Cyber Risks and Cybersecurity

Risk Communication and Regulation Strategies in the United States and Germany

Von der Fakultät Wirtschafts- und Sozialwissenschaften der Universität Stuttgart zur Erlangung der Würde eines Doktors der Wirtschafts- und Sozialwissenschaften (Dr. rer. pol.) genehmigte Abhandlung

Vorgelegt von

Kathrin Ulmer

aus Heidelberg

Hauptberichter:	Prof. Dr. Dr. h.c. Ortwin Renn
Mitberichter:	Prof. Dr. André Bächtiger

Tag der mündlichen Prüfung: 11. November 2020

Institut für Sozialwissenschaften der Universität Stuttgart

2021

Contents

Figures

Abbreviations

AI	Artificial Intelligence
BYOD	Bring Your Own Device
C3	Cyber Crimes Center
CBMs	Confidence Building Measures
CCIPS	Computer Crime and Intellectual Property Section
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CIO	Chief Information Officer
CIKR	Critical Infrastructure and Key Resources
CIP	Critical Infrastructure Protection
CIPAC	Critical Infrastructure Partnership Advisory Council
CISPA	Cyber Intelligence Sharing and Information Protection Act
CNAP	Cybersecurity National Action Plan
CNO forces	Computer Network Operation forces
CoE	Council of Europe
CSA	Cyber Security Act
CSF	Cybersecurity Framework
CTIIC	Cyber Threat Intelligence Integration Center
DARPA	Defense Advanced Research Projects Agency
DDoS attack	Distributed Denial of Service attack
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DoD	Department of Defense
DoJ	Department of Justice
ECTFs	Electronic Crimes Task Forces
EGC	European Governmental CERTs Group
ENISA	European Network and Information Security Agency
EO	Executive Order
EPCIP	European Programme for European Critical Infrastructure Protection
FBI	Federal Bureau of Investigation
FIRST	Forum for Incident Response and Security Teams
FISMA	Federal Information Security Management Act
G20	Group of 20
GCC	Government Coordinating Council
HSPD	Homeland Security Presidential Directive
IANA	Internet Assigned Numbers Authority
IC	Intelligence Community
ICANN	Internet Corporation for Assigned Names and Numbers
ICS	Industrial Control Systems
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team

ICT	Information and Communication Technologies
IoT	Internet of Things
IP	Intellectual Property
ITU	International Telecommunications Union
IWWN	International Watch and Warning Network
NATO	North Atlantic Treaty Organization
NCCIC	National Cybersecurity and Communications Integration Center
NCIJTF	National Cyber Investigative Joint Task Force
NCIRP	National Cyber Incident Response Plan
NIAC	National Infrastructure Assurance Council
NICC	National Infrastructure Coordinating Center
NICE	National Initiative for Cybersecurity Education
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NPPD	National Protection and Programs Directorate
NSA	National Security Agency
NTIA	National Telecommunications and Information Administration
NSTAC	National Security Telecommunications Advisory Committee
ODNI	Office of the Director of National Intelligence
OECD	Organisation for Economic Co-Operation and Development
OPM	Office of Personnel Management
OSCE	Organization for Security and Cooperation in Europe
PCCIP	President's Commission on Critical Infrastructure Protection
R&D	Research and Development
RFI	Request for Information
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SKAD	Sociology of Knowledge Approach to Discourse
SMEs	Small and Medium-sized Enterprises
SPOC	Single Point of Contact
SSA	Sector-Specific Agency
SSP	Sector-Specific Plan
UN	United Nations
US-CERT	United States Computer Emergency Readiness Team
UN GGE	United Nations Group of Governmental Experts
USCYBERCOM	U.S. Cyber Command
WH	White House

Translation of German Proper Names

Alliance for Cyber Security	Allianz für Cyber-Sicherheit
German Customs Investigation Bureau	Zollkriminalamt (ZKA)
German Federal Police	Bundespolizei (BPol)
Federal Association for Information Technology, Telecommunications and New Media	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom)
Federal Chancellery	Bundeskanzleramt
Federal Commissioner for Data Protection and Freedom of Information	Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)
Federal Criminal Police Office	Bundeskriminalamt (BKA)
Federal Foreign Office	Auswärtiges Amt (AA)
Federal Government Commissioner for Information Technology	Die Beauftragte der Bundesregierung für Informationstechnik (BfIT)
Federal Government Commissioner for the Federal Intelligence Services	Beauftragter für die Nachrichtendienste des Bundes
Federal Intelligence Service	Bundesnachrichtendienst (BND)
Federal Ministry for Economic Affairs and Energy	Bundesministerium für Wirtschaft und Energie (BMWi)
Federal Ministry for Family Affairs, Senior Citizens, Women and Youth	Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ)
Federal Ministry of Defence	Bundesministerium der Verteidigung (BMVg)
Federal Ministry of Education and Research	Bundesministerium für Bildung und Forschung (BMBF)
Federal Ministry of Finance	Bundesministerium der Finanzen (BMF)
Federal Ministry of Health	Bundesministerium für Gesundheit (BMG)
Federal Ministry of Justice and Consumer Protection	Bundesministerium der Justiz und für Verbraucherschutz (BMJV)
Federal Ministry of Labour and Social Affairs	Bundesministerium für Arbeit und Soziales (BMAS)
Federal Ministry of the Interior	Bundesministerium des Innern (BMI)
Federal Ministry of Transport and Digital Infrastructure	Bundesministerium für Verkehr und digitale Infrastruktur (BMVI)
Federal Network Agency	Bundesnetzagentur (BNetzA)
Federal Office for Information Security	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Federal Office for the Protection of the Constitution	Bundesamt für Verfassungsschutz (BfV)
Federal Office of Civil Protection and Disaster Assistance	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)
National Cyber Response Centre	Nationales Cyber-Abwehrzentrum

National Cyber Security Council	Nationaler Cyber-Sicherheitsrat
Military Counterintelligence Service	Amt für den Militärischen Abschirmdienst (MAD)
Parliamentarian Control Panel	Parlamentarisches Kontrollgremium

Zusammenfassung

Die Dissertation untersucht politische Kommunikations- und Regulierungsprozesse im Bereich von Cyberrisiken und Cybersicherheit in den USA und Deutschland im Zeitraum von 2007 bis 2016 mit einem Fokus auf Cybersicherheitsrisiken für kritische Infrastrukturen. Sie verwendet ein qualitativ-interpretatives Forschungsdesign auf Basis der Wissenssoziologischen Diskursanalyse (WDA) nach Reiner Keller, die durch die Integration von *Frames* und Regulierungsstilen innovativ erweitert wird. Die empirische Analyse erfolgt in drei Schritten: In einem ersten Schritt werden die institutionellen Strukturen und Kompetenzen im Bereich der Exekutive beider Länder für das junge Politikfeld Cybersicherheit anhand eines Kontextmappings dargestellt. In einem zweiten Schritt werden durch die Analyse der offiziellen Cybersicherheitsdiskurse in den USA und Deutschland die *Frames* herausgearbeitet, mit denen die Akteure über Cyberrisiken und Cybersicherheit kommunizieren. Hierbei zeigen sich jeweils zwei übergreifende Frames: Im Fall der USA ein *Homeland Security Frame* und ein *Technological Leadership Frame*, für Deutschland ein *Security of Supply Frame* sowie ein *Moderation Frame*. Schließlich untersucht die Arbeit für jedes Land ein regulatorisches Beispiel aus dem Bereich Cybersicherheit, verstanden als Diskurseffekt, im Hinblick auf dessen Konsistenz mit dem traditionellen Regulierungsstil des jeweiligen Landes. Im Fall der USA wird das *Cybersecurity Framework* untersucht, das im Zuge des *Executive Order 13636* erstellt wurde, für Deutschland das IT-Sicherheitsgesetz.

Abstract

The dissertation explores and analyzes political communication and regulatory processes related to cyber risks and cybersecurity in the United States and Germany in the time period from 2007 to 2016 with a focus on cybersecurity-related risks for critical infrastructure. The dissertation follows a qualitative-interpretative research design based on Reiner Keller's Sociology of Knowledge Approach to Discourse (SKAD) that is innovatively adapted by integrating *frames* and regulatory styles. The study proceeds in three steps: First, a context mapping reveals the institutional roles and responsibilities of the executive branches in both countries in the young field of cybersecurity policy. Second, official cybersecurity discourses in both countries are analyzed in order to identify which *frames* the respective executive actors use in their communication. Two overarching frames are found for each country: For the United States, a *homeland security frame* and a *technological leadership frame* can be

identified; for Germany, a *security of supply frame* as well as a *moderation frame* are found. Third, the study sheds light on regulation in the field of cybersecurity, understood as discourse effect. Therefore, one regulatory example is examined for each country in order to assess its consistency with the traditional regulatory style of the respective country. In the case of the United States, the Cybersecurity Framework following executive order 13636 is examined; for Germany, the IT Security Law is selected as regulatory example.

1 Introduction

Advancements in information and communication technologies and their widespread use have lead to what is frequently called a revolution: the "digital revolution" (D-48 AA 2014:2, own translation)[1], the "information revolution" (Dunn Cavelty 2008:12) or "the fourth industrial revolution" (Knitterscheidt and Weishaupt 2018:18, own translation) to name but a few. Many of these associations are linked to the Internet that was invented over 30 years ago (Louven and Steger 2018:18). Ever since, major technological innovations have been presented in the domain of information and communication technologies, for example cloud technology, the Internet of Things (IoT), and, more recently, blockchain and artificial intelligence (AI). Some technologies have led to very successful, even disruptive business models as proven by giant U.S. technology companies (see for example Hofer et al. 2018:4)[2]. Others are said to fundamentally change the way we are living as individuals and as society as a whole, which can be seen in the debate on AI (see for example Steinharter and Maisch 2018; Brächer 2018; Kerkmann 2018; Weddeling 2018).[3]

Risks for cybersecurity[4] constitute a constant and fundamental topic throughout all phases of digitalization, which is why it is the topic of this study. Following Craigen et al., cybersecurity is defined as "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights" (Craigen, Diakun-Thibault, and Purse 2014:13). As Stevens notes: "From obscure technical origins in computer science and information security, cybersecurity has emerged as a major political consideration for states, multilateral organizations, firms and civil society in the early twenty-first century" (Stevens

[1] The references U-01 to U-76 as well as D-01 to D-65 refer to the U.S. and German documents used for the frame analysis (for a complete list see sections 7.1 and 7.2).
[2] Hofer et al. state that Amazon manages nearly 50 per cent of Germany's e-commerce (Hofer et al. 2018:4).
[3] Among the topics in the debate on artificial intelligence, there are fundamental ethical questions on decision-making by machines, such as effects of discrimination of humans introduced by algorithms (Steinharter and Maisch 2018:28), but also the hope that AI will be beneficial for the world economy (ibid.) and solve problems that cannot be solved by humans (Brächer 2018:29).
[4] A note on orthography: Many words with the prefix "cyber" are used in this study. However, there is no uniform spelling for words with "cyber". Therefore, I follow the dominant spelling for each word as found in the U.S. discourse. That means in some cases, prefix and noun are separated (as in "cyber risk", "cyber terrorism", "cyber vandalism"), whereas in other cases, both are directly attached (as in "cybersecurity", "cybercrime").

2018:1). In the early days of digitalization, people worried about worms and viruses such as the worm with the famous email subject line "I love you" in 2000 (D-16 BSI 2016:30). However, cybersecurity is still a challenge today – one that gains in importance given the increasing pervasiveness of digitalization and ever more connected devices and things (see for example BSI 2018a:3,92,95; Welchering 2018; Jansen 2018).

Cybersecurity risks represent a highly relevant and controversial issue in several ways. There are strongly diverging views among experts on cyber risks. As Dunn Cavelty notes already in 2008: "[V]arious sorts of experts disagree on the gravity of the cyber-threats and grapple with the question of how likely they are and how soon an incident with a genuinely society-threatening impact might occur" (Dunn Cavelty 2008:139). Especially in the field of modern IT-enabled critical infrastructure, the potential for harm is great as technological advances are "vastly increasing the possibility for local risks to mutate into systemic risks" (Dunn Cavelty 2013:114).

Also, the impact of cybersecurity risks manifesting in the real world is high: In a quantitative regard, cyber attacks such as spam mails or ransomware have long turned into mass phenomena (see for example D-14 BSI 2015:48; D-33 BKA 2013:8; D-31 BKA 2011:12). In a qualitative regard, several attacks have gained high political attention. For example, the attacks in Estonia in 2007 resulted in the awareness that "this could be a thing that could threaten national security" (I-07:67)[5]. *Stuxnet*, occuring in 2010, was seen as a wake-up call with regard to critical process control systems in industrial infrastructure and demonstrated the high vulnerability of the latter (D-16 BSI 2016:3). More recently, *Meltdown/Spectre* that targets hardware pieces demonstrated a new quality of attack and high potential of damage (BSI 2018a:44,92). From an economic point of view, Munich Re points to the enormous financial cost resulting from cyber attacks: For 2018, the company estimated the cost amounting to 450 billion Dollar worldwide, and six trillion Dollar in 2021 (Herz 2018:22). According to the Allianz Risk Barometer 2019, companies assess cyber risks and business interruptions as the biggest business risks worldwide (Bayer 2019:8).[6] Many companies feel unable to cope with the challenges of defending their company against cyber risks (Ermisch

[5] The references I-01 to I-18 refer to the interviews conducted in the context of the study (see below section 2.4.2).

[6] Both risks obtained 37% of the responses respectively (Bayer 2019:8).

2018:48). Also, the lack of cybersecurity experts is striking (ibid.): According to one estimation, there is a need of 1.5 million specialists worldwide until 2020 (Dörner 2018:27).

Politics consists in the "regulation of common matters of a community by authoritative decisions" (Fuchs and Roller 2007:205, own translation). However, cybersecurity risks present an enormous challenge as laid out above: They constitute "a threat whose dimensions remain altogether uncertain – opening up a broad margin for political bargaining" (Dunn Cavelty 2008:138–139). Notably in the young field of cybersecurity policy, this aspect plays a crucial role as fundamental (goal) conflicts have to be settled and strategic decisions for future developments in the policy field have to be taken. Therefore, it is especially interesting to look at cybersecurity discourses as proposed in this study. In the light of discourse analysis, actors participate in "discursively structured symbolic fights for reality definitions" (Keller 2004:62, own translation) and those definitions and interpretations play an important role for legitimizing political action (Donati 2001:147–148). In this sense, the study aims at contributing to a better understanding of cybersecurity discourses and their effects in the form of regulation in the United States and Germany.

The goal of the study is to answer the overall **research question**: **How do the executives of the United States and Germany address cybersecurity risks? In particular, what is the approach to cybersecurity-related risks for critical infrastructure?**

"Addressing" has got a threefold meaning in the context of the study and regards institutions, discourses, and regulation. This threefold meaning translates into three research questions:

- *Institutions*: Who is doing what in the new field of cybersecurity policy in the United States and Germany?
- *Discourses*: How do representatives of the U.S. and German executives frame cybersecurity risks in their official communication?
- *Regulation*: Are the selected U.S. and German regulatory examples taken from the field of cybersecurity policy in line with the traditional regulatory style of the respective country?

In order to answer these research questions, the study follows a qualitative-interpretative design analyzing the United States and Germany in the period from 2007 to 2016.

The study is considered a relevant and helpful contribution to academic research as well as practical cybersecurity policy. The contribution for research most notably lies in using a particular theoretical analytical approach: I apply the *Sociology of Knowledge Approach to Discourse* (SKAD) and innovatively adapt it by integrating frames and regulatory styles into SKAD allowing for new insights. Also, the study's comparative design is considered promising as the field of cybersecurity is strongly characterized by U.S.-focused research. Moreover, the study's unique data set stands out: It covers nearly ten years of discourse and contains rich interview material from personal in-depth interviews. As the study examines a formative period of cybersecurity policy, the insights can also benefit practitioners in the field. Knowledge and understanding of both countries' long-term communication strategies and the country-specific political and institutional background in the cyber domain can be increased and lead to more reflected (mutual) communication and learning effects improving the political implementation of measures.

