the certification procedures, in particular the recertification required for each change, are high. Due to changes in risks and attack vectors, certificates must be limited in time. Even if these problems were solved, the member states would hardly be able to accept a Commission-exclusive decision on the security requirements for ICT products.

It remains to be seen how the new German government's approach to tightening liability can be reconciled with the European approach of voluntary certification.

### *5.7 International Cooperation*

Collaboration with other states and non-state actors at the international level is key to the advancement of Germany's and indeed any country's interests in the field of cybersecurity, relating to technical IT security, critical infrastructure protection, counter cyber crime and espionage, or national defence. The very basis of the Internet is globalized, and so are the organizations and companies that constitute and administer it (Hathaway & Klimburg, 2012, p. 30).

International diplomatic cooperation is a crucial means to prevent and manage interstate conflict in the digital realm in the absence of binding international legal rules. Cooperation can occur through internationally binding treaties, politically binding agreements, such as confidence building measures, as well as non-governmental agreements between technical bodies (Hathaway & Klimburg, 2012).

In light of growing political tensions between major powers such as the United States (US), Russia, and China, it is crucial that the German government, together with like-minded European and international partners, takes a leading role in reinvigorating an inclusive international effort to maintain peace and stability in cyberspace.  Since the emergence of the first IT security and critical infrastructure protection policies at the national level in the 1990s, the German government coordinated its efforts with the United States and other European Union (EU) member states. Throughout the past decade, Germany has assumed an active role in international cyber diplomacy as well as internet governance.

Cyber diplomacy can be understood as the general formal state engagement of a nation's diplomatic processes in the overall theme of global cybersecurity (Potter, 2002), (Luiijf & Healey, 2012). In particular, cyber diplomacy refers to multilateral or bilateral activity to manage interstate relationships in cyberspace, for example within the United Nations (UN). Internet governance, on the other hand, can loosely be defined as the decentralized, bottom-up policies and mechanisms under which the Internet community's many stakeholders – technical organizations such as the Internet Engineering Task Force (IETF) or the Internet Corporation of Assigned Names and Numbers (ICANN), private companies, civil society, academia, and governments – make decisions about the development and use of the Internet (Masters, 2014). [The World Summit on the Information Society's official definition can be found in (Tunis Agenda for the Information Society, 2005).] In this context, governments cooperate with various non-state stakeholders. Since 2005, stakeholders convene at the global UN Internet Governance Forum (IGF) on an annual basis to discuss all internet governance related issues.

As previously discussed, Germany has participated in negotiations on cybersecurity within the UN since 2004, as well as in other bilateral and multilateral formats. However, most of its international cooperation was limited to technical exchange. While the first national cybersecurity strategy in 2011 mentioned the international and diplomatic dimensions of cybersecurity policy, it was not until the Snowden revelations that Germany started to play a greater role on the international stage. In response to the revelations, which included details about the surveillance of German Chancellor Angela Merkel and Brazilian President Dilma Rousseff, Germany and Brazil sponsored a UN resolution that called on states to "respect and protect the right to privacy" in the digital age. On December 18, 2013, the UN General Assembly adopted the final resolution 68/167 (United Nations General Assembly, 2014). Thereby, Germany and Brazil assumed a leading role in efforts to enshrining the right to privacy online in international norms and law. Despite subsequent revelations exposing German intelligence agencies' close cooperation with the NSA and the British GCHQ, the resolution remains a major diplomatic achievement for Germany. It is also noteworthy, that Germany partnered with an ally outside of its European and transatlantic ties, which made it a more global effort.

In the following years, Germany has continued to be an active promoter of cyber diplomacy. Under German chairmanship in 2016, the Organization for Cooperation and Security in Europe's (OSCE) adopted a second package of confidence building measures (CBMs) in cyberspace (Organization for Security and Co-Operation in Europe, 2016). Moreover, its diplomatic representatives chaired the latest UN Group of Governmental Experts on Information Security (GGE) from 2016 to 2017. The UN GGE group had convened for five rounds since 2004 to address threats of armed conflict in cyberspace and drafted principles for norms and standards of responsible state behavior. In 2013, the group issued a landmark report in which 15 countries, including Russia, China, the US, India, the UK, France and Germany, agreed that "international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure peaceful and accessible ICT environment" (Assembly, 2013). A subsequent report in 2015 endorsed new norms to guide state activity in cyberspace during peacetime. This included the norm that states should refrain from targeting each other's critical infrastructure, that they should not target other states' authorized computer emergency response teams, known as "CERTs" or "CSIRTs", and that they should not knowingly let their territory be used for internationally wrongful acts using cyberspace (United Nations General Assembly, 2015). Germany chaired the fifth iteration of the group, which was tasked with discussing the application of the laws of war to an online conflict. Yet, in summer 2017, the process to write the rules that should guide state activity in cyberspace came to a halt. The GGE talks collapsed without a consensus report due to fundamental divides between a coalition of Western states on the one side and Russia, China and others, on the other. As Grigsby (2017) points out, a major problem was that the UN diplomatic efforts "looked increasingly divorced from the operational reality of state-sponsored cyber actions". Indeed, state-sponsored malicious cyber activities have intensified throughout the past years. For example, the US and Israel allegedly launched a covert operation called "Olympic Games" in 2008 which targeted Iranian nuclear facilities, and Russian state-sponsored hackers are suspected of having been responsible for cyber-attacks that caused power outages in Ukraine in 2015 and 2016, as well as attempting to influence democratic elections in other states through the use of hacking and online propaganda methods.

Other efforts to defend cyber-norms processes such as the EU's adoption of a "cyber toolbox", which enables the EU to levy sanctions in response to a state-sponsored cyber evidence, constitutes an important diplomatic initiative, but does not present a set of rules that are shared by states such as Russia or China (Grigsby, 2017).

With ever deepening divides among major powers over cybersecurity and international security more generally, Germany should cooperate with France as well as other European and international partners to develop a model code of good governance in cyberspace. The code should promote a free and secure cyberspace and include clear rejections of human rights violations online and propaganda manipulations of democratic processes (Schallbruch, Gaycken, & Skierka, 2018). Germany should specifically also look to rising non-Western democratic powers for cooperation, such as in the context of the UN resolution on the right to digital privacy in 2014 when it had partnered with Brazil. Moreover, to achieve an overarching acceptance, Germany could include non-state actors into these efforts.

In order to strengthen Germany's international role in cybersecurity and good governance of the internet, the government should specifically strengthen the German federal foreign office's role in national as well as international cybersecurity policy and equip it with personnel and organizational additional resources. In 2019, Germany will host the UN IGF in Berlin, which presents an additional opportunity for Germany to assume a leading role.

### *5.8 References*

Abel, W., & Schafer, B. (2009). The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822. *SCRIPT, 6*(1), 106-123.

Assembly, U. N. (2013). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98.*

Bundesministerium des Innern. (2011). *Cyber-Sicherheitsstrategie für Deutschland*. Berlin.

Bundesministerium des Innern. (2016). *Cyber-Sicherheitsstrategie für Deutschland*. Berlin.

Bundesministerium für Wirtschaft und Energie. (2014). *Der IT-Sicherheitsmarkt in Deutschland*.

Bundesregierung. (1999). *Bericht der Bundesregierung zu den Auswirkungen der Nutzung kryptografischer Verfahren auf die Arbeit der Strafverfolgungs- und Sicherheitsbehörden (Ziffer 4 der Eckpunkte der deutschen Kryptopolitik vom 2. Juni 1999) „Verschlüsselungsbericht“.*

Bundesverfassungsgericht. (2008). *NJW*, 822.

CDU/CSU, & SPD. (2018). Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land. Koalitionsvertrag zwischen CDU/CSU und SPD, 19. Legislaturperiode. Berlin.

Diekmann, Gesa. (2015). *Digitale Souveränität - Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa*. Berlin: Bitkom.

ENISA. (2014, July). *Europe's ICT sector - The need for coordinated and responsive EU policies*. Retrieved from https://www.enisa.europa.eu/events/enisa-events/enisa-high-level-event-2014-and-ecsm-launch/eu-digital-security-policy

European Commission. (2017). Title III of the Proposal for a Regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification '('Cybersecurity Act''), 2017-09-13, COM(2017) 477final.

Forschungszentrum Informatik, Accenture GmbH, Bitkom Research GmbH. (2017). *Kompetenzen für eine Digitale Souveränität*. Bundesministerium für Wirtschaft und Energie (BMWi).

Gallagher, S. (2014, May 14). *Photos of an NSA "upgrade" factory show Cisco router getting implant*. (Ars Technica) Retrieved March 31, 2018, from https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/

Gaycken, S. (2017). Recommendations for the Development of Vulnerability Equities Processes. *DSI Industrial and Policy Recommendations*(7).

Gerlach, C. (2015). Sicherheitsanforderungen für Telemediendienste – der neue § 13 Abs. 7 TMG. *CR*, 581.

Government of the United States. (2017). *Vulnerabilities Equities Policy and Process for the United States Government.*

Grigsby, A. (2017). The End of Cyber Norms. *Survival, 59*(6), 109-122.

Hathaway, M., & Klimburg, A. (2012). Preliminary Considerations: On National Cyber Security. In A. Klimburg, *National Cyber Security Framework Manual* (pp. 1-43). Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Herpig, S. (2017). Government Hacking. Global Challenges. *Stiftung Neue Verantwortung Impulse*(October), 1-18.

Hornung, G. (2008). Ein neues Grundrecht. Kommentierung zur BVerfG-Entscheidung. *CR*, 299.

Hornung, G. (2015). Neue Pflichten für Betreiber kritischer Infrastrukturen: Das IT-Sicherheitsgesetz des Bundes. *NJW*, 3334.

Kingdon, J. W. (2003). *Agendas, alternatives, and public policies*. New York: Harper Collins College Publishers.

KPMG. (2014). *IT-Sicherheit in Deutschland - Handlungsempfehlungen für eine zielorientierte Umsetzung des IT-Sicherheitsgesetztes*.

Krempl, S. (2017, June 23). *Staatstrojaner-Gesetz: Nächster Halt Bundesverfassungsgericht*. (heise online) Retrieved March 31, 2018, from https://www.heise.de/newsticker/meldung/Staatstrojaner-Gesetz-Naechster-Halt-Bundesverfassungsgericht-3754891.html

Lachow, I. (2013). Active Cyber Defense: A Framework for Policymakers. *Center for New American Security Policy Brief*(February).

Luiijf, E., & Healey, J. (2012). Organisational Structures & Considerations. In A. K. (ed.), *National Cyber Security Framework Manual* (pp. 108-145). Tallinn: NATO CCDCOE.

Masters, J. (2014, April 23). *What is Internet Governance?* (Council on Foreign Relations) Retrieved March 31, 2018, from https://www.cfr.org/backgrounder/what-internet-governance

Organization for Security and Co-Operation in Europe. (2016). *Decision No. 1202 - OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies*.

Potter, E. H. (2002). *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century*. Quebec: McGill-Queen's University Press.

Reinhold, T., & Schulze, M. (2017). Digitale Gegenangriffe. Eine Analyse der technischen und politischen Implikationen von "hack backs". *Arbeitspapier der Stiftung Wissenschaft und Politik*.(1).

Schallbruch, M. (2017). IT-Sicherheitsrecht – Schutz digitaler Dienste, Datenschutz und Datensicherheit. *CR*, 799-804.

Schallbruch, M. (2017). IT-Sicherheitsrecht – Schutz kritischer Infrastrukturen und staatlicher IT-Systeme. Zur Entwicklung des IT-Sicherheitsrechts in der 18. Wahlperiode (Teil 1). *CR*, 648-656.

Schallbruch, M., Gaycken, S., & Skierka, I. (2018). Cybersicherheit 2018-2020: Handlungsvorschläge für CDU/CSU und SPD. *DSI Industry & Policy Recommendations (IPR) Series*(1).

Singelnstein, T., & Derin, B. (2017). Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens. *NJW*, 2646.

Spindler, G. (2016). IT-Sicherheitsgesetz und zivilrechtliche Haftung. *CR*, 297.

Tanriverdi, H. (2017a, January 10). *Der gefährliche Wunsch nach digitalen Gegenangriffen*. Retrieved March 07, 2018, from http://www.sueddeutsche.de/digital/verfassungsschutz-der-gefaehrliche-wunsch-nach-digitalen-gegenangriffen-1.3327618

Tanriverdi, H. (2017b, June 21). *Bundesbehörde diskutiert digitale Gegenschläge*. Retrieved March 07, 2018, from http://www.sueddeutsche.de/digital/it-sicherheit-bundesbehoerde-diskutiert-ob-sie-zurueck-hacken-soll-1.3554124

(2005). *Tunis Agenda for the Information Society*. World Summit on the Information Society. Retrieved from https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

United Nations General Assembly. (2013). The right to privacy in the digital age. Resolution 68/167. 18 December 2013. New York.

United Nations General Assembly. (2014). *Revised draft resolution on the right to privacy in the digital age*.

United Nations General Assembly. (2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174*.

Verizon. (2015). *2015 Data Breach Investigations Report*.

Verizon. (2017). *2017 Data Breach Investigations Report, 10th Edition*.

# Chapter 6: Conclusion

**Abstract** With a strong defensive, technically and organizationally oriented approach, Germany has now achieved a high level of cybersecurity development. Following the US, Germany was one of the first countries with a far-reaching strategy to protect critical information infrastructures. Its implementation has been achieved through a mixture of a regulatory approach and a public-private partnership, and is well underway compared to other European countries. Germany has also made reasonably rapid progress in setting up and legally enforcing the fight against cyber crime. The country has had a strong influence on European strategy and regulation in these two areas, protecting critical infastructures and fighting cyber crime. Cybersecurity as an area of policy has attained high priority in Germany. The new federal government, formed in 2018, has recognized the need for a radical overhaul of the architecture of the German security agencies to meet the challenges of cybersecurity. However, it is doubtful whether the government will manage to restructure the complex distribution of responsibilities within the German state organisation. In any case, the further opening of the German cybersecurity policy towards more active cyber defence measures and the creation of corresponding legal regulations and practical facilities is likely. The central question of German politics will continue to be the right balance between ensuring cybersecurity and national security on the one hand and protecting civil liberties and privacy on the other. It would be a welcome development if the country, on the basis of these approaches, were to engage more strongly in the international debate.

**Keyword** Cybersecurity · National security · Civil liberties · Diplomacy

With a strong defensive, technically and organizationally oriented approach, Germany has now achieved a high level of cybersecurity development. Following the US, Germany was one of the first countries with a far-reaching strategy to protect critical information infrastructures. Its implementation has been achieved through a mixture of a regulatory approach and a public-private partnership and is well underway compared to other European countries. Germany has also made reasonably rapid progress in setting up and legally enforcing the fight against cyber crime. The country has had a strong influence on European strategy and regulation in these two areas, protecting CI and fighting cyber crime. Especially the large businesses in Germany have supported the national strategy through active involvement in public-private partnerships, such as UP KRITIS, or through the establishment of industry joint ventures such as the German Cybersecurity Organization (DCSO). Cybersecurity as an area of policy has become a very high priority in Germany—in government, industry and public perception. Until 2016, however, the overarching strategy remained very limited to CI protection and the fight against cyber crime. Since then, the focus has expanded. The Bundeswehr is more strongly concerned with international security and military aspects of cybersecurity. The technology policy discussion of cybersecurity is increasingly evolving from a purely political debate to an administrative strategy. The new federal government, formed in 2018, has recognized the need for a radical overhaul of the architecture of the German security agencies to meet the challenges of cybersecurity. However, it is doubtful whether the government will manage to restructure the complex distribution of responsibilities within the German state organisation. In any case, the further opening of the German cybersecurity policy towards more active cyber defence measures and the creation of corresponding legal regulations and practical facilities is likely. The central question of German politics will continue to be the right balance between ensuring cybersecurity and national security on the one hand and protecting privacy and civil liberties on the other. This question will become apparent in the discussions about data retention by providers, the law enforcement and intelligence rights and the handling of vulnerabilities. It would be a welcome development if the country were to introduce its approaches, which have emerged from intensive national discussions, more strongly into the international debate. Germany can make a significant contribution to the development and formulation of a balance between preventive cyber protection and reasonable active defence measures. The same applies to the pervasive experience with public-private partnerships covering many aspects of cybersecurity, which Germany could use as an example in international policy reflections.

The UN resolution "The right to privacy in the digital age", which came into effect following German and Brazilian action in 2013, shows, like the German work in the UN GGE, that Germany has the potential to successfully engage in the international community for common approaches to tackling the challenges of digitisation.

**Publication III**

Drott, Laura, Jochum, Lukas, Lange, Frederik, Skierka, Isabel, Vach, Jonas, van Asselt, Marjolein B. A. (2013). Accountability and risk governance: a scenario-informed reflection on European regulation of GMOs. *Journal of Risk Research*, *16*(9). https://doi.org/10.1080/13669877.2012.743161 (1.1).

# Accountability and risk governance: a scenario-informed reflection on European regulation of GMOs

Laura Drott [a], Lukas Jochum [a], Frederik Lange [a], Isabel Skierka [a], Jonas Vach [a] & Marjolein B.A. van Asselt [a]

[a] Faculty of Arts and Social Sciences, Maastricht University, Maastricht, The Netherlands

Submitted: 19 October 2012; Published: 21 January 2013

# Accountability and risk governance: a scenario-informed reflection on European regulation of GMOs

Regulating risks in the face of scientific uncertainty poses a particular challenge to policy-makers. Such problems are amplified when decisions are taken in a multi-level framework of supranational governance. The genetically modified organism (GMO) regulation in the European Union constitutes an especially salient issue of risk governance in a multi-lateral arena, as the topic is politically highly visible and decision-making is slow and contested. Furthermore, as authority is dispersed among multiple actors, European risk governance is in need of adequate mechanisms ensuring that decision-makers justify and account for their behavior. While legitimacy aspects of GMO governance have widely been examined, accountability relations within the field of GMO risk governance have hitherto only weakly been explored. Hence, this paper analyzes the question of who can be held accountable under the complex system of supranational risk governance. This paper claims that mere adherence by actors to the regulatory procedures during the decision-making process does not necessarily imply that overall accountability can be secured, resulting in 'organized irresponsibility'. Although certain piecemeal accountability may exist, establishing overall accountability is complicated, precisely as a result of the complex system of interwoven rules.

Keywords: accountability; GMO regulation; risk governance; uncertain risks; organized irresponsibility; multi-level governance

## 1. Uncertain risks, organized irresponsibility, and accountability problems

Scientific and technological progress in an ever more globalized economy has resulted in new innovations, which have often contributed to improved living conditions (Archibugi and Iammarino 1999; Archibugi and Pietrobelli 2003; Castells 1999; International Monetary Fund 2000). Yet, the very same progress has produced unprecedented risks, which are often uncertain and incalculable in nature (Beck 1999; Giddens 1991). Such 'uncertain risks' are usually associated with large-scale, long-term, and transboundary hazards with which society has no or only limited experience (Van Asselt and Vos 2008; Van Asselt, Vos, and Rooijackers 2009). As a result, their risk potential is highly contested. An exemplary uncertain risk is posed by genetically modified organisms (GMOs).[1] As it is contested whether GMOs constitute a risk to the environment and/or human health, scholars have pointed out that GMOs should be conceived of in terms of uncertainty (Ibid.; Lang and Hallmann 2005; Levidow, Carr, and Wield 2005). Indeed, even though scientific or historical proofs of harmful consequences with regard to GMOs are lacking, 'suspicions cannot be fully refuted either' (Van Asselt and Vos 2008, 281). A decisive question is thus how to take decisions in the face of uncertainty (Beck 1999; Löfstedt 2009).

The European Union (EU) plays a central role in addressing and dealing with uncertain GMO risks (Borrás 2006; Van Asselt, Vos, and Rooijackers 2009). The GMO regulation in the EU constitutes a salient issue of risk governance, as the topic is politically highly visible and decision-making is slow and contested (Lee 2008; Renn and Walker 2007; Van Asselt and Renn 2011). We understand risk governance as 'the identification, assessment, management and communication' of potential hazards in the complex network that produces collective binding decisions (International Risk Governance Council 2007; Van Asselt and Renn 2011). The supranational system of multi-level governance in the EU implies that authority is dispersed among many actors. Hence, GMO regulation is in need of adequate mechanisms ensuring that decision-makers justify and account for their behavior (e.g. Bovens 2007a; Fisher 2004; Harlow 2002). It has been pointed out that 'the shift from national, state-based policymaking to transnational and multilevel European governance is not being matched by an equally forceful creation of appropriate accountability regimes' (Bovens 2007b, 104; Harlow 2002). Lee (2008) demonstrates that the absence of accountability arrangements in the GMO regulatory framework constitutes a real gap. She argues that 'who is responsible if things go wrong should be a key element of the regulatory regime for any new technology' (107).

The EU's political attitude towards GMO regulation has been described as precautionary (Cantley and Lex 2011; Klinke et al. 2006; Levidow, Carr, and Wield 2005; Wiener 2011). Since the introduction of GMOs in Europe in 1997, Member States such as Austria, Luxembourg, and Italy repeatedly imposed national bans on genetically modified (GM) crops authorized on a European level. In spite of political controversy, the European Commission (hereafter the Commission) continued to advocate the approval of GM crops. The Commission's behavior arguably raises accountability concerns, which might ultimately result in declining legitimacy of the entire supranational system of risk governance (Skogstad 2011). In fact, Member States in the Council of Ministers (hereafter the Council) threatened with the rejection of any further authorizations until the regulatory procedures of the existing system are improved. Consequently, regulatory reforms took place between 2002 and 2004 and resulted in the present-day legal framework of GMO regulation.

Yet, important legitimacy and accountability problems of GMO regulation on the European level remain. While legitimacy aspects of GMO regulation have already been widely examined (e.g. Bengtsson and Klintmann 2010; Borrás 2006; Skogstad 2003; Tiberghien 2009), accountability relations within the field of GMO regulation have hitherto only been weakly explored (e.g. Skogstad 2011).[2] Nevertheless, it has been pointed out that 'accountability on the EU-level remains fragile and is not secured by a comprehensive formal accountability arrangement' (van de Steeg 2009, 3).

In this paper, we analyze who can be held accountable under the complex system of supranational risk governance with regard to GMO authorization should uncertain risks materialize. In conjunction with this question, we examine why a certain actor can or even should be held accountable. In order to develop a theoretically and empirically informed answer to these questions, we apply a conceptual framework of accountability to the specific case of the authorization of Bt-11 maize[3] in the EU. The Bt-11 case covers different authorization streams for (i) food and (ii) food and feed additives, each of which reveals different regulatory dynamics.[4] This allows for a thorough analysis of accountability relations with regard to different regulatory streams. We first present a conceptual framework of accountability. We then briefly outline EU regulation of GMOs in general and the two authorization streams of Bt-11 in particular. The case subsequently serves as the basis for the development a hypothetical scenario, which is used to assess accountability mechanisms. Eventually, this analysis may serve as a first step towards better understanding accountability relations within the EU authorization framework for GMOs.

We claim that the mere adherence to the regulatory procedures during the decision-making process does not necessarily imply that overall accountability can be secured, even though certain 'piecemeal' accountability may exist. The fact that overall accountability on the European level remains a delicate issue and may not be easily established within the framework of supranational risk governance can be related to Beck's (1999) notion of organized irresponsibility, which can be understood as the paradoxical situation in which contemporary society is incapable of dealing with long-term impacts of unprecedented risks notwithstanding sophisticated decision-making structures in place. Indeed, the complex system of interwoven rules can lead to a situation in which 'a conviction is blocked by the very thing that was supposed to achieve it' (54): adherence to the regulatory framework can make it difficult to hold a single actor accountable and might even lead to a void of accountability. In order to test accountability relations within the multi-level framework of GMO regulation, it is, as Bovens (2006) has pointed out, imperative to establish under what conditions a certain arrangement in fact qualifies as a form of accountability.

## 2. Conceptualizing accountability

Accountability is a contested and often elusive concept of which several definitions exist (Dowdle 2006; Flinders 2001; Mulgan 2000; Romzek and Dubnick 1987; Scott 2006) and it can have numerous meanings (Curtin, Mair, and Papadopoulos 2010). Accountability can be defined as a relationship between two parties: 'A is accountable to B when A is obliged to inform B about A's (past or future) actions and decisions, to justify them, and to suffer punishment in the case of eventual misconduct' (Schedler 1999, 13). In this paper, the focus is on ex-post accountability: the actor has to render account after the event has taken place (Bovens 2007b, 108; Harlow 2002). So, the question is whether actors involved in the authorization of Bt-11 might retrospectively be held accountable might risks materialize. We, furthermore, concentrate on public accountability: those who govern are accountable to those who are governed (Joss 2001). Depending on the forum, accountability can be classified as political (e.g. if the forum is a parliament), legal (e.g. if the forum is a court), or even administrative (e.g. if the forum is an administration such as the Court of Auditors) (Bovens 2007b, 108). Nevertheless, the *principal* forum in democracies is the public, which should ideally be able to scrutinize and judge the conduct of those who govern. Put briefly, for public accountability, also referred to as overall accountability,[5] to exist, it should always be possible to trace back the whole accountability chain to the principal forum, the citizenry. Accountability is thus defined in terms of an explicit actor–forum relationship (Bovens 2006, 2007a, 2007b). Bovens (2006, 10) argues that the relation between the actor and the forum has to be structured according to the following criteria in order to be qualified as overall accountability:

(1) there has to be a relation between an actor and a forum,

(2) where the actor is obliged to inform about,

(3) explain and justify his conduct to the forum,

(4) so that the forum can interrogate the actor,

(5) question the legitimacy of his conduct,

(6) and pass judgment on the actor's conduct,

(7) which might lead to sanctions of some kind.[6]

It is important to emphasize that only when *all* these criteria are met, overall accountability is established. Yet, Bovens' criteria are not beyond criticism. Whereas van de Steeg (2009) argues that the possibility of sanctions is an essential element, Harlow and Rawlings (2007) point out that it may 'rather than "thickening" accountability, act as a deterrent by creating incentives to deny responsibility' (546). But in contrast, to wider and less well-defined frameworks used by other authors (e.g. Behn 2001; Mulgan 2000), Bovens' criteria allow for a focused analysis: his criteria can be used as a kind of checklist. Although Bovens does not concentrate on the active process of holding to account, his accountability criteria can be employed to examine multiple accountability relations.

Our overall research question is therefore: who can be held accountable under the complex system of supranational risk governance with regard to GMO authorization in general and Bt-11 in particular should uncertain risks materialize? In conjunction with this, two main issues need to be explored. First, to whom is account to be rendered? Thus, to which forum is an actor required to render account? Often, accountability has to be rendered to numerous different forums (Bovens 2007a, 455). This is referred to as the *problem of many eyes*. Second, who should render account? Thus, who among the multiple actors involved has to appear in front of the forum? This has been called the *problem of many hands* as 'policies pass through many hands before they are actually put into effect' (457). In the case of GMOs, several actors (many hands) as well as several forums (many eyes) can be identified. Through the case of Bt-11, we will analyze whether all conditions for overall accountability have been met. Are the identified actors accountable to the identified forums and are these forums able to pass judgment on the actor's conduct?

As this brief review of established approaches to accountability indicates, the topic itself has received sufficient attention in the literature. However, in the context of GMO regulation in the EU, discussion has tended to focus on the issue of legitimacy, as already mentioned in the introduction. In these instances, however, it can be argued that there exists a close relationship between the two concepts, as, for example, Borrás (2006), Skogstad (2003), Bengtsson and Klintmann (2010), as well as Tiberghien (2009) suggest. Most prominent is the idea that recent tendencies in the EU towards 'quasi-autonomous or independent agencies has weakened the legitimacy of the Weberian and Diceyan systems of political control through the minister' (Bovens 2007b, 110–1). Consequently, accountability is argued to 'make up' for this democratic deficiency created by, for instance, 'technocratic and intergovernmental arenas such as comitology' (104). As a result, lack of appropriate accountability mechanisms is directly connected to problems of legitimacy, as '[a] ccountability deficits are said to be a key cause of the low public visibility and legitimacy of the EU' (Ibid.; Skogstad 2003, 2). Other authors, on the other hand, have pointed towards the fact that this relationship might, in fact, be more complicated. Brandsma and van de Steeg (2006) argue that accountability practices can both increase and decrease the perceived legitimacy of certain actors and institutions. On the one hand, accountability arrangements can appear to require actors to 'play by the rules', while the same arrangements can, on the other hand, create the idea that 'the wheeling and dealing of the actors involved is nasty and dirty business' (4) thus negatively effecting the legitimacy of the respective actors.

This shows that although the concept of accountability itself – as well as its relationship to legitimacy – has indeed been discussed, the actual accountability relations in a European context are yet to be fully explored.

## 3. GMO regulation in the EU

The present EU regulatory framework of GMOs is the result of regulatory reforms that took place between 2002 and 2004. In general, the authorization of GMOs is based on comitology, which is defined as 'delegation of powers to the Commission and the supervision of the Commission's use of these powers through Committees composed of Member States' representatives' (Christiansen and Polak 2009, 5). The two key legal documents are Directive 2001/18/EC[7] on the deliberate release of GMOs (experimental or on the market) in the environment, and the Food and Feed Regulation (EC) 1829/2003.[8] The objectives include, among others, ensuring a high protection of human and animal health, taking account of environmental and consumer interests, but also providing for the proper function of the internal market. Regulation (EC) 178/2002 also defines the role of the European Food Safety Authority (EFSA), which serves as the independent scientific advisory forum to the Commission. The Commission's draft decisions on the authorization of certain GMO are forwarded to the Standing Committee on the Food Chain and Animal Health[9] (hereafter the Standing Committee). If the Standing Committee is unable to deliver a decision within 3 months or cannot reach a decision by qualified majority voting (QMV), the Commission decision is passed on to the Council. If the Council, too, is unable to reach a decision by QMV, the authorization decision reverts back to the Commission.[10] The Commission is then in a position to take the final decision.[11]

### *3.1. Authorization of Bt-11 maize*

The authorization of Bt-11 is subdivided into three different streams (see Table 1). The authorization stream for cultivation of Bt-11 (Table 1 stream 1, not discussed in more detail) is still pending at the time of writing as the Council has yet to act. Bt-11 as food (stream 2) and Bt-11 as food and feed additive (stream 3) have been

Table 1. The different authorization phases of Bt-11 maize divided by product use (Table by authors based on GMO Compass (2012b)).

| Stream | (1) Cultivation | (2) Sweet maize as food | (3) Food and feed additive |
|---|---|---|---|
| Scope | Cultivation, feed, and industrial processing | Sweet maize as food (freshly or preserved) and food additives | Food and feed additives |
| Status | Risk assessment report | Valid authorization granted | Valid authorization granted |
| Relevant legal framework | Submitted under Directive 2001/18/EC (and under earlier Directive 90/220/EC).<br>Application appropriately expanded in 2003 | The application was submitted under previous Novel Food Regulation (EC) 258/97. Assessment and licensing under Regulation (EC) 1829/2003 | Submitted under earlier Directive 90/220/EC and Novel Food Regulation (EC) 258/97. Valid license transfer.<br>Renewal: Regulation (EC) 1829/2003 |
| Application date | 1996 in France | 11/02/1999 in the Netherlands | 1996 in the UK |
| Decision | No QMV in Standing Committee referred to Council, which has yet to act | 19/05/2004 (authorized by Commission Decision) until 18/05/2014<br>Renewal in one single decision: 28/07/2010 (authorized by Commission Decision) | 1998 (authorized by Commission Decision) until 18/04/2007 |
| Expiry date of authorization | Pending | 27/07/2020 | |

authorized for import and marketing in the EU. Due to our interest in ex-post accountability, we focus on streams 2 and 3.

Initially, the producer Novartis launched the authorization process of Bt-11 by applying for registration concerning food and feed additives (stream 3) in the UK in 1996. While the competent authority in the UK forwarded the dossier to the Commission with a favorable opinion, other Member States voiced their objections (Commission Decision 98/292/EC). Yet, on 12 February 1998, the Scientific Committee on Plants[12] concluded that 'there are no reasons to believe that […] [the] maize grain is likely to cause any adverse effects on human health and the environment' (preamble). Accordingly, the Commission decided in April 1998, that 'consent shall be given by the competent authorities of the United Kingdom to the placing on the market of the following product, notified by Novartis Seeds Inc' (Art.1(1)) and '[t]he consent shall cover the placing on the market of the product to be used as any other maize grain but not for cultivation' (Art.1(3)). Following Art.5 of Regulation 258/97/EC, Novartis notified the Commission about its intention to place food and feed additives containing Bt-11 on the market.[13] This finalized the authorization under stream 3 for the time being.

After Novartis' fusion with Astra Zeneca, in February 1999, the company applied to the Netherlands under its new name Syngenta for placing Bt-11 as food on the market (stream 2).[14] The application was first examined by the Dutch competent authority. The Dutch risk assessment, released in May 2000, described Bt-11 to be as safe as conventional maize (GMO Compass 2012b). After the Commission had forwarded the risk assessment to the Members States, some raised reasoned objections (Commission Decision 2004/657/EC, recital 5). Following the favorable opinion of the Scientific Committee on Food with regard to the safety of Bt-11 maize (recital 9),[15] the Commission passed a draft decision to the Standing Committee. However, the Standing Committee was not able to agree with QMV (GMO Compass 2012b). Likewise, the voting in the Council resulted in a stalemate. Thus, the proposal was returned to the Commission, which in May 2004 granted approval until May 2014 (Commission Decision 2004/657/EC).

In a comparable way, the Commission also decided on the renewal of authorization of Bt-11 food and feed additives, whose first-phase authorization expired in April 2007. On 28 January 2009, EFSA's GMO Panel gave its favorable opinion for renewal (GMO Compass 2012b). Yet, as neither the Standing Committee nor the Council could reach QMV, the authorization was renewed by the Commission in July 2010 for the next 10 years. The same decision also extended the authorization for Bt-11 as food until the same date, and thus combined the second and third stream into a single decision.[16] This implies that Bt-11, authorized in the EU since 1998 (stream 3) and 2004 (stream 2), can be used as food and as food and feed additive till mid-2020.

## 4. Testing current regulatory regimes against future events

When investigating innovative technologies such as GMOs, it is important to note that innovation is in itself a 'generator of uncertainty' (Nowotny 2008). In such a context, developing scenarios is helpful to imagine future situations (Bishop, Hines, and Collins 2007; Børjeson et al. 2006; Van Asselt et al. 2010; Van Notten et al. 2003). A hypothetical scenario can serve as a tool to explore how uncertainties could play out in the future and what impact these might have on accountability relations with regard to supranational risk governance.

Notwithstanding the favorable risk assessments produced in the authorization processes, there has been substantial disagreement in the scientific community as to potential adverse effects of Bt-11 (e.g. Hilbeck and Schmidt 2006; Prasifka et al. 2007). It is, therefore, reasonable to explore a hypothetical scenario in which such uncertain risks would materialize. On the basis of the Bt-11 case history, each juncture of the authorization process will be identified, including the actors involved and the accountability relationships between them. While several forums can be identified, the public remains the principal forum to which account should be rendered. The scenario investigates who might be 'blamed' by whom, for what reasons, and whether the accused actor can be held accountable by the forum in accordance with Bovens' criteria. To structure the analysis, actors are grouped according to their roles envisioned in the regulatory framework (compare Ravetz 2001; Van Asselt and Vos 2008): Syngenta as the risk producer, EFSA as the risk assessor,[17] and the Member States, the Commission and the Council as the risk managers.[18] As also Van Asselt and Vos (2008) have observed in authorization processes concerning other GMOs (i.e. NK603, GT73 and MON863 x MON810), in practice, role ambiguity reigns. While Syngenta is naturally the risk producer, it also functions as risk assessor as a result of procedures and resources, due to which EFSA and its predecessors actually merely review the risk producers' risk assessments (EFSA 2011). Due to the political deficit (no QMV and hence technocratic decision-making) and the Commission's rubber-stamping of EFSA's opinions, EFSA's role extends to that of a risk manager as will be elaborated below. Nevertheless, the default roles serve as a useful guidance in the scenario development.

### *4.1. Hypothetical scenario: adverse effects on human health*

Thirty years after the initial authorization, the consumption of GM maize, including Bt-11 gene products, is linked to an outbreak of new food allergies. As warnings from the scientific community are getting louder, the media and nongovernmental organizations (NGOs) are quick in picking up the topic and increase public awareness. Suddenly, retailers and the manufacturer find themselves under sharp attack. Consumers are highly worried and start boycotting most GM products. Similar to earlier food scares,[19] which are generally associated with 'spiraling public anxiety over food safety incidents and escalating media attention that supplements such events' (Knowles, Moody, and McEachern 2007, 43), consumer consumption and purchase behaviors are negatively affected. As a result, many retailers quickly withdraw GM products from sale. Fearing bad publicity and damage to corporate reputation, Syngenta immediately publishes a press release stating that it adhered to all legal rules and procedures. The company also emphasizes that EFSA at the time endorsed Syngenta's risk assessment. Member States inform the Commission of the need to take emergency measures, using the Rapid Alert System for Food and Feed (RASFF).[20] The Commission reacts by recalling all products containing Bt-11 from the market.[21] Who can be held accountable under the complex system of supranational risk governance with regard to GMO authorization?

#### *4.1.1. Risk producer: Syngenta*

Since the authorization process was initiated with an optimistic risk assessment by Syngenta, the first focal point is the company itself. International NGOs and the media are quick in denouncing the company for its apparent detrimental health impacts and question the credibility of Syngenta's risk assessment. In addition, some consumers seek to hold the company liable for damages occurred to them. In fact, the company's track record is not clean. Between 2001 and 2004, Syngenta mislabeled and sold unapproved and experimental Bt-10 as Bt-11 to US farmers, resulting in international public outbursts and corporate reputation damage (Bahnsen 2005; Herrera 2005). Yet, in this scenario, it is unlikely that the company can be sanctioned, as Syngenta at the time of authorization adhered to all relevant legal procedures and the European authorities approved its risk assessment.[22]

### *4.1.2. Risk assessor: EFSA*

As EFSA endorsed Syngenta's risk assessments and disqualified Member States' reservations, it is likely to be asked to justify its decision. However, holding EFSA accountable may prove difficult if not impossible, due to its largely independent status (Vos 2005). When creating EFSA, the Commission failed to distinguish between two models of delegation: (1) a mechanism under which EFSA is accountable to the Commission and (2) a clear emphasis on EFSA's independence (Collins 2003). The resulting inconsistency is visible in official EU documents. While the White Paper on Food Safety superficially states that the agency should be both independent and accountable to the European institutions (European Commission 2000, para 41), Regulation 178/2002/EC merely stresses the principle of independence (Art.37) and does not mention accountability. In this sense, accountability relationships are neither part of the institutional structures of the Commission 'nor is it [EFSA] answerable to it [the Commission] with regard to the quality of its scientific advice' (Kuiper 2009, 394).

Art.6(2) of Regulation (EC) 178/2002 states that the Commission is required to base its decision on a scientific risk assessment. However, as the Commission lacks the necessary resources and scientific expertise to conduct such assessments, it has been argued that it is difficult if not almost impossible for the Commission to deviate from EFSA's recommendation (Christiansen and Polak 2009). With the Commission simply following EFSA's opinion, the functional separation between risk management and risk assessment becomes diluted. This has led to much criticism, as EFSA, now de facto both risk assessor and risk manager, is consequently in a position to yield considerable power over the authorization process (Bengtsson and Klintman 2010; van Asselt and Vos 2008).