The dissertation is structured as follows: The conception of the study including a literature review, the specification of the theoretical analytical framework and research design, expectations, and methodology are laid out in chapter 2. Chapter 3 provides a context mapping presenting the discourse participants in the United States and Germany that are relevant in the context of the study. In chapter 4, I analyze executive cybersecurity discourses in both countries and identify frames in each country's communication. Chapter 5 presents an analysis of a selected regulatory example for each country against the background of the country's traditional regulatory style. Finally, chapter 6 provides a short summary of the study as well as some concluding remarks and implications.

2 Conception of the Study: Analyzing Political Communication and Regulation of Cyber Risks

In the following chapter, the conception of the study is presented. I start with a review of relevant literature in the field of constructing and interpreting cyber risks and cybersecurity before presenting my theoretical analytical framework and research design in detail.

2.1 Literature Review

According to Stevens, "[t]he term 'cybersecurity' can be traced back to at least the late 1980s and its conceptual antecendents much further" (Stevens 2018:1). However, in the political context, the term appeared much later: From 2000s onwards, the notion cybersecurity occurred in publications emanating from the political sphere (Stevens 2018:1). As cybersecurity is seen as "one of the most complex and diverse technical and political challenges of our contemporary world" (Stevens 2018:1), there is a necessity to examine and understand the issue and its diverse implications from a scientific point of view.

The body of literature on cyber topics is large and still growing in parallel to the increasing attention to and importance of cyberspace and its implications. The literature covers a broad and diverse range of issues and debates. An important branch of research centers on the existence or non-existance and characteristics of cyberwar (see for example Rid 2012; Stone 2012) and other military and defense aspects such as deterrence in cyberspace (see for example Cilluffo, Cardash, and Salmoiraghi 2012). Another branch is cyber-related literature in international relations that is concerned with diverse topics, for example, cyber power (Nye, Jr. 2010), the role of the BRICS (Brazil, Russia, India, China, South Africa) in cyber policy (Ebert and Maurer 2013), and "digital diplomacy" (Cull 2013:137). A third branch in literature deals with national and international norms and legal aspects of cyberspace and cybersecurity (see for example Schaller 2014). Moreover, there is research on cyber-related definitional issues (see for example Craigen, Diakun-Thibault, and Purse 2014; Di Camillo and Miranda 2011) as well as specific cyber risks such as cybercrime (see for example Grabosky 2013; Brodowski and Freiling 2011) or cyber-enabled economic espionage (see for example Friedman 2013).

A large amount of literature on cyber risks and cybersecurity is written from a U.S. perspective or on the United States (see for example Teplinsky 2013; Johanson 2013; Lord and Sharp 2011; Dunn Cavelty 2008). However, there is also a part of research focusing on other countries such as China (see for example Kolton 2017), Russia (see for example Johnston 2015), or Germany (see for example Kullik 2014). Finally, there is comparative research on different cyber-related topics, but it represents a rather small portion of cyber literature. Examples are a study on information infrastructure in the United States and Germany (Schulze 2006) and on cyber threat perception in Germany, France and the UK (Guitton 2013).

2.1.1 Cybersecurity Studies and the Construction and Interpretation of Cyber Risks

The following literature review is centered on the main aspect this study is concerned with: the construction and interpretation of cyber risks and cybersecurity. In this regard, Myriam Dunn Cavelty contributed an early and very influential work on "Cyber-Security and Threat Politics. US Efforts to Secure the Information Age" (Dunn Cavelty 2008) in 2008. In her study, she examines U.S. cyber politics from the perspective of the so-called "'Copenhagen School's' securitisation approach" (Dunn Cavelty 2008:8) and supplements this approach with theoretical elements from the research on framing and agenda-setting (ibid.).[7] Dunn Cavelty examines the political process of the "'cyber-threat story'; the story of how and why cyber-threats came to be considered one of the quintessential security threats of modern times in the United States" (Dunn Cavelty 2008:1). She takes a long-term perspective starting with the Reagan administration and ending with the Bush administration (ibid.:42,120). On the one hand, she finds a continuity regarding threat actors over the examined period of time, namely "a very broad range of actors" (ibid.:131). On the other hand, her findings show that the political perception of what is threatened varied from classified government information to economic aspects to critical infrastructure, among other things (ibid.:131). Especially the critical infrastructure threat frame turned out as particularly successful (ibid.:132). In the end, Dunn Cavelty finds that securitization, in a classical sense, as expected by her theoretical approach, did not take place (ibid.:137).

[7] As Stevens note, "[s]ecuritization studies record the discursive construction of cyber threats and identify tensions between political claims and the objective conditions to which they refer" (Stevens 2018:2).

Rather, a "new logic of security" (ibid.) emerged implying a "changing and very broad concept of security" (ibid.).

In a later article, Dunn Cavelty enlarges her perspective to "less visible actors inside and outside of government" (Dunn Cavelty 2013:105), thus the broad cybersecurity discourse by multiple actors (ibid.:106), and to how they "shape a reservoir of acceptable threat representations that influence everyday practices of cyber-security" (ibid.:105). In a linguistic analysis, she notably finds three different representations: The first uses "biological, and particularly virus-related, metaphors" (ibid.:109). The second one centers on "the lawlessness of cyberspace (or the Western Frontier) and (…) shady, invisible, but powerful foes" (ibid.), and the third representation deals with the triangle of technical complexity, dependency, and vulnerability (ibid.:109–110). The threat representations lead to different implications depending on their respective direction of impact: "If cyberspace is conceptualized as an auto-generating immune force, then the role of the state is that of a gardener and facilitator. If cyberspace is conceptualized as a problematic unruly place that needs to be tamed at all cost, then this inevitably leads to calls for strong(er) interference into the global cyber-system, including the topology of the Internet" (ibid.:119). She underlines that currently, the second pattern gains in importance (ibid.). However, this result is not automatically given, but rather "a matter of choice" (ibid.) – so, at least in theory, change is possible (ibid.).

Hansen and Nissenbaum present another study of cybersecurity based on the securitization approach from the Copenhagen School (Hansen and Nissenbaum 2009). In a first step, they elaborate on cybersecurity as a "sector" (ibid.:1157) in the sense of the Copenhagen School. Sectors are defined as "lenses or discourses" (ibid.) having specific "grammars of securitization" (ibid.:1163). In the case of cybersecurity, the authors identify the concepts of "*hypersecuritization*" (ibid.:1163–1165, emphasis in original)[8], "*everyday security practices*" (ibid.:1165–1166, emphasis in original)[9], and "*[t]echnification*" (ibid.:1166–1168, emphasis in

[8] This concept "has been introduced by Buzan (2004:172) to describe an expansion of securitization beyond a 'normal' level of threats and dangers by defining 'a tendency both to exaggerate threats and to resort to excessive countermeasures.'" (Hansen and Nissenbaum 2009:1163–1164).

[9] This concept "points to the way in which securitizing actors, including private organizations and businesses, mobilize 'normal' individuals' experiences in two ways: to secure the individual's partnership and compliance in

original)[10] as such grammers. They apply their framework on the case of the cyber attacks in Estonia in 2007 and find a "partial success of the Estonian securitization" (ibid.:1170). A success is seen in the extensive international media coverage on the attacks including the labeling as the "first real war in cyberspace" (ibid.:1169). But there are also constraints against a successful securitization, most notably the fact that "there was no accepted evidence of a clear digital trace to Russia" (ibid.:1170) and that critical infrastructure was not attacked, so "the truly cascading hypersecuritization scenario could hardly be sustained" (ibid.:1170). In concluding, the authors argue for a more interdisciplinary debate and assessment of cyber securitizations, as they imply political, security, as well as technological aspects (ibid.:1172).

Barnard-Wills and Ashenden provide a study of cybersecurity policy literature (Barnard-Wills and Ashenden 2012). Their approach is based on the "governmentality theory" (ibid.:11) after Mitchell Dean as well as discourse analysis (ibid.). They identify a "techno-political discourse of cyber security" (ibid.:1). The analysis of Barnard-Wills and Ashenden results in a strong pattern in the discourse that describes "virtual space as ungovernable, unknowable, problematically visible, vulnerable, inevitably threatening, and inhabited by a range of hostile and threatening actors" (ibid.:2). According to the authors, an important consequence of this type of discourse is that cyberspace gets increasingly militarized and pushed into national security thinking with detrimental effects on its open and inclusive structure (ibid.:11).

Another interesting perspective is offered by Lawson by bringing together threat constructions with empirical evidence (Lawson 2013). He starts his analysis from what Dunn Cavelty calls "[c]yber-doom scenarios" (Dunn Cavelty 2008:2), thus "hypothetical tales of cyberattacks resulting in the mass collapse of critical infrastructures, which in turn leads to serious economic losses, or even total economic, social, or civilizational collapse" (Lawson 2013:86–87). By drawing on historical research and research in the field of disaster sociology, he analyzes different historical cases such as strategic bombing in WWII,

protecting network security, and to make hypersecuritization scenarios more plausible by linking elements of the disaster scenario to experiences familiar from everyday life" (Hansen and Nissenbaum 2009:1165).

[10] Technification means the "privileged role allocated to computer and information scientists within cyber security discourse" (Hansen and Nissenbaum 2009:1167).

blackouts, the attacks of 9/11, and the hurricane Katrina (ibid.:91–95). He finds that "[m]odern societies and the systems upon which they rely have proved far more resilient than many have assumed" (ibid.:91). Even in the face of severe disasters such as the ones mentioned above, panic and antisocial behavior was a rare phenomenon and societies did not collapse (ibid.:93–94). To the contrary, people generally reacted in quite rational and helpful ways (ibid.). In the light of these research findigs, Lawson doubts the sense and usefulness of cyber-doom scenarios: "It (…) seems unlikely that a 'cyber- 9/11' or a 'cyber-Katrina' would result in the loss of life and physical destruction seen in the real 9/11 and Katrina. And if the real 9/11 and Katrina did not result in social or economic collapse, nor in a degradation of military readiness or national will, then it seems unlikely that their 'cyber' analogues would achieve these results" (ibid.:95). Against this background, basing policy responses on unrealistic cyber-doom scenarios is highly dangerous according to Lawson (ibid.:95) as they may lead to "counterproductive policies focused on control, militarization, and centralization" (ibid.:87). Ultimately, Lawson qualifies such scenarios as the "latest manifestation of longstanding fears about 'technology-out-of-control' in Western societies" (ibid.:87). For appropriate policy responses to the challenges posed by cyber risks, he recommends defining problems as accurately as possible, using insights of empirical research (ibid.:95–97), and taking measures in support of "resilience in technological and social systems" (ibid.:97).

A different view is presented by Lewis shedding light on the perceptions of cyber threats of countries (Lewis 2014). His overview includes 32 countries (ibid.:571). He mainly finds that "[n]ational perceptions of cyber threats largely conform to a country's existing security priorities, but the global attention paid to incidents like Estonia or Stuxnet helped to elevate cybersecurity as a national security concern" (ibid.:566–567). There are different mechanisms that have an influence on a country's threat perception: Discussions and processes in multilateral organizations such as the United Nations (UN), the International Telecommunications Union (ITU), the Organisation for Economic Co-Operation and Development (OECD) or the North Atlantic Treaty Organisation (NATO) constitute the key determinant that affects threat perception (ibid.:568–570,575). Being affected by a cyber attack as a government presents a second, very powerful factor (ibid.:571). Lewis concludes from his analysis that "[c]ybersecurity is better understood if we do not think of cyberspace

as a domain, but rather adopt Clausewitzian notions and see it as an extension of state-to-state relations" (ibid.:575).

Clement Guitton equally deals with national threat preceptions, albeit on a more detailed level for three selected countries: Germany, France, and the UK (Guitton 2013). In all three countries, he finds a contradiction between their respective strategy and the resources spent: Whereas all three countries identify cyber-related threats as crucial national security threats around the years 2005-2008 as shown by their strategic publications, they do not spent an adequate amount of resources in terms of financial means and personnel on the issue (ibid.:22–26). Also, the fight against cybercrime – being a crucial source of cyber threats – is barely given attention, which is inconsistent in Guitton's view (ibid.:22). Later strategic documents confirm the established threat perceptions and, at least for the German case, public spending this time corresponds to the importance given to the threat (ibid.:28). Where do the contradictory policy findings stem from? According to Guitton's analysis, the "governments' assessments of the situation are blurred by their lack of reliable and objective data. They have the capacity to collect such data that would be free of the interests that cyber security vendors have to inflate the cyber threat" (ibid.:32). For the German case, for example, he presents empirical evidence pointing to a report from the Federal Office for Information Security (BSI) from 2005 that "was documented only by the statistics of (…) three security vendors that shaped the perception of the threat by the government and the legislators" (ibid.:23).

A different perspective on the construction and interpretation of cyber risks is offered by Jarvis, Macdonald, and Whiting (Jarvis, Macdonald, and Whiting 2015). They conduct an analysis of English-speaking news media in seven countries in the time period from 2008 to 2013 in order to trace "media constructions of cyberterrorism" (ibid.:60). They find differences in the regional distribution of media coverage (ibid.:62–63) as well as a peak in October 2010, when the UK presented its *National Security Strategy* and the cyber incident Stuxnet entered the news (ibid.:69,71). Also, the authors analyze the tone of the coverage in their sample by rating the level of concern of the news items along six different categories (ibid.:65). Interestingly, they find that a large majority of items presents a high level of concern (ibid.:66). Jarvis et al. conclude that "news coverage has a constitutive rather than

corresponding relationship to the 'reality' of cyberterrorism: it is actively involved in the production of this potential security threat. Danger (…) is a product of framing and interpretation, in which meaning is given to the world via language, images and other discursive practices: be they pictures of hand grenades, discussion of hypothetical 'doomsday' scenarios, or headlines about 'malicious computer worms'. Thus, whether or not there exists a 'real' threat of cyberterrorism (…), media (and other) depictions thereof are important in their own right" (ibid.:73).

Finally, there is a branch of literature combining the analysis of cyber-related phenomena with normative considerations. I present one article in this regard in the following. It also deals with privacy, which is not in the focus of this study. Nevertheless, the article shall be included in this review in order to exemplarily present literature that examines the area where cybersecurity touches on aspects of privacy.

In her analysis, Dunn Cavelty identifies a "cyber-security dilemma" (Dunn Cavelty 2014:702), a situation where national security collides with human security (ibid.:703,708–710). She posits that the "threat arising from cyberspace to (national) security is presented as possible disruption to a specific way of life, one building on information technologies and critical functions of infrastructures, with relatively little consideration for humans directly" (ibid.:701). Current cybersecurity efforts as proceeded by states are notably focused on cyberdefense and military aspects (ibid.:708), including interests of intelligence services that actively buy vulnerabilities in order to exploit them according to their needs (ibid.:710). Moreover, big companies extensively collect and analyze data for advertising purposes and predicting behavior (ibid.:709). However, these aspects clash with the idea of human security, i.e. – transferred to the field of cyberspace – privacy and civil liberties (ibid.:704). Dunn Cavelty notes that "we cannot have both: a strategically exploitable cyberspace full of vulnerabilities – and a secure and resilient cyberspace that all the cyber-security policies call for" (ibid.:711). In order to achieve national *and* human security, the human-centered aspects must be emphasized and the use of vulnerabilities pushed back (ibid.:703,711). She proposes to build security on the approach of a "human-centric information ethics of the infosphere" (ibid.:703).

2.1.2 Contributions of the Study

As could be seen in the previous sections, there is a rich literature on the construction and interpretation of cyber risks and cybersecurity offering numerous substantial and interesting insights. This concluding section serves to specify how my dissertation adds to and expands on the existing body of literature. In particular, I would like to point out three contributions.