Notwithstanding the above, there are three relevant forums to which EFSA *should*, in principle, render account: the Member States, the Commission, and the public. First, EFSA should, in principle, be partly accountable to Member States. Yet, the fact that Member States are not represented in EFSA's Management Board and are thus not directly involved in scientific processes reinforces EFSA's independence. Scholars have, however, pointed to the significant role of the Advisory Forum. The agency's Advisory Forum, which serves as a platform for the exchange of scientific information, is comprised of representatives of national food safety authorities of all EU Member States and has to meet at least four times a year (EFSA 2012a). The 'conflict clause' laid down in Art.30(4) of Regulation 178/2002 holds that 'where a substantive divergence of scientific issues has been identified […] the Authority and the national body shall be obliged to cooperate'. Both representatives of the Commission and the European Parliament (EP) are free to join the Forum's meetings as stipulated by Regulation 178/2002, Art.27(7). Moreover, Art.30(4) holds that the Forum is supposed to 'address contentious issues and diverging opinions' and, if no compromise can be reached, it has to submit to the Commission a joint document in which controversial scientific issues are clarified. While the Advisory Forum has been seen as the Member States' important link with EFSA's executive director, who chairs the Forum (Groenleer 2009), the director in fact does not answer to either the Commission or the Member States. Rather, he is merely accountable to the board, which can remove him from office by a majority vote (Ibid.). As such, the Advisory Forum has, in practice, a rather limited role. Consequently, one might argue that while EFSA should, in principle, be accountable to the Member States, EFSA is, in fact, *not* formally required to render account to Member States. While Member States are able to ask for explanation and justification concerning EFSA's risk assessment and EFSA is required to cooperate with Member States in case of diverging scientific opinions, Member States are in no position to pass judgment, leading to sanctions.

A second forum to which EFSA should be accountable is the Commission. In principle, even though the Commission lacks legal supervision, it is able to partly control EFSA's activities through its representation in the Management Board. EFSA's Management Board includes one Commission representative as well as 15 members appointed by the Council after consulting the EP on the basis of a list drawn up by the Commission (EFSA 2012b). In addition, the Commission 'sees a role for itself in the approval of the annual reports, the budget and the financial control' (Vos 2005, 128). However, the fact that EFSA only delivers nonbinding opinions based on its risk assessment implies that the agency does not necessarily need to provide justification concerning its risk assessment, as it is ultimately the Commission's decision whether to follow EFSA's advice. As EFSA's role as risk assessor is thus, in principle, divorced from the Commission's role as risk manager, EFSA is indeed *not* answerable to the Commission. In case uncertain risks materialize, EFSA may argue to be merely the risk assessor and that it is ultimately up to the Commission's judgment whether or not to follow EFSA's advice. While the Commission may question the legitimacy of EFSA's conduct, it is unable to pass judgment, leading to sanctions. At best, a loss of reputation concerning EFSA's credibility might occur.

Third, the last and most important forum is the public. Regulation (EC) 178/2002, Art.10, clearly assigns the duty to EFSA to inform the public in a transparent manner concerning potential risks stemming from food products. In particular, Art.38 holds that EFSA should make public without delay '(a) agendas and minutes of the Scientific Committee and the Scientific Panels (b) the opinions of the Scientific Committee and the Scientific Panels immediately after adoption, minority opinions always being included (c) information on which its opinion is based'. In addition, the Regulation requires EFSA to guarantee the inclusion of concerns of relevant stakeholders and develop 'effective contacts with consumer representatives, producer representatives, processors and any other interested parties' (Art.42). The agency has created online public consultation forums, in which members of the public and interested parties can express concerns with regard to specific scientific issues and submit relevant information and data (EFSA 2012a). Yet, even though the agency has developed a relatively open structure of public consultation procedures and has willingly provided information in a transparent manner during the authorization process of Bt-11, the public is unlikely to be able to ask for justification or to actively interrogate EFSA. Indeed, while the public may question the legitimacy of EFSA's conduct in case uncertain risks materialize, it is in no position to pass judgment, leading to sanctions.

In sum, although EFSA is a highly influential body due to its role as risk assessor and de facto risk manager, it seems to be hardly accountable to any forum. In case uncertain risks materialize, EFSA may refer to its primary de jure role as merely risk assessor and ignore its de facto role as risk manager. Although in regulatory practice a 'gray zone' between risk assessment and risk management has emerged, the strict separation between risk assessment and risk management is inscribed in the regulatory framework (Vos and Wendler 2006). This is likely to be emphasized by EFSA to reject responsibility and it might well be an effective defense.

### *4.1.3. Risk managers: Member States, the Commission, and the Council*

Member States, the ministers in the Council, and the Commission are other important actors during the authorization process of Bt-11. Member States were involved in the authorization process by voting in the Standing Committee and in the Council. In principle, Member States are accountable to their public, as national voters through parliaments can hold national ministers to account for their conduct in the Council (Gallagher, Laver, and Mair 2005). Yet, considering the time passed between the initial authorization and the outbreak of food allergies, the term of office of the responsible ministers is likely to have already elapsed. In theory, their successors are accountable for all their acts, but – in practice – it might be more difficult to hold individual ministers to account, e.g. when their party affiliations are different or the new minister was a critical MP at the time of authorization.[23]

During the authorization for Bt-11 as food, the vote in the Council resulted in a stalemate. The decision, therefore, reverted back to the Commission who, in turn, decided to rely on its initial draft proposal and subsequently authorized Bt-11 for consumption. This complicates the situation as the final decision was made by a technocratic body, which is not as accountable as national ministers would be. The Commission inevitably took a decision not endorsed by QMV in the Council (Christiansen and Polak 2009; Van Asselt and Vos 2008), a situation, which Van Asselt and Vos (2008) qualify as a political deficit.

In principle, the Commission is accountable to the EP as well as to the public. Although the EP is not involved in the decision-making process of GMO authorization, it may retrospectively still act as an important forum to give voice to the European citizens.[24] Van Gerven (2005) shows that under current Community Law 'members of the Commission are bound to explain their action to the EP, and they can be held accountable by Parliament when those actions constitute wrongful behavior' (83). The EP's right to interrogate Commissioners is stated in Art.230 of the Treaty on the Functioning of the European Union (TFEU): 'The Commission shall reply orally or in writing to questions put to it by the EP or by its Members'. Moreover, the EP is able to censure the Commission according to Art.234 of the TFEU, or even force the whole body of the Commission to step down.[25] Here again, the more general problem for accountability arises, namely that after a considerable amount of time, accountability relations are likely to have weakened due to circumstances such as the elapse of the term of office of the Commissioners responsible for the authorization. So, the accountability relationship between the

Commission and the EP in case of future materialization of uncertain risks seems weak.

Admittedly, the public has the opportunity to make comments to the Commission following the publication of EFSA's opinion as stated in Regulation (EC) 1829/2003, Art.6(7). However, 'neither the scope nor the salience of such comments is outlined' and the Commission is 'not specifically mandated to take these [comments] into account' (Scott 2004, 20). In fact, the Commission is merely required to take into account EFSA's opinion. Only if the Commission's recommendation on authorization differs from EFSA's opinion, explanations of the underlying reasons are indispensable (Skogstad 2011, 9). Yet, this was not the case regarding Bt-11 as food and food and feed additives (streams 2 and 3). As a result, the public is retrospectively not in a position to ask for explanation and justification or to actively interrogate the Commission. While it may question the legitimacy of the Commission's conduct, it is unable to pass judgment, leading to sanctions. As such, accountability relations between the Commission and the public are as good as nonexistent.

The members of the Council are individually accountable to the public and their national parliaments. However, since the emergence of majority voting with the Single European Act of 1986, in their national parliaments, ministers are able to justify taken decisions by claiming that they did their best to secure a particular policy, but were outvoted (Bogdanor 2007). While this, of course, does not always happen, in principle, an individual minister 'cannot be made accountable to his or her national parliament for a decision that has been taken by others' (6). Nevertheless, the Council missed the chance of representing Member States' interests (and thereby national public's interests) by having been unable to reach a compromise and left the decision to an unelected and bureaucratic body. This political deficit, which was already undermining the legitimacy of the decision (Borrás 2006), might thus have severe consequences also in view of ex-post accountability. Here again, the public as the principal forum is in a difficult position to hold the Council to account. Only national parliaments are able to ask for explanation and justification and to actively interrogate the Council. While both the public and national parliaments might question the legitimacy of the actors' conduct, neither of the two forums is in a position to pass judgment, which might lead to sanctions. At best, informal sanctions might entail a loss of reputation. Thus, at the supranational level, accountability relationships get diffused, which relates to the problems of many hands and many eyes, as regulatory decisions pass through many hands before being implemented, and as account has to be rendered to numerous forums. However, none of the forums seem able to pass a judgment and sanction in case uncertain risks of Bt-11 would materialize in the way envisioned in this scenario.

## 5. Conclusion

We attempted to explore accountability relations within the supranational multi-level framework of GMO risk governance by means of a hypothetical scenario on adverse effects associated with GMOs in general and Bt-11 in particular. Informed by the regulatory history and state of affairs pertaining to Bt-11, we tested current regulatory standards and future events against the accountability criteria as developed by Bovens. We focused on ex-post accountability to assess whether actors can be retrospectively held accountable: do the rules, regulatory procedures and institutional arrangements sufficiently provide for accountability in case that the outcome of the decision-making process is not satisfactory? While legitimacy of GMO regulation has frequently been discussed in the academic literature, accountability issues are rather underrepresented. Still, as accountability is a necessary prerequisite for legitimacy, its significance should not be underestimated. Decreased accountability may lead to weaker legitimacy.

Our findings can be summarized in three points: first, each actor in the authorization process can, at best, be partly held accountable for his conduct. Hence, overall accountability cannot be established. Second, each actor is able to point to its compliance with the legal rules and procedures of GMO regulation at the times of authorization, which makes it difficult to pass a negative judgment. Third, each actor can refer to the involvement of other actors in reaching the final decision, by which the 'blame' can be shifted to other actors in the accountability chain. In sum, these points reflect Beck's hypothesis of organized irresponsibility: a situation where regulatory structures are unable to sufficiently address negative consequences and long-term impacts, notwithstanding that most actors adhered to the rules and procedures in place. Yet, we do not claim that no accountability is in place, as 'piecemeal accountability' can be established. We suggest the notion piecemeal accountability for situations in which one or more, but not all of Boven's criteria are satisfied. In European GMO regulation, overall accountability, with all Bovens' criteria met, is not in place.

With these findings, we are able to demonstrate that uncertain risks resulting from technological progress and innovation pose a particular governance challenge. The current system of European GMO regulation is unable to sufficiently hold actors accountable, should uncertain risks materialize. This adds an important dimension to ongoing scholarly and societal debates on risk governance. Our scenario-informed reflection based on the authorization of one GMO provides a basis for agenda-setting the issue of accountability and for arguing that this kind of scenario thinking is productive to explore accountability relationships. It does, however, not provide a sufficient basis for concrete suggestions what is needed to improve accountability relations in the EU risk regulatory system. It should, furthermore, be noted that our adoption of a strictly de jure approach has left no room to explore, in more detail, the political dynamic that our hypothetical scenario undoubtedly entails. While this is an important issue to be considered, further research is needed in this respect.

Nevertheless, it is clear that in the current European regulatory framework on GMOs in particular and probably on innovation induced risks more generally, the pursuit of accountability relations is simultaneous necessary but difficult to achieve.

## Acknowledgments

This paper resulted from a student research project in the so-called Marble program (Maastricht Research-based Learning), led by professors van Asselt and Vos at Maastricht University, the Netherlands. We acknowledge the fruitful input by the staff (Ellen Vos, Frederic Bouder, and Denise Prevost) as well as of our fellow students in the project: Carolin Ifländer, Felix Kartte, Sonja Koehler, Simon Reetz, Juliane Reschke, Nicole Rode, and Lea Tries. Furthermore, we would like to thank Ragnar Löfstedt (King's Centre for Risk Management, London) and Ruth Mampuys (COGEM, the Netherlands) for their constructive feedback and their insightful comments.

## Notes

[1] The term GMO refers to organisms whose genetic makeup has been restructured during the process of genetic engineering in order to alter an organism's behavior, its growth potential, or its resistance to diseases and pesticides.

[2] Skogstad (2011) examines difficult-to-reconcile conflicts between the internal accountability standards of Member State citizens and external accountability obligations to fellow World Trade Organization (WTO) members. Yet, we focus on the accountability relations between different actors within the process of multi-level EU risk governance.

[3] Bt toxin has a deadly effect on various insects and is produced by the soil bacterium Bacillus thuringiensis: 'by means of genetic engineering, the genes for the active agent (Bt toxin) can be transferred from Bt bacteria to plants' (GMO Compass 2012a). Thus, Bt-11 maize is able to produce the insect toxin on its own which is meant to protect it from damage from certain insect pests and, moreover, 'show tolerance to glufosinate ammonium herbicides' (Syngenta n.d., available online at http://www.infogm.org/IMG/pdf/snif_bt11_renew.pdf).

[4] Note that there is also a stream for cultivation, which has, however, not yet been finalized and will not be discussed in this paper.

[5] Throughout the paper, we will employ the term overall accountability.

[6] We read this as including the possibility of informal or soft sanctions, such as the loss of reputation.

[7] Directive 2001/18/EC replaced Directive 90/220/EC.

[8] Regulation (EC) 1829/2003 replaced the 1997 Novel Food Directive.

[9] Consisting of representatives of all Member States and chaired by a Commission representative.

[10] For an analysis of votings concerning GMOs in the Standing Committee and the Council, see: Navah, Versluis, and Van Asselt (forthcoming).

[11] Note that under the new comitology procedures, the Commission's ability to make the final decision has been limited (Council Decision 2006/512/EC and Treaty of the Functioning of the EU, Art. 290 and 291).

[12] In the beginning of the authorization procedures of Bt-11, EFSA had not yet been founded. Risks assessments and opinions to inform draft decisions were carried out by EFSA's predecessors, the Scientific Committee on Plants, and the Scientific Committee on Food.

[13] The product was included in a summary of notifications received by the Commission in Commission Notice 1999/C 181/15. After a valid license transfer, Bt-11 was referred to in a list of April 2005 concerning 26 authorized GM products that had been approved (or did not require approval) before the new legislative framework had come into effect (Europa Press Releases RAPID. Register of existing GM food and feed products published (IP/05/439)).

[14] The application was submitted under the outdated Novel Food Regulation 258/97.

[15] Validation studies were carried out by the Joint Research Center of the Commission working in collaboration with the European Network of GMO Laboratories. Recital (9) Commission Decision 2004/657/EC.

[16] Commission Decision 2010/419/EU (28 July 2010). By repealing Commission Decision 2004/657/EC that granted authorization of sweet maize as food, the Commission provided a single decision for: foods and food ingredients; feed containing, consisting of, or produced from Bt-11 maize; products other than food and feed containing or consisting of Bt-11 maize for the same uses as any other maize *with the exception of cultivation*.

[17] Risk assessment is a 'procedure for including science in decisions about whether and to what extend risks to health, safety, or the environment should be limited' (Charnley and Rogers 2011, 362). Yet, 'in nearly all cases the science, and hence the RA [risk assessment], is beset by uncertainties' (Ibid.).

[18] Risk management can be understood as 'the process of deciding what appropriate actions to take in order to avoid, reduce, or eliminate a risk when there is (or might be) one' (Charnley and Rogers 2011, 364).

[19] For instance the bovine spongiform encephalopathy (BSE) crisis in 1996, the Dioxin scandal in Belgium in 1999 or the enterohemorrhagic Escherichia coli in Germany in 2011.

20. The legal basis of the RASFF is Regulation (EC) 178/2002, which provides for emergency measures in case that food or feed (imported or of Community origin) constitutes a serious risk to human health, animal health, or the environment. Art.50(2) states that if Member States or the Authority have 'any information relating to the existence of a serious direct or indirect risk to human health deriving from food or feed, this information shall be immediately notified to the Commission under the rapid alert system'.
21. In case the Commission would fail to take measures, the Member States would have the opportunity to 'adopt interim protective measures' (Regulation (EC) 178/2002, Art.54(1)).
22. Private corporate liability is indispensable for fair market conduct and safeguarding consumers' interests, but the liability debate falls outside the scope of this paper. We would, however, like to emphasize that adequate and strict liability mechanisms could provide for a serious financial incentive for risk producers to conduct a more rigid risk assessment in the first place. This is of particular importance with regard to EFSA's reliance on the initial information provided by the applicant company (EFSA 2011).
23. It should, however, be noted that the problem of the elapse of term of office is not necessarily particular to the case, but constitutes, in fact, a more general problem for accountability. While it could be argued that accountability is not time-barred, the problem remains that accountability relations are likely to weaken, rather than strengthen, over time, if above-mentioned circumstances such as the elapse of term of office occur.
24. This has been demonstrated by the EP's inquiry report with regard to the management of the EU BSE crisis (EP 1997).
25. In 1999, for example, the Santer Commission was successfully pressured into resigning after having been accused of serious mismanagement and corruption.

## References

Archibugi, D., and S. Iammarino. 1999. The policy implications of the globalisation of innovation. *Research Policy* 28, nos. 2–3: 317–36.

Archibugi, D., and C. Pietrobelli. 2003. The globalisation of technology and its implications for developing countries: Windows of opportunity or further burden? *Technological Forecasting and Social Change* 70, no. 9: 861–83.

Bahnsen, U. 2005. Böse Panne auf dem Maisfeld. *Zeit Online*, March 31. http://www.zeit.de/2005/14/Boese_Panne_auf_dem_Maisfeld.

Beck, U. 1992. *Risk society*. New Delhi: Sage.

Beck, U. 1999. *World risk society*. Cambridge: Polity Press.

Behn, R.D. 2001. *Rethinking democratic accountability*. Washington, DC: Brookings Institution Press.

Bengtsson, B., and M. Klintmann. 2010. Stakeholder participation in the EU governance of GMO in the food chain. In *Environmental politics and deliberative democracy*, ed. K. Bäckstrand, J. Kahn, A. Kronsell, and E. Lövbrand, 105–22. Cheltenham: Edward Elgar.

Bishop, P., A. Hines, and T. Collins. 2007. The current states of scenario development: An overview of techniques. *Foresight* 9, no. 1: 5–25.

Bogdanor, V. 2007. Legitimacy, accountability and democracy in the European Union. *A Federal Trust Report*. http://www.fedtrust.co.uk/admin/uploads/FedT_LAD.pdf.

Børjeson, L., M. Hojer, I. Dreborg, T. Ekvall, and G. Finnveden. 2006. Scenario types and techniques: Towards a user's guide. *Futures* 38, no. 7: 723–39.

Borrás, S. 2006. Legitimate governance of risk at the EU level? The case of genetically modified organisms. *Technological Forecasting and Social Change* 73, no. 1: 61–75.

Bovens, M. 2005. Public accountability. In *The Oxford Handbook of Public Management*, ed. E. Ferlie, L.E. Lynn, and C. Pollitt, 182–201. Oxford: Oxford University Press.

Bovens, M. 2006. *Analysing and assessing public accountability: A conceptual framework*. European Governance Papers (EUROGOV) No. C-06-01. http://www.connex-network.org/eurogov/pdf/egp-connex-C-06-01.pdf.

Bovens, M. 2007a. Analysing and assessing accountability: A conceptual framework. *European Law Journal* 13, no. 4: 447–68.

Bovens, M. 2007b. New forms of accountability and EU-governance. *Comparative European Politics* 5, no. 1: 104–20.

Brandsma, G.J., and M.W. van de Steeg. 2006. Accountability in the European Union: The cases of the Comitology Committees and the European Council. *Utrecht School of Governance*. http://igitur-archive.library.uu.nl/USBO/2012–0328–200616/Accountability%20in%20the%20European%20Union_the%20cases%20of%20the%20Comitology%20Committees%20and%20the%20European%20Council.pdf.

Cantley, M., and M. Lex. 2011. Genetically modified foods and crops. In *The reality of precaution. Comparing risk regulation in the United States and Europe*, ed. J.B.Wiener, M. D. Rogers, J.K. Hammitt and P.H. Sand Eds, 39–64. Washington, DC: RFF Press.

Castells, M. 1999. Information technology, globalization and social development. *UNRISD Discussion Paper No. 114*. http://www.unrisd.org/unrisd/website/document.nsf/ab82a6805797760f80256b4f005da1ab/f270e0c066f3de7780256b67005b728c/$FILE/dp114.pdf.

Charnley, G., and M.D. Rogers. 2011. Frameworks for risk assessment, uncertainty, and precaution. In *The reality of precaution. Comparing risk regulation in the United States and Europe*, ed. J.B.Wiener, M.D. Rogers, J.K. Hammitt and P.H. Sand, 78–82. Washington, DC: RFF Press.

Christiansen, T., and J. Polak. 2009. Comitology between political decision-making and technocratic governance: Regulating GMOs in the European Union. *EIPAScope* 2009, no. 1: 1–7.

Collins, W.S. 2003. The Commission's delegation dilemma: Is the European Food Safety Authority an independent or accountable agency? *U.C. Davis International Law and Policy* 10: 277–300.

Craig, P. 2000. The fall and renewal of the Commission: Accountability, contract and administrative organisation. *European Law Journal* 6, no. 2: 98–116.

Curtin, D., P. Mair, and Y. Papadopoulos. 2010. Positioning accountability in European governance: An introduction. *West European Politics* 33, no. 5: 929–45.

Dowdle, M.W. 2006. Public accountability: Conceptual, historical, and epistemic mappings. In *Public accountability: Designs, dilemmas and experiences*, ed. M.W. Dowdle, 1–32. New York, NY: Cambridge University Press.

EFSA 2008. Request from the European Commission to review scientific studies related to the impact on the environment of the cultivation of maize Bt11 and 1507 – Question No EFSA-Q-2008-679. *The EFSA Journal* 851: 1–27.

EFSA. 2011. *FAQ on genetically modified organisms*. http://www.efsa.europa.eu/en/faqs/faqgmo.htm.

EFSA. 2012a. *Advisory Forum*. http://www.efsa.europa.eu/en/networks/af.htm.

EFSA. 2012b. *Management Board*. http://www.efsa.europa.eu/en/efsawho/mb.htm.

European Commission. 2000. White Paper on Food Safety. COM 1999 719 final.

European Parliament (EP). 1997. Report on alleged contraventions or maladministration in the implementation of Community law in relation to BSE, without prejudice to the jurisdiction of the Community and national courts. A4–0020/97.

Fisher, E. 2004. The European Union in the age of accountability. *Oxford Journal of Legal Studies* 24, no. 3: 495–515.

Flinders, M. 2001. *The politics of accountability in the modern state*. Aldershot: Ashgate.

Gallagher, M., M. Laver, and P. Mair. 2005. *Representative government in modern Europe: Institutions, parties, and governments*. 4th ed. Boston, MA: McGraw Hill.

Giddens, A. 1991. *Modernity and self-identity*. Stanford, CA: Stanford University Press.

GMO Compass. 2003. Syngenta's Risk Assessment of BT11 maize for Dossier C/F/96.05.10. http://www.gmocompass.org/pdf/regulation/maize/Bt11_sweetmaize_2001_snif.pdf.

GMO Compass. 2012a. *Bacillus thuringiensis* Bt. http://www.gmo-compass.org/eng/glossary/39.bacillus_thuringiensis_bt.html (accessed March 26, 2012).

GMO Compass. 2012b. GMO Database. http://www.gmo-compass.org/eng/gmo/db/ (accessed March 26, 2012).

Groenleer, M. 2009. *The autonomy of European Union agencies*. Delft: Eburon Uitgeverij.

Harlow, C. 2002. *Accountability in the European Union*. Oxford: Oxford University Press.

Harlow, C., and R. Rawlings. 2007. Promoting accountability in multi-level governance: A network approach. *European Law Journal* 13, no. 4: 542–62.

Herrera, S. 2005. Syngenta's gaff embarrasses industry and White House. *Nature Biotechnology* 23: 505–14.

Hilbeck, A., and J.E.U. Schmidt. 2006. Another view on Bt proteins – How specific are they and what else might they do? *Biopesticides International* 2, no. 1: 1–50.

International Monetary Fund. 2000. Globalization: Threat or opportunity? *IMF Issues Brief.* http://www.imf.org/external/np/exr/ib/2000/041200to.htm.

International Risk Governance Council. 2007. *Risk governance: Trends and challenges – Future forum for public security.* http://www.zukunftsforum-oeffentliche-sicherheit.de/downloads/ZOES-3-Bunting.pdf.

Joss, S. 2001. Modern challenges for public accountability and their implications for citizenship. *EC-Workshop 'European Citizenship: Beyond Borders, Across Identities'*. ftp://ftp.cordis.europa.eu/pub/improving/docs/ser_citizen_joss.pdf.

Klinke, A., M. Dreyer, O. Renn, A. Stirling, and P. van Zwanenberg. 2006. Precautionary risk regulation in European governance. *Journal of Risk Research* 9, no. 4: 373–92.

Knowles, T., R. Moody, and M.G. McEachern. 2007. European food scares and their impact on EU food policy. *British Food Journal* 109, no. 1: 43–67.

Kuiper, H.A. 2009. The role of scientific experts in risk regulation of foods. In *Uncertain risks regulated*, ed. M. Everson and E. Vos, 389–98. New York, NY: Routledge.

Lang, J.T., and W.K. Hallman. 2005. Who does the public trust? The case of genetically modified food in the United States. *Risk Analysis* 25, no. 5: 1241–52.

Lee, M. 2008. *EU regulation of GMOs: Law and decision making for a new technology.* Cheltenham: Edward Elgar.

Levidow, L., S. Carr, and D. Wield. 2005. European Union regulation of agri-biotechnology: Precautionary links between science, expertise and policy. *Science and Public Policy* 32, no. 4: 261–76.

Löfstedt, R.E. 2009. *Risk management in post-trust societies*. London: Earthscan.

Majone, G. 2000. The credibility crisis of community regulation. *Journal of Common Market Studies* 38, no. 2: 273–302.

Mulgan, R. 2000. Accountability: An ever-expanding concept? *Public Administration* 78, no. 3: 555–73.

Navah, M., E. Versluis, and M.B.A. Van Asselt. Forthcoming. The politics of risk decision making: The voting behaviour of the EU Member States of GMOs. In *Balancing between trade and risk: Integrating legal and social science perspectives*, eds. M.B.A. van Asselt, T. Fox, E. Versluis, and E. Vos. Abingdon: Routledge.

Nowotny, H. 2008. *Insatiable curiosity: Innovation in a fragile future*. Cambridge, MA: MIT Press.

Prasifka, P.L., R.L. Hellmich, J.R. Prasifka, and L.C. Lewis. 2007. Effects of Cry1Ab-expressing corn anthers on the movement of Monarch Butterfly larvae. *Environmental Entomology* 36, no. 1: 228–33.

Ravetz, J.R. 2001. Models of risk: An exploration. In *Knowledge, power and participation in environmental policy analysis*, ed. M. Hisschemöller, R. Hoppe, W.N. Dunn, and J.R. Ravetz, 471–92. London: Transaction Books.

Renn, O., and K. Walker. 2007. *Global Risk Governance: Concept and practice using the IRGC framework*. Dordrecht: Springer.

Romzek, B.S., and M.J. Dubnick. 1987. Accountability in the public sector: Lessons from the challenger tragedy. *Public Administration Review* 47, no. 3: 227–38.

Schedler, A. 1999. Conceptualizing accountability. In *The self-restraining state: Power and accountability in new democracies*, ed. A. Schedler, L. Diamond, and M.F. Plattner, 13–28. London: Lynne Rienner .

Scott, J. 2004. European regulation of GMOs: Thinking about 'judicial review' in the WTO. *Jean Monnet Working Paper* 04, no. 04: 1–29.

Scott, C. 2006. Spontaneous accountability. In *Public accountability: Designs, dilemmas and experiences*, ed. M.W. Dowdle, 174–94. New York, NY: Cambridge University Press.

Skogstad, G. 2003. Legitimacy and/or policy effectiveness? Network governance and GMO regulation in the European Union. *Journal of European Public Policy* 10, no. 3: 321–38.

Skogstad, G. 2011. Contested accountability claims and GMO regulation in the European Union. *Journal of Common Market Studies* 49, no. 7: 1–21.

Tiberghien, Y. 2009. Competitive governance and the quest for legitimacy in the EU: The battle over the regulation of GMOs since the mid-1990s. *Journal of European Integration* 31, no. 3: 389–407.

Van Asselt, M.B.A., and O. Renn. 2011. Risk governance. *Journal of Risk Research* 14, no. 4: 431–49.

Van Asselt, M.B.A., S.A. van't Klooster, P.W.F. van Notten, and L.A. Smits. 2010. *Foresight in action: Developing policy-oriented scenarios*. London: Earthscan.

Van Asselt, M.B.A., and E. Vos. 2008. Wrestling with uncertain risks: EU regulation of GMOs and the uncertainty paradox. *Journal of Risk Research* 11, nos. 1–2: 281–300.

Van Asselt, M.B.A., E. Vos, and B. Rooijackers. 2009. Science, knowledge and uncertainty in EU risk regulation. In *Uncertain risks regulated*, ed. M. Everson and E. Vos, 359–88. New York, NY: Routledge-Cavendish.

Van de Steeg, M. 2009. Public accountability in the European Union: Is the European Parliament able to hold the European Council accountable? *European Integration Online Papers* 13, no. 3: 1–24.

Van Gerven, W. 2005. *The European Union: A polity of states and peoples*. Stanford, CA: Stanford University Press.

Van Notten, P.W.F., J. Rotmans, M.B.A. van Asselt, and D.S. Rothman. 2003. An updated scenario typology. *Futures* 35, no. 5: 423–43.

Vos, E. 2005. Independence, accountability and transparency of European Regulatory Agencies. In *Regulation through agencies in the EU. A new paradigm of European Governance*, ed. D. Geradin, R. Munoz and N. Petit, 120–40. Cheltenham: Edward Elgar.

Vos, E., and F. Wendler. 2006. *Food safety regulation in Europe: A comparative institutional analysis*. Antwerp: Intersentia.

Wiener, J.B. 2011. The rhetoric of precaution. In *The reality of precaution. Comparing risk regulation in the United States and Europe*, ed. J.B.Wiener, M.D. Rogers, J.K. Hammitt and P.H. Sand, 1–39. Washington, DC: RFF Press.

**Publication IV**

Skierka, Isabel. (2018). The governance of safety and security in connected healthcare in Europe. *Living in the Internet of Things: Cybersecurity of the IoT – 28–29 March 2018. London: Institute of Electrical and Electronics Engineers (IEEE),* 1−12. https://doi.org/10.1049/cp.2018.0002 (3.1).

# The governance of safety and security risks in connected healthcare

***I Skierka****

**Digital Society Institute, ESMT Berlin, Germany, isabel.skierka@esmt.org*

**Keywords:** Safety, Security, Medical, IoT, Governance

## Abstract

As healthcare is increasingly digitized and interconnected, medical systems are exposed to IT security threats that can endanger patient health and safety. This paper examines how the convergence of safety and security risks in connected healthcare challenges the governance of medical systems safety in Europe. The analysis shows that the management of safety and security risks of medical systems requires the extension of existing governance mechanisms, including regulation, standards, and industry best practices, to combine both safety and IT security in healthcare. It puts forward policy and industry recommendations for the improvement of medical systems cyber security in Europe, including pre-market certification and post-market monitoring and surveillance programs, effective information sharing, vulnerability handling, and patch management. The paper draws comparisons with medical device cyber security guidelines in the United States, and with technical controls, standards, and best practices in the domain of industrial control systems (ICS) security.

## 1 Introduction

Cyber security[1] has become key for the dependability of infrastructures that societies rely on. Computing and communication technologies today are an inherent part of safety-critical systems such as medical devices, cars, aircraft, or nuclear power plants. As these physical systems are interconnected and become part of the ‘Internet of Things’ (IoT), adversaries can remotely exploit vulnerabilities in their software. Hence, cyber security increasingly intersects with public safety.

This development raises new challenges for the governance of public safety. Safety practices in critical sectors such as healthcare, transport, aerospace, and energy, are well-established and prescribed by safety-standards. Such standards stipulate how systems should be developed, verified and maintained to minimize the risks of accidents and failure over their lifetime. Yet, established safety practices fall short of addressing the cyber security threats that ensue from the growing interconnectivity of formerly isolated systems [1]. As systems become vulnerable to remote attacks, they require protection from both accidents as well as malicious cyber incidents – the safety and security requirements of these systems converge. As a result, engineers, decision-makers, and regulators need to expand established practices, risk management frameworks, standards, and regulations tailored to safety to also encompass cyber security [2].

The effects of converging safety and security risks are clearly manifest in healthcare, perhaps one of the most safety-critical and rapidly digitizing sectors. As healthcare is increasingly interconnected, medical systems are exposed to cyber security threats that can endanger patient health and safety.

This paper analyzes the convergence of security and safety of medical devices in the interconnected clinical care process, and its effects on established governance mechanisms in Europe, including best practices, standards, and European Union (EU) regulation. The paper will focus on the EU context for two reasons. First, most research on cyber security in healthcare originates from the US and focuses on the US context [3], [4] [5] [6] [7]. In comparison, the EU context has to date been underexplored. Second, the EU adopted a new regulation, the Medical Device Regulation, in May 2017, which addresses IT security and provides occasion to examine the new regulatory framework.

Previous research has shown that cyber security shortcomings in medical devices can systemically affect patient health and safety [8], [9], [5], [10], [3]. Despite strong safety regulation in Europe and most other parts of the world, medical device manufacturers and operators do not seem to sufficiently address cyber security requirements. As this paper illustrates, the absence of a coherent technical “state of the art” in Europe makes it difficult for manufacturers, operators, and certification bodies, respectively, to implement security requirements.

The paper argues that the management of safety and security risks of medical systems requires the extension of existing governance mechanisms, including regulation, standards, and industry best practices, to combine both safety and IT security.

The analysis and recommendations are based on a review of the relevant academic literature, technical reports, and official

[1] Throughout this paper, cyber security is understood as the state of protection of computer systems against unauthorized access or attack.

policy documents, as well as informal interviews with six decision-makers and experts[2], and a workshop with fifteen German representatives from health organizations, medical device manufacturers, IT security experts, safety engineers, regulators, and a notified body, which took place in Berlin in October 2017 [11].

In following, the paper first outlines smart medical devices' security risks, incidents and structural vulnerabilities. Second, the paper addresses shortcomings in the regulation and governance of medical device cyber security in Europe. Finally, the paper outlines policy recommendations for public authorities, operators, device manufacturers, and suppliers.

## 2 Connected medical devices' security risks

Over the past three decades, medical devices have evolved from analog to digital, interconnected systems. While computing and control technologies have been embedded in medical devices throughout the past decades already, modern medical devices rely on increasingly complex software and connectivity to external devices and servers. They can perform a range of functions, which allow healthcare organizations and professionals to diagnose and treat patients more efficiently and granularly, provide healthcare services in a homecare environment, or deliver expert medical practice remotely. Advancing technological innovation not only improves patient care, but also promises to provide care at a more affordable cost (due to savings in personnel or more exact diagnostics and therapy, for example) and to thereby help to manage the financial burden of healthcare systems as a whole in the future. According to a Roland Berger consultancy firm study, the digital healthcare market is set to grow at average annual growth rates of 21 percent until 2020 [12].

Yet, research and real-world incidents have shown that as medical devices are increasingly integrated with computing and communication technologies, IT security risks in healthcare have become systemic. The privacy risks of cyber attacks against health infrastructure have been extensively reported as a result of several data breaches (among them, the biggest healthcare breach to date – a cyber attack on Anthem health insurance during which 78.8 million patient records were stolen) [13]. More recently, cyber attacks' potential impact on patient health and safety has been raising concerns for healthcare organizations, regulators, and medical device manufacturers alike. The following section will explore these risks in more depth.

### 2.1 The evolution of medical devices

Per the EU definition in Article 2 of the Medical Device Regulation (MDR) 2017/745, a medical device is "any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:

- diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,
- diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,
- investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,
- providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations."

Software integrated into a device or standalone that corresponds to the above definition in that it is intended for medical use counts as a medical device, too.[3] Respective legal definitions in the United States (US), China, Japan, and other countries are similar to the EU's [14]. Fitness, lifestyle and well-being devices and applications are not medical devices, but mobile health products more generally. A comprehensive legal framework for mobile health products and associated privacy and safety concerns is still lacking.

On the basis of the taxonomy in [5], connected medical devices can broadly be categorized into four groups:

- Implantable medical devices, such as pacemakers and implanted cardiac defibrillators (ICDs). They are implanted in the patient, but communicate wirelessly with external devices, such as programmers and monitoring stations, via proprietary protocols or Bluetooth.
- Wearable medical devices, such as portable insulin pumps, also communicate with external remote controls and monitoring devices via wireless protocols.
- Mobile devices, such as glucose measuring devices or home transmitter/base stations, may connect wirelessly to a patient's insulin pump or implantable cardiac device for monitoring purposes. They may also transmit patient data via the internet for remote care purposes.
- Stationary medical devices, such as hospital based computer tomography scanners or chemotherapy dispensing stations, often use more traditional wireless networks such as WiFi networks, or local area networks, in hospitals.

As connected medical devices are complex and interconnected with external components, they need to be considered as larger systems composed by different hard- and software components

[2] The interviewees wish to remain anonymous. They comprised cyber security managers from two device manufacturers, one IT security service provider, one expert from an EU notified body, one IT security expert, and one expert from an EU national competent authority. The author also spoke about the topic with two German and one European policy makers in informal conversations.

[3] Under the EU Medical Device Regulation, any (standalone) software, including mobile applications, whose intended use it is to take decisions with diagnosis or therapeutic purposes are classified as a class IIa (moderate risk) device or higher, meaning it needs to undergo evaluation by a Notified Body in order to be approved for the EU market.

and sub-systems, as well as supporting IT infrastructure, such as cloud-based data processing technologies. Many stationary medical devices use web services interfaces for configuration purposes. The use of database back-ends for storing and retaining information for devices is also common [3]. Even implantable medical devices like cardiac pacemakers operate within a larger system that encompasses external monitoring and control devices, some of which are connected to the internet. Most cardiac devices come with base stations which patients keep at their home. These 'home transmitter' stations transfer patient data to the device makers' servers via the internet for remote care purposes.

In the future, such trends will continue to accelerate: medical devices will be part of a ubiquitously interconnected clinical care process in which data will be continually exchanged and processed with the aim of making patient care more effective and efficient. At the same time, the move towards more complex software and connectivity will further increase medical systems' attack surface and can have wide implications for patient safety.

### 2.2 Cyber security incidents in medical devices

The impact of cyber security threats in the form of unauthorized access to a system with impacts on the confidentiality, integrity, and availability of information systems can have real consequences for the safe and continuous operation of devices and their time-critical responsiveness [10], [3], [15], [16].