The *first* contribution consists in using a particular theoretical analytical approach: In contrast to a large portion of literature that is based on securitization theory, my study is based on Reiner Keller's *Sociology of Knowledge Approach to Discourse* (SKAD) and offers thus a new perspective on the subject of cyber risks and cybersecurity. Using SKAD is considered as particularly promising because of the openness of the approach and its focus on discourses and discursive effects. I innovatively adapt it by integrating frames and regulatory styles into the SKAD approach allowing for new insights. It also allows me to expand on solely discourse-focused research: By examining discourse effects, I also take into account the aspect of regulation in the studied field. My theoretical analytical approach is detailed below in section 2.2.3.

SKAD is especially appropriate for risk discourses, as outlined by Keller: In risk discourses, "disputes on contemporary risk reality are conducted as knowledge conflicts" (Keller 2014:19, own translation). SKAD offers appropriate tools in order to examine the "complex discursive arrangements and interdependences of highly different forms of knowledge, technologies, and practices" (ibid., own translation). So, my study contributes to a better understanding of risk discourses at the current example of the discourse on cybersecurity risks.

A *second* contribution of my study is to be found in its comparative design. By comparing the United States and Germany, new insights are expected and are added to the (limited) body of comparative research in a field that is strongly characterized by U.S.-focused research. As Daase notes, risks are "inherently (…) culturally determined" (Daase 2002:13, own translation). This is why a comparison between two countries seems particularly interesting. There is a long tradition of comparative risk research comparing the United States and Europe (see for example Wiener 2011; Vogel 2003; Wiener and Rogers 2002). Among other things, Wiener et al. find that "over the broad array of risks, neither the United States nor

Europe can claim to be 'more precautionary' across the board" (Wiener 2011:28). Rather, the authors find a "great diversity across risks and across policy domains on both sides of the Atlantic" (ibid.). My study contributes to examining the new field of cybersecurity policy and enhancing the understanding of how the United States and Germany handle cyber risks.

Third, it has to be noted that cyberspace and its implications are still considered as "novel environment" (Stevens 2018:1) not yet fully understood. That is why (more) scientific analysis is needed – all the more so as information and communication technology is in permanent evolution (Dunn Cavelty 2008:123), and thus research results become outdated rather quickly. My study is based on a broad and recent data set covering nearly ten years of discourse. In addition, the empirical basis is enriched by 18 personal in-depth interviews that were conducted for the purpose of this study, thus creating a unique data set. All in all, the particularity in the design of my study lies in the combination of its theoretical analytical framework with a focus on a specific actor group, a long time frame, and a "broad understanding of cyber-security" (Dunn Cavelty 2013:106) that allows for a more comprehensive understanding as compared to research focused on specific phenomena such as cybercrime (ibid.:105–106).

2.2 Theoretical Analytical Framework and Research Design

The following chapter presents the theoretical analytical framework[11] and research design of the study in detail. More precisely, the following sections deal with the definitions and focus of the study, its research questions, and the *Sociology of Knowledge Approach to Discourse* (SKAD) and how it is used as framework for the study. Finally, I shed light on the time frame and the examined countries.

[11] The basic ideas of the analytical framework in a preliminary version as well as reflections on some preliminary findings have been published in a working paper and an essay: Kathrin Ulmer, *Cyber Risks and Cyber Security – Risk Communication and Regulation Strategies in the U.S. and Germany*, SWP Working Paper, June 2014, https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/Ulm_WP_Cyber_Risks.pdf (accessed May 15, 2020); Kathrin Ulmer: *Cyber Policy in Germany and the U.S.: Challenges in an Emerging Policy Field*, AICGS Transatlantic Perspectives, Washington, D.C., December 2013, https://www.aicgs.org/publication/cyber-policy-in-germany-and-the-u-s-challenges-in-an-emerging-policy-field/ (accessed May 15, 2020).

2.2.1 Definitions and Focus of the Study

In order to clarify the studied area of cybersecurity and cybersecurity risks, I discuss some basic definitions of relevant terms and their relation to each other. Following the perspective of risk research (see for example Renn 2008), cybersecurity is understood as target of protection in this study, and cybersecurity risks – in short cyber risks – are the hazards threatening this target.[12] Cyberspace is defined as "the fusion of all communication networks, databases and sources of information into a vast, tangled and diverse blanket of electronic interchange" (Dunn Cavelty 2010:155). This space is "virtual and immaterial" (ibid.), but, at the same time, "grounded in physical reality" (ibid.). As will be seen, a clear and precise definition of cybersecurity and cyber risks is not obvious.

Regarding *cybersecurity*, Craigen et al. found that "the term is used broadly and its definitions are highly variable, context-bound, often subjective, and, at times, uninformative" (Craigen, Diakun-Thibault, and Purse 2014:13). In addition, Stevens notes that the "rapidity of cybersecurity's rise as concept and practice, and its convergences with other forms of security, has hindered definitional consensus" (Stevens 2018:1). In order to clarify the definition, Craigen et al. carried out a broad interdisciplinary literature review and conducted group discussions with experts (Craigen, Diakun-Thibault, and Purse 2014:13–16). These efforts resulted in an inclusive definition reflecting main substantial features of cybersecurity as well as perspectives of an interdisciplinary community working in the field of cybersecurity (ibid.:15–16). The definition states: "Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights" (ibid.:13). This definition addresses several main features of cybersecurity: It includes protection from all "occurences" (ibid.:17), that means all hazards, "including intentional, accidental, and natural hazards" (ibid.). Moreover, the definition relates to cyberspace, but also "cyber-enabled" (ibid.) systems in a larger sense, "such as computer control systems and cyber-physical systems" (ibid.). The authors state that, "[b]y extension, the protection

[12] Renn uses the term "sources of risks" (Renn 2008:4) and "hazardous agents" (ibid.:6). In our case, cybersecurity would be "what humans value" (ibid.:2).

applies to assets and information of concern within cyberspace and connected systems" (ibid.). Finally, aspects of "ownersphip and control" (ibid.) are included.[13]

Regarding *cyber risks*, the term "occurences" was already presented as a first definition including a diverse set of hazards. In order to define and classify these hazards more precisely, I refer to Cebula and Young (2010). They define "operational cyber security risks" (Cebula and Young 2010:2) as "operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems" (ibid.:1). Their taxonomy includes four classes with several subclasses:

- "actions of people – action, or lack of action, taken by people either deliberately or accidentally that impact cyber security
- systems and technology failures – failure of hardware, software, and information systems
- failed internal processes – problems in the internal business processes that impact the ability to implement, manage, and sustain cyber security, such as process design, execution, and control
- external events – issues often outside the control of the organization, such as disasters, legal issues, business issues, and service provider dependencies" (ibid.:2).

In the subclass of deliberate actions, the authors list "actions taken intentionally and with intent to do harm" (ibid.:4):

- Fraud: "a deliberate action taken to benefit oneself or a collaborator at the expense of the organization" (ibid.);
- Sabotage: "a deliberate action taken to cause a failure in an organizational asset or process, generally carried out against targeted key assets by someone possessing or with access to inside knowledge" (ibid.);
- Theft: "the intentional, unauthorized taking of organizational assets, in particular information assets" (ibid.);

[13] As to the concept of property rights, Craigen et al. explain as follows: "This aspect incorporates the two separate notions of ownership and control that dominate discussion of cybersecurity and digital assets introduced in the property rights framework of Ostrom and Hess (2007), which include access, extraction, contribution, removal, management, exclusion, and alienation. Any event or activity that misaligns actual (de facto) property rights from perceived (de jure) property rights, whether by intention or accident, whether known or unknown, is a cybersecurity incident" (Craigen, Diakun-Thibault, and Purse 2014:17).

- Vandalism: “the deliberate damaging of organizational assets, often at random” (ibid.).

Focus of the study. With regard to the political sphere, these intentional actions are particularly important as people are at their origin: As Dunn Cavelty notes, “[t]his category, even though not necessarily the most prominent one in terms of frequency of occurrence or impact, is of prime importance in the cyber-threats debate because of the actor dimension” (Dunn Cavelty 2010:155–156). This group of risks is at the center of interest in my study and serves as basic orientation for the context mapping (chapter 3) and the discourse analysis (chapter 4). Although the group comprises a large number of phenomena, I keep the perspective open and broad. On the one hand, a “broad understanding of cyber-security” (Dunn Cavelty 2013:106) allows for a more comprehensive understanding than research focused on specific phenomena such as cybercrime (ibid.:105–106). On the other hand, this is also necessary as the actors in the focus of this study, the political discourse participants, do themselves approach the topic in a rather broad fashion. At the high political level, the discourse analysis sheds light on – for example a speech of the U.S. president – there is, for the most part, only little specification, which precise cyber risk is addressed. This corresponds to a finding on threat perception by scholars of political psychology pointing to the psychological heuristic of simplicity found with political actors: “Political leaders trying to assess a threat need to make a very complex world somewhat simpler. To do so, they unconsciously strip the nuance, the context, the subtleties out of the problems they face in order to build simple frames” (Gross Stein 2013:371). The breadth of the discourse and the long time frame of nearly ten years I take into account allows me to see “the bigger picture” from a research perspective, and to find out, for example, if certain discourse participants have or develop a focus on certain phenomena, if this is a logic consequence of their specific role in the executive, or if there are changes in the course of time.

While applying a broad perspective on deliberate cyber risks, I have a particular interest in a specific target: *critical infrastructure*. That is why I put a special focus on cyber risks for critical infrastructure. In the United States, critical infrastructure is defined as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national

economic security, national public health or safety, or any combination of those matters" (WH 2013a:15). The following 16 sectors are defined as critical: "Chemical", "Commercial Facilities", "Communications", "Critical Manufacturing", "Dams", "Defense Industrial Base", "Emergency Services", "Energy", "Financial Services", "Food and Agriculture", "Government Facilities", "Healthcare and Public Health", "Information Technology", "Nuclear Reactors, Materials, and Waste", "Transportation Systems", and "Water and Wastewater Systems" (ibid.:15-16). In Germany, critical infrastructure is defined as "organizations or institutions with major importance for the public good, whose failure or damage would lead to sustainable supply bottlenecks, considerable disturbance of public security or other dramatic consequences" (D-03 BMI 2011:15). Critical infrastructure comprises the following sectors: "Energy, Information technology and telecommunication, Transport, Health, Water, Food, Finance and insurance sector, State and administration, Media and culture" (ibid.). In the IT security law, the list of sectors is the same with the exception that state and administration as well as media and culture are not part of the list (Bundestag 2015b:1324).

As outlined in the above definitions, critical infrastructure is of vital importance for societies, so attacks on this infrastructure can have severe effects (WH 2013a; Bundestag 2015b). At the same time, today's critical infrastructure is highly complex, interdependent and cybersecurity-related attacks are of major relevance, as many critical infrastructure systems significantly depend on IT (D-21 BBK 2011:5): "A failure or restriction of ICT [information and communication technology, K.U.] components in the operator's critical processes may (…) result in a restriction of service provisions and, in a worst-case scenario, to a complete interruption of supply. Dependencies between individual sectors or industries increase the risk of failures even further. Failures in one sector may lead to failures in other sectors, triggering a domino effect" (D-14 BSI 2015:42). So-called SCADA (Supervisory Control and Data Acquisition) systems that are used in many critical infrastructures constitute an example for a major point of vulnerability in critical infrastructure (D-21 BBK 2011:5). Against this background, it is particularly interesting to shed light on cybersecurity-related risks for critical infrastructure – in the discourse (chapter 4) and regarding regulation (chapter 5).

Finally, I would like to distinguish cybersecurity from *safety*. While cybersecurity is focused on the aspects outlined above, the term safety, in a technical context, "is built upon

reliability theory and looks into statistical malfunctions of components with small probabilities and how they will impact functionality" (Ebert and Lieckfeldt 2017:29–30). From the domain of automotive engineering, we can learn the difference between safety and security: "While safety deals with avoiding critical failure modes, security has to cope with intelligently introduced causes of faults, which is far more difficult, given that the attackers' intelligence, willingness, determinedness, and creativity often exceed that of the engineers looking to a problem from the – different – perspective of how to solve it, and not how to find loopholes and strange feature correlations" (ibid.:32). Again, the aspect of the intelligent attacker is fundamental in the area of cybersecurity, as was already discussed before. In the context of a car, it is easy to illustrate the relation between safety and security: "One might argue that safety is about criticality for the life and health of the system's user, while security is only about annoyances. It is however obvious that within a safety-critical system, such as a car, security meets safety because malfunctions can interact and cause disturbances that can result in accidents" (ibid.:29–30). So, cybersecurity is a "mandatory condition" (ibid.:43) for safety. We can transfer these findings to our context, above all regarding critical infrastructure: The topic of this study is cybersecurity, but attacks on the cybersecurity of a system can have safety implications, for example, a cyber attack on critical energy infrastructure can also compromise public safety as a result (see also D-14 BSI 2015:42).

2.2.2 Research Questions

The study aims at exploring and analyzing political communication and regulatory processes related to cyber risks. The goal of the study is to answer the overall **research question**: **How do the executives of the United States and Germany address cybersecurity risks? In particular, what is the approach to cybersecurity-related risks for critical infrastructure?** "Addressing" has got a threefold meaning in the context of the study:

- First, addressing the studied risks in an *institutional* sense: The roles and responsibilities in the area of cybersecurity policy in both countries are identified in order to find out: **Who is doing what in the new field of cybersecurity policy in the United States and Germany?** This is done in what I term "context mapping" (chapter 3).

- Second, the study wants to find out how the studied risks are addressed in the political *discourses* of the executives of both countries. The discourses are examined in a discourse analysis with the goal of identifying frames. **How do representatives of the U.S. and German executives frame cybersecurity risks in their official communication?** The discourse analysis (chapter 4) constitutes the main part of the empirical study.
- Third, addressing is understood in the sense of *regulation*. The study examines one regulatory example for each country: **Is the selected example taken from the field of cybersecurity policy in line with the traditional regulatory style of the country?** In contrast to the long-term analysis conducted in the disourse part, chapter 5 presents the analysis of a selected piece of regulation.

2.2.3 The Sociology of Knowledge Approach to Discourse as Framework for the Study

In order to answer the research questions outlined above, the study follows a qualitative-interpretative design analyzing the United States and Germany. In its theoretical analytical conception, the approach of my study is based on Reiner Keller's Sociology of Knowledge Approach to Discourse (SKAD) (Keller 2011b; Keller 2011a). SKAD is a "research programme embedded in the sociology of knowledge tradition in order to examine the *discursive construction* of symbolic orders which occurs in the form of conflicting social knowledge relationships and competing politics of knowledge" (Keller 2011b:48, emphasis in original). Knowledge in the context of SKAD includes more than proven facts, it rather is "a general expression to treat something as 'real'" (Keller 2014:16).

In general, discourse research is a heterogenerous field.[14] Keller's approach to discourse analysis is particularly suitable for my study for several reasons: The approach puts the emphasis on meaning and meaning construction (Keller 2014:16). Moreover, its theoretical

[14] According to Keller, several approaches can be distinguished, among them are: "discourse analysis" (Keller 2004:20–22) with a focus on "'natural' communication processes in different contexts" (ibid.:20, own translation), "(corpus-)linguistic-historical discourse analyses" (ibid.:22–26, own translation), "Critical Discourse Analysis" (ibid.:26–34) after van Dijk, Wodak, and Fairclough (ibid.:26–31) and after Jäger (*Kritische Diskursanalyse*) (ibid.:31–34) as well as "culturalistic discourse research" (ibid.:34–41, own translation). Despite this heterogeneity, Keller identifies four characteristics that most of the approaches have got in common: a constructivist theoretical base, a Foucauldian understanding of discourse (Keller et al. 2003:10), a "'post-positivist, descriptive-reconstructive methodology" (ibid.:11) as well as a focus on text-based working (ibid.).

foundations and the focus on collective actors (Ballaschk 2015:4) match with the research interest of this study. So does the high importance attached to the aspect of power (Keller 2011a:208) that is particularly relevant in a young policy field such as cybersecurity. Reiner Keller began to develop SKAD in the 90s (Keller 2011b:43), primarily in his dissertation on "Waste – The Societal Construction of What is Valuable" (Keller 1997a, own translation) and in following theoretical and methodological works. With the integration of two more elements into the SKAD framework, namely frames and regulatory styles, my study proposes an innovative way of adapting Keller's approach and applies it to a new empirical field.

Discourses. Keller, following Foucault, understands discourses as manifest social practice that is realized in communication in diverse ways of sign usages, such as documents or the spoken word (Keller 2014:16; Keller 2011b:53). They are able to stabilize meanings, which is to "fix them in time and by so doing, institutionalize a binding context of meaning, values and actions/agency within social collectives" (Keller 2011b:51). Other than the general meaning of discourse as equivalent to "conversation" (Keller 1997b:311, own translation) or "speech" (ibid., own translation), the term discourse designates "an institutionalized form of text production with a specific content or topic" (ibid., own translation). In this sense, a "public discourse" (ibid.) is "a sort of indirect conversation among absent persons" (ibid., own translation). There is a close relationship between discourse and power as "social control and power are increasingly transferred by discourse, i.e. by symbolic practices and communication" (Keller et al. 2001:8, own translation). In this sense, Keller states that "discourse structures are, at the same time, structures of power; discursive arguments are power-driven conflicts over the power of interpretation" (Keller 2011a:208, own translation; similarly Keller 1997b:316–317). In a political context, actors seek to translate their interpretations into political action (Keller et al. 2001:8). The element of power was notably introduced by Foucault, but also symbolic interactionism (Keller 2011b:47).

Actors. As Keller notes, discourses "come only 'alive' by actors and their speech acts" (Keller 2011a:253, own translation). In the SKAD framework, actors are understood as "speakers and representatives of more or less big social groups" (ibid., own translation) such as political parties or organizations (ibid.). It is important to note that SKAD focuses on the *roles* that actors take on in their positions, most notably being advocates of an organization's

interests, not on actors as individual human beings (ibid.). In my study I call the actors "discourse participants". The actor conception and level of analysis constitute a specific feature of SKAD: The approach is dedicated to find out "how *collective* actors, organizations, and institutions create, confirm or change discursive reality" (Ballaschk 2015:4, own translation, emphasis added). In contrast to other approaches of discourse analysis, SKAD is thus especially interested in "the collective level of processes of societal constructions of reality" (Keller 1997a:313, own translation). Therefore, SKAD fits well with the research interest of my study that examines ministries and other agencies as discourse participants, thus collective actors at the level of the executives in the United States and Germany. Another interest of SKAD is to identify particularly prominent actors in the discourse (Ballaschk 2015:4).

Field of research. SKAD's field of research is "the production and transformation of societal knowledge conditions by knowledge policies, i.e. discursively structured efforts of social actors to assert the legitimacy and recognition of their interpretation of the world effectively" (Keller 2011a:193, own translation). Under the SKAD framework, many different research questions can be studied empiricially (Keller 2011a:262). Among the possible research areas proposed by Keller (ibid.:262–263), my study notably concentrates on actors, interpretations and problem solutions, applied to the cybersecurity discourses in the United States and Germany. As Keller notes, SKAD needs to be adapted according to the specific research interest (Ballaschk 2015:4; Keller 2003:198). This is done at the end of this section.

Theoretical foundations. SKAD's theoretical foundations are based on three schools of thought:

- The first component is *sociology of knowledge* following Berger and Luckmann and their idea of the "social construction of reality" (Berger and Luckmann 1966). They developed a "fundamental theory of societal knowledge production, objectivation, circulation and appropriation" (Keller 2004:58, own translation). Keller notably underlines the authors' "dialectical perspective on society both as 'objective reality' and as 'subjective reality', becoming 'real' through all kinds of knowledge" (Keller 2011b:48). However, Keller distances himself from Berger's and Luckmann's explicit focus on "daily, basal stocks of knowledge" (ibid:58, own translation) of individual

people, and integrates the collective, discursive level in his SKAD framework (Keller 2011b:46; Keller 2004:58–59).

- A second component is provided by *symbolic interactionism* with its "comprehensive programme to analyse the collective battles of interpretation concerning contested social issues or 'social problems'" (Keller 2011b:45). So, symbolic interactionism strongly emphasizes the "acting of *collective actors*" (Keller 1997b:314, own translation, emphasis in original). An interpretative battle can consist of issues such as how a problem is defined, who is responsible or what solution should be favored (ibid.).
- The final component is *Foucault's* work on discourse theory and several of his concepts (Keller 2011b:48; Keller 1997b:313–314). According to Keller, "Foucault's fundamental achievement was to look at discourses as socio-historically situated 'practices', (…) and to 'liberate' discourse analysis from the specific linguistic issues" (Keller 2011b:46). Foucault provides many theoretical concepts used by Keller (Keller 2011b:48). Foucault's idea of "*dispositif*" (Keller 2011b:56, emphasis in original) is of special importance in the context of SKAD. A dispositif is "an installed infrastructure designed to 'solve a problem', for instance, consisting of a law, administrative regulations, staff, things like cars, computers and so on" (ibid.:49).[15] In this way, discourses have an impact in the real world (Keller 2011a:258–259). They are "the real means for the realization of the *external 'power*-effects' of a discourse" (Keller 2011b:56, emphasis in original). So, SKAD uses a Foucault-inspired double perspective on discourses, as it takes into account "the knowledge side and the 'power effects of discourses'" (Keller 2011b:63).

Finally, it has to be mentioned that SKAD is a *constructivist* approach (Keller 2011a:271). Constructivism in this case means "to orient the analysis towards the societal production of 'the order of things' within discursive knowledge politics" (ibid., own translation). Although SKAD is a constuctivist approach, it nevertheless implies a "'weak realism' in the sense of the pragmatist tradition" (ibid., own translation). The constructivist perspective fits well with my research focus on cybersecurity risks. It is interesting to note that scholars of threat

[15] Keller also mentions dispositifs of discourse (re-)production (Keller 2011b:63; Keller 2011a:258). However, the focus here is on external effects.

perception equally underline the importance of language and construction processes by emphasizing that "threats are not self-evident or easily measurable realities, but the outcome of a complex process of social and political construction through the means of language" (Meyer and Miskimmon 2009:625–626).

Adaptation of SKAD in the context of this study. In the following sections, I elaborate on how I use SKAD in order to answer my research questions. In a first step, I elaborate what I call a "context mapping". Then, I implement SKAD's double perspective on knowledge and power by integrating two concepts into the SKAD framework: frames and regulatory styles. The "knowledge side" (Keller 2011b:63) is examined by identifying frames used in the cybersecurity discourses in both countries. As example of "power-effects" (ibid:60), I analyze two examples of cybersecurity regulation, understood as external effects of the cybersecurity discourses. This twofold view is particularly interesting with regard to the empirical context of cybersecurity policy.

2.2.3.1 Context Mapping: SKAD and the Importance of Context Knowledge

In a first step, I develop a context mapping. The context mapping serves to answer my first research question: Who is doing what in the field of cybersecurity policy in the United States and Germany? At the same time, the context mapping prepares the discourse analysis. The relevance of the context mapping corresponds to the necessity, pointed out by Keller, to have a detailed knowledge of the context, in which a discourse takes place, in oder to be able to understand the language and meanings in this specific context (Ballaschk 2015:5; Keller 1997b:318). This step seems especially relevant in a young policy field such as cyber policy, where roles and responsibilities are still evolving.

The study examines the discourse of the executives in both countries, more precisely, those parts of the respective executives – i.e. federal departments or ministries and subordinate agencies – that are relevant in the context of cybersecurity policy. They are understood as discourse participants in the context of this study. I argue that this approach is useful in order to gain insights about the construction and interpretation of cyber risks and cybersecurity by this specific group. The focus of the study is on the executives of both

countries as those are seen in a special and leading position for shaping the political discourse and the implementation of measures.

In other fields, scholars use approaches centered on specific groups, too: For example, Meyer, in a study on terrorism, uses a differentiated model arguing that "threats are socially constructed within and among the discourses of experts, political actors and the public at large, each using their own lenses through which they see 'the threat'" (Meyer 2009:648). The intention of my study is to examine how executive actors communicate about cybersecurity risks. Of course, multiple factors influence the perception of political actors, as we can learn from threat perception scholars: "Political actors take (…) expert and professional opinions into account, but are also concerned about how threats fit in with other motivations such as gaining electoral advantage, enhancing reputation and power, as well as avoiding blame for threats that materialize" (Meyer and Miskimmon 2009:626). However, the focus of my study is not how perceptions come into existence, but how political actors officially communicate on cyber risks and cybersecurity.

The identification of relevant discourse participants is carried out in chapter 3 and based on a thorough examination of the roles and responsibilities of institutional actors in the field of cybersecurity policy.

2.2.3.2 The "Knowledge Side" of Discourse: Identification of Frames in the Discourse

Following the context mapping, I conduct the discourse analysis in a narrower sense. The goal in exploring the "knowledge side" (Keller 2011b:63) of discourse is to identify the frames used by discourse participants. Therefore, I use a frame concept that was developed in the U.S. social movements research, more precisely, the frame concept of Robert M. Entman (Entman 1993).[16] By the analysis, I can answer my second research question: How do representatives of the U.S. and German executives frame cybersecurity risks in their

[16] In order to explore the substance of discourses, Keller proposes different concepts, such as "interpretation patterns [*Deutungsmuster*, K.U.], classifications, phenomenon structures, and narrative structures" (Keller 2011a:240, own translation). Keller defines interpretation patterns as "basic schemes generating meaning that are disseminated by discourses and suggest what a phenomenon is about" (ibid: 243, own translation). Keller also mentions findings from the U.S. social movements research pointing to the strategic use of such interpretation patterns (ibid.). However, for the reasons laid out above, I use Entman's frame concept (Entman 1993).

official communication? As cyber risks like "[m]ost risks that modern societies faces are not directly experienced by human senses, but are learned through communication" (Renn 2008:99), it is particularly interesting to learn how political actors communicate about cyber risks and cybersecurity and which frames they use.

For my analysis, I use the frame definition of Robert M. Entman (Entman 1993). According to the definition of Entman (1993), frames have different functions: "Frames … *define problems* – determine what a causal agent is doing with what costs and benefits, usually measured in terms of common cultural values; *diagnose causes* – identify the forces creating the problem; *make moral judgments* – evaluate causal agents and their effects; and *suggest remedies* – offer and justify treatments for the problems and predict their likely effects" (Entman 1993:52, emphasis in original). Entman emphasizes the importance of selection as well as salience in the context of framing: "To frame is to *select some aspects of a perceived reality and make them more salient in a communicating text, in such a way as to promote a particular problem definition, causal interpretation, moral evaluation, and/or treatment recommendation* for the item described" (Entman 1993:52, emphasis in original). So, frames show, which specific key messages the examined actors intend to convey (see also Potthoff 2012:76). The fact of emphasizing some aspects means omitting others; Entman notes that omissions can have an effect as well: "Most frames are defined by what they omit as well as include, and the omissions of potential problem definitions, explanations, evaluations, and recommendations may be as critical as the inclusions in guiding the audience" (Entman 1993:54).

Potthoff evaluates Entman's definition as the "most well known frame definition" (Potthoff 2012:38, own translation) and acknowledges "Entman's important contribution for framing research" (ibid.:40, own translation). According to Matthes, Entman's definition of frames is the most frequently used definition in the context of empirical studies (ibid.:38-39). Also, Entman's definition inspired many frame definitions developed later on (ibid.:49).[17] In this study, Entman's definition is used for several reasons: It is compatible with the SKAD approach, and, against the background of my particular research interest, it has several

[17] However, Potthoff criticizes the lacking theoretical foundations of Entman's definition and perceives a bias in Entman's work because of his "critical perspective" (Potthoff 2012:40, own translation) towards framing as a sort of manipulation (ibid.). These aspects are considered of minor importance in the context of this study that is based on the SKAD framework as theoretical approach.

benefits, most notably its detailed definition and the designation of specific frame elements that are used as structuring elements in my research process.

As a background, I give a brief overview on the development and use of frame concepts in literature. Erving Goffman's study "Frame Analysis – An Essay on the Organization of Experience" (1974) can be considered as origin of frame analysis (Keller 2003:209) that inspired many subsequent approaches (Meiser 2011:26). Frames can be seen as a kind of "interpretive schemes" (Goffman 1993:31, own translation) that help people to give meaning to the situations and events they experience (ibid.:18). Benford and Snow find applications of the frame concept in diverse disciplines of the social sciences, however a particularly strong application in the sociological research on social movements (Benford and Snow 2000:611–612). This branch of research especially highlighted the aspect of "meaning work – the struggle over the production of mobilizing and countermobilizing ideas and meanings" (Benford and Snow 2000:613). The interest in this aspect is also shared by SKAD.

According to Benford and Snow, a frame "refers to an interpretative schemata that simplifies and condenses the 'world out there' by selectively punctuating and encoding objects, situations, events, experiences, and sequences of actions within one's present or past environment" (Snow and Benford 1992:137). Benford and Snow identify three "core framing tasks" (Benford and Snow 2000:615), in which a certain similiarity to Entman is found. These are (1) "diagnostic framing" (ibid.), which means "problem identification and attributions" (ibid.), (2) "[p]rognostic framing" (ibid.:616), which denotes "the articulation of a proposed solution to the problem, or at least a plan of attack, and the strategies for carrying out the plan" (ibid.), and (3) "[m]otivational framing" (ibid.:617) implying "a 'call to arms' or rationale for engaging in ameliorative collective action, including the construction of appropriate vocabularies of motive" (ibid.).

In general, we can differentiate between "*frames in thought*" (Druckman 2001:228, emphasis in original) and "*frames in communication*" (ibid.:227, emphasis in original). The former is a "set of dimensions that affect an individual's evaluation" (Chong and Druckman 2007:105), whereas the latter denote "the key considerations emphasized in a speech act" (ibid.:106). As to discourses of elites as in the context of this study, frames in communication

are of particular importance (Druckman 2001:227). Druckman outlines an example: "The frame that the speaker chooses may reveal what the speaker sees as relevant to the topic at hand (…). For example, a politician who emphasizes economic issues when discussing the campaign uses an 'economy frame' that suggests economic considerations are pertinent" (ibid.:227).

Snow underlines that symbolic interactionism and constructivism build the theoretical foundation of framing (Snow 2004:384). A crucial aspect in this theoretical basis is the idea "that meanings do not automatically or naturally attach themselves to the objects, events, or experiences we encounter, but often arise, instead, through interactively based interpretive processes" (ibid.). Accordingly, movement members in Snow's conception – or political actors in the case of this study – are engaged in "signifying work or meaning construction" (Snow 2004:384). Zald notes on the features of successful strategic framing that "[c]ompetent strategic framers typically seek to package their issues simply and in ways that are consistent with the ideals and contemporary themes of civic life" (McCarthy, Smith, and Zald 1996:309) and that, "[i]n their most truncated version, frames reduce complex issues into evocative phrases, metaphors, and slogans" (ibid.:311).
The identification of frames in the cybersecurity discourses of both examined countries is carried out in chapter 4.