Research over the past decade has shown that while medical devices are increasingly digitized and interconnected, the level of cyber security has been alarmingly low. Data from the US FDA shows that a growing number of medical device recalls is caused by software defects [17].

While no one is known to date to have caused a death by hacking into a medical device, several researchers have demonstrated that it is possible. In 2008, a team of researchers first demonstrated attacks against implantable cardiac defibrillators. With the help of a commercially available device programmer, the team was able to extract a patient's private data and reprogram the pacemaker to deny service [8]. Since then, several have demonstrated different possibilities for hacking pacemakers and insulin pumps [18], [19], [20], [21]. In May 2017, researchers from the security firm WhiteScope discovered a total of 8,665 open and known vulnerabilities in third party software libraries implemented across four different pacemaker programmers from four different manufacturers [22].

In 2015, the US Food & Drug Administration (FDA) issued the first-ever advisory urging hospitals to stop using a medical device, the Hospira Symbiq Infusion pump, because of cyber security vulnerabilities [23]. More recently, in August 2017, the FDA recalled 475 000 implantable pace maker devices manufactured by Abbott Laboratories (formerly St Jude Medical) in the US on the basis of cyber security vulnerabilities in the cardiac device system. The number of affected pacemakers worldwide is estimated at 745 000. As a result, Abbott Laboratories had to deploy software updates to fix the critical vulnerabilities in the devices [24]. These software updates are optimized product recalls [25]. Instead of physically removing and fixing an implantable device, doctors can deploy updates to fix vulnerabilities.

Due to the lack of publicly available data on safety incidents in Europe,[4] we cannot compare US safety incidents with European data. However, there is no reason to assume that devices deployed in the EU are less vulnerable to software failures and cyber security threats [26], [27], [28].

Not only implantable, but also stationary hospital devices are vulnerable to hacking. A 2014 report by the SANS Institute concluded that 94 percent of health care organizations have been the victim of a cyber attack, including attacks against medical devices and infrastructure [29]. Other reports have shown how vulnerable medical devices served as conduits for hackers to attack hospital networks [9], [30]. The 'WannaCry' ransomware worm, which compromised the networks of many global corporations earlier this year, also affected medical devices in hospitals and prompted the US Industrial Control System Computer Emergency Response Team (ICS-CERT) along with several medical device vendors, to issue security alerts about vulnerable devices [31].

These examples and others show that cyber security risks in healthcare are systemic. Many medical devices lack even basic security features, and the resulting risks are externalized mainly to users – health organizations and patients.

### 2.3 Threats

Cyber security risks of medical devices can only be assessed on a case-by-case basis. Such an assessment has to take into account the system's vulnerabilities and threats. A threat is the potential for a vulnerability to be exploited, which in turn depends on threat actors' skill level, motive, or opportunity, as well as on the vulnerability. A vulnerability is a weakness in technologies – such as hardware, software, physical engineered devices or networks – as well as in people and processes [32].

Cyber security threats can result from unintentional sources (for example, due to a software design fault), or from intentional sources (an attack exploiting IT security vulnerabilities in the computing and communication systems, targeted or untargeted). This paper's Annex offers a more detailed overview over different threat categories and medical cyber security incidents. According to the US Food & Drug

[4] Since 2011, safety incidents of medical devices reported to national competent authorities are stored in the European Database Eudamed. However, access is restricted to EU institutions, national authorities, notified bodies, and manufacturers only. The FDA's database on safety incidents is publicly accessible.

Administration (FDA) and other organizations, threats to medical devices include [33], [4], [34], [35]:

- Interference caused by electromagnetic signals in the environment
- Malware on devices/systems which alters data on a diagnostic device
- Denial of service attacks which make a device unavailable
- Unauthorized device reprogramming, setting changes, which alters device function
- Failure to provide timely security software updates and patches to medical devices and networks and to address related vulnerabilities in older medical device models (legacy devices)
- Untested or defective software and firmware
- Uncontrolled distribution of passwords, disabled passwords, hardcoded passwords for software intended for privileged device access (e.g., to administrative, technical, and maintenance personnel)
- Open, unused communication ports on a device which allow for unauthorized, remote firmware downloads
- Unauthorized access to the health care network, which allows access to other devices
- Misconfigured networks or poor network security practices
- Security vulnerabilities in off-the-shelf software due to poorly designed software security features

A 2017 Ponemon Institute study [6] found that 31 percent of device makers and 40 percent of health delivery organizations (HDOs) surveyed[5] are aware that patients experienced an adverse event or harm due to an insecure medical device. Most of the respondents (40 percent of device makers and 44 percent of HDOs) did not know what the cause for that adverse event was, but among the primary causes cited were that

- An attacker took control of the device (39 percent of device makers, 37 percent of HDOs)
- Additional software was installed on the device (33 percent of device makers, 40 percent of HDOs)
- Denial of service of the device (18 percent of device makers, 21 percent of HDOs)
- Inappropriate therapy delivered to the patient (only 10 percent of device makers, but 38 percent of HDOs)

In the worst case, such events can harm patient privacy and/or life and health. A widespread incident can also affect an entire health care system or lead to a loss of trust in digital technologies in health care as such, which would translate into massive economic damage.

According to the aforementioned Ponemon Institute study, device makers seem to be aware of the risk, but only few seem to act. 67 percent of device makers surveyed believe an attack on one or more medical devices they have built is likely, but only five percent conduct annual cyber security tests of released devices.

Many of the underlying reasons for medical device insecurity are structural and do not have an easy fix, as the following section illustrates.

### 2.4 Structural obstacles and vulnerabilities

A number of structural factors amplify cyber security threats to medical devices and complicate their protection. As medical devices are complex systems, security mechanisms need to be implemented across the system and its different layers. For example, some of the functionality of a medical device might lie outside the device, on an online server. Moreover, security is contextual. A mobile device like a smart phone can perform critical functions if it is used in a medical context, i.e. for monitoring or diagnosis purposes. Therefore, securing medical systems requires coordination of responsibilities among manufacturers and operators of different system components.

This section gives an overview over some structural factors affecting medical systems' vulnerabilities. These issues similarly occur in other cyber physical systems (CPS), where computational control systems are deployed in energy, transport, or manufacturing systems, for example [10].

*Tradeoffs between security, safety, and other essential system requirements*

Achieving a balance between medical systems' security goals and healthcare utility and safety is challenging. Most medical devices rely on embedded computer systems, which are constrained in their computation power, memory, and energy consumption. Security mechanisms can slow down their operation, reduce usable battery life and make devices less accessible in emergency situations.

Related dilemmas have been subject to a growing corpus of research and suggestions for innovative encryption and authentication solutions. Yet, to date none of these have been found to be secure enough for implementation [8], [21], [36], [37], [38].

Another key requirement of medical devices is usability. Generic security controls such as password access controls can hamper usability in fast-paced clinical environments. In a study titled "Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient?" [39], security researchers have demonstrated how health workers are ignoring, circumventing and sabotaging information security measures imposed by their IT departments. In doing so, they were prioritizing helping people and saving lives over information security. However, such practices can serve as gateways to cyber attacks, such as ransomware attacks, which have been crippling multiple

[5] The Ponemon Institute's report's final survey sample represents 242 individuals who are involved or have a role in a US device maker organization and 262 individuals who are involved or have a role in a US health delivery organization.

hospitals throughout previous years. Limited usability might prompt health staff to make wrong decisions and thereby can cost lives. Research by Masci et al. [40] shows that the largest number of avoidable deaths involving medical devices are usability failures. The authors demonstrate that a typical hospital might use infusion pumps from several vendors, all of which have different controls, which can easily lead to confusion among hospital staff. Medical devices' connectivity to web servers, data banks, and other web applications is also good for usability reasons, but bad for security.

Hence, security mechanisms need not only be secure, but also usable, efficient and compatible with the unique circumstances of these systems.

*Lifecycle conflicts*

The lifetime of medical devices (between 10 and 30 years) is much longer than the supported lifetime of most operating systems. As a result, software usually becomes outdated and unsupported over the course of a device's lifetime. As re-use of hardware and software systems in medical devices is common, a medical device is generally a mix of new and old legacy systems. Moreover, legacy systems may no longer be interoperable with newer systems. This leaves vulnerabilities such as misconfiguration and security holes [3]. Medical devices running on the Microsoft Windows XP operating system, for example, no longer receive vital software updates (unless hospitals or manufacturers pay a high fee to Microsoft) – an issue which became dramatically visible during the spread of the WannaCry ransomware worm.

*Lack of (timely) security patches*

Once a vulnerability is known, devices need to receive timely software security updates [3]. Yet, patching medical devices is much more complicated than patching IT desktop systems [41], [42], [43]. Patches bear security risks if they interact with the use environment in an unforeseen way or render systems unavailable. Not only must software updates fix security flaws in a particular software system, they must also ensure that they do not cause any unintended effects and incompatibilities concerning other soft- and hardware in the system, including aforementioned legacy systems. Moreover, if software updates are not securely deployed, they can also be manipulated to channel malicious software into systems. Finally, responsibilities for update deployment and installation are not always clear. Hospitals and other medical device users are often dependent on vendors to deploy patches and lose liability claims in case they upgrade or change devices' software independently. Device original equipment manufacturers (OEMs) in turn do not always have access to the software implemented in their devices and are dependent on software suppliers or integrators themselves.

*Proprietary and opaque software*

Most medical devices rely on proprietary software. OEMs do not have full access to it. Moreover, manufacturers and suppliers are rarely transparent regarding third party software components in their products. Hence, validating the software becomes a difficult task. In testing terms, OEMs must treat software as a 'black box'. Where software vendors make the software accessible to OEMs or to testing and certification labs, some security risks, such as known vulnerabilities or code errors, can be mitigated.

*Divergence of safety and security risk assessments*

Risk assessment and testing methods for safety and security of control systems have evolved separately over time [1], [15]. Safety mechanisms are mainly concerned with accidental risks originating from the system. Security mechanisms address malicious risks caused by intentional human behavior, for example by hackers [15], [16]. When it comes to attacks, security is a function of a threat agent and its capabilities, intent, and motivation. These are dynamic and constantly evolving. Therefore, security risks cannot be addressed by static risk assessment and management methods, such as functional testing for the presence or absence of specified behavior as well as static risk and failure rate calculation methods [44]. Attacks on security often exploit the existence of unspecified behavior and are found after the software has been released and is in use in larger systems [45]. As a result, the security risks need to be managed by the manufacturer after a device has already been marketed. This includes the continuous testing of software for vulnerabilities and the provision of software updates. As control systems in medical devices can be affected by cyber attacks, it is increasingly important to address the combination of safety and security in such modern control systems.

Cyber security in medical devices is a multifaceted issue that requires technical controls, risk management, governance, and regulation [3] – in short, comprehensive governance. Indeed, we are not starting from scratch: regulatory frameworks, standards, and risk management practices to ensure the safety of medical devices have been in place for a long time already. The challenge is to 'update' and complement these approaches with cyber security mechanisms.

## 3 Medical device regulation and governance

Medical device safety is strictly regulated in Europe and in other countries [14]. Yet, technological innovation in the health sector has outpaced safety regulations and standards. The challenge for regulators is to draft regulations that are specific enough to matter, yet general enough to outlast the constantly changing and innovating technologies as well as threats that mutate much faster than the products to be certified. Hence, regulators can refer to the technological "state of the art", but not prescribe specific technical requirements. The "state of the art" is in turn defined by technical industry standards. In the overlapping areas of the Internet of Things (IoT) and cyber physical systems (CPS), technical standards are still emerging. The dynamic nature of the technical "state of the art" makes it difficult for manufacturers, operators, and certification bodies, respectively, to implement regulatory requirements in a uniform manner. The following section gives an overview of the regulatory framework for medical device security in Europe and draws a comparison to the situation in the US.

In Europe, the Medical Device Directive 93/42/EC (MDD) and the Active Implantable Medical Device (AIMD) Directive 90/385/EC have regulated medical device safety at the EU level since the 1990ies. The two regulations have recently been replaced with the Medical Device Regulation (MDR) 2017/745. The MDR leaves the main regulatory framework intact but strengthens pre-market approval and post-market surveillance mechanisms for medical device safety, and for the first time specifically requires manufacturers to ensure the IT security of their devices.

In addition to medical device regulation, regulatory frameworks for critical infrastructure security and data protection play important roles for cyber security in healthcare more generally. The European Network and Information Security (NIS) Directive, which has to be implemented in European member states by May 2018, requires operators of essential services, including hospitals and large device manufacturers, to implement minimum IT security standards and to notify security breaches. From May 25, 2018, onwards, the General Data Protection Regulation (GDPR) 2016/679 will make security and privacy by design and default mandatory, requires impact assessments for data processing, introduces mandatory data breach notification requirements for data controllers and processors.

Within the general medical device approval process, manufacturers need to demonstrate their devices' conformity with the EU regulatory safety and performance requirements as defined in the MDD and now in the MDR. Depending on the level of risk of the device, the manufacturer can declare conformity with the requirements itself (for low-risk class I devices) or must submit its technical documentation of the device's safety and performance, including clinical tests and trials, to a certified 'Notified Body' (NB). NBs are for-profit entities which evaluate the conformity of the device with regulatory requirements for IIa and IIb moderate-risk, and III high-risk classes. Upon demonstration of conformity, they obtain a CE (Communauté Européenne) label and can be marketed in the entire EU.

The new MDR requires manufacturers develop devices in accordance with "state of the art" IT security (Annex I, Chapter II, para 17.2 of [46]), and to reduce risks associated with negative interaction between software and the IT environment within which it operates (Annex I, Chapter II, para 14.2). In addition, it requires manufacturers to set out minimum IT security requirements to run the software as intended (Annex I, Chapter II, para 17.4). The manufacturer's technical documentation of the device shall include detailed descriptions of software verification, validation and testing performed in-house and in a simulated or actual user environment (Annex II, para 6.1(b)).

Moreover, the MDR significantly strengthens the post-market management system for medical device safety. Member states will be required to analyze and risk assess incidents as well as the adequacy of corrective actions, and will monitor the manufacturer's incident investigation. Every device will receive a unique device identifier with which the device will be registered in the European Databank on Medical Devices (Eudamed). In addition, the MDR strengthens requirements for notified bodies (NBs) to conduct yearly audits and assessments of quality management systems of manufacturers at least yearly (Annex IX, sections 3.3 and 3.4 of [46]).

In summary, the MDR offers several advancements with respect to cyber security and safety requirements of medical devices. However, the regulation offers little guidance as to how the regulatory requirements to ensure better security should be implemented in compliance with the "state of the art". The European Commission regularly publishes lists of "harmonized" standards [47], which define the medical technical "state of the art". These standards prescribe how conformity with the regulatory requirements laid out in EU legislation should be implemented. Yet, among these harmonized standards, still very few relate to software and IT security. Standard IEC 62304:2006 on "medical device software – software life-cycle processes" is the main standard addressing software safety, and recently also security. In its Amendment I (2016), the standard's software lifecycle requirements include more specific information security provisions (para 5.2.2). Moreover, the standard classifies the risk of embedded software into levels of potential harm from software failure and malfunctions.

Yet, there is little else official guidance from the EU on how manufacturers should conform with regulatory requirements and according to which guidelines NBs should assess conformity. If they are left to define their own medical IT security certification and evaluation frameworks, the consequence is a risk of an uneven regulatory patchwork across the continent.

The US is a step further, where the FDA has assumed a leading role in the global regulation of cyber security of medical devices. It has issued two sets of guidelines for cyber security in medical devices for device manufacturers, most notably a premarket guidance in October 2014 [48], and a post-market guidance in December 2016 [49]. They are intended to support manufacturers in fulfilling the requirements of the pre-market approval and post-market surveillance processes with respect to cyber security risks. The guidelines advise manufacturers to address cyber security throughout a product's lifecycle, following a risk management approach, building on the US NIST Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity. The NIST framework adopts a risk management approach to cyber security and recommends core measures to guide an organization's cyber security efforts: Identify, Protect, Detect, Respond, Recover. The guidelines go beyond usual risk management requirements in that they also require a manufacturer to document plans for future software support, IT security instructions regarding their devices for operators, vulnerability handling, information sharing, or incident notification of users. Another notable guidance document in this context is the FDA's 2005 guidance on cybersecurity requirements of off-the-shelf software in medical devices for manufacturers and operators [50].

The FDA's guidelines constitute a risk management framework rather than specific cyber security prescriptions. Moreover, they are voluntary and legally non-binding. The aforementioned 2017 Ponemon Institute study shows that only 51 percent of device makers follow the FDA's cyber security guidance [6]. Yet, they represent the most comprehensive guide to organizational risk management for cyber security in medical devices to date and are therefore also consulted by manufacturers outside the US. Recent FDA safety notices and recalls indicate that these enforcement mechanisms, as well as liability for device failure and reputational damage, will raise the cost of bad security for manufacturers.

## 4 Recommendations for cyber security governance in connected healthcare

On the basis of the above analysis, this paper puts forward a number of recommendations for public authorities, industry, and operators, to improve medical device security in Europe.

*Common medical cyber security certification criteria*

European public authorities, in cooperation with manufacturers and NBs, should develop concrete common European cyber security criteria as a component of the medical device certification process. The European Commission has recently proposed an EU-wide cyber security certification framework that could serve as a basis for the certification of security properties of medical products and processes [51]. Within the framework, medical-device-specific schemes and security requirements could serve as a basis for evaluation, testing, and certification of cyber security along with other medical system requirements. Such schemes should be harmonized with other international standards as much as possible with the goal of creating internationally applicable schemes that also lower device vendors' transaction costs.

Guidance for such criteria can be deduced from international standards for the secure design and development of software components, FDA guidelines, and existing guidelines on Industrial Control Systems (ICS) security. ICS properties are in fact similar to those of medical devices since both are systems in which embedded computers control physical devices' interactions with their environments [10]. Hence, some of the measures used to secure embedded computer systems in ICS are equally applicable in the healthcare context. Examples for guidance documents include the international draft IEC 62443 standard series on industrial network and system security, the US National Institute of Standards and Technology's (NIST) ICS Security Guide [52], and the proposed European cybersecurity certification framework for industrial automated control system components [53]. The International Medical Device Regulators Forum's 2016 proposal for clinical evaluation of software [54] can offer additional guidance for manufacturers and evaluators, such as NBs, as to clinical evaluations of software as part of the medical device approval process to fulfil effectiveness, safety and performance requirements.

*Promoting transparency of IT security risks and incidents*

European and national medical and cyber security oversight agencies should make information about IT security risks and incidents in medical devices publicly available. At present, national authorities need to submit information about safety incidents to the European Database on Medical Devices (Eudamed), which is only accessible by EU institutions and national authorities. The MDR will increase transparency, as most information submitted to Eudamed will be accessible to a wider circle, including NBs, manufacturers, experts, and health organizations. Parts of it, such as information about recalls, will also be available to the public.

Information about software vulnerabilities concerning medical devices should also be made accessible to all stakeholders. The Common Vulnerability Scoring System (CVSS) is useful in assessing the information security risk of a vulnerability (in terms of impact on confidentiality, integrity, availability). In order to capture vulnerabilities' potential impacts on system safety in addition to security, the CVSS or other vulnerability assessment systems should be adapted to the safety context. The MITRE Corporation and the FDA have formed a working group, including medical device manufacturers, healthcare providers, and cyber security experts, to develop an approach for using CVSS to score medical device vulnerabilities [55].

*Information sharing*

European decision-makers should incentivize information sharing about security threats in the health care sector. Currently, information sharing is fragmented. Safety incidents are reported to national authorities and collected in the Eudamed database. Healthcare organizations classified as "operators of essential services" under the EU NIS Directive will need to report major security incidents to national information security authorities which differ from the medical CAs. EU institutions and national authorities as well as industry should set up an information sharing system that supersedes these fragmentations and ensures a better sharing of threat information within the healthcare sector. It should additionally promote the exchange of threat information with other sectors. Information sharing networks can be overseen by an Information Sharing and Analysis Center (ISAC), a sectoral coordinating Computer Emergency Response Team (CERT), or national CERTs. In the US, for example, a National Health Information Sharing & Analysis Center (NH-ISAC) provides threat information and exchange services.

*Guidelines for operation of medical devices in deployment setting*

Hospitals and health organizations, as well as other medical device users are responsible for securely operating medical devices within their networks. As mentioned previously, they are regulated under the EU NIS Directive and the GDPR. The international standard IEC 80001 offers guidance on the application of risk management for IT-networks incorporating medical devices for health organizations. Within their organizations, health organizations should integrate the management of medical devices and networks. Within health organizations, these responsibilities have traditionally separated with biomedical technicians being responsible for medical devices and the IT-department being tasked with network administration.

As medical devices operate within complex systems, standards and best practices should not only focus on the development and design risk assessment process, but also on the specificity required for cyber security within the complex deployment setting, as [3] points out.

*Security best practices for device manufacturers and suppliers*

In order to mitigate cyber security risks as far as possible, manufacturers should implement a number of security related pre-market practices (before the device is marketed) and post-market management mechanisms for monitoring, vulnerability handling, and information sharing. Those practices may also become part of common European baseline cybersecurity certification criteria.

Several medical device makers have adopted effective processes to implement cyber security in devices throughout their life cycle, including responsible patch management and disclosure programs, as Dräger and Siemens in [56] and [57]. These can serve as examples in the industry. The grassroots organization 'I Am The Cavalry', whose work focuses on issues of cyber safety, provides cross-sectoral expertise on how to improve cyber security in CPS. Their "Hippocratic Oath for Connected Medical Devices" can serve as an additional guideline for cyber security in medical devices, which is compatible with other aforementioned guidance documents [58].

Security by design

IT security should not be an afterthought, rather it should be designed into the devices from the start. The design of medical devices should follow proven secure lifecycle standards and secure supply chain management practices. All off-the-shelf hard- and software integrated into devices should be trustworthy and provide high technological assurance. Manufacturers should reduce devices' connectivity to the necessary minimum, and isolate safety critical system components from other potentially vulnerable components within the devices.

Integrated safety and security risk assessment

Manufacturers as well as notified certification bodies should apply integrated safety and security risk assessment and management methods to medical devices. Research in this field has presented a number of integrated risk assessment methods for (industrial) control systems that can complement established medical device risk management standards, i.e. the SAHARA or Unified Security and Safety Risk Assessment Methods [59]. The aforementioned FDA pre-market cyber security guidelines as well as the IEC 62433 standard offer additional guidance in this field.

Transparency about device security and risks

Device manufacturers and vendors should transparently declare how their devices fulfill medical IT security requirements. The manual for devices should not only include directions for their use, but also a threat model of the device in use contexts to clearly demonstrate the risks of the device's use. This would give device operators and users the necessary information about security trade-offs and the ability to decide about related risks.

Software and hardware suppliers should be equally transparent and explain the security mechanisms and threat models of their software and the effects of its use in a device.

Patch management

Manufacturers should operate an effective and usable patch management system. Once a vulnerability is known, devices need to receive timely software security updates. Since software updates themselves bear security risks, they should be tested in use environments before being deployed. Moreover, device makers need to implement secure channels for the deployment of updates in order to prevent their manipulation.

Vulnerability reporting

Manufacturers should operate a vulnerability reporting program through which they collaborate with third parties who discover software security flaws. Many medical device manufacturers, including Siemens, Draeger, Medtronic, and Philips, have implemented coordinated vulnerability disclosure pro-grams throughout the past years [60]. These developments are encouraging. Standards ISO/IEC 29147: Information Technology – Security Techniques – Vulnerability disclosure and ISO/IEC 30111:2013 Information Technology – Security Techniques – Vulnerability handling processes provide guidelines for manufacturers and their adoption should be promoted by public authorities.

## 5 Conclusion

The dependability of computing and communication technologies will be crucial for the future development of connected healthcare and its many benefits. The growing connectivity of medical devices and their recruitment into the IoT make them vulnerable to cyber attacks. Research and real-world incidents have demonstrated that the level of IT security in many medical devices is alarmingly low. Cyber security in medical devices is not merely a technical, but a governance problem, which requires technical controls, but also regulatory frameworks, standards, and risk management practices which are coordinated among all stakeholders involved – regulators, notified bodies, device manufacturers, technology suppliers, and device users.

This paper has shown that medical device safety is strictly regulated in Europe but has to date neglected cyber security aspects of medical devices. The lack of guidelines and definitions of a coherent technical "state of the art" to combine safety and security requirements complicates the implementation and certification of security requirements for manufacturers and EU notified bodies.

On this basis, the paper has put forward policy and industry recommendations for decision-makers, device manufacturers, suppliers, and operators. Medical device certification processes in Europe should be based on common cyber security criteria, which can be informed by existing cyber medical security guidelines in the US, as well as security standards for ICS and other cyber physical systems. All stakeholders should engage in information sharing about security threats, incidents, as well as vulnerabilities. Industry and operators should cooperate to develop standards and best practices that focus on cyber security requirements for medical systems within their complex deployment system. The medical device and IT industries should adopt best practices and standards for the secure design and development of devices, the management of vulnerabilities and the deployment of security patches.

Ongoing technological innovation in healthcare toward a "medical IoT" or "healthcare 4.0" will create new security and privacy governance challenges which will be similar to those we experience in other sectors, such as transport or manufacturing. This makes privacy and security governance in safety critical systems a salient issue to examine across sectors.

## ANNEX: Cyber security incidents in medical devices

This section gives an overview of case studies the IT security risks of medical devices. These cases are chosen on the basis that they are representatives for the range of threats that implantable and stationary medical devices face.

*Accidental malfunction or failure*

As explained above, the growing complexity of medical devices which are now controlled by software and networked IT systems can result in design and operation flaws, which can lead to accidental failure of the device [5]. Accidental failure of an implantable medical device (IMD) that controls life-critical functions in a patient's body, as well as safety-critical stationary medical devices, can have fatal consequences.

> Example: Security configurations error caused failure of diagnostic computer

In the middle of a heart catherization procedure, the diagnostic computer used to monitor, measure and record physiological patient data crashed. There was a delay in procedure whilst the application was rebooted, causing a delay in patient care that could have potentially harmed the patient. The cause for the device failure had been a configuration error of the anti-virus scan, which included directories that caused deletion of critical patient data. The FDA incident report details the cause to be the customer not following the manufacturer's instructions concerning the installation of anti-virus software [61].

*Attacks against medical devices*

Attacks against medical devices can be targeted against specific devices or untargeted. In an IT security attack, vulnerabilities are exploited to intentionally disrupt the operation of a medical device. Attacks targeting medical devices can be both passive and active. Passive attacks breach the confidentiality of data and systems. They include eavesdropping, information gathering, and 'sniffing' network data such as passwords. Active attacks interfere with the integrity and availability of data. For example, an active adversary can read, modify, and inject data over a communication channel, or tamper with device soft- and hardware, and thereby reprogram the device or execute a denial of service attack [19].

The motives for such attacks can be wide-ranging from the intent to collect or deny access to the device to gain a financial or competitive advantage, over harming a specific patient, to attacking the larger health care system.

As Healey, Pollard, and Woods [5] point out, an escalated version of the risk of a cyber attack on medical devices is the intentional widespread disruption of medical devices. Much like the Stuxnet virus affecting business IT and industrial control systems, a piece of malware tailored to specific medical devices could propagate over the Internet and only take action when it confirmed it was in a medical device. Another scenario is the injection of malware into a device vendor's software update deployed to an entire set of medical devices at the same time. Security researcher Barnaby Jack demonstrated the feasibility of a comparable attack against a pacemaker, explained below.

Research has shown that medical devices are susceptible to compromise, such as implantable cardiac devices, and insulin pumps [18]. Although these attacks have only been executed in a research setting, they demonstrate grave problems. According to the Ponemon Institute, 67 percent of device makers surveyed for the May 2017 study believe an attack on one or more medical devices they have built is likely, 56 percent of health delivery organizations believe such an attack is likely [6].

> Security vulnerabilities in implantable medical devices that enable targeted attacks

A number of studies have demonstrated attack possibilities against IMDs such as pacemakers, implantable cardiac defibrillators (ICDs), and wearable/semi-implantable devices such as insulin pumps. The majority of demonstrated hacks against implant-able or wearable devices focuses on threats against the wireless networking capabilities and telemetry systems of the devices. Telemetry systems are composed of sensors, radio-based communication, and recording devices, such as the programmer or home monitoring devices. Other studies found vulnerabilities in the systems' software architecture.

### Examples: Demonstration of passive and active attacks against commercial ICDs and pacemakers

Implantable cardiac devices, such as a pacemaker and an ICD are surgically implanted into the patient's body. A pacemaker sends electrical pulses to maintain the heart's regular rhythms. An ICD monitors heart rhythms and delivers an electric shock when it detects abnormal patterns. With the help of devices called 'programmers', health care practitioners can contact the implantable cardiac device to extract data, modify device settings remotely and reprogram it via radio signals. Moreover, most of ICD or pacemaker patients have a home monitoring device that monitors the patient's implantable cardiac device and transmits data via a wireless patient support network to the physician remotely. Implantable cardiac devices are closed-loop, cyber physical systems: under normal use circumstances, its sensing function alone dictates its actuation activities.

In 2008, a group of researchers demonstrated passive and active attacks against a commercial ICD which they had acquired via an online auctioning platform [8]. The attacks harmed both patients' privacy and safety. The researchers reverse-engineered the ICD's proprietary communication protocols and then launched attacks via a commercially available software defined radio. They were able to extract private data stored inside the ICD such as patients' vital signs and medical history, and to 'eavesdrop' on wireless communication with the device programmer. They were also able to make the ICD communicate indefinitely with an unauthenticated external device, which would lead to the depletion of the device's battery and to a resulting denial of service of the ICD. The study concluded that there were no "technological mechanisms in place to ensure that programmers can only be operated by authorized personnel" [8].

This highlights a tension between safety and security inherent in the system. The inability to distinguish between legitimate treatment requests originating from a doctor or illegitimate requests is, in fact, a safety feature. The mechanisms were designed to immediately respond to reprogramming instructions from health-care practitioners, for ex-ample in an emergency situation. Hence, the vulnerabilities exploited in the experiments were the very same safety features that enable the ICD to save lives.

Other studies of pacemakers demonstrate similar vulnerabilities. Security researcher Barnaby Jack found privacy and control vulnerabilities in the telemetry system of an ICD that allowed him to deliver a deadly 830-volt shock with a laptop from 30-50 feet away with a specially crafted software. Specifically, both the implants and the wireless transmitters were capable of using Advanced System Standard (AES) encryption, but it was disabled on the devices. Moreover, devices were built with 'backdoors' so that programmers could get access to the devices only by using the serial and model number. Again, this demonstrates a safety feature, allowing unauthenticated programmers to access the device in emergency situations, in conflict with security requirements. Jack also demonstrated that the ICD contained access to the software developer's remote servers. By uploading the specially crafted firmware to the servers an adversary would have the capability to infect multiple pacemakers and ICDs. Thereby, Jack demonstrated the first possibility to attack devices at scale and warned "we are potentially looking at a worm with the ability to commit mass murder" [35].

A recent paper from Belgian and British re-searchers demonstrates vulnerabilities in the proprietary communication protocols of at least 10 types of the latest generation of ICDs. They used black box reverse engineering techniques for a long-range RF channel. Subsequently, they identified several protocol and implementation weaknesses, which gave them the ability to conduct privacy and denial-of-service attacks, as well as spoofing and replay attacks of messages without needing to be in close proximity. These attacks can have potentially fatal consequences for the patient [21].

### Security vulnerabilities in cardiac device architecture

In a study published in May 2017, WhiteScope researchers Billy Rios and Jonathan Butts uncover vulnerabilities in the architecture and implementation interdependencies across the implantable cardiac device ecosystem. They discovered over 8 000 known vulnerabilities in third party software libraries implemented across four different pacemaker programmers from four different manufacturers [22]. This finding highlights an industry wide issue associated with the lack of software security updates and supply chain lock-ins.

### Examples: Attacks against wearable insulin pumps

Insulin pump systems are wearable, semi-implanted devices, as some components are physically attached to a patient and others are external. As Burleson et al. [19] summarize: "A typical insulin pump system (IPS) may include: an insulin infusion pump with wireless interface that subcutaneously delivers insulin, a continuous glucose monitor with wireless transmitter and subcutaneous sensor for glucose measurements, and a wireless remote control that the patient can use to alter infusion pump settings or manually trigger infusion injections". Current generation insulin pump systems are open-loop systems: they require patient interaction to change pump settings, such as via the remote control. Next generation devices might be closed-loop systems.

In 2011, a group of researchers targeted the telemetry system of a semi-implantable insulin pump in a similar manner as the attacks on cardiac devices described above [20]. They found that the communications between the IPS's remote control and the IPS were unencrypted, which could lead to patient information disclosure. They were also able to inject forged packets reporting incorrect glucose levels to the patient and pump, and to issue unauthorized pump-control commands. In a Black Hat conference talk, security researcher Jerome Radcliffe demonstrated how he was able to circumvent authentication mechanisms and gain full control over the IPS of his own insulin pump via the wireless communication channel [18]. Security researcher Barnaby Jack demonstrated similar vulnerabilities during a live demonstration in which he remotely controlled and shut down a volunteer's insulin pump. He also demonstrated privacy vulnerabilities in insulin pumps in which he found that certain IPSes respond to anonymous radio scanning with their serial numbers [62].

In 2016, Johnson & Johnson had to warn patients and doctors of a software vulnerability in one of its insulin pump model's 'One Touch Ping' system which attackers could exploit to overdose diabetic patients with insulin [63].

*Security vulnerabilities in stationary medical devices that can enable network attacks*

Data about the vulnerability of stationary medical devices – monitoring, diagnostic, or therapeutic – abound. A 2014 report by the SANS Institute concluded that 94 percent of health care organizations have been the victim of a cyber attack, including attacks on medical devices and infrastructures [29]. Security expert Scott Erven discovered around 30 flaws in medical systems such as MRI machines, cardiology systems, and infusion systems, some of which involved an old remote code execution flaw from 2008 (MS08-67). This vulnerability can enable outsiders to gain access to a network and is the same one used by the Conficker worm [64]. Other reports have highlighted the extraction of patient data from medical devices and their use as conduits to attack hospital networks (Independent Security Evaluators 2016). Many healthcare-related systems, including medical devices, are discoverable via the control system search engine Shodan. Security firm Trend Micro counted around 101 000 systems globally in 2017 [65]. Not all of these systems will be vulnerable to an attack, but at least pose a target for online attackers.

Once attackers have gained access to a health organization network, they can exploit their position for a number of different types of assaults, such as data theft or device manipulation. An increasingly popular and lucrative option for criminals is the infection of health organization's systems with ransomware.

Example: Malware 'hijacking' medical devices in hospitals

A study by the security firm TrapX found a specific type of exploit currently used, called 'MedJack'. The exploit introduces malware onto vulnerable medical devices, 'hijacks' them as an entry point into hospital networks, and then move laterally through the network to access patient record systems and exfiltration the data [66]. In a 2016 report, TrapX observed the attacks becoming more sophisticated. The attackers were intentionally using old malware to target legacy medical devices running on Windows XP and Windows Server 2003. The use of old malware allowed the attackers to avoid detection more easily: "By camouflaging old malware with new techniques, the attackers are able to successfully bypass traditional security mechanisms to gain entry into hospital networks and ultimately to access sensitive data" [30]. The motive behind the attacks is likely financial (sale of patient records). However, the black market value of health records plummeted in 2016 to around 1.50 to 10 US dollars in 2016 from around 50 US dollars in 2012. This is a major reason why criminals are switching from stealing patient data to spreading ransomware [67].

Example: Vulnerabilities in Hospira hospital drug pumps

In 2015, it emerged that a line of Austrian manufacturer Hospira's hospital drug pumps were exposed to a series of remotely exploitable vulnerabilities that could allow an attacker to take complete control of affected pumps or render them useless [23]. The incident marked the first time that, after initial hesitation [68], the FDA advised healthcare providers to discontinue use of a medical device because of a cyber-security vulnerability [23].

Ransomware attacks against hospitals

Ransomware is becoming an increasingly popular tool for cyber criminals to extract money from hospitals. Cases in which ransomware disrupted digital systems and rendered services unavailable include an attack on the Hollywood Presbyterian Medical Center in 2015, which knocked computers offline for a week [69], an attack on the German Lukas hospital in Neuss in 2015 [70]. In their investigation of malware in hospital systems, security Firm TrapX also found a type of ransomware called 'Citadel'. The attackers had not activated the mal-ware, but its presence is certainly unsettling. It is only a matter of time until ransomware will also target individual medical devices, which could directly affect patient safety.

*Unintentional Exploitation / Collateral damage*

Another common risk is that malware such as a virus or worm designed to indiscriminately disrupt computer systems or is targeted at other computer systems, breaches the security of medical devices based on the security profile of the device itself. As discussed, many devices in health organizations run on outdated and vulnerable operating systems and software, have poor security configurations, and/or are connected to insecure networks. As a result, these devices are vulnerable to malware that might not even specifically target medical devices, and is vulnerable even to old malware. As mentioned previously, researchers found Conficker malware on many operating medical devices in hospital networks.

In May 2017, the ‘WannaCry’ ransomware worm hit computer systems in over 150 countries. The malware affected systems running on outdated vulnerable versions of the Microsoft Windows operating system with Server Message Block version 1 (SMBv1) enabled. The malware severely affected several health organizations in the United Kingdom (UK), but also infected medical devices in hospitals worldwide. The incident prompted the US Industrial Control System CERT (ICS-CERT) along with several medical device vendors (including Siemens Healthineers, Draeger, and Medtronic) to issue security alerts about vulnerable medical device models and mitigations that should be implemented by hospitals that deploy software on vulnerable versions of Win-dows with SMBv1 enabled [31], [42], [71].

The risk emanating from such incidents will only increase. Wiper malware, such as the ‘Shamoon’ or ‘StoneDrill’ malware, which effectively wipes a victim’s machine, could also be deployed against medical devices, thereby disrupting or destroying them [72]. Distributed Denial of Service (DDoS) attacks, such as the one executed against the Dyn DNS resolver in October 2016, might also affect hospitals and medical devices in the future. In a US Congressional Hearing in November 2016, security expert Kevin Fu stated: “Hospitals survived [this attack] not by design, but by luck” [73] .

In conclusion, these cases demonstrate the gravity of structural security deficiencies of medical devices – whether they are deployed in a hospital environment or implanted in the patient’s body. To date, hospitals and patients have been spared from extreme attacks that cause injury or death to patient and/or affect health care at a large scale. Yet, the research generated over the past decade demonstrates the seriousness of this risk. Many of the underlying reasons for medical device insecurity are structural. Cyber security in medical devices is a multifaceted issue that requires technical controls, risk management, governance, and regulation. Indeed, we are not starting from scratch: regulatory frameworks, standards, and risk management practices to ensure the safety of medical devices have been in place for a long time already. The challenge now is to ‘update’ and complement these approaches with IT security mechanisms.

# References

[1] K. Hänninen, H. Hansson, H. Thane and M. Saadatmand, “Inadequate Risk Analysis Might Jeopardize The Functional Safety of Modern Systems,” Västeras, 2016.

[2] E. Leverett, R. Clayton and R. Anderson, “Standardisation and certification in the 'Internet of Things',” in *16th Annual Workshop on the Economics of Information Security (WEIS)*, 2017.