2.2.3.3 "Power-Effects" of Discourse: Analysis of Regulatory Examples

In a final step of my empirical analysis, I examine two regulatory examples understood as "power-effects" (Keller 2011b:60) of the cybersecurity discourses in both countries in order to answer the third research question: Is the selected example taken from the field of cybersecurity policy in line with the traditional regulatory style of the country? Risk regulatory styles have been developed in the research on environmental, health and safety risk regulation (Renn 2008:358–361; Renn 2001; O'Riordan and Wynne 1987; Vogel 1986; Brickman, Jasanoff, and Ilgen 1985). Research found different styles in the United States and Europe (ibid.). In particular, the United States was found to have an "adversarial approach to regulation" (O'Riordan and Wynne 1987:398; see also Renn 2008:359), whereas a "corporatist approach" (O'Riordan and Wynne 1987:403–404; see also Renn 2008:359) was attributed to Germany. The classification provides a helpful tool in order to find out,

whether these styles can be found in the field of cybersecurity policy, thus if the classification is also empirically valid in a new policy field. Extending the empirical use of the classification allows for new insights on regulatory styles. Some important research contributions on regulatory styles are presented in the following.

David Vogel conducts a comparison of environmental policies in two countries: Great Britain and the United States (Vogel 1986). He mainly focuses on the handling of pollution and hazardous substances as well as land-use planning (ibid.:11). In his comparison, Vogel finds that Great Britain and the U.S. have developed different ways of regulating these issues, they use "divergent approaches to controlling the externalities associated with industrial growth" (ibid.:9): "On balance, the American approach to environmental regulation is the most rigid and rule-oriented to be found in any industrial society; the British is the most flexible and informal" (ibid.:21). As the United States is one of the examined countries in this study, I briefly present Vogel's description of the U.S. regulatory style: The U.S. approach can be characterized as adversarial and strongly formalized, frequently using broad rules (ibid.:21,146,220). Mandatory impact assessments present regular features in U.S. regulatory processes (ibid.:21). Discretionary powers of the administration are very limited, and prosecution is frequent (idib.:21). Also, due to their open character, "[t]he entire regulatory process is subject to close scrutiny by the courts, the legislature, and the public as a whole" (ibid.:220). In consequence, there are intense political controversies (ibid.:222,261–263). An important element in the American system is pluralism: Interest groups compete openly and have large access to the regulatory process (ibid.:278–279). Both countries differ greatly regarding how government and business relate to each other: While cooperation prevails in Great Britain, "no other business community is so dissatisfied with its nation's system of environmental controls as the American business community" (ibid.:21). Accordingly, Vogel states a high level of conflict deepening the adversarial character (ibid.:147).

Brickman, Jasanoff and Ilgen provide another detailed work on regulatory styles in a comparative perspective (Brickman, Jasanoff, and Ilgen 1985). They examine and compare the regulation of toxic chemicals in four countries: The United States, Great Britain, France as well as Germany (ibid.:7). As a result, they find different ways of regulation on both sides of the Atlantic: "American regulatory processes stand apart in the complexity of their procedures, the heavy reliance on formal analysis of risks and benefits, the openness of

administrative decision making, and the active supervision of executive agencies by Congress and the courts. European processes, despite some notable differences among them, share simpler administrative procedures, greater informality in the analysis of evidence, less complete public access to decision makers, and relatively little oversight by parliament or the courts" (ibid.:23). Like Vogel (Vogel 1986:225), Brickman et al. state that, despite different regulatory styles, comparable regulatory measures were taken in all countries in the end (Brickman, Jasanoff, and Ilgen 1985:23).

Also, O'Riordan and Wynne underline the existence of different styles: According to them, "risk regulation is part of a national style of government" (O'Riordan and Wynne 1987:389). They mention four characteristics being part of all regulatory styles: (1) consultation or other ways of dialogue, (2) expertise, (3) "some degree of self-policing" (ibid.:396), and (4) political elements such as the decision which level of risk is acceptable (ibid.:395–397). Depending on the respective practical implementation and structure of these characteristics, four different regulatory approaches emerge (O'Riordan and Wynne 1987:397–404). Their main characteristics are presented in the following table (Figure 1).

Figure 1: Regulatory Approaches after O'Riordan and Wynne (1987)

Approach	**Characteristics**	**Associated Governing System/Country**
Adversarial Approach	- Large executive agencies - Precise rules - Formalized procedures - Frequent judicial review - Open documentation - Regulatory process easily accessible for diverse interests - High degree of conflict and bargaining	- "The adversarial approach tends to be found in governing systems where a strong central institution is expected to regulate very diverse and geographically dispersed client groups, where patterns of ownership, management skills, and environmental circumstances vary enormously. It also reflects a political culture of institutionalized distrust" (O'Riordan and Wynne 1987:399) - USA
Consensual Approach	- Trustful and cooperative relations	- UK

	between regulators and the regulated - Confidential arrangements - Flexible rules - Practicability as guideline for standard setting - Self-regulation - Rare use of prosecution	
Authoritative Approach	- Freedom of the regulator in standard setting and the enforcement of compliance - Very limited and selective consultation - Limited judicial review - Confidential negotiations	- "This approach is most likely to be found in countries with strong central government but weak legislatures, where local or regional government is constitutionally limited to executing commands from the center, and where the public have little tradition of militancy or distrust" (O'Riordan and Wynne 1987:402) - France as nearest example
Corporatist Approach	- Rather formalized mode of negotiation between major interest groups - Difficult access for less organized interest groups - Strong position of scientific advice/expertise - Application of some elements of the adversarial, consensual and authoritative approaches	- "In many respects the corporatist approach is an amalgam of the other three operating in a particular structure of relationships. Corporatism refers to collegiate forms of organization in which different interests maneuver to promote their common interests. Corporatism is found where powerful groups have mutual advantage of acting collectively" (O'Riordan and Wynne 1987:403) - Germany

Source: Own compilation on the basis of O'Riordan and Wynne 1987:398–404.

Finally, I present the summary of regulatory styles according to Renn (2001). They are in line with the literature already presented, but offer a "more analytical treatment of regulatory styles" (Renn 2001:406). Renn assumes that "[r]egulatory actions rest on two components: knowledge and legally prescribed procedures" (ibid.:406). How knowledge is included in policy processes depends on specific national characteristics embodied in "culture, political traditions, and social norms" (ibid.:407). National ways of dealing with risks depend on the specific configuration of the following sets of rules: (1) "The selection rules of what the policy makers regard as important and helpful" (ibid.): This element deals with the type of knowledge and arguments regarded as valuable and being integrated in a given regulatory policy process (for example, quantifiable vs. qualitative data) (ibid.). (2) "The processing rules for scientific information within the policy-making agencies" (ibid.): The second aspect concerns the status of experts and expertise (for example, the role of an expert as adviser vs. an active role as policy-designer) (ibid.). (3) "The rules for mixing expertise with anecdotal evidence and strategic maneuvering" (ibid.): This element deals with the status of scientific input in regulatory processes (ibid.). (4) "The rules for legitimizing policy decisions in the public" (ibid.): This last set of rules deals with the inclusion of public perceptions and which importance perceptions should have in comparison to scientific knowledge (ibid.). From the implementation of these rules, four regulatory styles emerge (ibid.:407–409). Renn's summary of these styles and their main characteristics are represented in the following table (Figure 2).

Figure 2: Summary of Regulatory Styles and their Characteristics after Renn (2001)

Style	Characteristics	Role of Scientific Expertise
Adversarial approach	- Open to professional and public scrutiny - Need for scientific justification of policy selection - Precise procedural rules - Oriented toward producing evidence	- Main emphasis on scientific evidence and pragmatic knowledge - Integration of adversarial positions through formal rules (due process) - Little emphasis on personal judgment and reflection on the side of scientists - Contingent on claims of methodological objectivity
Fiduciary approach (patronage)	- Closed circle of "patrons" - No public control, but public input - Hardly any procedural rules - Oriented toward producing faith in the system	- Main emphasis on enlightenment and background knowledge - Strong reliance on institutional in-house "expertise" - Based on bureaucratic efficiency - Contingent on personal relationships
Consensual approach	- Open to members of the "club" - Negotiations behind closed doors - Flexible procedural rules - Oriented toward producing solidarity with the club	- Main emphasis on (scientific) reputation - Strong reliance on expert judgment (also non-scientific experts) - Main emphasis on positive attitude - Contingent on social status and political position
Corporatist approach	- Open to interest groups and experts - Limited public control, but high visibility - Strict procedural rules outside of negotiation table - Oriented toward sustaining trust to the decision-making body	- Main emphasis on expert judgment and political prudence - Strong reliance on impartiality of experts - Integration by bargaining within scientifically determined limits - Contingent on senior status within science communities

Source: Table in Renn 2001:408.

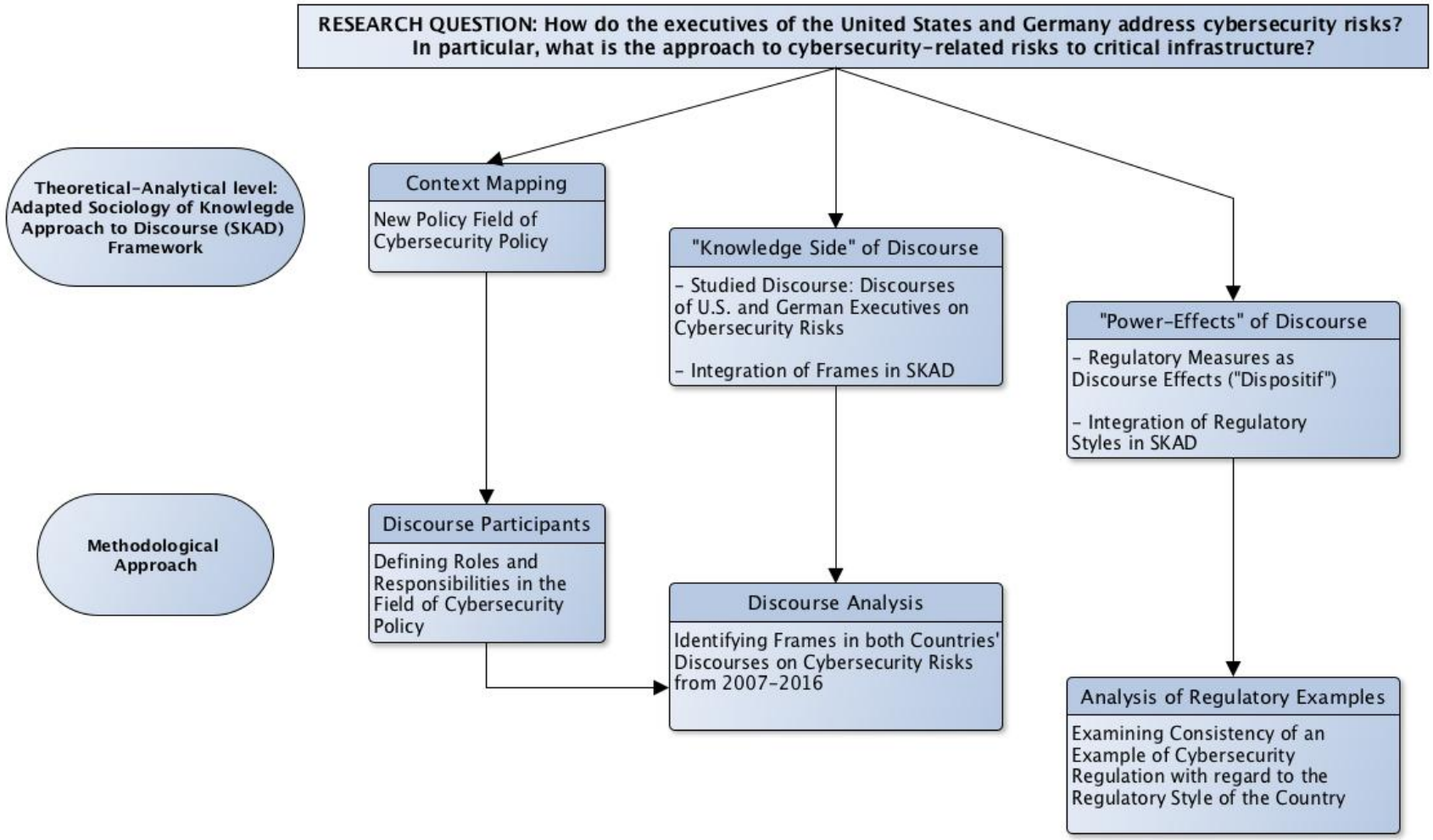
As a concluding remark on the presented regulatory styles it has to be noted that research has identified changing trends in the field of regulatory processes (Löfstedt and Vogel 2001; Renn 2001). At the same time, there is recent research on Germany stating a remarkable "stability of its regulatory model" (Bignami 2011:445). In any case, regulatory styles "cannot be found in pure form in any country" (Renn 2008:359; similarly O'Riordan and Wynne 1987:404). However, as Renn notes, "they form the backdrop of socio-political context variables against which specific risk governance structures are formed and operated" (Renn 2008:359). So, the regulatory styles should be understood as "*ideal types*" (O'Riordan and Wynne 1987:404, emphasis in original). O'Riordan and Wynne also underline their usefulness as indicators and framework (ibid.:404–405).[18] In this sense, the presented styles constitute the basis for my analysis of a U.S. and a German regulatory example in the field of cybersecurity policy (chapter 5).

2.2.3.4 Overview: Adapted SKAD Framework

The following graphic (Figure 3) summarizes the theoretical analytical framework presented before: The SKAD framework with the integration of frames and regulatory styles.

[18] Regulatory styles "can be treated as patterned indicators, providing descriptive categories which point to unidentified or unclarified underlying structural features of political culture that affect styles of government. (…) Second, these ideal types provide a framework within which different substantive elements of local 'style' can be identified and separately treated" (O'Riordan and Wynne 1987:404–405).

Figure 3: Adapted SKAD Framework



Source: Own compilation.

2.2.4 Time Frame

The time frame for the study is the period from 2007 to 2016. 2007 is taken as the starting date, as in April and May of 2007, the cyber attacks on Estonia took place (Rötzer 2007; Ziegler 2007).[19] The attacks involved "large-scale digital attacks on Estonian public and private institutions in response to the government's removal of a World War II memorial" (Hansen and Nissenbaum 2009:1156).[20] The particularity of the incident was that "[t]he coercive denial of service attacks against Estonia were the first overt political use of cyber techniques" (Lewis 2014:571). It was vividly discussed in international media: For example, the *New York Times* designated the attacks as "'the first real war in cyberspace'" (Hansen and Nissenbaum 2009:1168). According to Lewis, the attacks caused "broad international concern" (Lewis 2014:571). The Estonian government claimed that the attacks were an act of cyberwar launched by Russia (Ziegler 2007). However, NATO "decided that the denial of service attacks did not qualify as an armed attack, and thus did not trigger Article 5 obligations for collective self-defence" (Lewis 2014:570). The attacks also spurred an academic discussion, in which several experts articulated that the attacks do not qualify as cyberwar (Rid 2012; Rötzer 2007).

Overall, the attacks had a major impact on the international debate on cyber risks, as one interviewed U.S. expert put it: "[T]here was a change in focus and influence starting in 2007 with the Estonia attack and the debate in NATO about whether it would trigger article 5 or not. People became more aware that this could be a thing that could threaten national security" (I-07:67). Therefore, it is considered as an appropriate starting point for the

[19] Rid gives a detailed description of the attacks: "The cyber attacks started in the late hours of Friday 27 April. Initially the attackers used rather inept, low-technology methods, such as ping floods and simple denial of service attacks. Then the attacks became slightly more sophisticated. Starting on 30 April, simple botnets were used to increase the volume of distributed denial of service (DDoS) attacks, and the timing of these collective attacks was increasingly coordinated. Other types of nuisances included email and comment spam as well as the defacement of the Estonian Reform Party's website. Estonia experienced what was then the worst-ever DDoS. The attacks came from an extremely large number of hijacked computers, up to 85,000; and the attacks went on for an unusually long time, for three weeks, until 19 May. The attacks reached a peak on 9 May, when Moscow celebrates Victory Day. Fifty-eight Estonian websites were down at once. The online services of Estonia's largest bank, then known as Hansapank, were unavailable for 90 minutes on 9 May and for two hours a day later" (Rid 2012:11–12).