[3] P. Williams and A. J. Woodward, “Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem,” *Medical Devices. Evidence and Research,* vol. 8, pp. 305-316, 2015.

[4] U. GAO, “Medical devices: FDA should expand its consideration of in-formation security for certain types of devices,” U.S. Government Accountability Office, 2012.

[5] J. Healey, N. Pollard and B. Woods, “The Healthcare Internet of Things: Rewards and Risks.,” Atlantic Council, Washington, DC, 2015.

[6] Ponemon Institute, “Medical device security: An industry under attack and unprepared to defend,” 2017.

[7] K. Sandler, L. Ohrstrom, L. Moy and R. McVay, “Killed by Code: Software Transparency in Implantable Medical Devices - Software Freedom Law Center,” Software Freedom Law Center, 2010.

[8] D. Halperin, T. Heydt-Benjamin, B. Ransford, S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno and M. W., “Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero Power Defenses,” in *IEEE Symposium on Security and Privacy*, 2008.

[9] I. S. Evaluators, “Hacking hospitals,” Independent Security Evaluators, 2016.

[10] R. Piggin, “Cybersecurity of medical devices.,” BSI Group; BSI/UK/1014/ST/0217/EN/HL, 2017.

[11] “Digital Society Institute Workshop: Sicherheit in der vernetzten Medizin,” 18 October 2017. [Online]. Available: https://www.esmt.org/node/30763.

[12] Roland Berger Consultants, “Digital healthcare market to average 21 percent growth per year through 2020,” Roland Berger, 2016.

[13] N. Lord, “Top 10 Biggest Healthcare Data Breaches of All Time,” 28 March 2017. [Online]. Available: https://digitalguardian.com/blog/top-10-biggest-healthcare-data-breaches-all-time. [Accessed October 2017].

[14] D. B. Kramer, C. Sato and A. S. Kresselheim, “Ensuring Medical Device Effectiveness and Safety: A Cross-National Comparison of Approaches to Regulation,” *Food Drug Law Journal,* vol. 69, no. 1, pp. 1-23, 2014.

[15] L. Piètre-Cambacédès and C. Chaudet, “The SEMA referential framework: Avoiding ambiguities in the terms “security” and “safety”,” *International Journal of Critical Infrastructure Protection,* vol. 3, no. 2, pp. 55-66, 2010.

[16] L. M. B., O. Nordland, L. Rostad and I. Tondel, “Safety vs Security?,” in *International conference on probabilistic safety assessment and management - 0148*, 2006.

[17] H. Alemzadeh, K. Iyer and Z. Kalbarcyk, “Analysis of safety-critical computer failures in medical devices,” *IEEE Security and Privacy,* vol. 11, no. 4, pp. 16-25, 2013.

[18] J. Radcliffe, “Hacking medical devices for fun and insulin: Breaking the human SCADA system.,” in *Black Hat Conference*, 2011.

[19] W. Burleson, S. Clark, B. Ransford and K. Fu, “Design challenges for secure implantable medical devices,” in *Design Automation Conference*, San Francisco, 2012.

[20] C. Li, A. Raghunathan and N. K. Jha, “Hijacking an insulin pump: Security attacks and defences for a diabetes therapy system,” in *Proceedings of the 13th IEEE International Conference on e-Health Networking, Applications, and Services, Healthcom ‘11*, 2017.

[21] M. E., D. Singelée, F. D. Garcia, T. Chothia, R. Willems and B. Preneel, “On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them,” in *ACSAC '16 Proceedings of the 32nd Annual Conference on Computer Security Applications: 226-236*, 2016.

[22] B. Rios and J. Butts, “Security evaluation of the implantable cardiac device ecosystem and architecture and implementation interdependencies,” WhiteScope, 2017.

[23] “FDA Safety Communication: Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System,” US Food & Drug Administration, 31 07 2015. [Online]. Available: https://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm456815.htm. [Accessed 01 10 2017].

[24] “FDA Safety Communication: Cybersecu-rity Vulnerabilities Identified in St. Jude Medical’s Implantable Cardiac Devices and Merlin@home Transmitter,” US Food & Drug Administration, 19 01 2017. [Online]. Available: https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm. [Accessed 01 10 2017].

[25] R. Anderson, “Why information security is hard,” in *17th annual computer security applications conference*, 2001.

[26] “Diagnosing cyber threats for smart hospitals,” European Union Agency for Network and Information Security, 2016.

[27] “KRITIS-Sektorstudie Gesundheit,” Bundesamt für Sicherheit in der Informationstechnik, 2016.

[28] H. Tanriverdi, “Nächtliches Desaster,” *Sueddeutsche Zeitung,* 23 06 2015.

[29] B. Filkins, “Healthcare cyberthreat report: Widespread compromises detected, compliance night-mare on the horizon,” SANS Institute InfoSec Reading Room, 2014.

[30] “TrapX Labs Discovers New Medical Hijack Attacks Targeting Hospital Devices,” TrapX Labs, 27 06 2016. [Online]. Available: https://trapx.com/trapx-labs-discovers-new-medical-hijack-attacks-targeting-hospital-devices-2/. [Accessed 01 10 2017].

[31] ICS-CERT, “Indicators associated with WannaCry ransomware (Update I),” 15 05 2017. [Online]. Available: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-135-01I. [Accessed 01 10 2017].

[32] “Application Threat Modeling,” OWASP, [Online]. Available: https://www.owasp.org/index.php/Application_Threat_Modeling. [Accessed 01 10 2017].

[33] “FDA Safety Communication: Cybersecurity for medical devices and hospital networks,” US Food & Drug Administration, 13 06 2013. [Online]. Available: https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm. [Accessed 03 10 2017].

[34] H. C. I. C. T. Force, “Report on Improving Cybersecurity in the Health Care Industry,” 2017.

[35] D. Storm, “Pacemaker hacker says worm could possibly 'commit mass murder',” *Computerworld,* 17 10 2012.

[36] S. Gollakota, H. Hassanieh, B. Ransford and D. Katabi, “They Can Hear Your Heartbeats: Non-invasive Security for Implantable Medical,” in *SIGCOMM Computer Communication Review*, 2011.

[37] M. Rostami, W. Burleson, F. Koushanfar and A. Jules, “Balancing security and utility in medical devices?,” in *The 50th Annual Design Automation Conference 2013*, Austin, TX, 2013.

[38] F. Xu, Z. Qin, C. C. Tan, B. Wang and Q. Li, “Imdguard: Securing implantable medical devices with the external wearable guardian,” in *INFOCOM 2011, 30th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies*, Shanghai, China, 2011.

[39] R. Koppel, S. Smith, J. Blythe and V. Kothari, “Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient?,” *Studies in health technology and informatics,* vol. 208, pp. 215-220, 2015.

[40] P. Masci, R. Rukenas, P. Oladimeji, A. Cauchi, A. Gimblett, Y. Li, P. Curyon and H. Thimbelby, “The benefits of formalising design guidelines: A case study on the predictability of drug infusion pumps,” *Innovations in Systems and Software Engineering,* vol. 11, no. 2, pp. 73-93, 2015.

[41] S. Bellovin, “Patching is hard,” Columbia University, SM Blog, 12 05 2017. [Online]. Available: https://www.cs.columbia.edu/~smb/blog/2017-05/2017-05-12.html. [Accessed 01 June 2017].

[42] C. Brook, “Patches pending for medical devices hit by WannaCry,” Threatpost, 18 05 2017. [Online]. Available: https://threat-post.com/patches-pending-for-medical-devices-hit-by-wannacry/125758/. [Accessed 01 06 2017].

[43] M. Nunnikhoven, “WannaCry & the re-ality of patching,” Trend Micro, 14 05 2017. [Online]. Available: http://blog.trendmicro.com/wannacry-reality-of-patching/. [Accessed 01 06 2017].

[44] S. Kriaa, “Joint Safety and Security Modeling for Risk Assessment in Cyber Physical Systems,” Université Paris-Saclay, 2016.

[45] J. W. Bryans, “The internet of automotive things: vulnerabilities, risks and policy implications,” *Journal of Cyber Policy,* vol. 2, no. 2, pp. 185-194, 2017.

[46] “Commission Regulation (EU) 2017/745,” 2017.

[47] “Single Market and Standards - Medical Devices,” European Commission DG Growth, [Online]. Available: https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/medical-devices_en . [Accessed 01 10 2017].

[48] “Content of pre-market submissions for management of cybersecurity in medical devices. Guidance for industry and Food and Drug Administration staff,” US Food & Drug Administration, 2014.

[49] “Postmarket management of cybersecurity in medical devices. Guidance for industry and Food and Drug Administration staff,” US Food & Drug Administration, 2016.

[50] “Guidance for Industry – Cybersecurity for Networked Medical Devices Containing Off-the-Shelf Software,” US Food & Drug Administration, 2005.

[51] “COM(2017) 477 final. The EU cybersecurity certification framework. Proposal for a Regulation of the European Parliament and of the Council,” European Commission, Brussels, 2017.

[52] “SP 800-82, Revision 2. Guide to industrial con-trol systems (ICS) security,” National Institute for Standards and Technology, 2015.

[53] European Commission, “Introduction to the European IACS components Cybersecurity Certification Framework (ICCF),” European Commission, Brussels, 2016.

[54] “Proposed Document: Software as a Medical Device: Clinical Evaluation,” International Medical Device Regulators Forum, 2016.

[55] S. Carmody and M. Zuk, “The Evolving State of Medical Device Cybersecurity,” in *HIMSS Annual Conference, Feb 19-23, 2017*, 2017.

[56] “Cybersecurity,” Draeger, [Online]. Available: https://www.draeger.com/en_uk/Hospital/Insights-to-Solutions/Cyber-security. [Accessed 07 12 2017].

[57] “Cybersecurity at Siemens Healthineers,” Siemens Healthineers, [Online]. Available: https://www.healthcare.siemens.com/medical-imaging-it/cybersecurity. [Accessed 07 12 2017].

[58] “Hippocratic Oath for Connected Medical Devices,” I Am The Cavalry, 19 01 2016. [Online]. Available: https://www.iamthecavalry.org/domains/medical/oath/. [Accessed 01 10 2017].

[59] S. H. D. Chockalingam, W. Pieters, A. Teixera and P. van Gelder, “Integrated safety and security risk assessment methods: A survey of key characteristics and applications,” in *The 11th Interna-tional Conference on Critical Infrastructure Security*, 2016.

[60] “An overview of vulnerability disclosure programs,” I Am The Cavalty, [Online]. Available: https://www.iamthecavalry.org/resources/disclosure-programs/. [Accessed 07 12 2017].

[61] “Maude Adverse Event Report: Merge Healthcare Merge Hemo Programmable Diagnostic Computer,” U.S. Food & Drug Administration, 31 08 2016. [Online]. Available: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/detail.cfm?mdrfoi__id=5487204. [Accessed 01 10 2017].

[62] D. Goodin, “Insulin pump hack delivers fatal dosage over the air,” The Register, 27 10 2011. [Online]. Available: https://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/. [Accessed 01 10 2017].

[63] J. Finkle, “J&J warns diabetic patients: Insulin pump vulnerable to hacking,” Reuters, 04 10 2016. [Online]. Available: https://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e/jj-warns-diabetic-patients-insulin-pump-vulnerable-to-hacking-idUSKCN12411L. [Accessed 01 10 2017].

[64] R. Millman, “Vulnerabilities in healthcare de-vices show up woeful lack of security,” SC Magazine, 19 02 2016. [Online]. Available: https://www.scmagazineuk.com/vulnera-bilities-in-healthcare-devices-show-up-woeful-lack-of-security/article/531470/. [Accessed 01 10 2017].

[65] M. Rosario Fuentes, “Cybercrime and Other Threats Faced by the Healthcare Industry,” Trend Micro, 2017.

[66] “Anatomy of an Attack. Medjack (Medical Device Hijack),” TrapX Labs, 2015.

[67] M. Korolov, “Black market medical record prices drop to under $10, criminals switch to ransom-ware,” CSO Magazine, 22 12 2016. [Online]. Available: http://www.csoonline.com/article/3152787/data-breach/black-market-medical-record-prices-drop-to-under-10-criminals-switch-to-ransomware.html. [Accessed 01 10 2017].

[68] K. Zetter, “Hacker Can Send Fatal Dose to Hos-pital Drug Pumps,” WIRED Magazine, 08 06 2015. [Online]. Available: https://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/. [Accessed 01 10 2017].

[69] B. Barrett, “Hack Brief: Hackers Are Holding an LA Hospital’s Computers Hostage,” WIRED Magazine, 16 02 2015. [Online]. Available: https://www.wired.com/2016/02/hack-brief-hackers-are-holding-an-la-hospitals-computers-hostage/. [Accessed 01 10 2017].

[70] S. Steffens, “Hackers hold German hospital data hostage,” DW.com, 25 02 2016. [Online]. Available: http://www.dw.com/en/hackers-hold-german-hospi-tal-data-hostage/a-19076030. [Accessed 01 10 2017].

[71] T. Fox-Brewster, “Medical devices hit by ran-somware for the first time In US hospitals,” Forbes, 17 05 2017. [Online]. Available: http://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-med-ical-devices/. [Accessed 01 10 2017].

[72] C. Raiu, M. Hasbini, S. Belov and S. Mineev, “From Shamoon to StoneDrill,” Kaspersky Lab Securelist, 06 03 2017. [Online]. Available: https://securelist.com/from-shamoon-to-stonedrill/77725/. [Accessed 01 10 2017].

[73] K. Fu, “Infrastructure Disruption: Internet of Things Security. Statement submitted to the U.S. House Energy and Commerce Committee,” Subcommit-tee on Communications and Technology & Subcommit-tee on Commerce, Manufacturing, and Trade Joint Hearing on Understanding the Role of Connected De-vices in Recent Cyber Attacks, Washington, DC, 2016.

**Publication V**

Maurer, Tim, Skierka, Isabel, Morgus, Robert, Hohmann, Mirko. (2015). Technological sovereignty: Missing the point? *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace; Tallinn, Estonia; 26–29 May 2015.* IEEE Xplore: IEEE, 53−68. https://doi.org/10.1109/CYCON.2015.7158468 (3.1).

**2015 7th International Conference on Cyber Conflict:**
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

# Technological Sovereignty: Missing the Point?

**Tim Maurer**
Open Technology Institute
New America
Washington, DC, USA
maurer@newamerica.org

**Robert Morgus**
Open Technology Institute
New America
Washington, DC, USA
morgus@newamerica.org

**Isabel Skierka**
Global Public Policy Institute
Berlin, Germany
iskierka@gppi.org

**Mirko Hohmann**
Global Public Policy Institute
Berlin, Germany
mhohmann@gppi.net

**Abstract:** Following reports of foreign government surveillance starting in June 2013, senior officials and public figures in Europe have promoted proposals to achieve "technological sovereignty". This paper provides a comprehensive mapping and impact assessment of these proposals, ranging from technical ones, such as new undersea cables, encryption, and localized data storage, to non-technical ones, such as domestic industry support, international codes of conduct, and data protection laws. The analysis focused on the technical proposals reveals that most will not effectively protect against foreign surveillance. Ultimately, the security of data depends primarily not on where it is stored and sent but how it is stored and transmitted. In addition, some proposals could negatively affect the open and free Internet or lead to inefficient allocation of resources. Finally, proposals tend to focus on the transatlantic dimension, neglecting the broader challenge of foreign surveillance.

**Keywords:** *international affairs, foreign policy, cyber security, technological sovereignty, surveillance, encryption*

## 1. INTRODUCTION

In the months following the 2013 reports revealing surveillance by foreign governments, European government officials and public figures have promoted a variety of measures for gaining "technological sovereignty." The current German government's coalition agreement, for example, explicitly states that it will "take efforts to regain technological sovereignty."[1]

Technological sovereignty has been used as an umbrella term to suggest a spectrum of different technical and non-technical proposals, ranging from the construction of new undersea cables to stronger data protection rules. Many of them are not new but have developed greater political traction over the past year.

The main contribution of this paper is a comprehensive, systematic mapping and impact assessment of these technological sovereignty proposals.[2] Non-technical proposals such as a restructured Safe Harbor Agreement or a new European Union Data Protection Directive are also part of the debate and pose pros and cons of their own. However, that is outside the scope of this paper, which focuses on the technical measures and whether they will actually protect against foreign surveillance and gauge their impact on the open and free Internet. It builds upon existing literature,[3] but differs by distinguishing between types of proposals, and by considering whether they achieve their purported goal of protecting against foreign surveillance. This paper goes beyond analyses focused solely on data localization requirements[4] by providing a comprehensive overview of the proposals that have been advanced under the umbrella of technological sovereignty.

Research on the implications of these technological sovereignty proposals remains nascent. A growing body of literature examines the growth of "data localization" policies, meaning the "laws and guidelines which limit the storage, movement, and/or processing of digital data to specific geographies, jurisdictions, and companies."[5] Such proposals were the focus of attention in early 2014, because they were part of Brazil's debate over its Internet Bill of Rights, "Marco Civil da Internet." The term "technological sovereignty" remains vague. As it is used by European policymakers, it resembles terms like "data sovereignty," which has been defined as "a spectrum of approaches adopted by different states to control data generated in or passing through national [I]nternet." It is a subset of "cyber sovereignty," which is "the subjugation of the cyber domain to local jurisdiction."[6]

Our analysis builds on the scholarship and approach of Internet governance expert Laura DeNardis, who writes, "arrangements of technical architecture are also arrangements of power."[7] The Internet is a meta-network, composed of a constantly changing collection of individual networks and devices that communicate with each other through the Internet Protocol (IP). Through technical features, the physical and software architecture, or code, shapes human behavior on the Internet and beyond. Because the Internet has become a fundamental part of our modern way of life, changes to its technical architecture have major implications for many structures of society. This architecture constitutes a powerful tool for actors to further their interests. Code "sets the terms upon which [actors] enter, or exist, in cyberspace."[8] According to Stanford law professor Barbara van Schewick, policymakers who traditionally used the law can now use Internet technologies to bring about desired political or economic effects.[9] Building upon this scholarship, we designed a framework for classifying the proposals based on what part of the Internet they impact.

Our research identified proposals from over a dozen countries in Europe, ranging from technical ones, like localized or nationalize routing schemes, to non-technical ones, like a European wide data protection authority. The majority of proposals are from Germany. They come from academia, the government, and the private sector and differ even within government as different ministries brought forth different proposals. Upon further examination of the technical proposals, our analysis shows that most will not effectively protect against foreign surveillance. Ultimately, the security of data depends primarily not on where it is stored and sent but how it is stored and transmitted. In addition, some proposals could negatively affect the open and free Internet or lead to inefficient allocation of resources. Finally, proposals tend to focus on the transatlantic dimension, neglecting the broader challenge of foreign surveillance and ideas like the expansion of encryption tools that are more effective at securing data.

## 2. METHODOLOGY

We began this research by collecting proposals and statements[i] by European political decision-makers, as well as those of stakeholders from the private sector and academia, made after June 5, 2013, the day on which the first wave of articles about government surveillance was published.[ii] It is important to bear in mind that while these proposals were advanced in response to the surveillance affair, they address different dimensions of a complex problem, namely the protection of (1) government secrets; (2) individual citizens' privacy; and (3) industry secrets. An additional complexity is the fact that policymakers have been using the political attention to suggest new industrial policies aimed at supporting the European Information Technology (IT) sector through major public investments and IT sector-specific subsidies.

Upon completing the desk based collection phase of research, we proceeded in three steps to determine how each proposal affects the governing structures of the Internet, different types of data, and the Internet's underlying architecture.

### *Step 1: Dividing proposals into Two General Categories – Technical and Non-Technical*

A first review of the proposals revealed that they could be clustered into two general groups: technical and non-technical proposals. We then grouped technical proposals based on the type of technological change proposed: new undersea cables, national e-mail, localized routing, encryption, and localized data storage. These proposals directly affect the technical architecture of the Internet. Non-technical proposals are those that affect the Internet in other ways – for example, calls for new laws or for more transparency, which could affect the technical architecture but indirectly so.

Technical proposals are based on the type of technological change proposed: new undersea cables, national e-mail, localized routing and storage, and encryption. New undersea cables, for example, refer to suggestions to directly connect Latin America and Europe, avoiding data transfer through the United States. Likewise, national e-mail was suggested in Germany as a means of avoiding contact with American servers whenever possible. Localized routing goes a step further than national e-mail, in the sense that it would encompass all data, not just e-mail data, and route it solely through local servers. However, localized does not necessarily mean that the data is concentrated in one country. For example, localized could encompass the

[i] These proposals and their sources are detailed in Figure 2.

[ii] For greater detail on this topic, see: Maurer, Tim, Robert Morgus, Isabel Skierka, and Mirko Hohmann. 2014. "Technological Sovereignty: Missing the Point?" *Transatlantic Dialogues in Freedom and Security*. <http://www.digitaldebates.org/tech_sovereignty/>.

entirety of the European Union. Finally, there have been calls for improving encryption, making existing encryption more accessible to the general public, and extending it to mobile devices.

Non-technical proposals are sorted based on the changed mechanism: institution, law, norm, transparency, and business. The idea to establish a single EU Data Protection Agency exemplifies how actors consider institutions as a means of addressing a given challenge. A wide variety of laws have been proposed, and some implemented, ranging from changes to the US-EU Safe Harbor agreement[10] to domestic data protection laws. There are also several proposals aimed at increasing trust – not through regulation, but through the establishment of common norms, like a "no-spying" agreement between the US and European partners.[11] Another non-technological category is composed of proposals aimed at increasing transparency of how governments and businesses handle the data of citizens and customers. Proposals to advance the national production of hardware and software mainly originate in Germany, such as the "IT Security Made in Germany" brand or the production of an IT-Airbus in cooperation with France. Ideas like these fall into the business cluster, though there are technical components to the proposals. Generally, these non-technical proposals impact non-technical factors that shape the Internet, like laws, norms, markets, and institutions.

For the purposes of this paper, we focus on the proposals that have the highest likelihood of impacting the technical functionality of the Internet, which we call technical proposals.

## *Step 2: Determining Proposals' Political Traction*

Some proposals have gained more political traction than others over the past year and a half. For our purposes, high political traction means that proposals have been widely discussed and have been implemented, or plans for implementation have been set. Other proposals have been discussed, but their implementation remains uncertain. These are classified as having medium political traction. Some proposals have been barely discussed or were discussed and discarded, and these are classified as having low political traction.[iii]

## *Step 3: Integrating Different Types of Data: Data in Motion, Data at Rest, and Metadata*

To elevate the level of technical acumen informing this debate, it is important to note that several types of data exist: data in motion, data at rest, and metadata. Governance proposals depend on what type of data is to be governed.

The data we access on the Internet is stored on servers. When this data is inactive – meaning, it is not being changed or in motion – it is classified as data at rest. Data at rest can be the text, music, or video files we store in the cloud, or the data that is the content of a webpage stored on a company server.

Data in motion is data that traverses the physical infrastructure of the Internet. Because the Internet is a global network of computing devices, from laptops and PCs to smart phones, data must flow from the host device or server to the device trying to access it. The easiest way to explain this phenomenon is to picture an e-mail sent from one user to another. The sender generates the data that then travels over the cables and wires that make up the physical

[iii] We explain the degree of political traction of the technical proposals in the Impact Analysis, section 3.

infrastructure of the Internet, until it reaches the intended recipient. The same process happens when a user tries, for example, to access content through a webpage or download videos from a server. The route taken by the data depends on a number of factors, ranging from physical constraints like bandwidth to contractual considerations like peering agreements. Nonetheless, data is generally routed through what technologists refer to as the "cheapest" route. This ensures that the data reaches its recipient quickly and keeps Internet speeds high for everyone.

Metadata, simply put, is the data about data. Two types exist. Structural metadata "indicates how compound objects are put together."[12] This type of metadata is mostly used to present complex items. Structural metadata takes two separate streams of data, identifies them, and then ensures that they are properly synchronized for presentation. In other words, structural metadata ensures that the visual stream of the latest movie you are watching is synchronized with the audio stream. The second type of metadata is descriptive metadata, which "describes a resource for purposes such as discovery and identification."[13] This is the conceptualization of metadata. Descriptive metadata allows users to query databases and to identify data based on relevant criteria. It should be noted that even encryption does not necessarily protect metadata from surveillance. Figure 2 visualizes how the proposals are clustered.

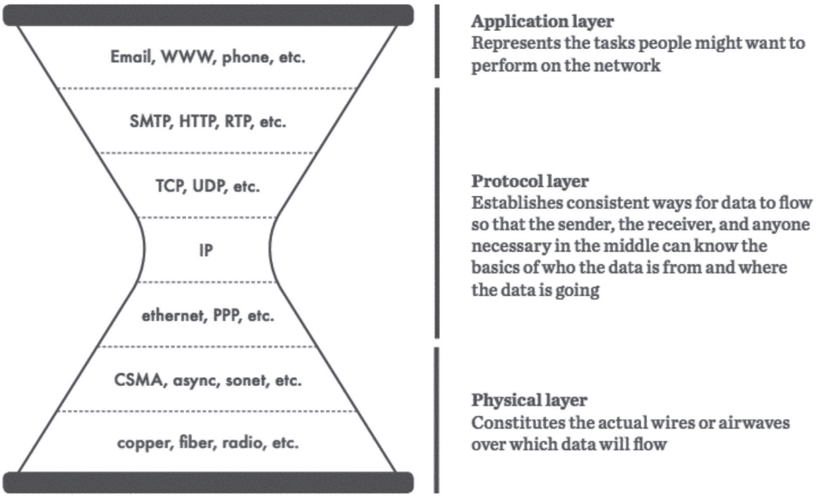
## *Step 4: Zooming in on Data in Motion: the Hourglass Model*

Several models exist to illustrate the intricacies of the technical architecture that underlies the Internet. Internet expert and Harvard law professor Jonathan Zittrain built upon those and the work of many other scholars by combining the technical and social components of the Internet with his interpretation of the Hourglass Model, which highlights the centrality of the IP for the Internet's coherence and interoperability.

At the bottom is the physical layer, or "the actual wires or airwaves over which data will flow."[14] Undersea and fiber-optic cables are physical examples of the physical layer, as are the servers that receive them and the satellites that transmit a limited amount of Internet traffic. Next is the protocol layer, which "establishes consistent ways for data to flow so that the sender, the receiver, and anyone necessary in the middle can know the basics of whom the data is from and where the data is going."[15] This layer includes the limited IP, as well as the HTTP and the Simple Transportation Management Protocols (STMP). The IP layer is the narrowest layer in the hourglass model, signifying that it is, for the time being, the least elastic feature of the Internet, but also the layer on which the rest rely for communication. While we can build new cables and add more end-user devices, we are constrained by a finite number of IP addresses. Moving up the Hourglass, we find the application layer, "representing the tasks people might want to perform on the network."[16] E-mail clients and websites, for example, make up this layer. Resting atop the Hourglass are Zittrain's final two layers: the content layer, which is the actual information exchanged through the other layers, and the social layer, "where new behaviors and interactions among people are enabled by the technologies underneath."[17] These layers and the implications they carry apply directly to the proposals that we classify as technical proposals.

The architecture constraint in real space is the constraint of code in cyberspace. As the Internet has become a fundamental part of our modern way of life, changes to its technical architecture have major implications for many structures of society. That’s why the technical proposals are a specific focus of this paper.

**FIGURE 1:** THE HOURGLASS MODEL



**Application layer**
Represents the tasks people might want to perform on the network

**Protocol layer**
Establishes consistent ways for data to flow so that the sender, the receiver, and anyone necessary in the middle can know the basics of who the data is from and where the data is going

**Physical layer**
Constitutes the actual wires or airwaves over which data will flow

Source: Zittrain, Jonathan (2008) *The Future of the Internet and How to Stop It*. Yale University Press. p. 67-68.

**FIGURE 2:** TECHNICAL PROPOSALS

| Type of Proposal | Summary | Proposing Actors | Country or Region | Time Range | Data Type | Layer | Political Traction |
|---|---|---|---|---|---|---|---|
| New Undersea cables | Lay a new fiber-optic submarine cable between Latin America and Europe; lay a new fiber-optic cable between Finland and Germany, circumventing Sweden[18, 19] | Public:<br>Herman Van Rompuy[iv]<br>Krista Kiuru[v] | EU, Finland | 12/11/2013 - 2/24/2014 | Motion | Physical | High |
| Localized routing | Data streams should flow within a geographically restricted zone; inter-Schengen data traffic should be routed within the Schengen zone[20, 21, 22, 23, 24, 25] | Public:<br>German government<br>Private:<br>Deutsche Telekom, Atos | France, Germany | 10/12/2013 - 7/27/2014 | Motion + Meta | Protocol (Content, Applica-tion, Physical) | Medium |

[iv] President of the European Council.

[v] Finnish Minister of Education, Science and Communication.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| National e-mail | Route all e-mails within Germany on German servers and cables[26] | Private: Deutsche Telekom | Germany | 8/1/2013 | Motion + Meta | Application | High |
| Localized data storage | Create a European or a Schengen cloud; create a European or Schengen zone for data[27, 28, 29, 30] | Public: French, German governments<br>Private: Green,[vi] Deltalis,[vii] Quantique,[viii] EuroCloud[ix] | France, Germany, Poland, Switzerland | 6/27/2013 - 5/14/2014 | Rest + Meta | Data at rest | High - Medium |
| Expansion of encryption tools | End-to-end encryption of communication data; encryption of end devices;[31, 32, 33]<br>End-to-end mobile voice encryption;[34, 35] Secure SIM data for corporate customers[36] | Public: European Parliament,<br>Academia: Stefan Katzenbeisser,[x] Mark Manulis[xi] | Germany, UK | 11/23/2013 - 2/24/2014 | Motion + Rest | Protocol, Content, Application, Physical, and Data at rest | Medium |

## 3. IMPACT ANALYSIS

This impact analysis examines whether the proposals actually achieve their purported goals of making data more secure in response to the surveillance debate, and then assesses the proposals' broader implications for the Internet, using the 2011 OECD Principles for Internet Policy-Making.[37]

The OECD principles provide concise guidance for policymakers crafting Internet policy, and they were designed to "help preserve the fundamental openness of the Internet while concomitantly meeting certain public policy objectives."[38] Given that the OECD member countries, as well as multiple other stakeholders, agreed upon these principles, they offer a useful anchor for transatlantic cooperation. We identified eight out of the 14 principles that are relevant to technological sovereignty and grouped them into four categories that constitute the foundation for our analysis of the proposals:[xii]

Human Rights:

| | |
|---|---|
| OECD #1: | Promote and protect the global free flow of information. |
| OECD #9: | Strengthen consistency and effectiveness in privacy protection at a global level. |

[vi] Switzerland.

[vii] Switzerland.

[viii] Switzerland.

[ix] Poland.

[x] Technische Universität Darmstadt, Germany.

[xi] University of Surrey, United Kingdom.

[xii] For a full list and explanation of the principles, see Annex 3 of Maurer, Tim, Robert Morgus, Isabel Skierka, and Mirko Hohmann. 2014. "Technological Sovereignty: Missing the Point?" *Transatlantic Dialogues in Freedom and Security*. <http://www.digitaldebates.org/tech_sovereignty/>.

Governance – Open Internet:

OECD #2: Promote the open, distributed, and interconnected nature of the Internet.
OECD #8: Ensure transparency, fair process, and accountability.

Economic:

OECD #4: Promote and enable the cross-border delivery of services.
OECD #11: Promote creativity and innovation.

Security:

OECD #13: Encourage cooperation to promote Internet security.
OECD #14: Give appropriate priority to enforcement efforts.

## *New Undersea Cables*

Public sector officials have suggested laying new undersea cables in order to circumvent foreign surveillance. Laying new undersea cables alters the physical layer of the Internet's architecture over which data will flow and does not harm the free flow of information *per se*. However, new undersea cables are not an effective strategy to protect against foreign surveillance because foreign law enforcement and intelligence agencies are adept at tapping undersea cables.[39] Thus, proposals for new undersea cables as a means to avoid foreign surveillance creates a false sense of security for users. While new and more undersea cables can positively contribute to an interconnected and distributed Internet, they do not make data more secure.

## *Localized Routing*

Parts of both the public and private sectors have suggested the implementation of localized routing. These schemes require the alteration of transmission protocols that dictate how data flows over the physical architecture of the Internet. However, despite physically altering the location of data flows, localized routing does not effectively protect data from foreign surveillance. For this reason, legally mandated localized routing schemes have lost nearly all their political traction in Europe. It would also make law enforcement easier, as data would be subject to national data protection laws, which usually contain law enforcement exemptions.[40] Therefore, the localization of routing is unlikely to actually secure communications and risks providing a false sense of security to Internet users.

Mandatory localized routing requirements could also have dire consequences for the Internet as a whole. It would require changes to the routing protocols and IP address allocation system, contra to one of the Internet's fundamental principles that data flows via the cheapest or most efficient route. Whether or not a localized routing scheme negatively affects the free flow of information depends on the rule of law in the location in question. This enhances domestic private and state actors' control over information and data flows, and several authoritarian regimes have sought to implement localized routing to increase their own control over data flowing across the Internet infrastructure geographically located within their country.[41] It should be noted that there has also been a debate about "Network Security Agreements" between the U.S. government and foreign telecommunications providers, such as Deutsche Telekom, to localize routing of national data traffic.[42]

## *National E-Mail*

National e-mail schemes, like E-Mail Made in Germany, were proposed and implemented by both Deutsche Telekom and United Internet, who are serving more than two thirds of e-mail users in Germany.[43] However, because the proposed service does not use a higher than normal security standard to this date it will not protect against surveillance any better than existing services of which many have used the Simple Mail Transfer Protocol Secure (SMTPS) with Transport Layer Security (TLS) for years already.[44] Moreover, the E-Mail Made in Germany initiative has been criticized for using a proprietary standard for secure data transmission (the "Inter Mail Provider Trust") instead of the openly available standard DANE (DNS-Based Authentication of Named Entities), which other smaller competitors have been using and is more easily auditable.[45] Finally, if data is stored unencrypted on the e-mail provider's servers, it can still be intercepted regardless of the encryption used for the data in transit.

National e-mail could in fact make law enforcement easier, since data is stored within national borders and subject to national data protection laws, which usually contain enforcement exceptions.[46] The proposed service highlights the risk of promoting proposals that give users a false sense of security by claiming enhanced security features without actually significantly enhancing security.

## *Localization of Stored Data*

Both public and private sector officials have proposed mandating localized data storage. Proposals to territorially localize data storage seek to store all data generated by Europeans on servers located in Europe. This action will not effectively protect data from surveillance and actually concentrates the data in a number of defined physical locations, potentially narrowing the search for intelligence and law enforcement agencies seeking specific data.

Adding to that, legal barriers for foreign intelligence agencies are often less strict when collecting data internationally. Although data stored in Europe is subject to EU data protection laws, this does not mean that the parties that own the data are exclusively subject to those same laws. Therefore, the security of data from foreign intelligence agencies depends not on where it is stored, but on comprehensive security practices, modern technology, and qualified security personnel.[47] Similar to other localization proposals, it risks providing a false sense of security to users.

Localized data storage would also harm the open and distributed nature of Internet, by forcing the "nodes" to be located in specific geographic areas, where their operations might be suboptimal from a global perspective.

Requiring localized data storage would impede cross-border delivery of services and raise costs and barriers to entry, particularly for smaller companies, which in turn risks hampering innovation.[48]

For these reasons, no steps have been taken to date to legally mandate localized data storage. Instead, policymakers have turned to the promotion of voluntary data security standards. For example, the European Commission issued the Common Service Level Agreements for Cloud Computing[49] and the European Cloud Partnership, which suggest common, non-binding security and encryption standards for European cloud providers storing data on European soil.[50]

## *Expansion of Encryption Tools*

Suggestions to expand encryption tools have come from the public sector and academia. While encryption may not protect individuals against sophisticated, targeted surveillance by intelligence agencies, the widespread use of encryption would significantly raise the cost of surveillance generally. The more individuals encrypt their communications, the more difficult and costly it will to decrypt those communications. Encryption can be applied to all layers of the Internet – to the physical layer (cable or radio communications), the protocol layer (i.e, Hypertext Transfer Protocol [HTTP] or Transmission Control Protocol [TCP]), and the application layer (e-mail, www, mobile). Thus, encryption can protect both data in motion through end-to-end encryption of communications, as well as data at rest through encryption of devices or servers at the end nodes.

Calls for stronger encryption have received growing political traction around the world. Several experts have called for the development of more easily accessible encryption tools,[51] and the European Parliament has called on the European Commission to "strengthen the protection of confidentiality of communication … by way of requiring state-of-the-art end-to-end encryption of communications."[52] Major technology companies like Apple and Google have also begun offering encryption by default,[53] and the Internet Engineering Task Force (IETF) has resumed work on building encryption by default into HTTP 2.0 after the initial surveillance reports, a project it had previously decided against in March 2012.[54]

The different forms of encryption tools proposed in Europe attempt to deliver better privacy through end-to-end encryption of mobile voice communication. The use of crypto phones can be an effective tool for protecting government and business secrets and individuals' private data. Various proposals also advocate for better end-to-end encryption of e-mail, instant messaging, cloud storage, and radio. Existing tools are often difficult and cumbersome to use, so engineers at the IETF and major US software companies are working on making encryption more easily accessible to the wider public.[55] It is possible for data encrypted from end-to-end to be accessed by intelligence or law enforcement agencies, but only through measures targeted at specific users and with much greater difficulty. While encryption enhances the protection of both data in motion and at rest, it does not necessarily protect metadata.

Different forms of encryption can be applied to various layers of the Internet while preserving its decentralized structure and strengthening the capacity of actors within the existing frameworks. Therefore, the use of encryption tools has no negative impact on the free flow of information. As long as encryption is promoted globally and encryption tools can be imported and exported without national restrictions, proposals to enhance encryption efforts can promote innovative, easier-to-use technologies. The use of encryption technologies strengthens overall Internet security, as well as individual and collective efforts for self-protection. However, encryption proposals are not without drawbacks.

First, encryption tools are generally regarded as difficult and cumbersome to use and adoption of strong encryption, though available, has been slow.[56] Second, law enforcement and counterterrorism agencies point to a tension between data privacy and national security and law enforcement.[57] Law enforcement in the United States, in particular, has argued that the expansion of encryption lends itself to the "going dark" problem and severely hinders law enforcement investigations.[58] Some have consequently advocated for a "golden key" to encrypted devices and communications, which should be provided to or stored with a third party, such as a trusted authority under the state's jurisdiction. However, such backdoors and keys stored elsewhere constitute a risk for Internet security, since they could be exploited by criminals.[59] This topic and how to approach physical and virtual security has been the subject of an emerging and important debate in the United States and the United Kingdom.[60]

## 4. CONCLUSION

Calls for technological sovereignty have not been limited to Europe. In Brazil, data localization proposals were hotly debated. In China, government offices are prohibited from using the Windows 8 operating system, and Cisco and IBM are under scrutiny.[61] The Australian government has banned China's Huawei from participating in building its National Broadband Network. And the United States has not been immune from this trend, as portrayed by Congress's creation of a cyber espionage review process in 2013 to limit government procurement of Chinese IT equipment.[62] Moreover, under "Network Security Agreements," the U.S. government legally obliges foreign communication infrastructure providers such as Deutsche Telekom to route their traffic exclusively within U.S. borders.[63]

This in-depth analysis of the European technological sovereignty proposals reveals several trends. First, it is unlikely that most technical proposals proposed to date will effectively protect data against surveillance from foreign government intelligence agencies. Only a limited number of proposals might achieve that – namely encryption – and they have not been at the center of attention in the European debate. Second, some proposals could in fact have a negative effect on the open and free Internet, or at least lead to an inefficient allocation of limited resources. Moreover, the specific impact often depends on how the proposals are implemented and remains uncertain without further research. Third, the proposals tend to be narrowly focused on the transatlantic dimension and generally neglect the larger challenge and the new technological reality. Finally, especially in the case of the expansion of encryption tools, tensions between privacy advocates, private companies, and law enforcement and national security officials emerge.

The impact of proposals often depends on the details of their implementation, which remain unknown to date. On the surface, a proposal might appear to have a positive impact but a closer look casts doubt on their effectiveness. For example, increasing funding for small businesses and establishing an "IT Security Made in Germany" brand will only increase data security if those companies produce, and are capable of producing, products and services with higher security standards than those of foreign companies. So far, the implementation of these proposals does not suggest that they offer significantly more secure services, which in some cases instead provides a false sense of security.

At first blush, restricting data from flowing through the physical infrastructure of other countries might seem like an effective measure for protecting against government surveillance. However, this is a false hope. Moreover, the laws in some countries lower the legal barrier for intelligence agencies to collect and analyze data if the data is collected outside of the intelligence agency's home country.[64] This reality means that measures forcing data to remain within a country's borders might lower the legal threshold for foreign intelligence agencies to conduct surveillance in the first place. Proposals focused on simply physically avoiding certain countries misunderstand current technological and legal realities and risk wasting important resources that could be used to effectively make data more secure.

Data privacy and security depend primarily not on where data is physically stored or sent, but on how it is stored and transmitted. A critical fact often ignored in the debate thus far is that the governments exposed by media reports since June 5, 2013 are unlikely to be the only countries with such technical surveillance capabilities. The issue is global, not Transatlantic, in nature and the challenge is the result of a new technological reality. It therefore requires a broader debate and approach. The proposals most likely to protect against any foreign surveillance focus on encryption tools. These deserve greater attention and scrutiny if the goal is to secure data more effectively.

## ACKNOWLEDGMENT

The authors would like to thank the members of the Steering Committee for the project Transatlantic Dialogues on Security and Freedom in the Digital Age (go to www.digitaldebates.org for more) as well as the participants of the workshops hosted in Washington, DC, and Berlin for their valuable input and feedback. All views, errors or omissions are solely the authors' responsibility.

## REFERENCES

[1] German Government. 2013. "Deutschlands Zukunft gestalten. Koalitionsvertrag zwischen CDU, CSU und SPD. 18. Legislaturperiode." <http://www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf;jsessionid=2820F3157BAD69B7313E63020CF9944C.s4t2?__blob=publicationFile&v=2>.

[2] A comprehensive list of proposals can be found in Annex II.

[3] Chander, Anupam and Uyen P. Le. 2014. "Breaking the Web: Data Localization vs. the Global Internet." *UC Davis Legal Studies Research Paper No. 378*; Hill, Jonah Force. 2014. "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders." *Lawfare Research Paper Series* 2, no. 3. <http://www.lawfareblog.com/wp-content/uploads/2014/07/Lawfare-Research-Paper-Series-Vol2No3.pdf>; Polatin-Reuben, Dana and Joss Wright. 2014. "An Internet with BRICS Characteristics: Data Sovereignty and the Balkansation of the Internet." *USENIX*. July 7. p. 1. <https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf>.

[4] Chander, Anupam and Uyen P. Le. 2014; Hill, Jonah Force. 2014.

[5] Chander, Anupam and Uyen P. Le. 2014. “Breaking the Web: Data Localization vs. the Global Internet.” *UC Davis Legal Studies Research Paper No. 378*; Hill, Jonah Force. 2014. “The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders.” *Lawfare Research Paper Series* 2, no. 3. <http://www.lawfareblog.com/wp-content/uploads/2014/07/Lawfare-Research-Paper-Series-Vol2No3.pdf>.

[6] Polatin-Reuben, Dana and Joss Wright. 2014. “An Internet with BRICS Characteristics: Data Sovereignty and the Balkansation of the Internet.” *USENIX*. July 7. p. 1. <https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf>.

[7] DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven: Yale University Press, p. 9.

[8] Lessig, Lawrence. 1998. “The Laws of Cyberspace.” *Presented at the Taiwan Net ’98 Conference*. p. 4.

[9] van Schewick, Barbara. 2010. *Internet Architecture and Innovation*. Cambridge: MIT Press.

[10] The Safe Harbor agreement is the process developed by the US Department of Commerce that allows US companies to more easily comply with EU Directive 95/46/EC, the initial EU Data Protection Directive from 1998. When the directive went into force in 1998, “it became clear that it actively threatened data flows between the two largest trading partners on earth.” Thus, the Safe Harbor agreement, which is unique to the US and EU, is “voluntary self-certification system for transmitting data from the EU to the United States.” For more on the Safe Harbor, see: Dowling, Jr., Donald C. 2009. “International Data Protection and Privacy Law.” *White & Case*. p. 12. <http://www.whitecase.com/files/publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/presentation/publicationattachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_intldataprotectionandprivacylaw_v5.pdf>.

[11] O’Donnell, John and Baker, Luke. 2013. “Germany, France demand ‘no-spy’ agreement with U.S.” *Reuters*. Oct. 24. <http://www.reuters.com/article/2013/10/25/us-eu-summit-idUSBRE99N0BJ20131025>.

[12] National Information Standards Organization. 2004. *Understanding Metadata*. NISO Press, p. 1-2. <http://marciazeng.slis.kent.edu/metadatabasics/types.htm>.

[13] Ibid.

[14] Zittrain, Jonathan L. 2008. *The Future of the Internet – And How to Stop It*. New Haven: Yale University Press, Chapter 4, p. 67-100.

[15] Ibid.

[16] Ibid.

[17] Ibid.

[18] European Council: The President. 2014. “Press Statement by the President of the European Council, Herman Van Rompuy, following the 7th EU-Brazil Summit.” *The European Council*. <http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/141144.pdf>.

[19] Ronnholm, Antton. 2014. “Minister Kiuru on submarine cable decision: Finland to be a safe harbor for data.” *Finnish Ministry of Transport and Communications*. Apr. 20. <http://www.lvm.fi/pressreleases/4402744/minister-kiuru-on-submarine-cable-decision-finland-to-be-a-safe-harbour-for-data>.

[20] Berke, Jürgen. 2013. “Telekom will innerdeutschen Internetverkehr ubers Ausland stoppen.” *Wirtschafts Woche*. Oct. 12. <http://www.wiwo.de/unternehmen/it/spionage-schutz-telekom-will-innerdeutschen-internetverkehr-uebers-ausland-stoppen/8919692.html>.

[21] Schäfer, Louisa. 2013. “Deutsche Telekom: ‘Internet data made in Germany should stay in Germany.’ Interview with Philipp Blank.” *Deutsche Welle*. Oct. 18. <http://www.dw.de/deutsche-telekom-internet-data-made-in-germany-should-stay-in-germany/a-17165891>.

[22] Gaugele, Von Jochen, Kade, Claudia, Malzahn, Claus Christian and Vitzthum, Thomas. 2014. “Dobrindt will mit ‘Netzallianz’ an die Weltspitze.” *Die Welt*. Jan. 12. <http://www.welt.de/politik/deutschland/article123774038/Dobrindt-will-mit-Netzallianz-an-die-Weltspitze.html>.

[23] Thombansen, Hannah. 2014. “Video-Podcast der Bundeskanzlerin #2/2014.” *Bundesregierung*. Feb. 15. <http://www.bundesregierung.de/Content/DE/Podcast/2014/2014-02-15-Video-Podcast/links/download-PDF.pdf;jsessionid=0BC9A500E8D948E37C285341160692B2.s4t1?__blob=publicationFile&v=3>.

[24] Breton, Thierry. 2013. “Atos CEO calls for ‘Schengen for data.” *Thierry Breton’s blog*. Sept. 2. <http://www.thierry-breton.com/lire-lactualite-media-41/items/atos-ceo-calls-for-schengen-for-data.html>.

[25] von Altenbockum, Jasper und Lohse, Eckart. 2014. “Verfassungsschutz-Präsident ‘Wir werden unsere Abwehr verstärken.’” *Frankfurter Allgemeine Zeitung*. July 28. <http://www.faz.net/aktuell/politik/inland/interview-mit-hans-georg-maassen-abwehr-verstaerken-13067331.html>.

[26] Deutsche Telekom. 2013. “Deutsche Telekom, WEB.DE and GMX launch ‘E-mail made in Germany’ initiative.” *Deutsche Telekom Media*. Aug. 9. <http://www.telekom.com/media/company/192834>.

[27] Iwankiewicz, Maciej W. 2013. “The Polish Approach to EU Cloud Computing Strategy.” *EuroCloud*. July 5. <http://www.eurocloud.org/the-polish-approach-to-the-eu-cloud-computing-strategy/>.

[28] Deutscher Bundestag. 2013. “Unterrichtung durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.” *German Bundestag*. Nov. 15. <http://dip21.bundestag.de/dip21/btd/18/000/1800059.pdf>.

[29] Juskailian, Russ. 2014. “For Swiss Data Industry, NSA Leaks Are Good as Gold: here’s how the Swiss promise to keep your data safe.” *Technology Review*. Mar. 18. <http://www.technologyreview.com/news/525546/for-swiss-data-industry-nsa-leaks-are-good-as-gold/>.

[30] Le Maire, Bruno. 2014. “Bruno Le Maire: Pour un Cloud europeen.” *Slate*. May 14. <http://www.slate.fr/tribune/87057/bruno-le-maire-cloud-europeen>.

[31] European Parliament. 2014. “Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens’ fundamental rights and on transatlantic cooperation in Justice and Home Affairs.” Feb. 21. <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2014-0139&language=EN>.

[32] Ward, Mark. 2014. “Can Europe go its own way on data privacy?” *BBC Technology*. Feb. 17. <http://www.bbc.com/news/technology-26228176>.

[33] Schutz, Colin. 2014. “Tech Companies Are Trying to Make NSA-Proof Encrypted Phones and Apps.” *Smithsonian Magazine*. Feb. 24. <http://www.smithsonianmag.com/smart-news/tech-companies-are-responding-nsa-revelations-encrypted-phones-and-apps-180949874/?no-ist>.

[34] Sawall, Achim. 2013. “Simko 3 zugelassen.” *Golem.de*. Sep. 9. <http://www.golem.de/news/simko-3-zugelassen-hintertueren-lassen-sich-bei-smartphones-nicht-ausschliessen-1309-101467.html>.

[35] Deutsche Telekom. 2013. “Data Privacy and Data Security: Report 2013.” *Deutsche Telekom AG*. <http://www.telekom.com/dataprotection>.

[36] Gandhe, Shreyas. 2014. “Vodafone Germany starts rolling out SIM card based encryption.” *Neowin.net*. Mar. 12. <http://www.neowin.net/news/vodafone-germany-starts-rolling-out-sim-card-based-encryption>.

[37] OECD. 2011. “Communiqué on Principles for Internet Policy-Making.” *OECD High Level Meeting, The Internet Economy: Generating Innovation and Growth*. June 29. p. 3. <http://www.oecd.org/internet/innovation/48289796.pdf>.

[38] Ibid.

[39] Khazan, O. 2013. “The Creepy, Long-Standing Practice of Undersea Cable Tapping.” *The Atlantic*. Jul. 16. <http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/>.

[40] Dowling, Jr., Donald C. 2009. “International Data Protection and Privacy Law.” *White & Case*. p. 20. <http://www.whitecase.com/files/publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/presentation/publicationattachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_intldataprotectionandprivacylaw_v5.pdf>.

[41] See, for example: Aryan, Simurgh, Homa Aryan, and J. Alex Halderman. 2013. “Internet Censorship in Iran: A First Look.” *Censorship Project*. Aug. <https://jhalderm.com/pub/papers/iran-foci13.pdf>; and Roberts, Hal, David Larochelle, Rob Faris, and John Palfrey. 2011. “Mapping Local Internet Control.” *Berkman Center for Internet & Society at Harvard University*. May 13. <http://cyber.law.harvard.edu/netmaps/mlic_20110513.pdf>.

[42] Public Intelligence. 2013. “U.S. Government Foreign Telecommunications Providers Network Security Agreements”. <https://publicintelligence.net/us-nsas/>. July 9, 2013>. See also NSA with Deutsche Telekom. <https://info.publicintelligence.net/US-NSAs/US-NSAs-Voicestream.pdf>.

[43] Deutsche Telekom. 2014. <http://www.telekom.com/medien/produkte-fuer-privatkunden/220370>.

[44] Dierks, T. and E. Rescorla. 2008. “The Transport Layer Security (TLS) Protocol Version 1.2.” *Internet Engineering Task Force Network Working Group*. <http://tools.ietf.org/html/rfc5246>.

[45] Emert, M. 2014. “RIPE diskutiert bedenkliche Entwicklungen: Das Google-Net und EmiG”. 19 May. < http://www.heise.de/netze/meldung/RIPE-diskutiert-bedenkliche-Entwicklungen-Das-Google-Net-und-EmiG-2192176.html>.

[46] Dowling, Jr., Donald C. 2009. “International Data Protection and Privacy Law.” *White & Case*. p. 20. <http://www.whitecase.com/files/publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/presentation/publicationattachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_intldataprotectionandprivacylaw_v5.pdf>.

[47] Bob Butler, Irving Lachow, Jonah Force Hill. 2014. “Cloud computing under siege.” *Few.com*. Sept. 12. <http://fcw.com/articles/2014/09/12/cloud-under-siege.aspx>.

[48] Plaum, Alexander. 2014. “The impact of forced data localisation on fundamental rights.” *Access Now*. April 4.. <https://www.accessnow.org/blog/2014/06/04/the-impact-of-forced-data-localisation-on-fundamental-rights>.

49] European Commission. 2014. “Cloud Service Level Agreement Standardisation Guidelines”. <https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines>.

[50] European Cloud Partnership Steering Board. 2014. “Establishing a Trusted European Cloud.” <http://www.kowi.de/Portaldata/2/Resources/horizon2020/coop/Report-Establishing-trusted-cloud-Europe.pdf>.

[51] Waidner, Michael. 2014. "Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 26. Juni 2014." June 26. <https://www.bundestag.de/blob/285122/2f815a7598a9a7e9b4162d70173ecedb/mat_a_sv-1-2-pdf-data.pdf>.

[52] European Parliament. 2014. "Motion for a European Parliament Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs." *European Parliament*. Feb. 21. Paragraph 95. <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2014-0139&language=EN>.

[53] Vance Jr., Cyrus R. 2014. "Apple and Google threaten public safety with default smartphone encryption." *The Washington Post*. Sept. 26. <http://www.washingtonpost.com/opinions/apple-and-google-threaten-public-safety-with-default-smartphone-encryption/2014/09/25/43af9bf0-44ab-11e4-b437-1a7368204804_story.html>.

[54] Jackson Higgins, Kelly. 2013. "NSA Leaks Bolster IETF Work On Internet Security." *DarkReading*. Nov. 14. <http://www.darkreading.com/risk/nsa-leaks-bolster-ietf-work-on-internet-security/d/d-id/1140891>.

[55] Protalinski, Emil. 2014. "Gmail now always uses an HTTPS connection and encrypts all messages moving internally on Google's servers." *The Next Web*. Mar. 20. <http://thenextweb.com/google/2014/03/20/gmail-now-uses-encrypted-https-connection-check-send-email/>; Armasu, Lucian. 2014. "Huge: Cloudflare's Free SSL Service Brings Encrypted-By-Default Web Closer Than Ever." *Tom`s Hardware*. Sept. 29. <http://www.tomshardware.com/news/cloudflare-security-encryption-ssl-https,27780.html>; Perey, Juan Carlos. 2014. "Microsoft makes email encryption for Office 365 easier." *Tech Central.ie*. Oct. 6. <http://www.techcentral.ie/microsoft-makes-email-encryption-office-365-easier/#ixzz3Ix0eOXHl>; O'Neill, Patrick Howell. 2014. "Tor executive director hints at Firefox integration." *The Daily Dot*. Sept. 29. <http://www.dailydot.com/politics/tor-mozilla-firefox/>; Meyer, David. 2014. "Pretty Easy Privacy project aims to make encryption easier for regular people to use." *Gigaom*. Oct. 6. <https://gigaom.com/2014/10/06/pretty-easy-privacy-project-aims-to-make-encryption-easier-for-regular-people-to-use/>.

[56] For a broader discussion of the usability of encryption, see: Lee, Timothy B. 2013. "NSA-proof encryption exists. Why doesn't anyone use it?" Washington Post. June 14. <http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/14/nsa-proof-encryption-exists-why-doesnt-anyone-use-it/>.

[57] For more on this debate in the UK, see: Price, Rob. 2015. "David Cameron Wants to Ban Encryption." *Business Insider*. Jan. 12. <http://www.businessinsider.com/david-cameron-encryption-apple-pgp-2015-1>.

[58] FBI Director James Comey has been particularly outspoken on this issue. For more, see: Brookings Institution. 2014. "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" *Brookings Institution*. Oct. 16. <http://www.brookings.edu/events/2014/10/16-going-dark-technology-privacy-comey-fbi>.

[59] Schneier, Bruce. 2014. "Stop the hysteria over Apple encryption." *CNN*. Oct. 31. <http://edition.cnn.com/2014/10/03/opinion/schneier-apple-encryption-hysteria/>.

[60] The Brookings Institution. 2014. "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" *The Brookings Institution*. Oct. 16. <http://www.brookings.edu/events/2014/10/16-going-dark-technology-privacy-comey-fbi>; Street, Jon. 2014. "Eric Holder: Apple, Google Not Giving Law Enforcement Access to Encrypted Data Is 'Worrisome.'" *The Blaze*. Oct. 1. <http://www.theblaze.com/stories/2014/10/01/ eric-holder-apple-google-not-giving-law-enforcement-access-to-encrypted-data-is-worrisome/>; Hosko, Ronald T. 2014. "Apple and Google's new encryption rules will make law enforcement's job much harder." *The Washington Post*. Sept. 23. <http://www.washingtonpost.com/posteverything/wp/2014/09/23/i-helped-save-a-kidnapped-man-from-murder-with-apples-new-encryption-rules-we-never-wouldve-found-him/>.

[61] Tiezzi, Shannon. 2014. "In Cyber Dispute With US, China Targets IBM, Cisco." *The Diplomat*. May 28. <http://thediplomat.com/2014/05/in-cyber-dispute-with-us-china-targets-ibm-cisco/>.

[62] Rogers, Mike and Dutch Ruppersberger. 2012. *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*. Permanent Select Committee on Intelligence. Oct. 8. <https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf>.

[63] Public Intelligence. 2013. "U.S. Government Foreign Telecommunications Providers Network Security Agreements". <https://publicintelligence.net/us-nsas/>. July 9, 2013>. See also NSA with Deutsche Telekom. <https://info.publicintelligence.net/US-NSAs/US-NSAs-Voicestream.pdf>.

[64] Willis, Aidan. 2010. "Guidebook: Understanding Intelligence Oversight." *Geneva Centre for the Democratic Control of Armed Forces (DCAF)*. <http://www.dcaf.ch/Publications/Guidebook-Understanding-Intelligence-Oversight>.

**Publication VI**

Skierka, Isabel. (2021). Messung, Prüfung und Nachweis von IT-Sicherheit [IT security measurement, evaluation, and proof]. In Gerrit Hornung & Martin Schallbruch (Eds.), *Handbuch IT-Sicherheitsrecht* [Handbook IT Security Law] (pp. 154−180). Nomos Verlag. (3.1).

## § 8 Messung, Prüfung und Nachweis von IT-Sicherheit

**Literatur:** *Aizuddin*, The Common Criteria ISO/IEC 15408 – The Insight, Some Thoughts, Questions and Issues. SANS Institute, 2001, abrufbar unter https://www.sans.org/reading-room/whitepapers/standards/paper/545; *Baldini/Giannopoulos*, Analysis and Recommendations for a European certification and labelling framework for cybersecurity in Europe. Luxembourg: European Commission Joint Research Centre, 2017; *Bartels/Backer/Schramm*, Der „Stand der Technik“ im IT-Sicherheitsrecht. Bundesamt für Sicherheit in der Informationstechnik, 2017; *BITKOM,* Kompass der IT-Sicherheitsstandards Leitfaden und Nachschlagewerk, abrufbar unter https://www.kompass-sicherheitsstandards.de/, 2013; *Bundesamt für Sicherheit in der Informationstechnik*, Hinweise für Antragsteller für die IT-Sicherheitszertifizierung von Produkten, Schutzprofilen und Standorten; *Bundesamt für Sicherheit in der Informationstechnik*, German eID based on Extended Access Control v2 – LoA mapping: Mapping of the characteristics of the German eID scheme to the eIDAS Level of Assurance, 2017; *Bundesamt für Sicherheit in der Informationstechnik*, Anforderungen an Antragsteller zur Anerkennung als Prüfstelle im Bereich Common Criteria, Version 1.2, [VB-CC-Prüfstellen], 2018; *Bundesamt für Sicherheit in der Informationstechnik*, Verfahrensbeschreibung zur Zertifizierung von Auditoren, Version 1.0, [VB- Auditoren], 2019; *Bundesamt für Sicherheit in der Informationstechnik*, Verfahrensbeschreibung Kompetenzfeststellung und Zertifizierung von Personen, Version 3.0, [VB-Personen], 2019; *Bundesamt für Sicherheit in der Informationstechnik,* Verfahrensbeschreibung Anerkennung von Prüfstellen und Zertifizierung von IT-Sicherheitsdienstleistern, Version 3.4, [VB-Stellen], 2019; *Bundesamt für Sicherheit in der Informationstechnik*, Verfahrensbeschreibung zur Anerkennung von Prüfstellen und Zertifizierung von IT-Sicherheitsdienstleistern, Version 3.4, [VB-Stellen], 2019; *Bundesamt für Sicherheit in der Informationstechnik*, Zertifizierungsschema nach ISO 27001 auf der Basis von IT-Grundschutz, Version 2.1, 2019; *Bundesamt für Sicherheit in der Informationstechnik,* IT-Grundschutz Standards, 20.1.2020, abrufbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html; *Bundesamt für Sicherheit in der Informationstechnik*, Fragen und Antworten zum Inkrafttreten des IT-Sicherheitsgesetzes, abrufbar unter https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/FAQ/FAQ_IT_SiG/faq_it_sig_node.html#faq6636766; *Bundesamt für Sicherheit in der Informationstechnik*, Schutzprofile im Kontext elektronische Ausweise, abrufbar unter https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/ElektronischeIdentitaeten/Schutzprofile/schutzprofile_node.html; *Bundesamt für Sicherheit in der Informationstechnik*, Übersicht der Schutzprofile und der Technische Richtlinien für "eHealth VSDM“, abrufbar unter https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eHealth/Schutzprofile_TR/schutzprofile_tr_node.html; *Bundesamt für Sicherheit in der Informationstechnik*, Übersicht über die Schutzprofile und Technischen Richtlinien nach § 22 Abs. 2 Satz 1 MsbG, abrufbar unter https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/UebersichtSP-TR/uebersicht_no; *Bundesamt für Sicherheit in der Informationstechnik*, Verzeichnisse – als Nachschlagewerk für Interessenten und Beteiligte an Zertifizierungs- und Anerkennungsverfahren, Version 2.1; *Bundesministerium des Innern, für Bau und Heimat*, Handreichung zum Erlass an das Beschaffungsamt des BMI (BeschA) (Erlass vom 30.4.2014, O4–11032/23#14); *CIO der Bundesregierung*, Handreichung zur „technischen no-spy-Klausel, 1.2.2018, abrufbar unter https://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Beschaffung/evb_it_handreichung_z_techn_no_spy_klausel_download.pdf?__blob=publicationFile; *Deutsche Akkreditierungsstelle GmbH*, Akkreditierungsurkunde D-ZE-19615–01–00 nach DIN EN ISO/IEC 17065:2013, 2019; *Ernsthaler/Strübbe/Bock*, Zertifizierung und Akkreditierung technischer Produkte, 2017; *European Commission*, Commission Staff Working Document Impact Assessment, Accompanying the document Proposal for a Regulation of the European Parliament and of the Coucil of ENISA, the "EU Cybersecurity Agency“; *European Union Agency for Cybersecurity,* ENISA Baseline Security Recommendations for IoT, 2018; *Hänninen/Hansson/Thane/ Saadatmand,* Inadequate Risk Analysis Might Jeopardize The Functional Safety of Modern Systems, 2016; *Hasso-Plattner-Institut*, Studie zur Messbarkeit von Sicherheit in SOA. Bundesamt für Sicherheit in der Informationstechnik, 2010; *Hofmann*, Dynamische Zertifizierung – Datenschutzrechtliche Zertifizierung nach der Datenschutz-Grundverordnung am Beispiel des Cloud Computings. 2019; *International Society of Automation*, ISA99, Industrial Automation and Control Systems Security, abrufbar unter https://www.isa.org/isa99/; *IoT Security Foundation*, Security Compliance Framework, 2016; *Kersten/Klett/Reuter/Schröder*, IT-Sicherheitsmanagement nach der neuen ISO 27001, 2020; *Kleinhans*, IT-Sichehreit im Internet der Dinge. Stiftung Neue Verantwortung, 2016; *Krcmar/Eckert/Roßnagel/Sunyaev/Wiesche*, Management sicherer Cloud-Services: Entwicklung und Evaluation dynamischer Zertifikate, 2018; *Kriaa*, Joint Safety and Security Modeling for Risk Assessment in Cyber Physical Systems, 2016; *Leverett/Clayton/Ander-*

*son*, Standardisation and certification in the 'Internet of Things'. 16th Annual Workshop on the Economics of Information Security (WEIS), 2017; *National Institute of Standards and Technology NIST*, Special Publication 800–30, Revision 1, Guide For Conducting Risk Assessments, 2012; *National Institute of Standards and Technology NIST*, Special Publication 800–160 – Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, 2018; *Raabe/Schallbruch/Steinbrück*, Empfehlungen zur Systematisiernug des IT-Sicherheitsrechts, 2018; *Rannenberg,* Zertifizierung mehrseitiger IT-Sicherheit: Kriterien und organisatorische Rahmenbedingungen, 1998; *Refsdal/Solhaug/Stolen*, Cyber-Risk Management, 2015; *Röhl/Schreiber*, Konformitätsbewertung in Deutschland, 2006; *TeleTrusT Bundesverband IT-Sicherheit e.V.*, Handreichung zum Stand der Technik in der IT-Sicherheit, 2020; *TÜViT*, Whitepaper Industiral Security based on IEC 62443, Version 1.0, abrufbar unter https://www.tuvit.de/fileadmin/Content/TUV_IT/pdf/Downloads/WhitePaper/whitepaper-iec-62443.pdf; *Voigt*, IT-Sicherheitsgesetz 2.0 – Referentenentwurf von März 2019, 11.4.2019, abrufbar unter https://www.cr-online.de/blog/2019/04/11/it-sicherheitsgesetz-2-0-referentenentwurf-von-maerz-2019/; *Zentralverband Elektrotechnik- und Elektronikindustrie ZVEI*, Orientierungsleitfaden für Hersteller zur IEC 62443, 2017, abrufbar unter https://www.zvei.org/presse-medien/publikationen/orientierungsleitfaden-fuer-hersteller-zur-iec-62443/.

## A. Einleitung

Moderne Gesellschaften sind mittlerweile fast vollständig von funktionsfähigen Informations- und Kommunikationstechnologien (IKT) abhängig. Daraus ergibt sich eine zunehmende Anzahl von Anforderungen an die IT-Sicherheit von Komponenten, Systemen und Prozessen, die in die Steuerung alltäglicher und kritischer Prozesse involviert sind. Betreiber Kritischer Infrastrukturen, Anbieter von Online-Diensten, Verarbeiter personenbezogener Daten und zunehmend auch Hersteller von Informations- und Kommunikationstechnologien (IKT) unterliegen einer wachsenden Anzahl von gesetzlichen Verpflichtungen zur Gewährleistung von IT-Sicherheit. Im Sinne der **Legaldefinition** aus § 2 Abs. 2 BSIG bedeutet **IT-Sicherheit** „die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen 1

1. in informationstechnischen Systemen, Komponenten oder Prozessen oder
2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen."

2 Das **IT-Sicherheitsrecht** umfasst dementsprechend alle rechtlichen „Anforderungen an die IT-Sicherheit von Systemen, Diensten und Produkten und diejenigen, die sie herstellen, vertreiben und benutzen".[1]

3 Um die **Umsetzung und Effektivität** der Maßnahmen zu kontrollieren, erfordern die meisten Gesetze Bewertungen und Prüfungen von IT-Sicherheit, sowie Nachweise darüber, beispielsweise in Form von Zertifikaten. Sowohl das allgemeine IT-Sicherheitsrecht, wie beispielsweise das BSI-Gesetz, die Datenschutz-Grundverordnung[2] oder die Verordnung über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik[3] der EU, wie auch das fachspezifische IT-Sicherheitsrecht, beispielsweise im Bereich des Messwesens (§ 22 MsbG)[4] oder des Gesundheitswesens (§ 291 b SGB V), umfassen Vorschriften für Betreiber, Anbieter und Hersteller zu Prüfungen und Nachweisen von IT-Sicherheit.

4 Ziel dieses Kapitels ist es, Verfahren zur Messung, Prüfung und dem Nachweis von IT-Sicherheit zur Erfüllung von rechtlichen Anforderungen zu erläutern. Der erste Abschnitt gibt einen Überblick über Prüf-, Bewertungs- und Nachweisverfahren, sowie rechtliche Grundlagen und Zuständigkeiten im IT-Sicherheitsrecht. Anschließend unterscheidet das Kapitel systematisch zwischen unterschiedlichen Prüf- und Bewertungsebenen bzw. -gegenständen im Sinne der Sicherheit von IT-Systemen in Institutionen und der IT-Sicherheit von Software und Hardware.

5 Der zweite Abschnitt erläutert die Messung, Prüfung und den Nachweis von IT-Sicherheit in Institutionen. Er fasst die einschlägigen Standards für Systeme zum Management von Informationssicherheit zusammen, benennt Methoden zur Messung von IT-Sicherheit innerhalb von Risikoanalysen und erläutert Audits und Zertifizierungen. Der letzte Teil dieses Abschnitts zeigt, in welchen Bereichen des IT-Sicherheitsrechts diese Methoden verlangt werden.

6 Der dritte Abschnitt widmet sich der Messung, Prüfung und dem Nachweis von IT-Sicherheit von Software und Hardware, einschließlich IT-Produkten, -Diensten und -Prozessen. Er bietet eine Übersicht über Kriterien zur Messung, Evaluation und Prüfung von Software und Hardware und über Zertifizierungsverfahren. Darauf aufbauend erläutert der Abschnitt, wie diese Verfahren bei der Prüfung und Zertifizierung von IT-Produkten, -Diensten und -Prozessen im allgemeinen und fachspezifischen IT-Sicherheitsrecht zum Einsatz kommen.

7 Ein kurzer abschließender Abschnitt zeigt die Grenzen der bestehenden Ansätze und zukünftige Herausforderungen auf.

## B. Grundlagen der Prüfung und Bewertung von IT-Sicherheit

8 IT-Sicherheitsanforderungen können sich auf IT-Systeme, Managementprozesse und Personen innerhalb einer Institution beziehen oder auf die Software und Hardware von IT-Komponen-

[1] Raabe/Schallbruch/Steinbrück, 2018, S. 7.

[2] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DSGVO), ABl. Nr. L 119/1.

[3] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17.4.2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit).

[4] Dazu näher Singler in → § 24 Rn. 1 ff. in → § 24 Rn. 1 ff.

ten und -Produkten. Dementsprechend unterscheiden sich auch die Verfahren zur Messung, Bewertung und Prüfung von IT-Sicherheit je nach **Prüf- bzw. Bewertungsgegenstand**.

Die meisten gesetzlichen Vorschriften zur Gewährleistung von IT-Sicherheit durch technische und/oder organisatorische Maßnahmen enthalten sich konkreter technischer Vorgaben und Kriterien zur **Ausgestaltung** der allgemeinen Anforderungen. Indes verweisen viele Gesetze, wie beispielsweise § 8 a Abs. 1 und § 8 c Abs. 2 BSIG, Art. 32 DSGVO, § 13 Abs. 7 TMG, § 291 b Abs. 1 SGB V, auf den **„Stand der Technik".** Grund dafür ist, dass sich Technologien und Bedrohungslage sehr viel dynamischer verändern als die rechtlichen Regeln diese Entwicklungen abbilden können. 9

Der **„Stand der Technik"** ist zwischen dem innovativeren Technologiestand „Stand der Wissenschaft und Forschung" und dem bewährten Technologiestand „allgemein anerkannte Regeln der Technik" angesiedelt.[5] Er umfasst die „verfügbaren Verfahren, Einrichtungen oder Betriebsweisen, deren Anwendung die Erreichung der jeweiligen gesetzlichen Schutzziele am wirkungsvollsten gewährleisten kann".[6] Jedoch ist er nie eindeutig definiert. Das für IT-Sicherheit in Deutschland zuständige Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt fest, dass es nicht möglich sei, den „Stand der Technik" allgemeingültig und abschließend zu beschreiben. Er lasse sich jedoch „anhand existierender nationaler oder internationaler Standards und Normen von beispielsweise DIN, ISO, DKE oder ISO/IEC oder anhand erfolgreich in der Praxis erprobter Vorbilder für den jeweiligen Bereich ermitteln".[7] Einige Gesetze verweisen auch auf konkrete Standards, Normen oder technische Richtlinien, oder geben Betroffenen die Möglichkeit, Standards selbst zu bestimmen. Die Betreiber Kritischer Infrastrukturen und ihre Branchenverbände beispielsweise haben zur Bestimmung des „Standes der Technik" nach § 8 a Abs. 2 BSIG die Möglichkeit, branchenspezifische Standards zu erarbeiten. Bis zu einem gewissen Grad ist eine subjektive Bewertung des Standes der Technik jedoch nicht vermeidbar. Auch die darauf aufbauenden Sicherheitsmaßnahmen müssen individuellen Schutzanforderungen und dem Risikoumfeld entsprechen.[8] 10

Weltweit existieren zahlreiche **Standards und Normen**, welche Sicherheitsanforderungen an IT-Produkte und -Systeme über Entwicklungsverfahren bis hin zu Managementprozessen auf Organisationsebene definieren. Sie liefern Methoden für ein leistungsfähiges IT-Sicherheitsmanagement oder definieren die IT-Sicherheit von ausgewiesenen Produkten.[9] Außerdem dienen sie als Prüf- und Bewertungsgrundlage für IT-Sicherheit. 11

In den Grundzügen folgen Verfahren zur Bewertung, Prüfung und zum Nachweis von IT-Sicherheit einem System der **Konformitätsbewertung**, welches auch in anderen Bereichen der Produktsicherheit oder des Qualitätsmanagements eingesetzt wird – insbesondere im Rahmen der EU-Richtlinien des „New Legislative Framework" (NLF). Die NLF-Richtlinien legen grundlegende Anforderungen an die Sicherheit und Leistungsfähigkeit von bestimmten Produktgruppen wie Maschinen, Spielzeugen, elektrischen Betriebsmitteln, Medizinprodukten oder Bauprodukten fest. Gemäß der Definition aus der Norm DIN EN ISO/IEC 17000:2004 dient eine Konformitätsbewertung der „Darlegung, dass festgelegte Anforderungen bezogen auf ein Produkt, einen Prozess, ein System, eine Person oder eine Stelle erfüllt sind"[10]. Diese 12

[5] TeleTrusT, 2020, S. 11. In der Rechtswissenschaft ist diese Unterscheidung weithin üblich, seit das BVerfG sie in der grundlegenden Kalkar-Entscheidung vom 8.8.1978 verwendet hat, s. BVerfGE 47, 89 (135 ff.); näher zB Seibel NJW 2013, 3000.

[6] Bartels/Backer/Schramm, 2017, S. 503.

[7] Bundesamt für Sicherheit in der Informationstechnik, „Fragen und Antworten zum Inkrafttreten des IT-Sicherheitsgesetzes", abrufbar unter https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/FAQ/FAQ_IT_SiG/faq_it_sig_node.html#faq6636766.

[8] Raabe/Schallbruch/Steinbrück, 2018, S. 10 f.

[9] Für eine Übersicht vgl. Bitkom/DIN, 2013, S. 5 ff.

[10] DIN EN ISO/IEC 17000:2004 – Konformitätsbewertung – Allgemeine Begriffe und Grundlagen.

Anforderungen können sich aus gesetzlichen Regelungen ergeben, aus vertraglichen Vereinbarungen zwischen Hersteller und seinen Zulieferern bzw. Anwendern und Herstellern, oder auch aus Verbraucher- bzw. Anwendererwartungen. Sie umfasst die Ermittlung und Messung bestimmter Eigenschaften sowie die Bewertung und Bestätigung der Einhaltung vorgegebener Anforderungen.[11]

13 Bewertungen und Prüfungen können von unterschiedlichen Parteien vorgenommen werden:[12]

- durch eine „erste Seite“: eine Person oder Organisation, die den Prüfgegenstand (beispielsweise ein Produkt oder eine Dienstleistung) herstellt, anbietet oder, wie im Fall eines internen Betriebsprozesses, durchführt. Meist reicht als Nachweis eine (Eigen-)Erklärung des Herstellers bzw. des Anbieters oder Betreibers aus.
- durch eine „zweite Seite“: eine Person oder Organisation, die als Anwender ein Interesse an dem Produkt haben könnte, zum Beispiel ein Kunde.
- durch eine „dritte Seite“: eine von beiden Seiten unabhängige „Konformitätsbewertungsstelle.

14 **Konformitätsbewertungsstellen** können unter anderem Laboratorien, Inspektionsstellen und Zertifizierungsstellen (für Personen, für Managementsysteme oder für Produkte, Prozesse und Dienstleistungen) sein. Die Qualität und Kompetenz von Konformitätsbewertungsstellen wiederum werden im Rahmen einer formalen **Akkreditierung** durch eine unabhängige Stelle bestätigt.[13] Sie kann nur durch spezifische Akkreditierungsstellen auf Landes- oder Bundesebene vergeben werden.[14]

15 Eine oft eingesetzte Form der Konformitätsbewertung ist die **Zertifizierung** oder die „Maßnahme durch einen unparteiischen Dritten, die aufzeigt, dass ein angemessenes Vertrauen besteht, dass ein ordnungsgemäß bezeichnetes Erzeugnis, Verfahren oder eine ordnungsgemäß bezeichnete Dienstleistung in Übereinstimmung mit einer bestimmten Norm oder einem bestimmten anderen normativen Dokument ist.“[15]

16 Eine am Ende des Prüfverfahrens ausgestellte **Konformitätserklärung** des Betreibers, Anbieters oder Herstellers oder das **Zertifikat** einer Zertifizierungsstelle dienen als **Nachweis**, dass ein Produkt, eine Dienstleistung, ein System, eine Person oder eine Organisation zu definierten Kriterien und Anforderungen konform ist. Ein Nachweis, insbesondere ein allgemein anerkanntes Zertifikat, kann Vertrauen in die Sicherheit und/oder Qualität von Produkten, Dienstleistungen oder Personen schaffen, die Verbraucherakzeptanz fördern und den Marktzugang erleichtern. Zudem kann er gegenüber dem Gesetzgeber die Erfüllung gesetzlicher Anforderungen oder gegenüber Versicherungen und Kapitalgebern angemessene Vorkehrungen zur Kontrolle von Sicherheitsrisiken bestätigen.[16]

17 Im Bereich der IT-Sicherheit ist in Deutschland gemäß § 3 Abs. 1 Satz 4–6 BSIG das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** die zentrale zuständige Behörde für

- die Entwicklung von Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit von IT-Systemen oder Komponenten,
- die Erteilung von Sicherheitszertifikaten,

[11] Ensthaler/Strübbe/Bock, 2007, S. 7.