[20] To the background of removel of the war memorial, Hansen and Nissenbaum note: "This act was constituted by a significant proportion of the ethnic Russian minority as a threat to their cultural and political status: large demonstrations led to the arrest of 1,300 people, the injury of 100, and the death of one (Traynor 2007). Ethnic Estonians on their part constituted the memorial as a residue of Soviet inter-war and Cold War occupation, and the removal as significant for the manifestation of cultural identity and the demarcation of political sovereignty vis-à-vis Russia" (Hansen and Nissenbaum 2009:1169).

analysis in the study. The time frame ends in 2016 and thus takes into account nearly a decade of cybersecurity policy discourse in the United States and Germany.

2.2.5 Studied Countries

The countries chosen for this study are the United States and Germany – two countries that are among the most relevant political and economic actors in the world (see for example bpb 2016). They have remarkable commonalities and differences, which makes a comparative study particularly interesting.

While both are democracies of the Western World, the Unites States has got a presidential system (Lösche 2008a) and Germany is characterized by a parliamentarian system (Rudzio 2006:40–42). With a view on both countries' executives that are at the center of this study, a powerful president characterizes the United States, especially in times of crises, as the president is "commander-in-chief and head of state, (…) and personified symbol of the Nation" (Lösche 2008b, own translation). The president is at the top of the executive that Lösche qualifies as fragmented (ibid.). Moreover, he points to a "permanent and aggressive rivalry between authorities, offices, and government agencies" (ibid., own translation). Also, departments frequently pursue their own agenda oriented towards their interests and respective stakeholders (ibid.). In contrast, the German executive is characterized by three crucial principles: "chancellor principle, cabinet principle, and department principle" (Rudzio 2006:241, own translation). The chancellor is attributed an "outstanding leadership position in the circle of government members" (ibid.:242, own translation). Article 65 of the German Basic Law formulates that "[t]he Federal Chancellor shall determine and be responsible for the general guidelines of policy" (BMJV 2019). However, the same article also underlines the autonomy of the departments and the importance of the cabinet: "Within these limits [the limits of the general guidelines of policy, K.U.] each Federal Minister shall conduct the affairs of his department independently and on his own responsibility. The Federal Government shall resolve differences of opinion between Federal Ministers" (ibid.). Thus, both countries have these specific fundamental differences regarding the functioning of their executive. The study aims at finding out, how they play out empirically in the field of cybersecurity policy.

As to the policy development in the area of cybersecurity and digital policies more generally, both countries started from a different position. The United States is generally considered "the dominant actor in IT issues" (Dunn Cavelty 2008:9) and "the country with the most activity in this domain" (ibid.). It is worth noting that the country implemented a first set of cyber-related policies already in the 80s: The *Computer Abuse Act* was adopted in 1984 and the *Computer Security Act* in 1987 (ibid.:42).[21] In the 80s and early 90s, debates and political initiatives notably centered on espionage (ibid.:55), before the Oklahoma City bombing in 1995 paved the way for a strong and lasting focus on critical infrastructure (ibid.:91). In this regard, the work of the *President's Commission on Critical Infrastructure Protection* (PCCIP) was of particular relevance and ultimately led to the *National Plan for Information Systems Protection* in 2000 (ibid.).

In contrast, cyber-related issues were of minor political importance in Germany for a long time (Rieger 2014:3).[22] Digitalization was "primarily regarded as technical issue and frequently attributed to the area of responsibility of IT divisions" (ibid., own translation). An analysis of the coalition treaties from 1998 onwards shows that only in 2009, coalition partners included substantial initiatives in the field of cybersecurity (Kullik 2014:85). An intense process to shed light on the topic of digitalization was started with the so-called "Enquete Commission 'Internet and Digital Society'" (Bundestag 2010, own translation) of the Bundestag that was in force from 2010 to 2013 (Bundestag 2013). According to an interviewed policy expert, the commission worked in an inclusive and interactive way and produced substantial outcomes (I-16:218–219). However, he observes little enduring effects of the commission on the political level (ibid.). Regarding critical infrastructure, we find a similar development in Germany compared to the United States regarding the time frame: Since the end of the 90s, measures to protect critical infrastructure in general constituted a "key element of the state's security-related preparedness system" (D-02 BMI 2009:5). The protection of critical information infrastructure has been put on the agenda in 2005 with the publication of the *National Plan for Information Infrastructure Protection* (NPSI) (Bundesministerium des Innern 2005). Both countries also have in common that the largest

[21] The Computer Abuse Act of 1984 is "a piece of legislation that set the stage for computer crime prosecution in the years to come" (Dunn Cavelty 2008:42). The Computer Security Act of 1987 regarded "the protection of federal agencies' computer data from espionage" (ibid.).

[22] Nevertheless, Guitton notes that "Germany was the first country to react to the cyber threat in Europe" (Guitton 2013:23).

part of the property of critical infrastructure is in the hands of the private sector (DHS 2019; BSI 2017:9).

In order to shed light on the current level of digital performance of both examined countries, we take into account the *Digital Economy and Society Index* (DESI) by the European Commission. DESI is a digitalization index composed of five indicators: "Connectivity", "Human Capital/Digital skills", "Use of Internet Services by citizens", "Integration of Digital Technology by businesses", and "Digital Public Services" (European Commission 2019a).[23] In 2019, Germany ranks 12th in the EU 28 with a score of 54.4, that is slightly above the EU score of 52.5 (European Commission 2019b:3). In 2017, Germany's score was at 49.4 (ibid.). In contrast, the United States achieved a score of 66.7 in the International DESI in 2016 (EU average I-DESI 2016: 58.9) (European Commission 2018a:14). Altogether, their respective digital performance makes both countries an attractive target for cyber attacks and underlines the goal of this study to examine both countries' way of coping with this challenge.

2.3 Expectations

In order to guide my analysis, I formulate several expectations. They regard domestic cultural traditions and values as well as the political and regulatory traditions of both countries:

- For both countries, I expect that some important *political and cultural traditions and values* will be mirrored in the respective discourses and that there will be differences in the resulting frames of the United States and Germany. For the United States, I expect a continuation of the prominence of security associated with critical (information) infrastructure protection and a continued strong military component in the cybersecurity discourse and measures as found in previous literature (Dunn Cavelty 2008:9,132; see also Wallace 2013a; Barnard-Wills and Ashenden 2012:11). Moreover, I expect that the idea of "American Exceptionalism" (Fluck 2016:15)[24]

[23] For more information on DESI see: https://ec.europa.eu/digital-single-market/en/desi (accessed July 10, 2019).

[24] Exceptionalism means a concept stemming from puritanism underlining "the historical uniqueness of the American experiment" (Fluck 2004:706, own translation) as well as the U.S.'s "world historical function as

manifests in the area of cyber risks and cybersecurity. For Germany, I expect a strong presence of critical (information) infrastructure protection because of the long-standing tradition in this field in Germany (Guitton 2013:23–24).[25] In addition, I expect a strong orientation towards European policy in the communications and in measures taken. I also expect that political discourses on cybersecurity risks get more specific and differentiated in both countries in the course of time.

- Against the background of the *regulatory styles* found in literature (Renn 2008:358–361; Renn 2001; O'Riordan and Wynne 1987; Vogel 1986; Brickman, Jasanoff, and Ilgen 1985), I expect them to be applicable in the examined regulatory examples in the field of cybersecurity policy. Accordingly, for the United States, I expect to find evidence that the regulatory example is in line with the *adversarial* regulatory style. For Germany, I expect to find evidence for the *corporatist* regulatory style.

2.4 Methodology

The following chapter describes the methodology I use in this study. I borrow the basic steps of my methodology from Keller's SKAD framework (Keller 2004:61–113). Some other helpful elements are borrowed from methodological literature.

2.4.1 General Remarks on Methodology

SKAD belongs to the tradition of "social science hermeneutics" (Hitzler and Honer 1997:22–23, own translation; see also Keller 2011a:268–269). According to Hitzler and Honer, approaches in this tradition "aim at pushing through the superficial information content of a text to underlying (…) levels of sense and meaning in a methodically controlled fashion, and at making this reconstruction process intersubjectively comprehensible" (Hitzler and Honer 1997:23, own translation).

In general, SKAD is aimed at the "reconstruction of the discursive construction of reality" (Keller 2011a:272, own translation). In order to carry out the reconstruction, two related elements are necessary: "Understanding" (ibid., own translation) and "explaining" (ibid.,

example" (ibid., own translation). Exceptionalism became a "crucial legitimation strategy of American political rhetoric" (ibid., own translation).

[25] Guitton also notes a focus on critical information infrastructure in Germany (Guitton 2013:28) and that the country "has by far deployed the largest resource if compared with its neighbouring countries" (ibid.) in terms of budget in the period 2009-2011.

own translation). Understanding is mainly oriented towards the "rules, actors, and contents of discourse production" (ibid., own translation), whereas explaining or, more precisely, developing "explaining hypotheses" (ibid., own translation) refers to the background, reasons for and effects of discourses (ibid.). Interpretation is thus a key element of SKAD (Keller 2011a:273). In order to comply with scientific rules, it is essential for researchers to be open about how they do interpretations and to take care of intersubjective comprehensibility (ibid., 274).

Keller emphasizes the combination of "precise analysis" (Keller 2011a:268, own translation) and "hermeneutically reflected and controlled interpretation" (ibid., own translation) in his approach of discourse analysis. There should be "self-reflection" (Keller 2011a:269, own translation) in the research process as well as an "attitude of methodical doubt" (ibid.:270, own translation, similarly Hitzler and Honer 1997:24). Also, researchers have, of course, to (be able to) substantiate their findings (Keller 2011a:270). In general, validity and reliability in the sense of quantitative research are difficult to establish (Keller 2004:111). Therefore, "'soft' quality criteria" (ibid.:111, own translation) such as the ones mentioned before as well as internal consistency are all the more important (ibid.).

Keller underlines that it is dependent on the specific research interest which methods a researcher chooses in order to collect data and carry out the analysis (Keller 2011a:268), above all how to proceed for the precise analysis of a specific text (Keller 2011a:275). In general, it is important to base data selection on a criteria-based process (Keller 2004:86). For the analysis of the texts, I follow the basic steps of what Keller calls "detailed analysis" ("*Feinanalyse"*) (Keller 2004:95, own translation). I present my proceeding in detail below.

2.4.2 Overview on Data

As it is the usual case in SKAD and discourse analysis more generally (Keller 2011a:268), my data consists of texts. Keller speaks of "natural data" (ibid.:270, own translation), which basically consists of "oral, written, audio-visual statements, [and] observable practices (…) from the field" (Keller 2011a:274, own translation). Moreover, interview data created in the context of a study can be examined as discourse analytical data (Keller 2011a:274). On the one hand, I use official written documents of the U.S. and German executives. On the other hand, I conducted 18 personal interviews for the specific purpose of the study.

Ten interviews were conducted with U.S. interview partners in Washington, D.C., between October and December 2013. Eight interviews with German interview partners were conducted in Berlin between August 2014 and February 2015. The interviews had got an average duration of more than one hour each. I recorded and transcribed all interviews. The rule system of the transcription was based on the recommendations of Dresing and Pehl (Dresing and Pehl 2013:19–24). English-speaking interview transcripts were proofread for linguistic correction with the help of a native speaker. For the analysis in the study, the interviews were coded using the software *f4analyse*.[26]

Regarding the selection of interview partners, I applied two main criteria: On the one hand, I wanted to cover a broad range of cybersecurity expertise. On the other hand, I was interested in talking to experts involved (or formerly involved) in the political process, i.e. representatives of departments, for example, as well as outside experts, i.e. scientific experts and policy analysts, for example of associations. Regarding the experts from the political sphere in the United States, I could talk to interview partners with government experience in different departments as well as staffers from the Homeland Security Committee and the Intelligence Committee of the House of Representatives. German political and administrative interview partners were representatives of the Federal Ministry of the Interior (BMI), the Federal Foreign Office (AA), the Federal Ministry of Defence (BMVg) and the Federal Office for Information Security (BSI).

Methodologically, I follow the basic rules and recommendations for qualitative interview research after Kruse (Kruse 2011) and the considerations on "Interview Methods in Political Science" of the *American Political Science Association* (APSA) (Leech 2002; Goldstein 2002; Aberbach and Rockman 2002). All interviews follow the basic style of semistructured interviews (Leech 2002) and were prepared and conducted with the help of a guideline of questions. For the specific field of expert interviews, I notably draw on Bogner, Littig, and Menz (Bogner, Littig, and Menz 2009). In the light of their typology of expert interviews, my interviews can be described as "systematizing expert interview" (Bogner and Menz 2009:64, own translation) mainly interested in "exclusive expert knowledge" (ibid.:64, own translation).

[26] For more information on the software see: https://www.audiotranskription.de/english/f4-analyse (accessed May 1, 2019).

2.4.3 Context Mapping

For Keller, understanding the context aspects of a discourse is highly important and, accordingly, it represents an essential step in the research process (Keller 2004:65). Keller considers these aspects as "autonomous fields of data collection" (ibid.:65, own translation). In my study, the context mapping aims at identifying the relevant discourse participants. It is based on a thorough examination of the executive actors in the policy field cybersecurity and their respective roles and responsibilities. I qualify those institutional actors that have got a significant share or function in cybersecurity policy as relevant discourse participants. The context mapping is done in three steps:

- Extensive research of the websites of departments/ministries, their divisions and offices, as well as other authorities.
- Check findings with secondary literature and interview data.
- Compilation of relevant discourse participants in a schematic representation for each country.

The context mapping is a crucial step in order to prepare the frame analysis: After having identified the main discourse participants, the documents they published during the period examined in this study are checked. A selection of the most relevant documents of the discourse participants in both countries constitutes the text corpus for the frame analysis. The process is explained in the following section.

2.4.4 Frame Analysis

In a first step, the *data corpus* for the frame analysis is prepared as follows:

- Compilation of a large collection of executive texts from the identified U.S. and German discourse participants from the period between 2007 and 2016 and first read-through.
- Selection of texts for the data corpus for the frame analysis according to the following criteria:
    - The text is an official, high-level publication of the executive, issued in the period between 2007 and 2016 and publicly available.
    - Cyber risks and/or cybersecurity is the unique or at least a main topic of the text.

    - The text is of strategic relevance or part of a series that is regularly published (e.g. the BSI's annual reports on cybersecurity).
- Numbering of the selected texts for the United States (U-01 to U-76) and Germany (D-01 to D-65) and integration in the software used for coding (*f4analyse*). The complete data corpus comprises a total of 141 texts.

Second, I create what I call an "*inventory*" of all texts in the data corpus. The inventory contains a short summary of each selected text and notes regarding following aspects:

- Main contents.
- Type of text: Is the character of the text rather strategic, judging, descriptive (or other)?
- Relation to critical infrastructure: Is the content of the text related to critical infrastructure?
- Selection of parts for coding (if not complete text). Against the background of the large amount of data collected, I partially follow Keller's recommendation to concentrate on key sequences of texts (Keller 2011a:275, similarly Lüders and Meuser 1997:73). This is notably done in the case of very long texts and in texts, where the key parts on cybersecurity are concentrated in specific sections.
- Personal thoughts/ideas on the text.

Exemplary parts of the inventory are displayed in the appendix (section 8.1).