[12] Vgl. Röhl/Schreiber, 2006, S. 6 f.

[13] DIN EN ISO/IEC 17011:2018–03 — Konformitätsbewertung — Anforderungen an Akkreditierungsstellen, die Konformitätsbewertungsstellen akkreditieren.

[14] Die Anforderungen, welche die Konformitätsbewertungsstellen für eine Akkreditierung erfüllen müssen, sind in der DIN EN ISO/IEC 17000er-Normenreihe erläutert.

[15] DIN EN ISO/IEC 17000:2004 – Konformitätsbewertung – Allgemeine Begriffe und Grundlagen.

[16] Ensthaler/Strübbe/Bock, 2007, S. 191 ff.

- die Prüfung und Bewertung der Konformität im Bereich der IT-Sicherheit, einschließlich der Prüfung und Bestätigung der Konformität von IT-Systemen und Komponenten mit technischen Richtlinien des Bundesamtes,
- die Prüfung, Bewertung und Zulassung von IT-Systemen oder Komponenten, die für die Verarbeitung amtlich geheim gehaltener Informationen nach § 4 des Sicherheitsüberprüfungsgesetzes eingesetzt werden sollen.

Die **Zertifizierung** ist eine der Hauptaufgaben des BSI. Eine Zertifizierung im Verantwortungsbereich des BSI kann laut § 2 Abs. 7 BSIG vorgenommen werden, um festzustellen, dass ein Produkt, ein System, ein Schutzprofil (Sicherheitszertifizierung), eine Person (Personenzertifizierung) oder ein IT-Sicherheitsdienstleister bestimmte Anforderungen erfüllt. Die Kompetenzen des Bundesamtes im Bereich der Zertifizierung regelt § 9 BSIG. Nach § 9 Abs. 2 BSIG kann das BSI für bestimmte Produkte oder Leistungen eine Sicherheits- oder Personenzertifizierung oder eine Zertifizierung für IT-Sicherheitsdienstleister ausstellen. Außerdem ist das BSI nach § 9 Abs. 1 BSIG die nationale Zertifizierungsstelle der Bundesverwaltung für IT-Sicherheit. 18

Die Prüfung und Bewertung können gemäß § 9 Abs. 3 BSIG entweder durch das BSI selbst oder eine anerkannte sachverständige Stelle erfolgen. **Prüfungen** werden in Form von Audits und/oder Zertifizierungen durchgeführt. **Audits** sind Untersuchungsverfahren, die meist im Rahmen eines Qualitätsmanagements erfolgen. Ein **Zertifikat** wird nach § 9 Abs. 4 Nr. 1 BSIG dann erteilt, wenn IT-Systeme, Komponenten, Produkte oder Schutzprofile den vom BSI festgelegten Kriterien entsprechen. Eine Bedingung für Zertifizierungen ist zudem gemäß § 9 Abs. 4 Nr. 2 BSIG immer, dass keine überwiegenden öffentlichen Interessen, insbesondere sicherheitspolitische Belange, dieser Erteilung entgegenstehen. 19

Nach § 9 Abs. 6 BSIG verantwortet das BSI die **Anerkennung bzw. Akkreditierung von Prüfstellen** und die Zertifizierung als IT-Sicherheitsdienstleister. Voraussetzung für die Anerkennung als Prüfstelle ist die Umsetzung und Aufrechterhaltung der Norm DIN EN ISO/IEC 17025:2018 „Allgemeine Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien“ für den entsprechenden Geltungsbereich. Ziel der Anerkennung ist die Sicherstellung der Fachkompetenz, Qualität und Vergleichbarkeit der Konzepte, Vorgehensweisen und Arbeitsergebnisse der Stellen.[17] Zudem kann das BSI **IT-Sicherheitsdienstleister** zertifizieren, welche beispielsweise Audits durchführen.[18] Das BSI selbst ist von der Deutschen Akkreditierungsstelle (DAkkS) nach DIN EN ISO/IEC 17065 als **Zertifizierungsstelle** für IT-Produkte (Software und Hardware) akkreditiert.[19] 20

Außerdem führt das BSI im Bereich der Konformitätsbewertung **Zertifizierungen von Personen** durch. Das BSI kann im Rahmen eines Verfahrens zur Kompetenzfeststellung Mitarbeiter, die bei anerkannten Prüfstellen und zertifizierten IT-Sicherheitsdienstleistern beschäftigt sind, prüfen. Diese Prüfung erfolgt jedoch im Rahmen des Verfahrens zur **Anerkennung von Prüfstellen** und **Zertifizierungen von IT-Sicherheitsdienstleistern**. Außerdem können sich natürliche Personen vom BSI auf Grundlage des BSI-Gesetzes zertifizieren lassen. Im Rahmen des Verfahrens müssen sie ihre Fachkompetenz nachweisen. Das BSI stellt entsprechende Informationen in Verfahrensbeschreibungen zur Verfügung.[20] 21

[17] Das Verfahren zur Anerkennung von Prüfstellen ist in dem Dokument „[VB-Stellen] Verfahrensbeschreibung zur Anerkennung von Prüfstellen und Zertifizierung von IT-Sicherheitsdienstleistern“ des BSI beschrieben. Prozessbezogene Anforderungen für die Evaluierung durch Stellen sind in dem Dokument „Anforderungen an Antragsteller zur Anerkennung als Prüfstelle im Bereich Common Criteria“ des BSI dargelegt.

[18] Vgl. BSI, 2019, [VB-Stellen].

[19] Deutsche Akkreditierungsstelle, 2019, „Akkreditierungsurkunde D-ZE-19615–01–00“.

[20] BSI, 2019, „[VB-Personen] Verfahrensbeschreibung Kompetenzfeststellung und Zertifizierung von Personen, Version 3.0“; BSI, 2019, „[VB-Auditoren] Verfahrensbeschreibung zur Zertifizierung von Auditoren, Version 1.0“.

22 Generell ist die Bestätigung von Konformität mit Normen und Standards jedoch nicht gleichzusetzen mit **tatsächlicher Sicherheit oder Qualität**. Eine Konformitätsbestätigung einschließlich eines Zertifikats trifft lediglich eine Aussage darüber, wie gut ein Produkt, eine Dienstleistung, ein System, oder eine Organisation die als relevant definierten Sicherheitsanforderungen erfüllen, jedoch nicht darüber, wie sicher sie de facto sind.

## C. IT-Sicherheit in Institutionen

23 Da die in Organisationen eingesetzten IKT-Einrichtungen typischerweise immer auch technische Schwachstellen enthalten, reichen rein technische Maßnahmen zur Absicherung von Systemen bzw. der Einsatz von zertifizierten IT-Produkten und Systemen nicht aus. Die Gewährleistung von IT-Sicherheit in Organisationen erfordert einen Ansatz, welcher sowohl **technische, organisatorische als auch personelle Maßnahmen** zum Management der betrieblichen IT-Sicherheit zusammenfasst. Dafür wird meistens ein **Informationssicherheitsmanagementsystems** (**ISMS**) angewendet.[21]

### I. Grundlegende Standards und Normen

24 Für die Planung und Umsetzung eines ISMS existieren mehrere Standards und Normen, welche als Grundlage für den „Stand der Technik“ herangezogen werden können. Die ISO/IEC-27000er-Normenreihe bildet den Kern für den Aufbau der meisten ISMS und ist in der Anwendung am weitesten verbreitet. Auf ihr basiert auch der in Deutschland und einigen anderen Ländern gennutzte IT-Grundschutz des BSI.

#### 1. ISO/IEC 27000er Normenreihe und IT-Grundschutz

25 Laut der **ISO/IEC 27000er-Reihe** ist ein ISMS „ein systematischer Ansatz für die Einrichtung, Implementierung, den Betrieb, die Überwachung, die Überprüfung, die Wartung und die Verbesserung der Informationssicherheit einer Organisation, um die Geschäftsziele zu erreichen“[22]. Ein ISMS umfasst die Planung, Steuerung und Kontrolle von Sicherheitsmaßnahmen, die Erstellung eines Sicherheitskonzepts, die Festlegung von Verantwortlichkeiten und die Analyse von Bedrohungspotenzialen, Schwachstellen und Risiken.[23] Es bezieht sich auf IT-Systeme, Prozesse, sowie Personen und ist sektorübergreifend anwendbar. Innerhalb der Reihe ist die Norm ISO/IEC 27001 die grundlegendste. Sie definiert die Anforderungen an ein ISMS. Andere Normen der Reihe beschreiben konkretere Empfehlungen für Kontrollmechanismen (ISO/IEC 27002), einen Leitfaden zur Umsetzung der ISO 27001 (ISO/IEC 27003), die Bewertung der Effektivität des ISMS (ISO/IEC 27004), ein Risikomanagementsystem (ISO/IEC 27005), oder das Security Incident Management (Vorfalls- und Notfallmanagement) (ISO/IEC 27035). Die Normenreihe beschreibt ebenfalls Anforderungen an branchenspezifische Anwendungen, wie die von Telekommunikationsanbietern (ISO/IEC 27011), Cloud-Computing-Dienste (ISO/IEC 27017) oder an Energieversorgungsunternehmen (ISO/IEC TR 27019). Eine Zertifizierung ist nur nach der ISO 27001 möglich, wobei die anderen Normen der Reihe als Ergänzung hinzugezogen werden können.

26 Auf der ISO 27000er-Normenreihe basiert auch der **IT-Grundschutz** des BSI, welcher in den BSI-Standards 200–1, 200–2, 200–3 und 100–4 festgehalten ist.[24] Der IT-Grundschutz ermög-

[21] TeleTrusT, 2020, S. 60.

[22] DIN EN ISO/IEC 27000:2017–10 – Informationstechnik – Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie.

[23] Hasso-Plattner-Institut, 2010, S. 16.

[24] BSI, IT-Grundschutz Standards, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html.

licht ein pauschalisiertes Vorgehen zur Minimierung von IT-Sicherheitsrisiken. Die Standards definieren bereits typische Gefährdungen und empfehlen technische Schutzmaßnahmen sowie organisatorische, infrastrukturelle und personelle Sicherheitsmaßnahmen, welche einer Organisation als Grundlage für einen Basisschutz verwenden kann. Aus diesem Grund ist der IT-Grundschutz mit über 4.000 Seiten auch sehr viel umfangreicher als allgemeinere Standards.

27 Der IT-Grundschutz umfasst drei an dem Schutzbedarf einer Organisation orientierten **Absicherungskategorien**: die Basis-Absicherung, die Standardabsicherung und die Kernabsicherung. Letztere bezieht sich auf den Schutz besonders schützenswerter Daten einer Institution. Eine individuelle Risikoanalyse der Institution ist bei der Absicherung nach IT-Grundschutz bei normalen Sicherheitsanforderungen nicht vorgesehen. Nur Organisationen bzw. Teile von Organisationen mit hohem Schutzbedarf müssen eine individuelle Risikoanalyse durchlaufen. Dafür stellt das BSI den Standard 200–3 für eine individuelle Risikoanalyse, welche auf dem Standard ISO/IEC 27005 basiert, zur Verfügung. Das Vorgehen zum Notfallmanagement ist in dem BSI-Standard 100–4 definiert.

28 ISMS nach ISO/IEC 27001 und dem IT-Grundschutz folgen einem **zyklischen Prozessansatz**, welcher sich in die Phasen „Plan, Do, Check, Act“ (PDCA) unterteilen lässt. In der Phase „Plan“ konzipiert die Organisation das ISMS und das gewünschte Maß an Sicherheit, in „Do“ setzt sie das Konzept um, in „Check“ findet eine Überprüfung statt und in „Act“ wertet sie die Prüfergebnisse aus und erfasst gegebenenfalls einen Änderungsbedarf. Mit den sich aus dem Änderungsbedarf ergebenden Anforderungen steigt die Organisation wieder bei „Plan“ in den Zyklus ein.[25] Der zyklische Ansatz der Norm ermöglicht somit die dynamische Messung, Bewertung und Gewährleistung von IT-Sicherheit innerhalb einer sich stetig verändernden Organisation.

### 2. IEC 62443 Normenreihe

29 Im Bereich der industriellen Steuerungs- und Automatisierungstechnik gewinnt die noch junge Normenreihe IEC 62443 „Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme“ zunehmend an Bedeutung. Sie gilt als führende Norm für die Prüfung und Zertifizierung von Produkten, Prozessen und Dienstleistungen im Bereich der **industriellen IT-Sicherheit**. Die IEC 62443 befasst sich mit der IT-Sicherheit von Industrial Automation Control Systemen (IACS), die als IT-Systeme, bestehend aus mehreren Komponenten wie zB Aktoren und Sensoren, der Steuerung von Produktionsstraßen und Prozessstrecken dienen. Des Weiteren bezieht die IEC 62443 auch Anforderungen an die Produktentwicklung sowie Sicherheitsanforderungen an IACS Produkte mit ein.[26] Dieser Leitfaden gilt für Anwender (d.h. Eigentümer von Anlagen), Systemintegratoren, Sicherheitspraktiker und Hersteller von Steuerungssystemen, die für die Herstellung, das Design, die Implementierung oder das Management von industriellen Automatisierungs- und Steuerungssystemen verantwortlich sind. Die Normenreihe gliedert sich in vier Teile: Allgemeines, Policies und Prozesse, Systeme sowie Komponenten/Produkte. Unter Policies und Prozesse beschreibt die Norm ein ISMS für industrielle Automatisierungssysteme, welches sich an der ISO 27000-Reihe orientiert. Auf der Systemebene beschreibt es Sicherheitsanforderungen und Risikobewertungen für IT-Systeme, die in einem IACS-Umfeld eingesetzt werden.[27] Der letzte Teil zu Komponenten und Produkten enthält Anforderungen für Hersteller von IKT-Produkten, die in IACS-Umgebungen eingesetzt werden.

[25] Kersten/Klett/Reuter/Schröder, 2020, S. 12.

[26] ZVEI, 2017, S. 9 ff; TÜViT, S. 8 ff.

[27] ISA, n.d.

30 Die IEC 62443 dient zunehmend als Grundlage für die Umsetzung von IT-Sicherheitsanforderungen durch KRITIS-Betreiber für die Absicherung vernetzter Steuerungs- und Automatisierungstechnik. Auch andere Branchen, in denen entsprechende Normen für industrielle IT-Sicherheit fehlen, wenden diese Normenreihe an, beispielweise der Bereich Medizinprodukte.

## II. Messung und Bewertung von IT-Sicherheit in Institutionen

31 Jeder Betreiber, Anbieter oder Hersteller von IT-Systemen muss im Rahmen der Auswahl und Implementierung von IT-Sicherheitsmaßnahmen eine **Risikoanalyse** vornehmen. Dieser Prozess umfasst laut der Definition des BSI die Beurteilung von Risiken im Sinne deren Identifikation, Einschätzung und Bewertung sowie die Behandlung von Risiken.[28] Sie dient als Grundlage für die Auswahl technischer und organisatorischer Maßnahmen zur Risikobewältigung. Innerhalb der Risikobeurteilung ist eine **Messung** und **Bewertung der Risiken** bzw. des IT-Sicherheitsniveaus anhand der Schutzziele und des Schutzbedarfs erforderlich. Das Messen von Sicherheitsaktivitäten in Institutionen ist ein kontinuierlicher Prozess mit dem Ziel, die Sicherheit durch gezielte Maßnahmen kontinuierlich zu verbessern.[29]

32 Die **IT-Grundschutz**-Kataloge des BSI enthalten bereits Standard-Sicherheitsmaßnahmen, die bei normalen Sicherheitsanforderungen eine angemessene organisationale, technische und personelle Absicherung für Institutionen sicherstellen. Sie basieren auf der Annahme pauschalisierter Risiken. Für Bereiche und Institutionen mit hohem oder sehr hohem Schutzbedarf sowie für spezifische Einsatzszenarien ist jedoch die Durchführung einer individuellen Risikoanalyse notwendig, welche im BSI-Standard 200–3 erläutert ist. Innerhalb eines ISMS helfen Methoden zur Messung von IT-Sicherheit bei der Erfassung des vorhandenen Risikos und der Bewertung der zu schützenden Assets (Informationen, Systeme, Applikationen, Prozesse, Gebäude etc).

### 1. Risikoanalyse

33 Ein **Risiko** kann allgemein als der mögliche Eintritt eines Schadens definiert werden. In der Grundform wird es aus der Kombination (Multiplikation) der Wahrscheinlichkeit des Eintritts mit dem Ausmaß des Schadens berechnet.[30] Für die Bestimmung von Risiken existieren darüber hinaus zahlreiche quantitative und qualitative Verfahren. Auf Grundlage der Analyse und Bewertung von Risiken kann das Risikomanagement Maßnahmen entwickeln, welche die Wahrscheinlichkeit des Eintretens der Risiken und die möglichen Auswirkungen auf die Organisation reduzieren.

34 Jeder Risikoanalyse geht die Analyse des **Schutzbedarfs** in einer Organisation voraus. Der Schutzbedarf bezieht sich auf die Ressourcen, die geschützt werden müssen (**Assets oder Informationswerte**), welche sowohl materielle als auch immaterielle Eigenschaften umfassen können. Informationswerte können durch unterschiedliche Ansätze ausgedrückt werden, zum Beispiel durch eine (qualitative) Klassifizierung von Schutzbedarfsklassen, durch ein Ranking der Informationswerte oder durch quantitative Ansätze wie Kosten-, Markt- oder Gewinnbewertungen.[31] Am häufigsten wird eine Klassifizierung von Informationswerten verwendet, welche auch immaterielle Werte in die Bewertung mit einbeziehen kann. Auch der IT-Grundschutz

[28] BSI 200–3, S. 6. Nach den einschlägigen internationalen Standards ISO/IEC 31000 und ISO/IEC 27005 bezeichnet die Risikoanalyse nur einen Teilprozess im Rahmen der Risikobeurteilung, welche aus Identifikation, Analyse und Evaluation oder Bewertung von Risiken besteht. Im deutschen Sprachgebrauch hat sich allerdings der Begriff „Risikoanalyse" für den kompletten Prozess der Risikobeurteilung und -behandlung etabliert. In diesem Sinne verwendet auch der IT-Grundschutz den Begriff.

[29] Hasso-Plattner-Institut, 2010, S. 33.

[30] Vgl. NIST SP 800–30, 2012, S. B-9; Refsdal/Solhaug/Stolen, 2015, S. 9.

[31] NIST SP 800–30, S. 14 f.; Hasso-Plattner-Institut, 2010, S. 3 ff.

verwendet Klassifizierungen, nach denen der Schutzbedarf beispielsweise als „normal, hoch, sehr hoch" dargestellt wird, je nachdem ob die Schadensauswirkungen begrenzt, beträchtlich oder katastrophal wären.[32]

In der Risikoanalyse wird dann die **Gefährdungslage** in Hinblick auf einen spezifischen Informationswert analysiert. Mit einbezogen werden daher der Schutzbedarf des Informationswerts, der Umfang der Gefährdung, der ein Wert ausgesetzt ist, sowie die Wahrscheinlichkeit einer potenziellen Schwachstelle, die von einem Angreifer ausgenutzt werden kann.[33] 35

Anschließend können das Risiko und seine Faktoren mithilfe von verschiedenen Methoden bewertet werden, unter anderem quantitativ, qualitativ oder semi-quantitativ. **Quantitative** Ansätze nutzen numerische Werte zur Berechnung und Klassifikation von Risiken. Dazu müssen die Risikofaktoren (Informationswert, Eintrittswahrscheinlichkeit, Schadenhöhe) zahlenmäßig bestimmbar sein. Diese Art der Bewertung unterstützt insbesondere Kosten-Nutzen-Analysen von IT-Sicherheitsmaßnahmen zur Risikobewältigung. Eine Quantifizierung der Eintrittswahrscheinlichkeit und des Schadenausmaßes ist eine Voraussetzung für die Berechnung eines Risikos und der darauf basierenden Errechnung eines Budgets, das für potenzielle Sicherheitsmaßnahmen bereitgestellt werden kann. 36

In der quantitativen Risikoanalyse sind vor allem drei **Formeln** gebräuchlich: Die Single Loss Expectancy (SLE) oder Einzelverlusterwartung, die Annualized Loss Expectancy (ALE) oder jährliche Verlusterwartung, und der Return on Security Invest (ROSI).[34] 37

- SLE: Das Risiko wird anhand einer Multiplikation von Informationswert (asset value) und Gefährdungsfaktor (exposure factor) berechnet. So lässt sich der erwartete Verlust im Fall eines einzelnen Zwischenfalls berechnen. Der Gefährdungsfaktor stellt den prozentualen Verlust des Informationswertes beim Eintreten der Bedrohung dar.
- ALE: Das Risiko wird anhand von einer Multiplikation des SLE und der zu erwartenden jährlichen Eintrittsrate eines Risikos berechnet. Die jährliche Eintrittsrate wiederum – also die Wahrscheinlichkeit des Eintritts eines Risikos und dessen Häufigkeit – kann nur anhand von statistischen Daten berechnet werden.
- ROSI: Das Risiko wird berechnet anhand der Reduzierung der jährlichen Schadenerwartung (die Differenz zwischen der ALE vor und der ALE nach der Installation von Sicherheitsmechanismen) minus der jährlichen Kosten zur Implementierung der Sicherheitsmechanismen.

Quantitative Ansätze haben einige Vorteile. Nach einer bestimmten Messgröße quantifizierte Risiken sind vergleichbar und finanziell bewertbar. Darauf aufbauend lässt sich beispielweise anhand des Budgets einer Organisation berechnen, in welche Sicherheitsmaßnahmen zur Risikobewältigung investiert werden sollte (siehe ROSI). Ein bedeutender Nachteil ist jedoch, dass quantitative Risikoanalysen höchst komplex und mit hohem Kosten- und Zeitaufwand verbunden sind.[35] In der Praxis lassen sich Risiken in der IT-Sicherheit zudem oft nicht rein quantitativ berechnen. Meistens liegen nicht ausreichend genaue Daten vor, um exakte Einschätzungen zu Informationswert, Eintrittswahrscheinlichkeit, Gefährdungspotenzial, Schwachstellen oder Schadensausmaß vornehmen zu können. Da IT-Sicherheit höchst dynamisch ist, ändern sich diese Faktoren zudem stetig, was den Aufbau eines Datenpools sehr komplex macht. Die Wahrscheinlichkeit eines IT-Sicherheitsvorfalls (verursacht durch einen Angriff oder eine Fehlfunktion) lässt sich nur selten akkurat quantifizieren.[36] Zudem können 38

[32] BSI 200–1, S. 42.

[33] Hasso-Plattner-Institut, 2010, S. 40 ff.

[34] Vgl. Hasso-Plattner-Institut, 2010, S. 40 ff.; Refsdal/Solhaug/Stolen, 2015, S. 107 ff.

[35] BSI 200–3, 26.

[36] Refsdal/Solhaug/Stolen, 2015, S. 117 ff.; Kersten/Klett/Reuter/Schröder, 2020, S. 56.

nicht alle Schäden beziffert werden (beispielsweise langfristige Folgen eines Reputationsverlusts oder der Verlust von Privatsphäre). Oft fließen in scheinbar objektive Werten auch subjektive Einschätzungen ein.[37] Daher sehen viele Verfahren semi-quantitative oder qualitativ-quantitative Mischformen vor.

39 **Qualitative** Risikobeurteilungen verwenden Methoden, Prinzipien oder Regeln zur Risikobewertung auf der Basis von nichtnumerischen Kategorien oder Stufen (zB „sehr gering, niedrig, mittel, hoch, sehr hoch"). Informationswerte und Bedrohungspotenziale werden in solchen Verfahren durch qualitative Methoden, wie die Befragung von Experten und Mitarbeitern, ermittelt. Darauf aufbauend können Kosten abgeschätzt und Sicherheitsmaßnahmen bestimmt werden.

40 Zu den Vorteilen qualitativer Verfahren zählt, dass sie weniger aufwändig als quantitative Verfahren sind, weniger von statistischen Daten abhängen und auch immaterielle Faktoren in die Analyse mit einbeziehen. Sie basieren jedoch meist auf subjektiven Bewertungen, was ein Nachteil sein kann. Die methodischen Anforderungen an klare Definitionen der untersuchten Werte sind innerhalb qualitativer Verfahren sehr hoch. Sind diese unklar definiert und nicht mit aussagekräftigen Beispielen unterlegt, können verschiedene Experten, die sich auf ihre individuellen Erfahrungen stützen, zu signifikant unterschiedlichen Bewertungsergebnissen kommen. Die Wiederholbarkeit und Reproduzierbarkeit von qualitativen Bewertungen erfordern eine präzise Annotation der Werte (zB Gründe, warum sich ein spezifischer Wert ergibt) und die Verwendung von klar definierten Funktionen zur Kombination qualitativer Werte. Eine eindeutige Kosten-Nutzen-Analyse und eine Entscheidung über die Allokation von finanziellen Ressourcen auf Grundlage qualitativer Ergebnisse sind weniger eindeutig als auf Grundlage quantitativer Risikobewertungen.[38]

41 **Semi-quantitative** Methoden zur Risikobewertungen verwenden oft Skalen oder repräsentative Zahlen, deren Werte und Bedeutungen in anderen Zusammenhängen nicht immer beibehalten werden. Werteskalen oder -bereiche (zB 1–10 % oder 90–95) lassen sich leicht in qualitative Begriffe übersetzen, die die Risikokommunikation für die Entscheidungsträger in Klassifizierungen wie „niedrig, sehr hoch" unterstützen und gleichzeitig relative Vergleiche zwischen Werten in verschiedenen Wertebereichen ermöglichen. Wenn die Skalen oder Kategorien eine ausreichende Granularität bieten, wird zudem die relative Priorisierung der Ergebnisse besser unterstützt als bei einem rein qualitativen Ansatz. Auch in diesen Ansätzen gilt es, das Einfließen subjektiver Urteile, ungenauer Kategorien und Bezeichnungen zu vermeiden.[39]

42 Das **BSI** empfiehlt im Standard 200–3 für die Einschätzung von Schadenshöhe und Eintrittshäufigkeit eine Kombination von qualitativen und quantitativen Bewertungsschritten, weist aber auf die Schwierigkeiten der quantitativen Risikobetrachtung hin. Zur Abschätzung von Risiken empfiehlt es daher als Ausgangspunkt ein System der qualitativen Klassifikation und Kombination.[40]

43 Auf Grundlage einer Risikoanalyse kann eine Institution adäquate Maßnahmen zur **Bewältigung von Risiken** auswählen. Allgemein sieht das Risikomanagement dafür unterschiedliche Optionen vor. Je nach Risikoeinschätzung und Kontext kann ein Risiko vermieden, kontrolliert, mitigiert, reduziert, akzeptiert, oder an eine dritte Partei übertragen werden. Für die Kontrolle, Mitigation oder Reduktion von Risiken wählt eine Institution entsprechende technische und organisatorische Sicherheitsmaßnahmen aus. Eine Übertragung eines Risikos auf

[37] NIST SP 300–69; BSI 200–3.
[38] NIST SP 800–30, 2012, S. 14.
[39] NIST SP 800–30, 2012, S. 14.
[40] BSI 200–3, 26 ff.

eine dritte Partei könnte zum Beispiel ein „Outsourcing“ des finanziellen Risikos durch eine Versicherung bedeuten.

### 2. Messung und Bewertung der Effektivität von Sicherheitsmaßnahmen

Nach der Implementierung von Sicherheitsmaßnahmen sieht ein ISMS die kontinuierliche Messung und Bewertung der Effektivität dieser Maßnahmen vor. Der ISO/IEC 27001 Standard schreibt vor, dass die Wirksamkeit des ISMS konstant überwacht, gemessen und bewertet werden muss. Zu diesem Zweck müssen Organisationen geeignete **Metriken** entwickeln, welche ebenfalls als Grundlage für interne und externe Audits dienen können. 44

Die notwendigen Messungen und Kennzahlen müssen aus den Kontrollzielen für die jeweiligen Sicherheitskriterien (wie physische Sicherheit, personelle Sicherheit, operationale Sicherheit, technische IT-Sicherheitsmechanismen etc) abgeleitet werden. Konkretere Richtlinien mit generischen Kennzahlen gibt der Standard ISO/IEC 27004 vor.[41] Auch der Standard Cobit[42], welcher im IT Governance-Bereich zur Anwendung kommt, stellt Metriken zur Verfügung, um die Effektivität und Effizienz von IT-Prozessen im Allgemeinen zu messen.[43] 45

### 3. Schranken des IT-Risikomanagements

Die Durchführung einer Risikoanalyse und nachfolgende Erstellung eines Risikomanagementplans sowie die Implementierung von Sicherheitsmaßnahmen bieten jedoch kein Patentrezept gegen IT-Sicherheitsbedrohungen. Die **inhärente Beschränkung** von IT-Risikomanagement ist, dass Risiken zwar reduziert, aber nie eliminiert werden können. Ein gewisses Sicherheitsrisiko wird immer bleiben, selbst wenn eine Organisation Sicherheitsmaßnahmen für den höchsten Schutzbedarf anwendet. Ein wichtiger Faktor bei der Durchführung von Risikoanalysen und der Implementierung von Sicherheitsmaßnahmen ist ebenfalls die „Angemessenheit“ und „Wirtschaftlichkeit“. Die Maßnahmen müssen immer im Verhältnis zu der Größe und den finanziellen Möglichkeiten eines Unternehmens oder einer Organisation stehen. Aus diesem Grund sieht zum Beispiel der IT-Grundschutz ein pauschalisiertes Vorgehen vor, welches zumindest ein auch für kleinere Unternehmen implementierbares grundlegendes Niveau an Sicherheit schafft. Selbst das Vorgehen nach IT-Grundschutz ist jedoch sehr aufwendig und der Katalog umfasst insgesamt über 4.000 Seiten. Aufgrund dieser Schranken des IT-Risikomanagements sind Organisationen dazu verpflichtet, Vorsorge für den Eintritt des nicht auszuschließenden Restrisikos zu ergreifen. Dazu gehören reaktive IT-Sicherheitsmaßnahmen wie ein IT-Notfallmanagement und eine Planung zur Wiederherstellung der Systeme und Informationen.[44] 46

## III. Prüfung und Nachweis von IT-Sicherheit in Institutionen

Die **Überprüfung der Einhaltung und Effektivität von IT-Sicherheitsmaßnahmen** kann je nach Gesetz freiwillig oder verpflichtend sein. KRITIS-Betreiber sind beispielsweise nach § 8 a Abs. 3 BSIG dazu verpflichtet, die Einhaltung von Maßnahmen durch eine Prüfung bzw. ein Sicherheitsaudit und gegebenenfalls ein Zertifikat nachzuweisen. 47

Die Prüfung der Umsetzung von technischen und organisatorischen IT-Sicherheitsmaßnahmen erfolgt meist durch ein **Audit** eines ISMS. Audits können intern in Organisationen durch eigenes Personal und/oder extern durch ein qualifiziertes Auditteam vorgenommen werden. 48

[41] Kersten/Klett/Reuter/Schröder, 2020, S. 64 ff.

[42] Control Objectives for Information Related Technology (Cobit).

[43] Hasso-Plattner-Institut, 2010, S. 17 f.; S. 45 ff.

[44] So zB empfohlen in BSI, 2019, „Orientierungshilfe zu Nachweisen gemäß § 8 a Absatz 3 BSIG, Version 1.0“, S. 20.

49 Sowohl die **Testierung** der IT-Grundschutz-Basis-Absicherung als auch die **Zertifizierung des IT-Grundschutzes** erfordern eine Prüfung durch einen durch das BSI zertifizierten Grundschutz-Auditor, im Falle einer Zertifizierung auch ein qualifiziertes Auditteam. Das Audit besteht aus einer Dokumentenprüfung und einer Umsetzungsprüfung vor Ort, welche im Rahmen einer Zertifizierung umfangreicher ist als im Rahmen einer Testierung. Die Ergebnisse eines Audits müssen immer in einem schriftlichen Auditbericht festgehalten werden.[45] Zusätzliche Normen und Standards der ISO/IEC 27000er Reihe, ITIL oder andere spezifizieren die Ausgestaltung. Details für interne und externe Audits beschreibt die Norm ISO/IEC 27007, technische Audits bei IT-Systemen und Netzwerken beschreibt die Norm ISO/IEC 27008. Als **Nachweis** für die Umsetzung des IT-Grundschutzes dient entsprechend entweder ein Testat nach der Basis-Absicherung oder das IT-Grundschutz-Zertifikat nach der Standard- bzw. Kernabsicherung durch das BSI. Für kleinere Organisationen bietet sich die kostengünstigere Basis-Absicherung an.

50 Eine **Zertifizierung** nach ISO/IEC 27001 auf Basis des IT-Grundschutz können Institutionen beim BSI beantragen. Die **Zertifizierungsstelle des BSI** übernimmt die Rolle einer unabhängigen dritten Instanz, welchen den Auditbericht prüft und bei positivem Prüfergebnis ein ISO/IEC 27001-Zertifikat erteilt. Dieses ist in der Regel drei Jahre lang gültig. Darin integriert sind jährliche Überwachungsaudits. Nach drei Jahren wird eine Re-Zertifizierung erforderlich,[46] allerdings kann nach anderen Vorgaben ein kürzerer Zeitraum erforderlich sein (zB im KRITIS-Bereich nach zwei Jahren, s. § 8 a Abs. 3 Satz 1 BSIG). Eine Zertifizierung nach der Normenreihe IEC 62443 wird international bisher nur vereinzelt angeboten.

## IV. Anwendung im IT-Sicherheitsrecht

### 1. Betreiber Kritischer Infrastrukturen nach dem BSI-Gesetz

51 **KRITIS-Betreiber** gem. § 2 Abs. 10 BSIG und den konkretisierenden Bestimmungen der KritisV[47] unterliegen umfassenden Pflichten zur Bewertung, Prüfung und dem Nachweis von IT-Sicherheit. Laut § 8 a Abs. 1 BSIG sind sie dazu verpflichtet, „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind.“ Dabei soll der „Stand der Technik“ eingehalten werden. Gem. § 8 a Abs. 3 Satz 1 BSIG haben die Betreiber dem BSI gegenüber mindestens alle zwei Jahre einen Nachweis über die Erfüllung der rechtlichen Anforderungen zu erbringen, welcher „durch Sicherheitsaudits, Prüfungen oder Zertifizierungen“ erfolgen kann (§ 8 a Abs. 3 Satz 2 BSIG). Auf welche in § 8 a Abs. 3 BSIG genannte „geeignete Weise“ ein solcher Nachweis zu erbringen ist und welche Anforderungen konkret zu erfüllen sind, definiert das BSI in einer 2019 veröffentlichten „Orientierungshilfe zu Nachweisen gemäß § 8 a Absatz 3 BSIG“.[48]

[45] Vgl. Kersten/Klett/Reuter/Schröder, 2020, S. 75 ff.

[46] BSI, 2019, „Zertifizierungsschema nach ISO 27001 auf der Basis von IT-Grundschutz, Version 2.1“.

[47] Kritische Infrastrukturen umfassen die Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen. Die betroffenen Unternehmen sind in der KritisV bestimmt. Laut dem Entwurf für ein IT-Sicherheitsgesetz 2.0 ist die Ausweitung der adressierten Unternehmen vorgesehen. Eine neue Kategorie der „Infrastrukturen im besonderen öffentlichen Interesse“, welche Unternehmen aus der Rüstungswirtschaft, dem Bereich Kultur und Medien, börsliche Infrastrukturen sowie höchstwahrscheinlich auch aus der Automobil- und Chemiebranche umfasst, soll denselben Anforderungen wie KRITIS-Betreiber unterliegen. Zu den KRITIS nach § 2 Abs. 10 BSIG sollen gem. Art. 1 Nr. 1 lit. D RefE zukünftig auch Einrichtungen des Entsorgungs-Sektors zählen, wenn sie von „hoher Bedeutung für das Funktionieren des Gemeinwesens sind“. Ebenso soll das BSI gem. Art. 1 Ziff. 16 RefE in einem neuen § 8 g BSIG Betreibern mit „Cyberkritikalität“ im Einzelfall die Pflichten von KRITIS-Betreibern auferlegen können.

[48] BSI, 2019, „Orientierungshilfe zu Nachweisen gemäß § 8 a Absatz 3 BSIG, Version 1.0“.

Die gem. § 8 a Abs. 3 BSIG notwendige **Prüfung** muss durch eine prüfende Stelle durchgeführt und das Prüfergebnis in Form des Prüfberichts dem Betreiber vorgelegt werden. Die Prüfung muss dabei den vollen Geltungsbereich der Kritischen Infrastruktur (dh der jeweiligen Anlage gemäß BSI-KritisV) umfassen. Zum Prüfgegenstand gehören sowohl die Anlage, Dienstleistungen und damit verbundene Systeme und Schnittstellen als auch alle IT-Systeme, Komponenten, Prozesse, Rollen, Personen und Organisationseinheiten, die für die Funktionsfähigkeit der erbrachten Dienstleistung erforderlich sind.[49] 52

Die Prüfgrundlage kann ein **branchenspezifischer Sicherheitsstandard (B3S)** nach § 8 a Abs. 2 BSIG sein, der im Vorfeld von Betreibern oder Verbänden kritischer Infrastrukturen erarbeitet und vom BSI für den jeweiligen Geltungsbereich als geeignet befunden wurde. Liegt kein B3S vor, müssen Betreiber und Prüfstelle sicherstellen, dass die Anforderungen nach § 8 a Abs. 1 BSIG auf andere Weise erfüllt sind. Als Orientierungshilfe zur Erarbeitung von B3S hat das BSI gemeinsam mit dem UP KRITIS und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) einen Leitfaden für Autoren von B3S entwickelt.[50] 53

Eine Prüfgrundlage kann dann aufgrund der B3S-Orientierungshilfe oder aufgrund einschlägigen Standards (zB Zertifizierungsschemata für den IT-Grundschutz, nach der Norm ISO/IEC 27001) erstellt werden.[51] Für die Bereiche des Energiewirtschaftsgesetzes (EnWG)[52] sowie des Telekommunikationsgesetzes (TKG)[53] gelten spezifische Anforderungen, für die die Bundesnetzagentur (BNetzA) als Aufsichtsbehörde zuständig ist. Sie hat zwei Sicherheitskataloge[54] für den Geltungsbereich des EnWG und einen überarbeiteten Entwurf des Sicherheitskatalogs für den Geltungsbereich des TKG herausgegeben (*Hornung/Schindler* in → § 21 Rn. ■■■), *Guckelberger* in → § 23 Rn. 9). Laut den Sicherheitskatalogen für den Bereich Energie ist die Einrichtung eines ISMS nach ISO 27001 und die Zertifizierung Pflicht, unter Berücksichtigung der ISO 27002 und ISO 27019. Für weitere Sektoren hat das BSI bereits B3S als geeignet beurteilt.[55] 54

Zur **Nachweiserbringung** gegenüber dem BSI übermitteln die Betreiber dem BSI nach § 8 a Abs. 3 Satz 3 BSIG Informationen über Art und Umfang sowie die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen wie auch die dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann gemäß Satz 4 die Vorlage der vollständigen Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Bei Sicherheitsmängeln kann es nach Satz 5 – im Einvernehmen mit der zuständigen Aufsichtsbehörde – die Beseitigung der Sicherheitsmängel verlangen. Bleiben offene Fragen zur Umsetzung der Sicherheitsvorkehrungen bestehen, kann das BSI gem. § 8 a Abs. 4 BSIG außerdem selbst eigene Prüfungen der Sicherheitsvorkehrungen des Betreibers vor Ort vornehmen.[56] 55

[49] BSI, 2019, „Orientierungshilfe zu Nachweisen gemäß § 8 a Absatz 3 BSIG, Version 1.0", S. 7 f.

[50] BSI, 2017, „Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8 a (2) BSIG, Version 1.0".

[51] BSI, 2019, „Orientierungshilfe zu Nachweisen gemäß § 8 a Absatz 3 BSIG".

[52] S. näher Guckelberger in → § 23 Rn. 1 ff. und Singler in → § 22 Rn. 1 ff.

[53] S. näher Hornung/Schindler in →§ 21 Rn. 1 ff.

[54] IT-Sicherheitskatalog gemäß § 11 Absatz 1 a Energiewirtschaftsgesetz, Bundesnetzagentur, August 2015; IT-Sicherheitskatalog gemäß § 11 Absatz 1 b Energiewirtschaftsgesetz, Bundesnetzagentur, August 2015.

[55] Branchen, für die Anfang 2020 bereits B3S als geeignet festgestellt wurden, umfassen Wasser und Abwasser (Wasserversorgung, Abwasserbeseitigung), Ernährung (Ernährungswirtschaft, Lebensmittelhandel), Informationstechnik, Energie (Strom, Fernwärme), Gesundheit (Medizinische Versorgung, Arzneimittel und Impfstoffe, Labore), Transport und Verkehr (Straßenverkehr), Finanz- und Versicherungswesen (Versicherungen). Vgl. BSI, Übersicht über Branchenspezifische Sicherheitsstandards (online), https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/Was_tun/Stand_der_Technik/B3S/B3S.html.

[56] BSI, Orientierungshilfe zu Nachweisen gemäß § 8 a Absatz 3 BSIG, Version 1.0, 15.5.2019.

### 2. Betreiber und Anbieter von IT-Systemen in fachspezifischen Bereichen

56 Abgesehen von allgemeinen Gesetzen, wie dem BSIG, schreiben einige fachspezifische Gesetze Prüf- und Nachweisverfahren von IT-Sicherheit für Diensteanbieter vor. Darunter sind beispielsweise § 29 Abs. 2 PAuswV für die Zertifizierung von **Identifizierungsdiensteanbietern**, § 25 MsbG für die Zertifizierung der Umsetzung eines spezifischen ISMS durch **Smart-Meter-Gateway (SMG) Administratoren**[57], § 17 De-Mail-G für die Akkreditierung von **De-Mail Anbietern**[58] und § 109 TKG für die **Betreiber öffentlicher Telekommunikationsnetze und die Erbringer öffentlich zugänglicher Telekommunikationsdienste**.

### 3. Verarbeiter personenbezogener Daten

57 Aus der DSGVO[59] ergeben sich angepasste Regelungen über die **Datensicherheit**[60]. Auf technischer Ebene überschneiden sich die Anforderungen an Datensicherheit und IT-Sicherheit, ihre Erfüllung erfordert jedoch teilweise andere Bewertungskriterien und -verfahren.[61] Art. 32 DSGVO zur Sicherheit der Verarbeitung verpflichtet die für die Datenverarbeitung Verantwortlichen (und auch die Auftragsverarbeiter) zu technisch-organisatorischen Maßnahmen zum Schutz der IT-Systeme, die personenbezogene Daten verarbeiten. Dabei ist der „Stand der Technik" zu berücksichtigen. Dazu zählt Art. 32 Abs. 1 DSGVO einige Beispiele auf, definiert den „Stand der Technik" jedoch nicht abschließend. Unter den Beispielen legt die Norm fest, dass die Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus unter anderem ein Verfahren zur regelmäßigen Überprüfung, Bewertung, Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einschließen können (Art. 32 Abs. 1 lit. d) DSGVO). Zum Nachweis der Einhaltung der Anforderungen nach Art. 32 Abs. 1 kann gemäß Abs. 4 auch eine Zertifizierung gem. Art. 42 DSGVO herangezogen werden. Aufgrund der starken Überschneidungen in der Ermittlung des Standes der Technik im Datenschutz- und IT-Sicherheitsrecht empfiehlt es sich, die Maßnahmen gemeinschaftlich zu betrachten, wie es beispielsweise durch die Arbeitshilfe wie die Handreichung zum „Stand der Technik" des TeleTrusT e.V. – Bundesverband IT-Sicherheit (2020) getan wird.

## V. Zusammenfassung

58 Die Umsetzung von technischen und organisatorischen IT-Sicherheits-Maßnahmen in Institutionen erfordert in den meisten Fällen den Aufbau eines ISMS. Die Messung von IT-Sicherheit ist bis zu einem gewissen Grad mithilfe von qualitativen und, wo möglich, quantitativen Verfahren der Risikoanalyse möglich. Entsprechende Methoden bilden auch einen Teil der Prüf- und Nachweisverfahren im Rahmen von Audits und Zertifizierungen ab. Aufgrund der hohen Komplexität von IT-Systemen und der Dynamik von IT-Sicherheitsbedrohungen und Umfeld ist eine genaue Messung oder eine Eliminierung der Risiken jedoch nie abschließend möglich. Eine Prüfung und/oder Zertifizierung kann insofern je nach Prüftiefe eine Absicherung gegen die Ausnutzung bekannter Schwachstellen und Angriffsverfahren bieten, jedoch nicht gegen hoch entwickelte neuartige Angriffe. Zur Abwehr dieser Angriffe müssen Institutionen zusätzliche Sicherheitsmaßnahmen und organisatorische Prozesse implementieren, was aufgrund des

[57] S. Singler in → § 24 Rn. 1 ff.

[58] S. Roßnagel in → § 14 Rn. 1 ff.

[59] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DSGVO), ABl. Nr. L 119/1.

[60] Raabe/Schallbruch/Steinbrück, DSI IPR (2).

[61] Ausführlich zum Verhältnis zwischen IT-Sicherheit und Datenschutz Jandt in → § 17 Rn. 1 ff.

hohen Aufwandes jedoch meist nur für größere Organisationen und Unternehmen möglich ist.

## D. IT-Sicherheit von Software und Hardware

59 Die Funktionsfähigkeit und Sicherheit von Software und Hardware in IT-Komponenten und Systemen machen die wesentlichen Grundlagen für die Sicherheit von Infrastrukturen und der Gesellschaft aus. Aufgrund der zunehmenden Komplexität von IT-Systemen ist eine Beurteilung ihrer Sicherheit durch „Draufschau" in einem einfachen Verfahren in der Regel unmöglich. Die Sicherheitseigenschaften von IKT sind nur durch eingehende Prüfungen zu ermitteln und prüfen. Dieses Kapitel gibt einen Überblick über die Kriterien und Verfahren zur Evaluierung und Prüfung bzw. Zertifizierung von IT-Sicherheit von Software und Hardware.

### I. Evaluationskriterien für die IT-Sicherheitseigenschaften von Software und Hardware

60 Zur methodischen Bewertung der Sicherheit von Soft- und Hardware-Komponenten und Systemen wurden seit den 1980er Jahren **Kriterienkataloge** entwickelt. Beispiele sind die europäischen ITSEC- (Information Technology Security Evaluation Criteria), die US-amerikanischen TCSEC- (Trusted Computer System Evaluation Criteria, auch als „Orange Book" bekannt) und die Common Criteria for Information Technology Security Evaluation, welche unter anderem aus den TCSEC-, ITSEC-Kriterien hervorgegangen sind. Die ITSEC-und TCSEC-Kriterien werden jedoch heute in der Regel nicht mehr angewendet oder aktualisiert. Die ITSEC-Kriterien sind nur noch für „spezifische Sonderfälle" in Anwendung.[62] Daher werden sie in diesem Kapitel nicht eingehender betrachtet.

61 Die Kriterienkataloge umfassen Bewertungsschemata für IT-Sicherheitseigenschaften von Produkten und gewährleisten, dass die Sicherheitsniveaus unterschiedlicher Systeme, die eine ähnliche Funktionalität haben, vergleichbar sind. Sie eignen sich zur Beschreibung, Prüfung und Bewertung von Sicherheitseigenschaften von Produkten sowie zur Spezifikation von Sicherheitsvorgaben. Darüber hinaus schaffen die Kriterien Leitlinien zur Entwicklung sicherer, vertrauenswürdiger Systeme selbst.[63] Eine Zertifizierung auf Grundlage von Common Criteria-Schutzprofilen oder anderen Kriterien ist eine verbreitete Methode, um die IT-Sicherheit eines Produkts nachzuweisen. Jedoch stellen sich zunehmend Herausforderungen für die Bewertung und Prüfung von IT-Sicherheit von Produkten, Diensten und Prozessen, welche dieser Abschnitt ebenfalls beleuchten wird.

#### 1. Common Criteria

62 Die **Common Criteria** (CC), die gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, bilden die international am weitesten verbreitete Grundlage für die Bewertung und Prüfung der Sicherheitseigenschaften von IT-Produkten und -Systemen. Sie sind seit 1999 weltweit einheitlich als internationaler Standard ISO/IEC 15408 anerkannt und aktuell seit 2006 in der CC Version 3.1 verfügbar.

63 Im Kern ermöglichen die CC eine unabhängige technische Evaluierung der Funktionalität und Vertrauenswürdigkeit eines sogenannten **Evaluationsgegenstandes** (EVG). Der EVG kann praktisch jedes IT-Produkt oder System sein, Software, Firmware und/oder Hardware. Bei einer Evaluierung nach CC werden zunächst die funktionalen Sicherheitsanforderungen und dann die Anforderungen an die Vertrauenswürdigkeit geprüft.

[62] BSI, IT-Sicherheitskriterien und Evaluierung nach ITSEC, https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/ITSicherheitskriterien/ITSEC/itsec_node.html.

[63] Eckert, 2009, S. 211; Rannenberg, 1998, S. 3.

64 Für grundsätzliche Anforderungen an eine Kategorie von Produkten können auf der Basis von CC **Schutzprofile** (protection profiles) erstellt werden. Sie bilden gemäß der CC verallgemeinerte und implementierungsunabhängige Sicherheitsziele und -anforderungen. Laut BSI ist ein Schutzprofil „eine implementierungsunabhängige Menge von Sicherheitsanforderungen, die eine identifizierbare Teilmenge von Sicherheitszielen abdeckt."[64] Anwender können daher durch Erstellung eines Schutzprofils oder Verweis auf ein solches ihre IT-Sicherheitsbedürfnisse ausdrücken, ohne Bezug auf einen konkreten EVG zu nehmen.

65 Schutzprofile existieren etwa für Datenbanken, Smartcards, Schlüsselmanagement, Betriebssysteme und Produkte zur Erstellung digitaler Signaturen. Das deutsche BSI hat beispielsweise ein Schutzprofil für maschinenlesbare Reisedokumente (EVG: kontaktloser Chip) und für die elektronische Gesundheitskarte (EVG: Smartcard) festgelegt.[65]

66 Innerhalb einer konkreten Evaluierung werden die Schutzprofile auf einen EVG abgebildet. Mit Beginn der Evaluierung werden die Sicherheitsvorgaben des Schutzprofils in ein **Sicherheitsziel** (Security Target) für einen bestimmten EVG überführt. Das Sicherheitsziel drückt aus, welche spezifischen Sicherheitsanforderungen eines oder mehrerer Schutzprofile in der Evaluierung erfüllt werden. In einem Sicherheitsziel einer spezifischen Evaluation werden über die Informationen eines Schutzprofils hinaus noch weitere Informationen und Beschreibungen über die genaue Einsatzumgebung und den Gegenstand der Evaluierung hinzugefügt. Liegt für das EVG kein Schutzprofil vor, können Sicherheitsvorgaben auch direkt formuliert werden.

67 Bei der Evaluierung sind die Tiefe und Ausführlichkeit der Prüfung entscheidend. Die Analyse von Schwachstellen und deren Ausnutzbarkeit sowie potenzielle Gefährdungen durch Angreifer, einschließlich des Angriffspotenzials (erforderliche Fachkenntnisse, Ressourcen, Motivation etc), ist bei den meisten Evaluierungsaspekten ein zentrales Ziel.[66] Die Prüftiefe wird durch **Evaluierungsstufen**, sogenannte Evaluation Assurance Level (EAL), ausgedrückt. Es gibt sieben hierarchisch geordnete EALs, die in Bezug auf die Sicherheit zunehmen und dazu dienen, allgemeine Sicherheitspakete anzubieten. Mit wachsenden EAL-Stufen erhöht sich der Analyse- und Prüfaufwand und damit das evaluierte Sicherheitsniveau. Wenn das Gefährdungspotenzial als eher gering angesehen wird und der Evaluationsgegenstand vor allem verlässlich funktionieren sollte, ist eine Evaluation nach EAL 1 ausreichend. Ab der Stufe EAL 2 ist ein niedriges bis moderates Niveau von „security assurance" erforderlich. Ab EAL 4 muss beispielsweise der Quellcode mit analysiert werden, ab EAL 5 kommen formale Spezifikations- und Verifikationsmethoden hinzu.[67] Die Evaluierungsstufen der CC sind an die Stufen der ITSEC-Kriterien angelehnt, weshalb die Ergebnisse von ITSEC-Evaluierungen vergleichbar mit denen von CC-Evaluierungen sind.[68]

68 Zur Unterstützung der Evaluierung und Zertifizierung von Produkten können auch **Entwicklungs- und Produktionsstandorte** separat nach CC evaluiert und zertifiziert werden. Die Evaluierung von Standorten erfolgt entsprechend im Rahmen einer „Life-Cycle"-Klasse der CC-Evaluierung.[69]

[64] BSI, „Verzeichnisse – als Nachschlagewerk für Interessenten und Beteiligte an Zertifizierungs- und Anerkennungsverfahren, Version 2.1, S. 26.

[65] Eckert, 2009, S. 228 ff.

[66] Aizuddin, 2001, S. 4 f.

[67] BSI, CC Evaluation Assurance Level (EAL), online abrufbar unter: https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/ITSicherheitskriterien/CommonCriteria/eal_stufe.html.

[68] Eckert, IT-Sicherheit, S. 222.

[69] BSI, „[BSI 7138] Hinweise für Antragsteller für die IT-Sicherheitszertifizierung von Produkten, Schutzprofilen und Standorten".

Ziel einer Evaluierung nach CC ist die Bestätigung, dass die vom Hersteller behauptete Sicherheitsfunktionalität wirksam ist (im Englischen wird dies oft als „assurance“ bezeichnet). Dazu ist eine Prüfung notwendig, welche → Rn. 74 ff. erläutert. 69

### 2. Weitere IT-Sicherheitskriterien

In Deutschland können bestimmte IT-Produkte auf Grundlage von **Technischen Richtlinien (TR) des BSI** geprüft und zertifiziert werden. Eine TR ist ein Kriterienwerk und eine technische Prüfvorschrift des BSI für Konformitätsprüfungen. TR existieren beispielsweise für Smart Card Leser, ID Clients, „De-Mail“-Infrastrukturen und -Dienste, Gesundheitskarten und andere. In einer Prüfung nach TR führt eine anerkannte dritte Stelle eine Evaluation des EVG durch, welche eine anwendungsorientierte Risikoanalyse in einer definierten Einsatzumgebung beinhaltet. In dieser Hinsicht unterscheiden sich TR von CC-Schutzprofilen, welche verallgemeinerte und implementierungsunabhängige Sicherheitsziele und -anforderungen umfassen. 70

Abgesehen von den CC existieren weitere internationale IT-Sicherheitsstandards zur Bewertung der Sicherheit von Hard- und Software. Die **Federal Information Processing Standards FIPS-140** US-amerikanischen Ursprungs legen die Anforderungen an kryptografische Module fest und werden vom US-amerikanischen National Institute for Standards and Technology (NIST) zertifiziert. Der Standard identifiziert vier Sicherheitsstufen und elf „Anforderungsbereiche“, für welche jeweils Anforderungen auf jeder Sicherheitsebene spezifiziert sind. Je höher das Sicherheitsniveau, desto höher die Anforderungen an die physischen Sicherheitsvorkehrungen und Authentifizierungsmechanismen. 2001 wurde die aktuelle Version, FIPS-140–2, veröffentlicht. Diese war eine wichtige Grundlage für die internationale Norm ISO/IEC 19790:2006 zu Sicherheitsanforderungen für kryptografische Module. 71

Das **ISASecure Zertifizierungsprogramm** bündelt Zertifizierungs- und Konformitätsbewertungsaktivitäten im Automatisierungsbereich. Es ist ein Schema für die Evaluierung und Zertifizierung von Systemen der industriellen Automatisierung und Steuerung. Es soll gewährleisten, dass die Systeme robust gegen Netzwerkangriffe abgesichert und frei von bekannten Schwachstellen sind. Es orientiert sich an dem Standard IEC 62443 für Automatisierungssysteme (→ Rn. 29 f.) und umfasst den gesamten Lebenszyklus von Systemen. Die Secure Development Lifecycle Assurance Zertifizierung soll die Sicherheit des Entwicklungsprozesses und damit die Qualität und Sicherheit der IAC Systeme selbst gewährleisten. ISASecure zertifiziert nur kommerzielle „off-the-shelf“ (seriengefertigte) Systeme, jedoch keine Angebote zur Überprüfung von umgebungsspezifischen Systemen oder deren Installation. 72

Mit der zunehmenden Vernetzung von alltäglichen Geräten im „Internet der Dinge“ (IoT) wächst auch die Nachfrage an **Bewertungsschemata für IoT-Geräte**, insbesondere im „Consumer“ bzw. Verbraucher-Bereich. Das Consumer IoT umfasst Produkte wie vernetzte Spielzeuge, Türschlösser, smarte Kameras, Fernseher, Fitnessgeräte und Wearables, Home-Automation und Alarmsysteme, vernetzte Weißware wie Kühlschränke und Waschmaschinen und Smart Home Assistenten. Diese sollten weniger aufwendige Prüfungen als die CC-Evaluierungen und ein Basis-Niveau an IT-Sicherheit ermöglichen. Hierfür existieren bisher jedoch noch keine einschlägigen Standards oder Kriterienkataloge. Verschiedene Organisationen, darunter das European Telecommunications Standards Institute (ETSI)[70], das US-amerikanische National Institute for Standards and Technology (NIST)[71], die IoT Security Foundation[72], die Euro- 73

[70] ETSI, Technical Specification 103 645: Cyber Security for Consumer Internet of Things.

[71] NIST, 2018, “Special Publication 800–160 – Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems”.

[72] IoT Security Foundation, 2016.

pean Union Agency for Cybersecurity (ENISA)[73], das Open Web Application Security Project (OWASP)[74] und weitere arbeiten an Richtlinien und Standards für die sichere Entwicklung und Bewertung von IT-Produkten und Systemen, die in den Consumer-IoT Bereich fallen.

## II. Prüfung und Nachweis von IT-Sicherheit von Software und Hardware

### 1. Zertifizierung von IT-Produkten, Komponenten und Systemen

74 Nach dem BSI-Gesetz, insbesondere § 9 BSIG, und der BSI-ZertV[75] hat das BSI die Aufgabe, **Zertifizierungen von IT-Produkten, Komponenten und Systemen** durchzuführen. Eine Zertifizierung von IT-Produkten nach technischen Richtlinien des BSI oder CC-Schutzprofilen kann ausschließlich von Herstellern, Vertreibern oder Entwicklern von IT-Produkten beantragt werden. Die Bewertung und Evaluation bzw. Prüfung der IT-Sicherheit von Produkten und Diensten kann anhand der oben genannten oder anderer Bewertungsschemata durch den Hersteller bzw. Anbieter selbst oder von dritter Seite durchgeführt werden. Analog zu dem in → Rn. 12 ff. beschriebenen Verfahren kann der Hersteller als Nachweis eine Herstellererklärung abgeben oder den Prüfbericht einer dritten Stelle bzw. ein IT-Sicherheitszertifikat präsentieren. Die Prüfung durch eine dritte Stelle im Bereich der CC kann nach dem oben beschriebenen Verfahren vorgenommen werden.

75 Für die **Zertifizierung von IT-Produkten** nach CC muss grundsätzlich ein vom BSI zertifiziertes oder als geeignet anerkanntes **Schutzprofil** im Zertifizierungsverfahren angewandt werden. Neben den Anforderungen aus dem Schutzprofil können zusätzliche Funktionalitäten und Anforderungen berücksichtigt und je nach EAL angepasst werden. Auch **CC-Schutzprofile** selbst können im Rahmen einer Konformitätsbewertung mit dem CC-Standard zertifiziert werden. **Standorte** können ebenfalls auf Antrag nach CC zertifiziert werden.[76] Prüfgrundlage für Zertifizierungen von IT-Produkten nach **TR** sind entsprechend die unmittelbar in der TR dargelegten Kriterien.

76 Die Prüfung kann gem. § 9 Abs. 3 BSIG durch eine anerkannte sachverständige Stelle erfolgen. Die Zertifizierungsstelle des BSI muss die von der Prüfstelle durchgeführte Evaluierung begleiten. Ein **Zertifikat** wird gem. § 9 Abs. 4 BSIG dann erteilt, wenn IT-Systeme, Komponenten, Produkte oder Schutzprofile sowie Personen oder IT-Sicherheitsdienstleister, den vom BSI festgelegten Kriterien entsprechen. Eine Bedingung ist außerdem immer, dass das Bundesministerium des Innern, für Bau und Heimat festgestellt hat, dass keine überwiegenden öffentlichen Interessen, insbesondere sicherheitspolitische Belange, dieser Erteilung entgegenstehen.

77 Im Rahmen von Zertifizierungen von IT-Produkten bestimmt das BSI gem. § 4 BSI-ZertV technische Geltungsbereiche und bedarfsgerechte Prüfkriterien (Sicherheitskriterien, Schutzprofile, Technische Richtlinien und BSI-Standards). Zertifizierungen können für ein **fertiges Produkt** gelten, **entwicklungsbegleitend** (im Rahmen einer entwicklungsbegleitenden Zertifizierung) erfolgen oder als **Re-Zertifizierung** eines bereits zertifizierten Produkts durchgeführt werden. Ein Zertifikat kann sich nie auf einen gesamten Produkttyp beziehen, sondern gilt entweder für eine bestimmte Version oder für ein Release eines Produktes. Da sich Software dynamisch verändert und oft Updates erhält, sind Re-Zertifizierungen in kurzen Abständen notwendig. Das Ergebnis der Evaluierung ist ein Zertifizierungsbericht. Der Bericht beschreibt die Sicherheitseigenschaften des EVG relativ zu den aufgeführten Bedrohungen, bewertet die Wirksamkeit der eingesetzten Sicherheitsmechanismen und vergibt eine Evaluierungsstufe, um

[73] European Union Agency for Cybersecurity, 2018.

[74] OWASP IoT Security Guidance. Abrufbar unter: https://www.owasp.org/index.php/IoT_Security_Guidance.

[75] BSI-Zertifizierungs- und -Anerkennungsverordnung vom 17.12.2014 (BGBl. I S. 2231), die durch Art. 40 des Gesetzes vom 29.3.2017 (BGBl. I 626) geändert worden ist.

[76] Übersicht vgl. BSI, [VB-Produkte].

den Grad des Vertrauens in die Korrektheit der Funktionalität des Produkts zu bescheinigen. Zudem enthält der Bericht Anforderungen an die Installation und Einsatzumgebung des Evaluierungsgegenstandes sowie eine Beschreibung der inhärenten Schwachstellen und mögliche Gegenmaßnahmen.[77]

78 IT-Sicherheitszertifikate für Produkte sind grundsätzlich fünf Jahre lang gültig. Bei sicherheitsrelevanten Änderungen am Produkt oder den Entwicklungs- oder Produktionsprozessen oder anderen umfangreichen Änderungen („major change") ist eine **Re-Zertifizierung** erforderlich. Diese kann unterschiedlich aufwendig ausfallen, die Angriffsresistenz muss jedoch in jedem Fall nach dem aktuellen Stand der Technik neu bewertet werden und auch Audits der Entwicklungs- und Produktionsumgebung müssen nach zwei Jahren erneut durchgeführt werden. Handelt es sich um eine Änderung mit überschaubarem Umfang („minor change"), kann ein bestehendes Zertifikat auf die neue Version erweitert werden.[78]

### 2. Anerkennung von Zertifizierungen

79 In Deutschland regelt § 9 Abs. 7 BSIG, dass das BSI grundsätzlich Sicherheitszertifikate anderer anerkannter Zertifizierungsstellen aus der EU anerkennt, „soweit sie eine den Sicherheitszertifikaten des Bundesamtes gleichwertige Sicherheit ausweisen und die Gleichwertigkeit vom Bundesamt festgestellt worden ist." Hier kommen die internationalen Abkommen SOG-IS MRA und CCRA (→ Rn. 80 ff.) zum Tragen, welche das BSI unterzeichnet hat. Die Anerkennung eines Zertifikats kann das BSI verwehren, wenn das Bundesministerium des Innern, für Bau und Heimat festgestellt hat, dass der Anerkennung überwiegende öffentliche Interessen – insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland – entgegenstehen (§ 9 Abs. 4 Satz 2 BSIG). Standortzertifikate unterliegen grundsätzlich nicht der Anerkennung durch das BSI.

#### a) CCRA

80 Das Common Criteria Recognition Arrangement (CCRA) ist eine internationale Vereinbarung, die die **gegenseitige Anerkennung gemeinsam entwickelter CC Schutzprofile** (collaborative Protecion Profiles, ccP) und Zertifikate für IT-Produkte gewährleistet. In der Vereinbarung erklären sich die unterzeichnenden Staaten bereit, die Ergebnisse der CC-Bewertungen durch andere CCRA-Mitglieder zu akzeptieren.

81 Einige Mitglieder **stellen Zertifikate aus und erkennen sie an** („Authorizing"). Dazu gehören unter anderem Australien, Frankreich, Großbritannien, Deutschland, Japan, Kanada, die Niederlande, Großbritannien oder die USA. Andere Mitglieder erkennen Zertifikate an, stellen aber selbst keine aus und führen keine Zertifizierungen durch („Consuming"). Dazu gehören unter anderem Österreich, die Tschechische Republik, Dänemark, Finnland, Ungarn, Israel, Katar und Singapur.[79]

82 Innerhalb der CCRA werden jedoch nur Bewertungen bis zum **niedrigen EAL 2 gegenseitig anerkann**t. Die europäischen Länder erkennen im Rahmen des früheren ITSEC-Abkommens in der Regel auch höhere EALs an.

#### b) SOG-IS MRA

83 Auf europäischer Ebene kooperieren die im Rahmen der IT-Sicherheit kompetenten Stellen von Mitgliedstaaten der EU und der European Free Trade Association (EFTA), beispielsweise

[77] Eckert, 2009, S. 237 f.

[78] BSI, [VB-Produkte].

[79] Common Criteria Portal, abrufbar unter https://www.commoncriteriaportal.org/index.cfm.

das deutsche BSI oder das französische ANSSI, innerhalb der Senior Officials Group Information Systems Security (SOG-IS). Die Behörden arbeiten innerhalb des SOG-IS MRA zusammen, um die Standardisierung von CC-Schutzprofilen und Zertifizierungsrichtlinien zwischen den europäischen Zertifizierungsstellen zu koordinieren und dadurch einen gemeinsamen Standpunkt innerhalb der internationalen CCRA-Gruppe zu vertreten. Außerdem empfiehlt das SOG-IS MRA sogenannte „empfohlene" Schutzprofile, die im Interesse aller Mitglieder und untereinander abgestimmt sind und von der EU verpflichtend vorgeschrieben werden können, zum Beispiel im Rahmen einer EU-Richtlinie. Zertifikatserzeugende Nationen erkennen untereinander Zertifikate bis EAL4 an, also zwei Stufen höher als innerhalb des CCRA.[80]

### III. Gesetzliche Regelungen zur Bewertung, Prüfung und dem Nachweis von IT-Sicherheit von IT-Produkten, Diensten und Prozessen

84 Hersteller und Anbieter von **IKT-Produkten und Diensten** sind in mehreren Bereichen zur Einhaltung und zum Nachweis technischer Maßnahmen für die IT-Sicherheit verpflichtet. Gesetzliche Anforderungen an die IT-Sicherheit von IKT-Produkten und Diensten ergaben sich bisher meistens aus bereichsspezifischen Gesetzen, etwa § 22 MsbG für intelligente Stromzähler, § 291 b SGB V für die Telematikinfrastruktur im Gesundheitsbereich oder § 3 PAuswV für den elektronischen Personalausweis. Auf EU-Ebene gelten seit 2014 zudem IT-Sicherheitsanforderungen für Identifizierungssysteme und Vertrauensdienste.[81] Der im Juni 2019 in Kraft getretene Rechtsakt zur Cybersicherheit der Europäischen Union schafft als erstes Gesetz ein allgemeines Rahmenwerk für die Zertifizierung der IT-Sicherheit von IKT-Produkten, Diensten und Prozessen.

#### 1. Fachspezifische Regelungen

85 Im deutschen IT-Sicherheitsrecht existieren zahlreiche bereichspezifische Regelungen, die IT-Sicherheitsanforderungen und darauf basierende Konformitätsbewertungen für IT-Produkte und Dienste vorschreiben.

86 Nach § 22 Abs. 1 und 2 MsbG müssen **Hersteller** von **Smart-Meter-Gateways** Mindestanforderungen an die IT-Sicherheit umsetzen und diese nach entsprechenden CC-Schutzprofilen und Technischen Richtlinien (TR) des BSI zertifizieren lassen[82]. Das Zertifikat müssen Hersteller dem Smart-Meter-Gateway Administrator vorlegen. Auch für die Interoperabilität des Smart-Meter-Gateways besteht eine Zertifizierungspflicht zum Nachweis der Konformität mit entsprechenden Technischen Richtlinien des BSI.

87 Auch für die **elektronische Gesundheitskarte und die Telematikinfrastruktur** bestehen laut § 291 b SGB V IT-Sicherheitsanforderungen, deren Einhaltung durch eine Zertifizierung nachzuweisen ist. Laut § 291 b Abs. 1 a SGB V werden die Komponenten und Dienste der Telematikinfrastruktur von der Gesellschaft für Telematik zugelassen. Die Gesellschaft für Telematik prüft die Funktionsfähigkeit und Interoperabilität. Der Nachweis der IT-Sicherheit erfolgt nach den Vorgaben des BSI. Für die Gesundheitskarte und Telematikinfrastruktur hat das BSI

[80] SOG-IS, abrufbar unter: https://www.sogis.eu/.

[81] S. näher Roßnagel in → § 14 Rn. 1 ff.

[82] Bundesamt für Sicherheit in der Informationstechnik, Übersicht über die Schutzprofile und Technischen Richtlinien nach § 22 Abs. 2 Satz 1 MsbG, abrufbar unter: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/UebersichtSP-TR/uebersicht_node.html; s. näher Singler in → § 24 Rn. 1 ff.

entsprechend CC-Schutzprofile sowie TR entwickelt, nach denen die einzelnen Komponenten von anerkannten Prüfstellen evaluiert und darauf aufbauend vom BSI zertifiziert werden[83].

Bestimmte **Systemkomponenten der Personalausweisbehörden, des Ausweisherstellers und der Diensteanbieter und ihrer Auftragnehmer** müssen nach § 3 PAuswV ebenfalls nach TR des BSI zertifiziert werden. Für elektronische Ausweisdokumente sowie die Lesegeräte, dazugehörigen Prozesse und Protokolle bestehen mehrere Schutzprofile und TRs des BSI.[84] 88

### 2. Identifizierungsdienste und Vertrauensdienste

Auf EU-Ebene ist die Sicherheit von **Identifizierungsdiensten und Vertrauensdiensten** im Rahmen der **eIDAS Verordnung** (EU) Nr. 910/2014 geregelt, welche ebenfalls Konformitätsbewertungsverfahren vorsieht.[85] Die Sicherheitsniveaus elektronischer **Identifizierungssysteme** (eID-Systeme) klassifiziert die eIDAS-VO auf Grundlage eines **risikobasierten Ansatzes** in die Stufen „niedrig“, „substanziell“ und „hoch“ (Art. 8 eIDAS-VO). Das BSI hat die Ausgestaltung der Sicherheitsniveaus in einem offiziellen „Mapping“[86] spezifiziert und entsprechende TR[87] erlassen, welche als Prüf- und Bewertungsgrundlage für Identifizierungsdienste durch das BSI dienen. Im Rahmen der **Notifizierung** eines eID-Systems muss ein Mitgliedstaat gemäß Art. 9 eIDAS-VO relevante Informationen über das eID-System, dessen Sicherheitsniveau sowie über die Aufsichtsstrukturen an die EU-Kommission übermitteln. Die EU-Kommission kann darauf basierend eine Konformitätsbestätigung vornehmen. Ist ein eID-System auf dem Vertrauensniveau substanziell oder hoch notifiziert, muss der jeweilige Mitgliedstaat auch alle anderen europäischen notifizierten Systeme mit dem gleichen Sicherheitsniveau für die Authentifizierung für öffentliche Dienstleistungen akzeptieren. Somit soll die gegenseitige Anerkennung nationaler eID-Systeme gewährleistet werden. 89

**Qualifizierte Vertrauensdiensteanbieter** wie zum Beispiel Anbieter elektronischer Signaturen müssen gemäß Art. 20 eIDAS-VO ebenfalls eine Konformitätsprüfung durchlaufen, die mindestens alle zwei Jahre wiederholt wird. Die Prüfung bezieht sich auf die Implementierung der technischen und organisatorischen IT-Sicherheitsmaßnahmen nach dem jeweils neuesten Stand der Technik und muss gemäß Art. 20 eIDAS-VO von einer staatlich akkreditierten Konformitätsbewertungsstelle durchgeführt werden. Relevante Normen hat die EU-Kommission in einem Durchführungsbeschluss spezifiziert.[88] **Qualifizierte elektronische Signaturerstellungseinheiten** müssen gemäß Art. 30 eIDAS-VO durch eine von dem Mitgliedsstaat öffentliche oder private benannte Stelle zertifiziert werden. Nach Erwägungsgrund 55 eIDAS-VO soll die Zertifizierung möglichst auf Grundlage der CC erfolgen. Die Anforderungen an Vertrauensdienste beschreibt *Roßnagel* in → § 14 Rn. 7 ff. 90

[83] Bundesamt für Sicherheit in der Informationstechnik, Übersicht der Schutzprofile und der Technische Richtlinien für "eHealth VSDM", abrufbar unter: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eHealth/Schutzprofile_TR/schutzprofile_tr_node.html.

[84] Bundesamt für Sicherheit in der Informationstechnik, Schutzprofile im Kontext elektronische Ausweise, https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/ElektronischeIdentitaeten/Schutzprofile/schutzprofile_node.html.

[85] Dazu umfassend Roßnagel in → § 14 Rn. ■■■.

[86] Bundesamt für Sicherheit in der Informationstechnik, German eID based on Extended Access Control v2 – LoA mapping: Mapping of the characteristics of the German eID scheme to the eIDAS Level of Assurance, 20.2.2017.

[87] TR-03107–1 und TR-03107–2.

[88] Durchführungsbeschluss (EU) 2016/650 der Kommission vom 25.4.2016 zur Festlegung von Normen für die Sicherheitsbewertung qualifizierter Signatur- und Siegelerstellungseinheiten gemäß Artikel 30 Absatz 3 und Artikel 39 Absatz 2 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt.

### 3. Allgemeines Rahmenwerk zur Zertifizierung von IT-Produkten, Diensten und Prozessen nach dem Rechtsakt zur Cybersicherheit der Europäischen Union

91 Mit dem im Juni 2019 verabschiedeten Rechtsakt zur Cybersicherheit der Europäischen Union VO (EU) Nr. 881/2019, auch EU Cybersicherheitsakt (CSA) genannt[89], haben die EU Institutionen und Mitgliedsstaaten erstmals einen Rahmen für die Ausarbeitung spezifischer Zertifizierungsschemata für bestimmte IKT-Produkte[90], -Dienste[91] und -Prozesse[92] errichtet (Art. 43–54 CSA). Mit der Schaffung von einheitlichen Anforderungen soll der CSA den Markt für zertifizierte Produkte stärken. Die Zertifizierungsschemata folgen einem **risikobasierten Ansatz** und sollen überprüfbare IT-Sicherheits-Anforderungen auf **drei unterschiedlichen Vertrauenswürdigkeitsstufen** definieren: niedrig, mittel und hoch (Art. 46 CSA-VO). Die Stufe „niedrig“ beschränkt sich auf die Minimierung von bekannten Cybersicherheitsrisiken und -vorfällen und eine Bewertung anhand mindestens einer Durchsicht einer technischen Dokumentation (Art. 52 Abs. 5 CSA-VO). Für diese Stufe ist eine Selbstbewertung der Konformität durch den Hersteller möglich (Art. 53 CSA-VO). Auf der Stufe „mittel“ sollen bekannte Cyberrisiken, Cybervorfälle und Cyberangriffe von Akteuren mit begrenzten Fähigkeiten und Ressourcen minimiert sein und eine Angreifbarkeit über öffentlich bekannte Schwachstellen ausgeschlossen werden können (Art. 52 Abs. 5 CSA-VO). Für das Vertrauenswürdigkeitsniveau „mittel“ ist eine Zertifizierung durch eine anerkannte Konformitätsbewertungsstelle erforderlich (Art. 56 Abs. 4 CSA-VO). Ein Zertifikat, welches der Stufe „hoch“ entspricht, bietet Gewissheit, dass das jeweilige Produkt, der Dienst oder der Prozess einer Bewertung unterzogen wurde, die darauf ausgerichtet ist, das Risiko von dem neuesten Stand der Technik entsprechenden Cyberangriffen durch Akteure mit umfangreichen Fähigkeiten und Ressourcen möglichst gering zu halten. Eine Prüfung in diesem Rahmen erfordert zum Beispiel neben der Prüfung des Produktes oder Dienstes auf bekannte Schwachstellen und Sicherheitsfunktionalitäten nach dem Stand der Technik auch Penetrationstests (Art. 52 Abs. 7 CSA). Diese Stufe kann für Komponenten Kritischer Infrastrukturen (nach Definition der EU-Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit, in Deutschland umgesetzt durch das IT-Sicherheitsgesetz) genutzt werden. Für die Stufe „hoch“ ist eine Zertifizierung durch eine nationale Cybersicherheits-Zertifizierungsbehörde oder eine Konformitätsbewertungsstelle erforderlich (Art. 56 Abs. 6 CSA).