Third, the *frame analysis* is carried out. This is done in accordance with some basic ideas of Matthes and Kohring (2008). They evaluate different methods for the identification of frames and develop a method on their own in order to increase reliability and validity in the frame identification process (Matthes and Kohring 2008:258).[27] The basic idea of Matthes and Kohring is "to understand a frame as a certain pattern in a given text that is composed of several elements. (…) Rather than directly coding the whole frame, we suggest splitting up the frame into its separate elements" (ibid.:263). By proceeding in this way, reliability is increased as "single frame elements can be more reliably coded than holistic, abstract

[27] Matthes and Kohring also use Entman's definition (Matthes and Kohring 2008:264). The goal and design of their study is different from my approach as they aim at finding media frames and conduct a quantitative cluster analysis in order to identify systematic groupings of frame elements (thus, frames) (ibid.:263). However, the basic idea of their approach can be applied in my study.

frames" (ibid.:274). The method also avoids an ex-ante identification of frames (ibid.:264). So, a certain openness in the analyzing process is given. Matthes and Kohring also point to beneficial effects on validity, among other things, because "the operationalization of the frame is completely tied to its theoretical definition" (ibid.:275). The authors acknowledge that the shortcomings of manual coding are not completely resolved (ibid.:276), but at least their method allows to open the "methodological black box" (ibid.:263) a little.

So, in order to prepare the frame analysis, I split up Entman's frame definition in its four functions[28] or elements and specify them for the purposes of my study. That means the abstract frame functions are specified with concrete frame elements corresponding to the discourse on cybersecurity risks examined in this study. The results of this process are laid out in the following table (Figure 4):

Figure 4: Frame Functions after Entman and Corresponding Frame Elements

Frame Function (Entman)	**Corresponding Frame Element in this Study**	**Example**
Problem definition	Description of cybersecurity risks	Theft of intellectual property
Diagnosing causes	Description of drivers and actors creating cybersecurity risks	Driver: dependence on ICT, actor: China
Making moral judgments	Evaluation of cybersecurity risks and the drivers and actors responsible for them	Growing cyber threat
Suggestion of remedies	Articulating solutions: actors responsible for solving the problem of cyber risks, the goals of solutions and concrete problem-solving measures	Responsible actors: the state and the private sector, goal: increased cybersecurity, measure: a campaign for awareness raising

Note: Own compilation.

On this basis, the coding system is developed. The overall codes are taken from Entman's frame definition, so the specified frame elements are used as main codes. Subordinate codes are developed from the analysis of the text inventory. Additionally, one open subcode is defined for every main code. Two remarks have to be made on the frame function moral judgments: First, the term "moral" in Entman's definition is somewhat misleading in the

[28] "Frames … *define problems* – determine what a causal agent is doing with what costs and benefits, usually measured in terms of common cultural values; *diagnose causes* – identify the forces creating the problem; *make moral judgments* – evaluate causal agents and their effects; and *suggest remedies* – offer and justify treatments for the problems and predict their likely effects" (Entman 1993:52 emphasis in original).

context of my study and is therefore left aside. I put the emphasis on judgments, evaluations, and assessments in general, not only moral judgments. Second with regard to judgments: There are elements in the discourse solely representing judgments; however, frequently, judgments are connected with or included in other elements, for example the description of a cyber risk. So, in the coding system, there is no main code on evaluation. Otherwise, numerous double codings would occur. Subcodes for evaluation are created and integrated into the main code of "Description of cybersecurity risks". In the presentation of findings, there is a section on evaluation within the description of the risks and as separate frame element.

The overall goal is to establish a systematic codebook, but nevertheless to remain open in the process of analyzing so the coding system can be adapted if needed. The final coding system is displayed in the appendix (section 8.2).

In order to identify frames in the data, I proceed by completing the following steps:

- Coding[29] the texts according to the following basic rules:
    - In general, complete sentences or paragraphs are coded.
    - In case of more than one applicable code for a sentence, the main message of the sentence and the context, in which it appears, are used in order to decide which code is selected.
    - Coding with more than one code shall be made only exceptionally.
    - Refining and adapting coding system if needed.
- The codings (= coded sentences or paragraphs) of each code are examined with regard to their overall topics, main messages, important statements, patterns, and particularities. Findings are summarized.
- Findings regarding the frame elements are aggregated. Keller points to an important characteristic of discourse analysis: It assumes that elements and structures of the discourse occur *across the data corpus* (and not: one document represents one type) (Keller 2011a:275). So, findings across different texts have to be brought together (ibid.).

[29] As this study is conducted as individual project and not in the context of a larger research project, it is not possible to use inter-coder-reliability in order to increase reliability. In return, the research process as done in the case of this study allows for high internal consistency.

- Overarching frames resulting from the frame elements are identified for both countries. As Entman notes, "[a] single sentence may perform more than one of these four framing functions, although many sentences in a text may perform none of them. And a frame in any particular text may not necessarily include all four functions" (Entman 1993:52).
- Findings are discussed, interpreted and examined in the light of the interview data.

2.4.5 Analysis of Regulatory Examples

The third and final empirical part of the study is the analysis of two regulatory examples understood as effects of both countries' discourses on cybersecurity risks. For the United States, I select Executive Order 13636 leading to the so-called Cybersecurity Framework. For Germany, I select the IT Security Act (*IT-Sicherheitsgesetz*, ITSiG). The term regulation is understood in a broad sense: An executive order is not a law by Congress, but has got "the same legal weight" (Dunn Cavelty 2008:39).[30] The selected regulatory measures are comparable with regard to several aspects: They were politically discussed and adopted during the same period of time (starting in 2013 and ending in 2014/2015). Both deal with the protection of critical infrastructure against cybersecurity risks with the help of standards and information sharing. They both have got risk management-oriented elements and are implemented across sectors.

In order to analyze if and to which extent both selected regulatory examples can be understood as examples following the tradition of the country's respective regulatory style, I shed light on the following three elements:

- Openness and control of the regulatory process
- Procedural rules, and
- Orientation of policy-making and the role of science.

For the analysis, I notably use my interview data as well as policy documents. The analysis is followed by a discussion on more general aspects of cybersecurity regulation and regulatory culture in both countries.

[30] As Dunn Cavelty notes, an "Executive Order (...) is a legally binding edict issued by a member of the executive branch of a government, usually the head of that branch. Executive Orders are usually based on existing statuory authority and require no action by Congress or the state legislature to become effective, but they have the same legal weight as laws passed by Congress (Olson and Woll 1999)" (Dunn Cavelty 2008:39).

After having presented the conception of the study, we now turn to the first empirical part of the study dealing with the context mapping.

3 Context Mapping: Discourse Participants in the United States and Germany

In the following, I present the main participants of the political discourses on cybersecurity in the executives of the United States and Germany, starting with the U.S. discourse participants. Please note that the following presentation is not a fully exhaustive description of *all* cybersecurity actors of the entire U.S. and German executives, but a selection of those being relevant in the context of this study. The presentation presents the state as of 2016, corresponding to the end of the time frame of this study.

3.1 Discourse Participants in the United States

3.1.1 President and White House

As the U.S. is organized as presidential system, the president and its staff at the White House (WH)[31] have got a significant share in cybersecurity policy. The president has got a range of advisers on different cyber-related topics, most notably in the context of this study the White House *Cybersecurity Coordinator*. President Obama created this office in 2009 (U-02 2009 WH:2). He determined that the coordinator should be "a member of the National Security Staff as well as the staff of my National Economic Council" (ibid.:3). The most important tasks of the coordinator are the following ones: "[O]rchestrating and integrating all cybersecurity policies for the government; working closely with the Office of Management and Budget to ensure agency budgets reflect those priorities; and, in the event of major cyber incident or attack, coordinating our response" (ibid.:3). President Obama selected Howard Schmidt, who had also advised President Bush on cybersecurity (Roberts 2017), as Cybersecurity Coordinator (White House 2018a). Later on, Michael Daniel was in charge of the position (White House 2018b).

[31] A note on wording regarding government agencies: When they are first mentioned, government agencies are presented with their full (English) name, for example "U.S. Department of Homeland Security" or "Federal Ministry of the Interior", followed by the commonly used (English or German) abbreviations, in our example "DHS" and "BMI". In the continuation of the text, only the abbreviations are used in order to simplify the language. Also, for simplicity reasons, when quoting incumbents of political positions, the name of the position is used, for example "President Obama", without adding "then" ("then President Obama"). A time indication is given by the date in the reference following a quotation.

3.1.2 Intelligence Community

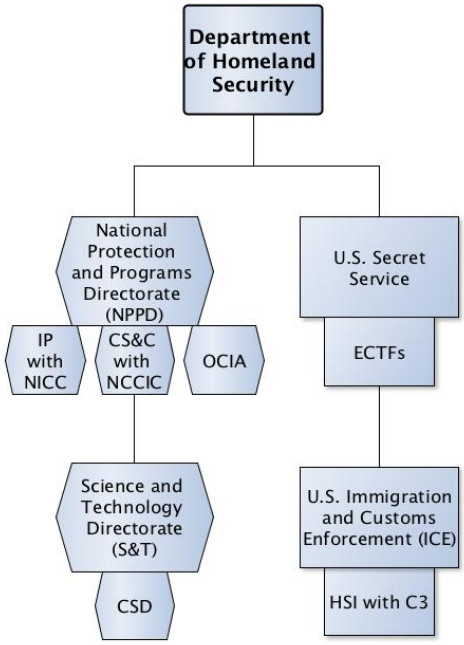
The Intelligence Community (IC) is an important discourse participant regarding cybersecurity policy as it publishes a very influential annual threat assessment that includes a detailed evaluation of cyber risks (see below section 4.1.1.3). The Intelligence Community is lead by the *Director of National Intelligence* (DNI) (ODNI 2017) and comprises 17 agencies, among them the *Office of the Director of National Intelligence* (ODNI), the *Central Intelligence Agency* (CIA) and intelligence agencies that are part of a federal department or agency such as the *National Security Agency* (NSA) or the *Federal Bureau of Investigation* (FBI)[32] (ODNI 2018). The Director of National Intelligence serves as "principal intelligence adviser to the President" (ODNI 2017).

3.1.3 U.S. Department of Homeland Security

The Department of Homeland Security (DHS) is another important discourse participant in the government discourse. For DHS, cybersecurity is a part of homeland security: "In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an important homeland security mission" (DHS 2018a). With regard to this study, two of DHS's responsibilities are especially relevant: the protection of critical infrastructure, including digital infrastructure (DHS 2018b) and the fight against cybercrime (DHS 2018c). The following schematic representation (Figure 5) presents the DHS units that are relevant in the context of the study. The units are described below.

[32] For more information about the FBI see below section 3.1.7.

Figure 5: Cybersecurity Roles and Responsibilities within DHS



Note: Own compilation.

As to the protection of critical infrastructure, DHS's *National Protection and Programs Directorate* (NPPD), established in 2007, leads "the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure" (DHS 2018d). Within the directorate, three offices have got responsibilities regarding the area of this study: First, the *Office of Infrastructure Protection* (IP) is in charge of protecting critical infrastructure from diverse hazards (DHS 2018e). The office is especially active in providing assessments, information, and risk management tools to stakeholders (ibid.). One of its divisions is the *National Infrastructure Coordinating Center* (NICC) that serves as "24/7 coordination and information sharing operations center that maintains situational awareness of the nation's critical infrastructure for the federal government" (DHS 2018f). Second, the *Office of Cybersecurity and Communications* (CS&C) focuses on the (civilian) critical information infrastructure of the U.S. government (".gov" domain) as well as the private sector's networks (DHS 2018g). Among its five divisions, the *National Cybersecurity and Communications Integration Center* (NCCIC) is of particular importance as it fulfills the function of a permanent government-wide cyber risk management body: "a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement" (DHS 2018h). Four branches help the NCCIC to fulfill its

tasks, among them the *United States Computer Emergency Readiness Team* (US-CERT) and the *Industrial Control Systems Cyber Emergency Response Team* (ICS-CERT) (ibid.). Whereas US-CERT focuses on analysis and providing information on diverse cyber risks to partners in the public and private sectors, ICS-CERT concentrates on the protection of control systems of critical infrastructures (ibid.). Finally, a third NPPD office, the *Office of Cyber and Infrastructure Analysis* (OCIA), shall be briefly mentioned: It is a unit providing in-depth analysis and evaluation in order to give strategic advice for political decision-making (DHS 2018i).

The *Science and Technology Directorate* (S&T) serves as "research and development (R&D) arm of the Department of Homeland Security" (DHS 2018j). It provides "tools, technologies, and knowledge products" (ibid.) for different areas, among them cybersecurity and critical infrastructure (ibid.). A specialized *Cyber Security Division* (CSD) was established in 2011 (DHS 2018k).

The second cyber-related responsibility of DHS is the fight against cybercrime. In this regard, two DHS components play a major role: The *U.S. Secret Service* and the *U.S. Immigration and Customs Enforcement* (ICE) (DHS 2018c). The U.S. Secret Service operates 40 *Electronic Crimes Task Forces* (ECTFs) (U.S. Secret Service 2018) that are in charge of "identifying and locating international cyber criminals connected to cyber intrusions, bank fraud, data breaches, and other computer-related crimes" (DHS 2018c). The U.S. Immigration and Customs Enforcement (ICE) has got a force called *Homeland Security Investigations* (HSI) (DHS 2018c). HSI's *Cyber Crimes Center* (C3) has specialized in cybercriminal investigations and notably provides technical expertise, for example in digital forensics (ICE 2018).

3.1.4 U.S. Department of Defense

The Department of Defense (DoD) is another crucial discourse participant in the cybersecurity policy discourse of the United States. Other than defending its own digital infrastructure, the department has to "defend the United States and its interests against cyberattacks of significant consequence; and provide integrated cyber capabilities to support military operations and contingency plans" (DoD 2015). DoD operates a special military command for the cyber domain called U.S. Cyber Command (USCYBERCOM) (U-57 DoD 2011:5). In order to comply with the National Defense Authorization Act of 2014, DoD

created the "Office of the Principal Cyber Advisor to the Secretary of Defense" (U-63 DoD 2015:29). Moreover, DoD has got a unit dealing with issues related to cybercrime in the military context, the Department of Defense Cyber Crime Center (DC3) (Cyber Crime Center 2018). The center focuses on numerous technical aspects, for example forensics (ibid.)

3.1.5 U.S. Department of State

The Department of State (State) is in charge of international aspects of U.S. policies regarding digitalization with topics ranging from cybersecurity to Internet governance and Internet freedom (U-48 State 2011:2). Regarding cybersecurity more specifically, State works to enhance international cooperation in order to improve international cybersecurity and the fight against cybercrime (U-47 State 2011:3). In 2011, the State Department established an office responsible for dealing with all cyber-related policy aspects, the "Office of the Coordinator for Cyber Issues" (State 2018).

3.1.6 U.S. Department of Commerce

The Department of Commerce (Commerce) mainly takes into account the business side of digitalization, which also includes cybersecurity aspects. Commerce's work regarding digitalization aims at "fostering a policy environment that (1) supports investment and innovation in the digital economy, (2) sustains the Nation's global leadership on Internet and technology issues, (3) preserves the fundamentally open nature of the Internet, and (4) secures the Nation's digital infrastructure and assets from cybersecurity threats" (U-70 Commerce 2014, 17-18).

At the Department, notably one institution performs tasks related to cyber security: The *National Institute of Standards and Technology* (NIST). NIST is basically a research institute working on measurement and standardization in different technology areas (NIST 2018b). For IT issues, NIST operates an *Information Technology Laboratory* (ITL) that "develops and disseminates standards, measurements, and testing for interoperability, security, usability, and reliability of information systems, including cybersecurity standards and guidelines for Federal agencies and U.S. industry" (NIST 2018c). ITL, in particular its *Computer Security Division* (CSD), had a crucial role in the process of elaborating the Cybersecurity Framework (Stine, Quill, and Witte 2014) that will be analyzed in chapter 5.

The *National Telecommunications and Information Administration* (NTIA) is another agency of Commerce. It is mainly charged with the expansion of broadband and spectrum (NTIA 2018a). NTIA's tasks are rather indirectly linked to cybersecurity in the sense of this study. Nevertheless, it is interesting to note as background information that, until 2016, NTIA had an oversight function for an important part of the administration of the Internet, the so-called "Internet Assigned Numbers Authority (IANA) functions"[33] (NTIA 2018b; NTIA 2018c). Until 2016, the "Internet Corporation for Assigned Names and Numbers (ICANN) performed the IANA functions, on behalf of the United States Government, through a contract with NTIA" (NTIA 2018b).