92 Die Zertifizierungsschemata sollen durch die EU-Cybersicherheitsbehörde **ENISA** in **Konsultation** mit den relevanten **Stakeholdern**, insbesondere den nationalen Cybersicherheitsbehörden wie dem BSI, erarbeitet werden. Die EU-Kommission entscheidet über die Annahme der Schemata und erlässt dazu einen entsprechenden **Durchführungsrechtsakt** nach Art. 49 Abs. 7 CSA.

93 Die Zertifizierung von Produkten, Diensten und Prozessen nach einem Schema ist **freiwillig,** sofern nicht anderweitig im Unionsrecht oder nationalem Recht festgelegt. Innerhalb jedes Zertifizierungsschemas soll die Höchstdauer der Zertifikate definiert werden, typischerweise sollte diese für die Dauer von einem bis drei Jahren reichen. Nach Ablauf der Frist sind die

[89] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17.4.2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit).

[90] „IKT-Produkt“ bezeichnet jedes Element oder jede Gruppe von Elementen von Netz- und Informationssystemen (Art. 2 Nr. 12 CSA-VO).

[91] „IKT-Dienst“ bezeichnet jeden Dienst, der ganz oder überwiegend aus der Übertragung, Speicherung, dem Abruf oder der Verarbeitung von Informationen über ein Netzwerk und Informationssysteme besteht (Art. 2 Nr. 13 CSA-VO).

[92] „IKT-Prozess“ bezeichnet eine Reihe von Tätigkeiten, die zur Entwicklung, Bereitstellung und Wartung eines IKT-Produkts oder -Dienstes durchgeführt werden (Art. 2 Nr. 14 CSA-VO).

Zertifikate verlängerbar. Zertifizierungsverfahren und Datenschutzsiegel gemäß der DSGVO bleiben vom CSA gemäß dessen Erwägungsgrund 74 unberührt.

**Nationale Schemata** für die IT-Sicherheitszertifizierung und die zugehörigen Verfahren für die IKT-Produkte, -Dienste und -Prozesse, die unter ein europäisches Schema für die Cybersicherheitszertifizierung fallen, werden nach Erlass eines entsprechenden Durchführungsrechtsaktes für das europäische Schema **unwirksam** (Art. 57 CSA). 94

Obwohl der CSA die Zertifizierung reguliert, setzt er **keine gemeinsamen Regeln für die Marktüberwachung** von Produkten, Diensten und Prozessen auf – mit Ausnahme einer Website, auf der Informationen zu den Zertifikaten erscheinen sowie einer von den jeweiligen Herstellern betriebene Website mit Sicherheitsinformationen (Art. 44 CSA). Laut dem CSA obliegt die Marktüberwachung jeweils den nationalen Cybersicherheitsbehörden. Im Cybersicherheitsbereich fallen unter die zu beaufsichtigten Tätigkeiten zum Beispiel das Schließen von Sicherheitslücken durch den Hersteller sowie die Sanktionierung im Fall einer Nichteinhaltung der Anforderungen. 95

Der CSA schafft zwar die Voraussetzung für die Erarbeitung von Zertifizierungs-Schemata. Bisher ist jedoch unklar, **welche Kategorien von Produkten und Diensten** unter dem CSA zertifiziert werden sollen. Sollen hauptsächlich Produkte, Prozesse und Dienste aus dem Consumer IoT zertifiziert werden oder auch Komponenten von Kritischen Infrastrukturen? Der CSA eignet sich insbesondere dazu, grundlegende Security-Anforderungen an IKT-Produkte, Dienste und Prozesse zu stellen, die für einen Vertrieb auf dem EU-Binnenmarkt eingehalten werden müssen. In diesem Kontext stellt sich ebenfalls die Frage, ob die Schemata auf bereits im Rahmen der Regulierungen des **New Legislative Framework** (**NLF**, → Rn. 12) regulierte Produkte und Dienste angewandt werden, beispielsweise Medizinprodukte. 96

Des weiteren ist bisher unklar, wie der **„Stand der Technik“** für die Anforderungen der Sicherheitsniveaus **ausgestaltet** werden sollen und **wie die Sicherheitsniveaus international vergleichbar** sein werden. Um internationale Vergleichbarkeit zu gewährleisten, müssten die in den Sicherheitsniveaus definierten Anforderungen auf internationalen Standards basieren und die Entstehung von parallelen, markthinderlichen heterogenen Sicherheitsstandards vermeiden. Dies wird die ENISA bei der Erarbeitung der Schemata zu berücksichtigen haben. 97

Damit hängt ebenfalls die Frage zusammen, ob der CSA die Zertifizierung von Diensten, Produkten und Systemen **skalierbarer** gestalten können wird. Den mit einer Produktzertifizierung, insbesondere nach CC, verbundenen hohen finanziellen und zeitlichen Aufwand können nur wenige Hersteller und Anbieter leisten. Im „Internet der Dinge“ mit Millionen heterogener Geräte ist dieses Modell der Konformitätsbewertung nur schwer skalierbar. Daher stellt sich die Frage, inwiefern der CSA auf weniger aufwändige Bewertungskriterien und -verfahren zurückgreifen wird. Alternativ könnten, wie die europäische Cybersicherheitsagentur ENISA vorschlägt, modulare Prüf- und Zertifizierungsverfahren angewendet werden, in denen einzelne Sicherheitselemente zertifiziert sind, welche in vielen unterschiedlichen Produkten und Systemen eingesetzt werden.[93] Die überarbeiteten Common Criteria (Normenreihe ISO/IEC 15408) bieten bereits einen flexiblen Ansatz für die Bewertung von IoT-Produkten, die „composite evaluation“ oder „zusammengesetzte Bewertung“, welche auch die ENISA in ihrer Analyse von IoT Standards vorschlägt. 98

[93] Vgl. European Union Agency for Cybersecurity, 2017.

### 4. Ergänzungen aus dem Entwurf für ein IT-Sicherheitsgesetz 2.0

99 Laut einem öffentlich bekannt gewordenen ersten Entwurf des BMI für ein IT-Sicherheitsgesetz 2.0[94] sollen Hersteller von **KRITIS-Kernkomponenten**, welche unmittelbar für den Betrieb der kritischen Anlage notwendig sind oder deren Störung eine Störung der kritischen Dienstleistungen bewirken würde, vor deren Vertrieb eine **Vertrauenswürdigkeitserklärung** über die gesamte Lieferkette abgeben (Art. 1 Ziff. 13 lit. b RefE). Die Vertrauenswürdigkeit des Herstellers, einschließlich seines Personals und des Entwicklungsprozesses, kann durch ein Zertifizierungsverfahren aber nicht überprüft werden. Daher schlägt die Bundesregierung dieses Instrument vor, welches nach den Enthüllungen über die Tätigkeiten ausländischer Nachrichtendienste durch Edward Snowden sowie im Kontext der Debatte um den Einsatz chinesischer Netzwerkkomponenten in Mobilfunknetzen an politischer Bedeutung gewonnen hat. Den genauen Inhalt dieser Erklärung soll das Bundesministerium des Innern, für Bau und Heimat (BMI) bestimmen (Art. 1 Ziff. 13 lit. b RefE). Als Orientierung können „no-spy-Klauseln“ für Vergabeverfahren[95] der Bundesregierung und eine Handreichung einer „technischen no-spy-Klausel“[96] aus den vergangenen Jahren dienen. Diese Pflicht soll ein zusätzlicher Absatz 6 in § 8 a BSIG bestimmen. In Bereichen, in denen aufgrund von Gesetzen die KRITIS-Kernkomponenten einer Zertifizierung zu unterziehen sind – wie es beispielsweise bei Telekommunikationsausrüstung durch eine Änderung des TKG geplant ist –, soll die Abgabe der Vertrauenswürdigkeitserklärung [nach dem mit dem RefE geplanten neuen § 8 Abs. 6 Satz 3 BSIG] Voraussetzung für die Zertifizierung sein (Art. 1 Ziff. 17 RefE). Diese Pflicht soll in § 9 BSIG durch einen neuen Absatz 8 verankert werden.

100 Außerdem plant das BMI im Rahmen des IT-Sicherheitsgesetzes 2.0 die Einführung eines **freiwilligen IT-Sicherheitskennzeichens**, welches in einem neuen § 9 a BSIG geregelt werden soll (Art. 1 Ziff. 18 RefE). Demnach soll das BSI nach Maßgabe einer Rechtsverordnung auf Antrag ein einheitliches IT-Sicherheitskennzeichen für verschiedene Produktkategorien erteilen. Die Nutzung des IT-Sicherheitskennzeichens soll für Hersteller und Produkte freiwillig sein.

101 Laut Gesetzentwurf soll das Kennzeichen beinhalten

- „eine Erklärung des Herstellers der jeweiligen Produkte, in welcher dieser das Vorliegen bestimmter IT-Sicherheitseigenschaften des Produkts für zutreffend erklärt (Herstellererklärung), und
- eine Information des Bundesamtes über Sicherheitslücken oder sonstige Informationen über sicherheitsrelevante IT-Eigenschaften (BSI-Sicherheitsinformation).“

102 Grundlage für die Erklärung sollen die jeweilige Produktkategorie umfassenden Technische Richtlinien des BSI sein – soweit solche vorliegen. Auch branchenabgestimmte IT-Sicherheitseigenschaften können im Rahmen der **Herstellererklärung** nach einer Eignungsfeststellung durch das BSI verwendet werden. Das BSI würde laut (dem neuen) § 9 a Abs. 3 BSIG auf Antrag die Freigabe zur Nutzung des Kennzeichens erteilen. Die **Prüfung des Herstellerversprechens** soll auch durch einen **qualifizierten Dritten** erfolgen können. Laut (dem neuen) § 9 a Abs. 6 BSIG soll das BSI in regelmäßigen Abständen sowie anlassbezogen prüfen können, ob die Vorgaben des IT-Sicherheitskennzeichens eingehalten werden. Bei Feststellung von Abweichungen vom Herstellerversprechen oder Sicherheitslücken kann das BSI Informationen

[94] Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat (BMI) v. 27.3.2019, abrufbar unter: http://intrapol.org/wp-content/uploads/2019/04/IT-Sicherheitsgesetz-2.0-_-IT-SiG-2.0.pdf. Überblick: Voigt, 2019.

[95] Bundesministerium des Innern, für Bau und Heimat, Handreichung zum Erlass an das Beschaffungsamt des BMI (BeschA) (Erlass vom 30.4.2014, O4–11032/23#14).

[96] CIO der Bundesregierung, 2018, Handreichung zur „technischen no-spy-Klausel“.

darüber in geeigneter Weise darstellen (BSI-Sicherheitsinfo) oder die Freigabe zur Nutzung des IT-Sicherheitskennzeichens widerrufen.

Wie dieses Kennzeichen und die dazugehörigen Anforderungen mit den in dem **EU-Rechtsakt zur Cybersicherheit** vorgesehenen Zertifizierungsschemata zusammenhängen werden, wird im Gesetzentwurf und der Begründung nicht thematisiert. Um Parallelstrukturen zu vermeiden, wird in dieser Hinsicht eine Abstimmung erforderlich sein. 103

## IV. Zusammenfassung und Ausblick

Für die Evaluierung und Bewertung der IT-Sicherheitseigenschaften von Software und Hardware existieren mehrere Kriterienkataloge. Die am weitesten verbreitete Grundlage bilden die Common Criteria. Das BSI kann gemäß § 9 BSIG Zertifikate für die IT-Sicherheit von IT-Produkten, Systemen und Diensten erteilen. Voraussetzung dafür ist eine erfolgreiche Prüfung durch eine anerkannte Prüfstelle. Gesetzlich war die IT-Sicherheit von IT-Produkten, Diensten und Prozessen lange nicht übergreifend, sondern nur fachspezifisch reguliert. Seit 2019 stellt der EU-Rechtsakt zur Cybersicherheit ein Rahmenwerk für die Erstellung von Zertifizierungsschemata auf EU-Ebene zur Verfügung, die je nach weiterem Vorgehen der EU-KOM die nationalen Kriterienkataloge sukzessive ersetzen könnten. 104

Die Zertifizierung hat sich über Jahre hinweg als Instrument zur Qualitätssicherung von Produkten und Systemen bewährt. Die wachsende **Komplexität** von IT-Produkten und Systemen, deren zunehmende Verbreitung im Alltag und der hohe mit der Zertifizierung verbundene Aufwand stellen sie als taugliches Instrument jedoch zunehmend in Frage. Dies gilt insbesondere im Zeitalter des „Internet der Dinge“, in dem alltägliche Nutzgegenstände und Infrastrukturen vernetzt werden. Zudem verschwimmen Grenzen zwischen IT-Produkten, -Diensten und -Prozessen zunehmend durch die **Virtualisierung** von Funktionalitäten, welche vorher an Hardware gebunden war. 105

Zudem verschwimmen Grenzen zwischen „**Safety**“ (also funktionaler Sicherheit) und **IT-Sicherheit**. Die Methoden zur Bewertung und Prüfung von Safety und IT-Sicherheit von Systemen haben sich im Laufe der Zeit separat entwickelt. Safety-Mechanismen befassen sich hauptsächlich mit unbeabsichtigten Bedrohungen, die durch Naturkatastrophen, technische Ausfälle oder menschliches Versagen verursacht werden. IT-Sicherheitsmechanismen adressieren vorsätzliche Bedrohungshandlungen, die beispielsweise Systemschwachstellen ausnutzen. Das Ausmaß der Bedrohung hängt dabei von den Bedrohungsakteuren und ihren Fähigkeiten, Absichten und ihrer Motivation sowie von den Schwachstellen im System ab. Daher sind Cyberbedrohungen höchst dynamisch – sie entwickeln sich ständig weiter. Jederzeit kann eine neue Schwachstelle gefunden oder eine neue Angriffstechnik bekannt werden. IT-Sicherheitsangriffe nutzen oft die Existenz von unspezifiziertem Verhalten aus. 106

Daher können IT-Sicherheitsrisiken nicht nur durch statische Risikobewertungs- und -management-Methoden, wie zB Funktionstests, auf das Vorhandensein von einem spezifischen Verhalten sowie statische Ausfallratenberechnungsmethoden, erfasst und kontrolliert werden. Eine zentrale Herausforderung ist daher – für Safety-relevante Produkte – die **Kombination von Safety und Security in Prüf- und Zertifizierungsverfahren**.[97] Dies wird in besonderem Maße bedeutsam für IT-Systeme, deren Betrieb mit Gefahren für Leib und Leben verbunden ist, wie etwa autonome Fahrzeuge oder vernetzte Medizinprodukte. 107

Eine fundamentale Herausforderung der Zertifizierung ist außerdem, dass Software dynamisch ist und kontinuierlich Updates zum Schließen von Schwachstellen oder zur Verbesserung von ihrer Funktionalität erfordert. Da Zertifizierung im Grundsatz statisch ist, dh die 108

[97] Vgl. Leverett/Clayton/Anderson, 2017; vgl. Kriaa, 2016; vgl. Hänninen/Hansson/Thane/Saadatmand, 2016.

Erfüllung von Anforderungen zu einem bestimmten Zeitpunkt feststellt, muss die Wartung von Produkten und Diensten durch Updates anders gehandhabt werden. Die wiederholte Prüfung oder Re-Zertifizierung eines Produkts nach jedem Software-Update ist wegen des damit verbundenen Aufwandes nicht skalierbar. Diese Herausforderungen muss ein auf IKT ausgerichtetes Zertifizierungs-Rahmenwerk bewältigen. Zukünftige Prüf- und Nachweismechanismen müssen diesen Konflikt zwischen einmaliger Zertifizierung und der konstanten Softwareentwicklung auflösen.[98] Daher werden Ansätze benötigt, die die Aussagekraft von Zertifikaten über die gesamte Produktlebensdauer erhalten und die wachsende Komplexität von Technologien abbilden kann. Entsprechende Ansätze existieren bereits in der Fachliteratur.[99]

[98] Vgl. Kleinhans, 2016.

[99] Vgl. Krcmar/Eckert/Roßnagel/Sunyaev/Wiesche (Hrsg.) Management sicherer Cloud-Services. Entwicklung und Evaluation dynamischer Zertifikate, 2018; Aus rechtlicher Sicht außerdem Hofmann Dynamische Zertifizierung – Datenschutzrechtliche Zertifizierung nach der Datenschutz-Grundverordnung am Beispiel des Cloud Computings, 2019.

# Curriculum vitae

## Personal data

| | |
|---|---|
| Name: | Isabel Skierka-Canton |
| Date of birth: | 25.05.1989 |
| Place of birth: | Hamburg, Germany |
| Citizenship: | German |

## Contact data

| | |
|---|---|
| E-mail: | Isabel.skierka-canton@proton.me |

## Education

| | |
|---|---|
| 2018–2023 | Tallinn University of Technology – PhD studies (Public Administration) part-time / external |
| 2011–2012 | Department of War Studies, King's College London – MA, with distinction (International Conflict Studies)<br>- German Academic Exchange Service (DAAD) Scholarship for graduate students |
| 2010–2011 | Institut d'Etudes Politiques (Sciences Po) Paris – BA Exchange semester<br>- German Academic Exchange Service (DAAD) Scholarship for undergraduate students |
| 2008–2011 | Maastricht University – BA, with distinction (European studies)<br>- Top 3% Prize 2010/2011<br>- MARBLE Research Programme<br>- Honours Programme |
| 2006–2007 | Lycée Descartes Tours – Baccalauréat de Français Niveau Première Littéraire (High school year abroad) |
| 1999–2008 | Gymnasium Eppendorf – Abitur (High school) |

## Language competence

| | |
|---|---|
| German | Native |
| English | Fluent |
| French | Fluent |
| Spanish | Intermediate |

## Professional employment and affiliations

| | |
|---|---|
| 2016–… | Digital Society Institute, European School of Management and Technology (ESMT) Berlin – Researcher (2016-…) and Program Lead for Technology Politics (2020-…)<br>- Interdisciplinary research and consulting on strategic technology policy, cybersecurity, IT security & risk management, e-governance, digital identity with and for government partners, private companies, foundations, think tanks |
| 2014–2016 | Global Public Policy Institute – Research Associate, Internet Politics |
| 2014–2014 | NATO Headquarters, Smart Defence Initiative – Carlo Schmid Fellow |
| 2013–2014 | DG Connect, European Commission, Task Force for Internet Policy Development – Blue Book Trainee |

| | |
|---|---|
| 2013–2013 | Institute of Computer Science, Free University of Berlin – Research and Teaching Fellow |
| 2012–2013 | German Marshall Fund of the United States, Berlin – Intern and Research Assistant |

**Affiliations and memberships**

| | |
|---|---|
| 2021–… | Forum for New Security Politics - Heinrich-Böll-Stiftung – Member |
| 2017–… | Transatlantic Cyber Forum of Stiftung Neue Verantwortung – Member |
| 2016–… | GPPi – Non-Resident Fellow |
| 2016–2019 | Internet Governance Forum Germany – Next-Generation-Co-Chair and member of the Steering Committee |

**Publications (selected)**

***Books and Book Chapters***

**Skierka, I.** (2022). Digitale Identitäten. In F. N. Tanja Klenk Göttrik Wewer (Ed.), *Handbuch Digitalisierung in Staat und Verwaltung, 2nd edition* (pp. 1–12). Springer VS. https://doi.org/10.1007/978-3-658-23669-4_66-1

Lahmann, H., & **Skierka, I.** (2022). Cybersecurity in the Trade and Cooperation Agreement between the EU and the United Kingdom. In *Handbuch Handels- und Kooperationsvertrag EU/GB* (pp. 619–638). Nomos.

**Skierka, I.** (2021). Messung, Prüfung und Nachweis von IT-Sicherheit. In M. S. Gerrit Hornung (Ed.), *Handbuch IT-Sicherheitsrecht* (pp. 154–180). Nomos (Verlag). https://www.beck-shop.de/hornung-schallbruch-it-sicherheitsrecht/product/30826832

Schallbruch, M., & **Skierka, I.** (2018). *Cybersecurity in Germany*. Springer. https://doi.org/10.1007/978-3-319-90014-8

Benner, T., & **Skierka, I.** (2015). Digitale Souveränität—Begriffsdefinition. In W. V. Woycke Johannes (Ed.), *Handwörterbuch Internationale Politik* (Vol. 13, pp. 45–49). Verlag Barbara Budrich. https://books.google.ee/books?id=tKqeDQAAQBAJ&lpg=PP1&ots=h12WVslV2F&dq=warwick%20handw%C3%B6rterbuch%20internationale%20politik&pg=PA45#v=onepage&q&f=false

***Articles (journal articles, conference papers, policy papers)***

**Skierka, I.**, & Parycek, P. (2023). Einwurf – Kann Deutschland seine eID noch retten? *HMD Praxis der Wirtschaftsinformatik*, 1–6. https://doi.org/10.1365/s40702-023-00958-0

**Skierka, I.** (2023). When shutdown is no option: Identifying the notion of the digital government continuity paradox in Estonia's eID crisis. *Government Information Quarterly*, *40*(1), 101781. https://doi.org/10.1016/j.giq.2022.101781

**Skierka, I.** (2021). Governing the Digital ID: How Germany and the EU plan to reclaim our digital sovereignty. In *ESMT Update Summer 2021* (pp. 32–35). ESMT Berlin. https://esmt.berlin/sites/main/files/2021-06/ESMT_Update_Summer_2021.pdf

Schallbruch, M., **Skierka, I.**, & Strüve, T. (2020). Digital identity in 2020—Conference. In *Konferenzpapier -Digitale Identitäten* (pp. 1–6). European School of Management and Technology Berlin. http://static.esmt.org/publications/Reports/dsi-ipr_2020-1_de-en.pdf

**Skierka, I.** (2020). 5G and beyond: A test for "technological sovereignty" in Europe? In *The Convergence Puzzle: Australia, Germany and Emerging Cybersecurity Trends* (pp. 37–44). Konrad Adenauer Foundation. https://www.kas.de/documents/274425/8492225/Periscope+Volume+3+-+5G+and+Beyond.pdf/48229669-0e6e-a44a-e75c-4478d67027d3?t=1589163346668

**Skierka, I.** (2018). *The governance of safety and security in connected healthcare in Europe*. 1–12. https://doi.org/10.1049/cp.2018.0002

**Skierka, I.**, & Schallbruch, M. (2018). *Requirements for a German 'Blockchain Strategy'* (pp. 1–14). http://static.esmt.org/publications/Reports/dsi-ipr_2018-3_en-de.pdf

**Skierka, I.** (2017). Cybersecurity International – Unterschiedliche Prioritäten. In *Digitalpolitik – Eine Einführung* (pp. 19–26). Wikimedia e.V. and iRights. https://irights.info/wp-content/uploads/2017/05/Digitalpolitik_-_Eine_Einfuehrung.pdf

**Skierka, I.** (2016). *Military Cybersecurity, the German way*. *3*, 37–42. https://www.globalpolicyjournal.com/projects/gp-e-books/digital-debates-cyfy-journal-volume-3-2016

**Skierka, I.** (2015). *Amerika abwickeln* (pp. 138–141). DGAP. https://internationalepolitik.de/de/amerika-abwickeln

**Skierka, I.** (2015). *Krieg der Knöpfe* (pp. 134–138). https://internationalepolitik.de/de/krieg-der-knoepfe

**Skierka, I.**, & Gaycken, S. (2015). *Cybertaktik und Cyberstrategie* (pp. 1–202). Free University of Berlin. http://www.inf.fu-berlin.de/inst/ag-si/pub/Cybertaktik_und_Strategie.pdf

**Skierka, I.**, Morgus, R., Hohmann, M., & Maurer, T. (2015). *CSIRT Basics for Policy-Makers: The History, Types & Culture of Computer Security Incident Response Teams* (pp. 1–29). https://www.gppi.net/media/CSIRT_Basics_for_Policy-Makers_May_2015_WEB.pdf

Maurer, T., **Skierka, I.**, Morgus, R., & Hohmann, M. (2015). *Technological sovereignty: Missing the point?* 53–68. https://doi.org/10.1109/CYCON.2015.7158468

Morgus, R., **Skierka, I.**, Hohmann, M. & Maurer, T. (2015). *National CSIRTs and their role in computer security incident response* (pp. 1–33). http://www.digitaldebates.org/fileadmin/media/cyber/National_CSIRTs_and_Their_Role_in_Computer_Security_Incident_Response__November_2015_--_Morgus__Skierka__Hohmann__Maurer.pdf

**Skierka, I.** (2014). *Die Illusion vom „sauberen Krieg"* (pp. 134–137). DGAP. https://internationalepolitik.de/de/die-illusion-vom-sauberen-krieg

Drott, L., Jochum, L., Lange, F., **Skierka, I.**, Vach, J., & van Asselt, M. B. A. (2013). Accountability and risk governance: A scenario-informed reflection on European regulation of GMOs. *Journal of Risk Research*, *16*(9), 1123–1140. https://doi.org/10.1080/13669877.2012.743161

***Other publications (Op-Eds, Expert Testimonies)***

Tiirmaa-Klaar, H. & **Skierka, I.** (2023). Germany's National Security Strategy: A Chance to Pivot to Adaptive Cyber Resilience. *49security*. https://fourninesecurity.de/en/2023/01/17/germanys-national-security-strategy-a-chance-to-pivot-to-adaptive-cyber-resilience

**Skierka, I.** (2022). *Sachverständigenstellungnahme für die Sitzung des Bundestagsausschusses für Digitales am 04.07.2022 zum Thema 'Digitale Identitäten'* (pp. 1–9). Deutscher Bundestag / German Parliament. https://www.bundestag.de/resource/blob/902266/55d480a952db3dde1444fb21ca59b452/Skierka-data.pdf

**Skierka, I.**, & Schallbruch, M. (2020). Digitale Identitäten: Gemeinsam eine Lösung schaffen! In *Tagesspiegel Background Digitalisierung & KI*. https://background.tagesspiegel.de/digitalisierung/digitale-identitaeten-gemeinsam-eine-loesung-schaffen

**Skierka, I.** (2019). *Sachverständigenstellungnahme: Anhörung im Deutschen Bundestag, Ausschuss Digitale Agenda, Anhörung 'IT-Sicherheit von Hard- und Software als Voraussetzung für Digitale Souveränität' am 11.12.2019*. 1–10. https://www.bundestag.de/resource/blob/672536/b2b63aeeaffe54e40f8c62571cc628c4/Stellungnahme-Skierka-data.pdf

**Skierka, I.**, & Stenkamp, D. (2019). Bessere Kontrolle für KI: Ein Tüv für Algorithmen muss her. In *Handelsblatt Newspaper*. https://www.handelsblatt.com/meinung/gastbeitraege/gastkommentar-bessere-kontrolle-fuer-ki-ein-tuev-fuer-algorithmen-muss-her/25269900.html?ticket=ST-5967522-Y1s1OLVUVWskpMcSOJ3T-ap6

**Skierka, I.** (2016). Neues Mandat, neues Glück? – Das 11. Internet Governance Forum in Mexiko. In *Deutsche Gesellschaft für die Vereinten Nationen*. United Nations Association for Germany. http://www.dgvn.de/meldung/neues-mandat-neues-glueck-das-11-internet-governance-forum-in-mexiko/

# Elulookirjeldus

## Isikuandmed

| | |
|---|---|
| Nimi: | Isabel Skierka-Canton |
| Sünniaeg: | 25.05.1989 |
| Sünnikoht: | Hamburg, Saksamaa |
| Kodakondsus: | saksa |

## Kontaktandmed

| | |
|---|---|
| E-post: | Isabel.skierka-canton@proton.me |

## Hariduskäik

| | |
|---|---|
| 2018–2023 | Tallinna Tehnikaülikool – PhD (Avalik haldus) osalise tööajaga / väline |
| 2011–2012 | King’s College London, Sõjauuringute keskus – MA Rahvusvahelise konflikti uuringud<br>- Saksa Akadeemilise Vahetusteenistuse (DAAD) stipendium kraadiõppuritele |
| 2008–2011 | Maastrichti ülikool – BA Euroopa õpingud<br>- Parima 3% tunnustus 2010/2011<br>- MARBLE teadusprogramm<br>- Kiitusega lõpetamine |
| 2010–2011 | Pariisi Poliitika Uuringute Instituut (Sciences Po) – BA vahetusüliõpilane<br>- Saksa Akadeemilise Vahetusteenistuse (DAAD) stipendium bakalaureuseõppe üliõpilastele |
| 2006–2007 | Lycée Descartes Tours – vahetusõpilane, prantsuse küpsustunnistus esimene kirjanduslik tase |
| 1999–2008 | Eppendorfi gümnaasium – Keskharidus |

## Keelteoskus

| | |
|---|---|
| Saksa keel | Emakeel |
| Inglise keel | Kõrgtase |
| Prantsuse keel | Kõrgtase |
| Hispaania keel | Kesktase |

## Teenistuskäik

| | |
|---|---|
| 2016–... | Digitaalse ühiskonna instituut, Berliini Euroopa Juhtimis- ja tehnoloogiakool (ESMT) – Tehnoloogia poliitika programmijuht<br>- Interdistsiplinaarsed teadusuuringud ja konsultatsioonid strateegilise tehnoloogiapoliitika, küberturvalisuse, IT-turvalisuse ja riskijuhtimise, e-valitsemise ja digitaalse identiteedi valdkonnas koostöös valitsuspartneritega, eraettevõtete, sihtasutuste ja mõttekodadega |
| 2016–... | Global Public Policy Institute – koosseisuväline teadur |
| 2014–2016 | Global Public Policy Institute – teadur |
| 2014 | NATO peakorter – Carlo Schmid programmi teadur |

| | |
|---|---|
| 2013–2014 | DG Connect, Euroopa Komisjon – Blue Book programmi praktikant |
| 2013 | Informaatika instituut, Berliini Vaba ülikool, õppe- ja teadustöötaja |
| 2012–2013 | USA Saksamaa Marshalli Fond, Berliini kontor – praktikant ja uurimisassistent |

**Ühingud ja liikmelisus**

| | |
|---|---|
| 2021–... | Forum for New Security Politics - Heinrich-Böll-Stiftung – liige |
| 2017–... | Stiftung Neue Verantwortung Atlandi-ülene küberfoorum – liige |
| 2016–... | GPPi - mitteresidendist stipendiaat |
| 2016–2019 | Internet Governance Forum Germany – Next-Generation-Co-Co-Chair ja juhtkomitee liige |

**Väljaanded (valitud)**

***Raamatud ja raamatupeatükid***

**Skierka, I.** (2022). Digitale Identitäten. In F. N. Tanja Klenk Göttrik Wewer (Ed.), *Handbuch Digitalisierung in Staat und Verwaltung, 2nd edition* (pp. 1–12). Springer VS. https://doi.org/10.1007/978-3-658-23669-4_66-1

Lahmann, H., & **Skierka, I.** (2022). Cybersecurity in the Trade and Cooperation Agreement between the EU and the United Kingdom. In *Handbuch Handels- und Kooperationsvertrag EU/GB* (pp. 619–638). Nomos.

**Skierka, I.** (2020). Messung, Prüfung und Nachweis von IT-Sicherheit. In M. S. Gerrit Hornung (Ed.), *Handbuch IT-Sicherheitsrecht* (pp. 154–180). Nomos (Verlag). https://www.beck-shop.de/hornung-schallbruch-it-sicherheitsrecht/product/30826832

Schallbruch, M., & **Skierka, I.** (2018). *Cybersecurity in Germany*. Springer. https://doi.org/10.1007/978-3-319-90014-8

Benner, T., & **Skierka, I.** (2015). Digitale Souveränität—Begriffsdefinition. In W. V. Woycke Johannes (Ed.), *Handwörterbuch Internationale Politik* (Vol. 13, pp. 45–49). Verlag Barbara Budrich. https://books.google.ee/books?id=tKqeDQAAQBAJ&lpg=PP1&ots=h12WVslV2F&dq=warwick%20handw%C3%B6rterbuch%20internationale%20politik&pg=PA45#v=onepage&q&f=false

***Artiklid (ajakirjaartiklid, konverentsiartiklid, poliitikadokumendid)***

**Skierka, I.**, & Parycek, P. (2023). Einwurf – Kann Deutschland seine eID noch retten? *HMD Praxis der Wirtschaftsinformatik*, 1–6. https://doi.org/10.1365/s40702-023-00958-0

**Skierka, I.** (2023). When shutdown is no option: Identifying the notion of the digital government continuity paradox in Estonia’s eID crisis. *Government Information Quarterly*, *40*(1), 101781. https://doi.org/10.1016/j.giq.2022.101781

**Skierka, I.** (2021). Governing the Digital ID: How Germany and the EU plan to reclaim our digital sovereignty. In *ESMT Update Summer 2021* (pp. 32–35). ESMT Berlin. https://esmt.berlin/sites/main/files/2021-06/ESMT_Update_Summer_2021.pdf

Schallbruch, M., **Skierka, I.**, & Strüve, T. (2020). Digital identity in 2020—Conference. In *Konferenzpapier -Digitale Identitäten* (pp. 1–6). European School of Management and Technology Berlin. http://static.esmt.org/publications/Reports/dsi-ipr_2020-1_de-en.pdf

**Skierka, I.** (2020). 5G and beyond: A test for "technological sovereignty" in Europe? In *The Convergence Puzzle: Australia, Germany and Emerging Cybersecurity Trends* (pp. 37–44). Konrad Adenauer Foundation. https://www.kas.de/documents/274425/8492225/Periscope+Volume+3+-+5G+and+Beyond.pdf/48229669-0e6e-a44a-e75c-4478d67027d3?t=1589163346668

**Skierka, I.** (2018). *The governance of safety and security in connected healthcare in Europe*. 1–12. https://doi.org/10.1049/cp.2018.0002

**Skierka, I.**, & Schallbruch, M. (2018). *Requirements for a German 'Blockchain Strategy'* (pp. 1–14). http://static.esmt.org/publications/Reports/dsi-ipr_2018-3_en-de.pdf

**Skierka, I.** (2017). Cybersecurity International – Unterschiedliche Prioritäten. In *Digitalpolitik – Eine Einführung* (pp. 19–26). Wikimedia e.V. and iRights. https://irights.info/wp-content/uploads/2017/05/Digitalpolitik_-_Eine_Einfuehrung.pdf

**Skierka, I.** (2016). *Military Cybersecurity, the German way*. *3*, 37–42. https://www.globalpolicyjournal.com/projects/gp-e-books/digital-debates-cyfy-journal-volume-3-2016

**Skierka, I.** (2015). *Amerika abwickeln* (pp. 138–141). DGAP. https://internationalepolitik.de/de/amerika-abwickeln

**Skierka, I.** (2015). *Krieg der Knöpfe* (pp. 134–138). https://internationalepolitik.de/de/krieg-der-knoepfe

**Skierka, I.**, & Gaycken, S. (2015). *Cybertaktik und Cyberstrategie* (pp. 1–202). Free University of Berlin. http://www.inf.fu-berlin.de/inst/ag-si/pub/Cybertaktik_und_Strategie.pdf

**Skierka, I.**, Morgus, R., Hohmann, M., & Maurer, T. (2015). *CSIRT Basics for Policy-Makers: The History, Types & Culture of Computer Security Incident Response Teams* (pp. 1–29). https://www.gppi.net/media/CSIRT_Basics_for_Policy-Makers_May_2015_WEB.pdf

Maurer, T., **Skierka, I.**, Morgus, R., & Hohmann, M. (2015). *Technological sovereignty: Missing the point?* 53–68. https://doi.org/10.1109/CYCON.2015.7158468

Morgus, R., **Skierka, I.**, Hohmann, M. & Maurer, T. (2015). *National CSIRTs and their role in computer security incident response* (pp. 1–33). http://www.digitaldebates.org/fileadmin/media/cyber/National_CSIRTs_and_Their_Role_in_Computer_Security_Incident_Response__November_2015_--__Morgus__Skierka__Hohmann__Maurer.pdf

**Skierka, I.** (2014). *Die Illusion vom „sauberen Krieg“* (pp. 134–137). DGAP. https://internationalepolitik.de/de/die-illusion-vom-sauberen-krieg

Drott, L., Jochum, L., Lange, F., **Skierka, I.**, Vach, J., & van Asselt, M. B. A. (2013). Accountability and risk governance: A scenario-informed reflection on European regulation of GMOs. *Journal of Risk Research*, *16*(9), 1123–1140. https://doi.org/10.1080/13669877.2012.743161

***Muud väljaanded (arvamusavaldused, eksperdiarvamused)***

Tiirmaa-Klaar, H. & **Skierka, I.** (2023). Germany’s National Security Strategy: A Chance to Pivot to Adaptive Cyber Resilience. *49security*. https://fourninesecurity.de/en/2023/01/17/germanys-national-security-strategy-a-chance-to-pivot-to-adaptive-cyber-resilience

**Skierka, I.** (2022). *Sachverständigenstellungnahme für die Sitzung des Bundestagsausschusses für Digitales am 04.07.2022 zum Thema ‘Digitale Identitäten’* (pp. 1–9). Deutscher Bundestag / German Parliament. https://www.bundestag.de/resource/blob/902266/55d480a952db3dde1444fb21ca59b452/Skierka-data.pdf

**Skierka, I.**, & Schallbruch, M. (2020). Digitale Identitäten: Gemeinsam eine Lösung schaffen! In *Tagesspiegel Background Digitalisierung & KI*. https://background.tagesspiegel.de/digitalisierung/digitale-identitaeten-gemeinsam-eine-loesung-schaffen

**Skierka, I.**, & Stenkamp, D. (2019). Bessere Kontrolle für KI: Ein Tüv für Algorithmen muss her. In *Handelsblatt Newspaper*. https://www.handelsblatt.com/meinung/gastbeitraege/gastkommentar-bessere-kontrolle-fuer-ki-ein-tuev-fuer-algorithmen-muss-her/25269900.html?ticket=ST-5967522-Y1s1OLVUVWskpMcSOJ3T-ap6

**Skierka, I.** (2019). *Sachverständigenstellungnahme: Anhörung im Deutschen Bundestag, Ausschuss Digitale Agenda, Anhörung ‘IT-Sicherheit von Hard- und Software als Voraussetzung für Digitale Souveränität’ am 11.12.2019*. 1–10. https://www.bundestag.de/resource/blob/672536/b2b63aeeaffe54e40f8c62571cc628c4/Stellungnahme-Skierka-data.pdf

**Skierka, I.** (2016). Neues Mandat, neues Glück? – Das 11. Internet Governance Forum in Mexiko. In *Deutsche Gesellschaft für die Vereinten Nationen*. United Nations Association for Germany. http://www.dgvn.de/meldung/neues-mandat-neues-glueck-das-11-internet-governance-forum-in-mexiko/

ISSN 2585-6901 (PDF)
ISBN 978-9916-80-017-1 (PDF)