Finally, Commerce's *Internet Policy Task Force* shall be mentioned: It was created in 2010 and brings together experts from NTIA, NIST, and other department agencies[34] (U-68 Commerce 2011, iv). The task force works on issues at the "nexus between privacy policy, copyright, global free flow of information, cybersecurity, and innovation in the Internet economy" (NTIA 2018d).

3.1.7 U.S. Department of Justice

The Department of Justice (DoJ) is another participant in the U.S. government discourse on cybersecurity. In its strategic plan 2014-2018, DoJ lists the fight against cyber risks as national security goal (DoJ 2018a). DoJ notably "retains primary authority over the investigation and prosecution of cybercrimes, including those that have national security implications" (ibid.). Within DoJ, the *Computer Crime and Intellectual Property Section* (CCIPS), part of DoJ's *Criminal Division*, leads the fight against cybercrimes (DoJ 2018b). In 2014, a special *Cybersecurity Unit* was added to CCIPS (DoJ 2018c).

Moreover, the *Federal Bureau of Investigation* (FBI) belongs to DoJ. The FBI serves as "lead federal agency for investigating cyber attacks by criminals, overseas adversaries, and terrorists" (FBI 2018a). It is important to note the FBI's "unique dual responsibility" (FBI

[33] The IANA functions comprised four tasks: "(1) The coordination of the assignment of technical Internet protocol parameters; (2) the administration of certain responsibilities associated with Internet DNS root zone management; (3) the allocation of Internet numbering resources; and (4) other services related to the management of the .ARPA and .INT top-level domains" (NTIA 2018b).

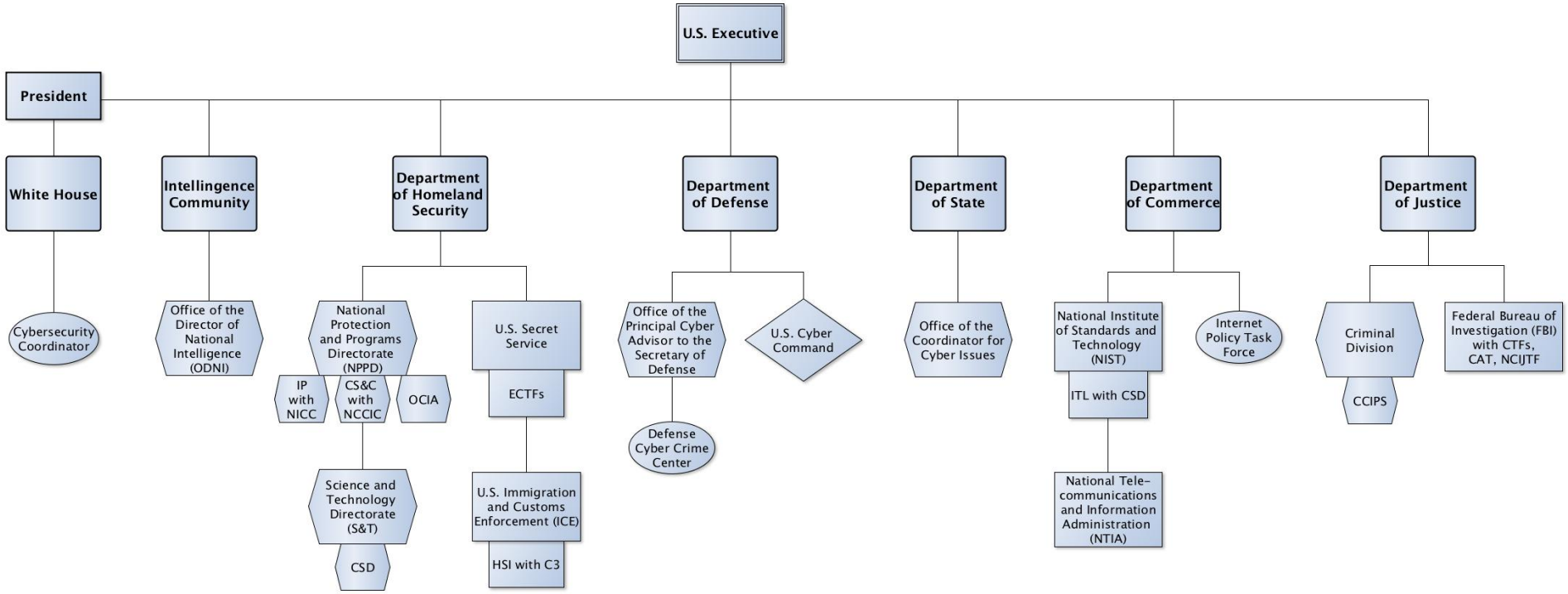
[34] Task force experts belong to the following agencies: the "Economic and Statistics Administration, the International Trade Administration, the National Institute of Standards and Technology, the National Telecommunications and Information Administration, the Office of the Secretary, and the U.S. Patent and Trademark Office" (U-68 Commerce 2011, iv).

2018b) combining intelligence and law enforcement. In the realm of the FBI, several units perform cybersecurity-related tasks, for example the numerous *Cyber Task Forces* (CTFs) operating locally all over the country (FBI 2018c) or the FBI *Cyber Action Team* (CAT) that is active in emergencies in order "provide rapid incident response on major computer intrusions and cyber-related emergencies" (FBI 2018a). The FBI also leads the *National Cyber Investigative Joint Task Force* (NCIJTF) that was created in 2008 and serves as "multi-agency cyber center" (FBI 2018d) in order to coordinate the participating agencies' efforts (ibid.).

3.1.8 Overview: Discourse Participants in the United States

After having identified and described the most important discourse participants and their roles and responsibilities regarding cybersecurity within the U.S. executive, the following schematic representation (Figure 6) summarizes the findings presented above.

Figure 6: Discourse Participants in the United States



Source: Own compilation. Note: The different geometric forms indicate different types of institutional entities (for example, offices of a department (such as DHS-NPPD), agencies of a department (such as Commerce's NIST) or special bodies (such as Commerce's Internet Policy Task Force).

3.2 Discourse Participants in Germany

3.2.1 Chancellor and Chancellery

In general in the German parliamentarian democracy, the chancellor has got the "power to determine policy guidelines" (*Richtlinienkompetenz*) (Bundeskanzlerin 2018). This power is defined by Article 65 of the German Basic Law that, at the same time, lays down the "principle of ministerial autonomy" (*Ressortprinzip*) (ibid.).

Moreover, it shall be mentioned that the German intelligence services[35] are coordinated by the Federal Chancellery (Bundesregierung 2018). The latter is also the parent agency of the *Federal Intelligence Service* (BND) (BND 2018). In the context of the study, BND is only a theoretical discourse participant. This is due to the fact that no relevant cyber-related documents were identified that are publicly accessible and relevant in the context of this study.

3.2.2 Federal Ministry of the Interior

The Federal Ministry of the Interior (BMI) is a very important discourse participant in the German government discourse on cybersecurity. BMI is responsible for many cyber-related topics, for "IT policy in all its aspects – from e-government and the protection of critical infrastructure to data protection, the Digital Agenda and the fight against crime and espionage on the Internet" (BMI 2016:4, own translation). In particular, two units of the ministry have responsibilities in the area of cybersecurity: the "Directorate-General IT" (BMI 2017) working on "Information Technology, Digital Society and Cyber Security" (ibid.) and the "Directorate-General ÖS Public Security" (ibid.). The *Chief Information Officer* (CIO) is part of the *Directorate-General IT* and notably responsible for strategic policy questions (BMI 2018). Issues related to the protection of critical infrastructure are in the responsibility of the "Directorate-General KM Crisis Management and Civil Protection" (BMI 2017).

BMI is the parent agency of four agencies with cybersecurity-related tasks: The Federal Office for Information Security (BSI), the Federal Criminal Police Office (BKA), the Federal

[35] There are three federal intelligence services: The Federal Intelligence Service (BND), Federal Office for the Protection of the Constitution (BfV), and the Military Counterintelligence Service (MAD).

Office for the Protection of the Constitution (BfV), and the Federal Office of Civil Protection and Disaster Assistance (BBK).

Among these agencies, the *Federal Office for Information Security* (BSI) is the one with the most comprehensive cybersecurity-related tasks: "BSI as national cybersecurity authority shapes information security in [the process of, K.U.] digitalization by prevention, detection, and reaction for state, economy, and society" (BSI 2018b, own translation). It has got manifold tasks including awareness raising for cybersecurity issues as well as developing and certifying products (ibid.). Moreover, BSI operates "CERT-Bund (Computer Emergency Response Team for federal agencies)" (BSI 2018c), is responsible for monitoring the state of cybersecurity on a permanent basis (BSI 2018d) and has the capacity to act as *IT Crisis Reaction Centre* (BSI 2018e). In this function, it "ensure[s] immediate responses to serious incidents in order to allow timely countermeasures and avoid large-scale damage" (ibid.). The agency exists since 1991 (D-16 BSI 2016:27); the BSI Act of 2009 and the IT Security Act of 2015 considerably strengthened its functions (ibid.:29,32).

The *Federal Criminal Police Office* (BKA) has got a special unit for dealing with cybercrime within its division *Serious and Organised Crime* (BKA 2018). The unit is tasked with cybercriminal investigations, but also analyzing the cybercrime domain (ibid.). Among other aspects, the unit hosts the "central point of contact for cybercrime" (ibid.) that works "as an intermediary and adviser to the business sector and co-ordinates police investigations in case of an incident" (ibid.).

The *Federal Office for the Protection of the Constitution* (BfV) serves as "domestic intelligence service of the Federal Republic of Germany" (BfV 2018). In order to fulfill its mandate, the agency "collects and analyses information about extremist, terrorist, and any other efforts posing a threat to security, and about foreign intelligence services' activities directed against our country" (ibid.). Cyber risks are also on the agenda of BfV and represent a growing field of activity (Maaßen 2018).

The *Federal Office of Civil Protection and Disaster Assistance* (BBK) is the agency that is, among other things, responsible for the protection of critical infrastructure (BBK 2018a). In this regard, BBK is notably in charge of "providing information on the significance of KRITIS for the State and for society, (…), of establishing and intensifying cooperation between authorities and enterprises, of developing and refining analysis and protection concepts for KRITIS, and of proposing short-, medium- and long-term measures to protect critical

infrastructures" (BBK 2018b). Regarding digital infrastructure, BSI and the *Federal Network Agency* (BNetzA) are important partners of BBK (BBK 2018c).

The *National Cyber Response Centre* and the *National Cyber Security Council* also belong to the realm of BMI. As both are institutional measures taken in the wake of the first German cyber strategy, they are presented as part of the discourse analysis (see below section 4.1.2.4.3).

3.2.3 Federal Ministry of Defence

Cybersecurity is an important issue for the Federal Ministry of Defence (BMVg). In 2016, thus at the end of the examined time period, the ministry opened the division "Cyber/Information Technology" (BMVg 2018a, own translation) with two sub-divisions, "Cyber and IT Governance" and "IT Services/Information Security" (BMVg 2018b, own translation). Moreover, BMVg establishes a special military command for the cyber domain called "Cyber and Information Space" (*KdoCIR*) (D-57 BMVg 2016:1, own translation).

3.2.4 Federal Foreign Office

The Federal Foreign Office (AA) is responsible for "international cyber policy" (AA 2017) and is thus tasked to advocate German cybersecurity interests and other digital issues in European and international organizations (ibid.). In 2011, AA created an "International Cyber Policy Coordination Staff" (ibid.). From 2013 onwards, there was the position of a "Special Commissioner for International Cyber Policy" (AA 2014, own translation); in 2015, the position was turned into the "Director for the United Nations, International Cyber Policy and Counterterrorism" (AA 2017).

3.2.5 Federal Ministry for Economic Affairs and Energy

The Federal Ministry for Economic Affairs and Energy (BMWi) is a discourse participant favoring digitalization, but underlines that it has to be "shaped fairly for the benefit of consumers, businesses and employees" (BMWi 2018a). Much of its work regards the creation of a "favourable framework and targeted funding schemes" (ibid.). Regarding cybersecurity, BMWi is notably interested in advancing awareness and practical security

measures in small and medium-sized enterprises (ibid.). BMWi has got a division on “digital and innovation policy” (BMWi 2018b, own translation), with cybersecurity topics located in the sub-division on “Standardization and Security” (ibid., own translation).

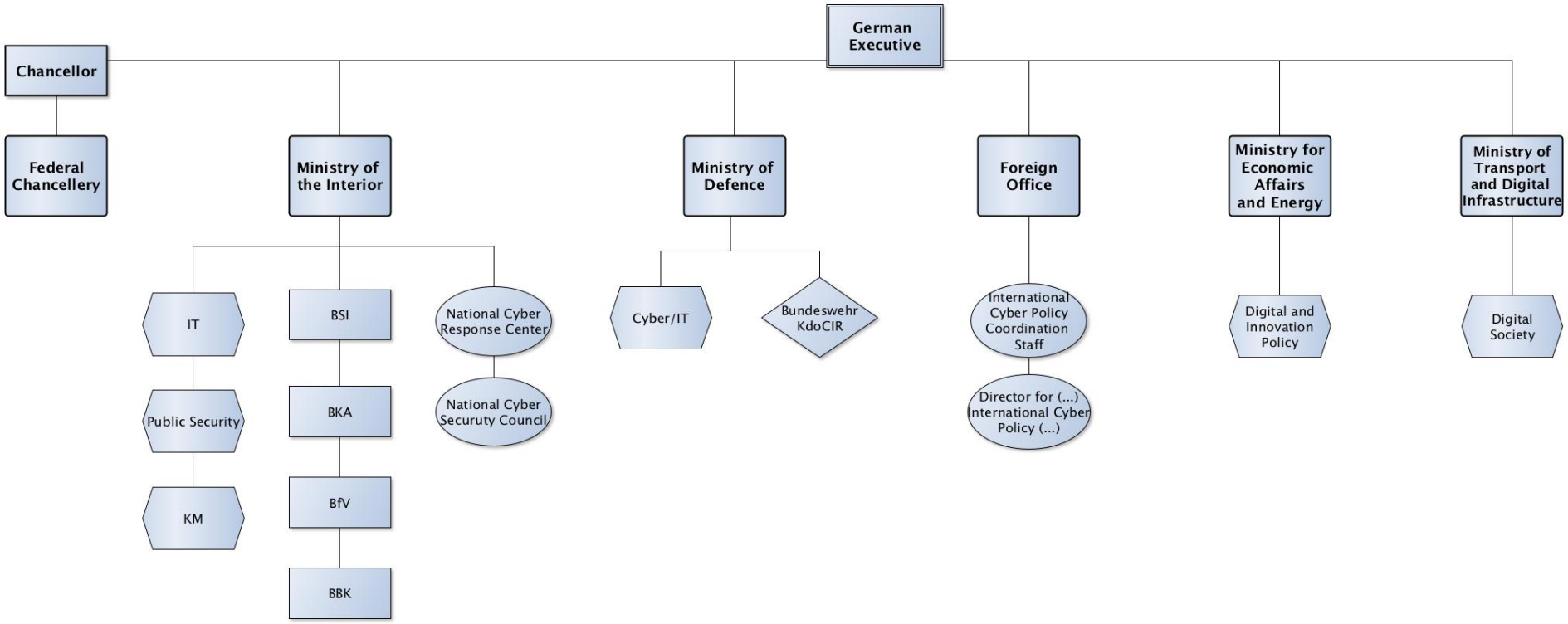
3.2.6 Federal Ministry of Transport and Digital Infrastructure

The Federal Ministry of Transport and Digital Infrastructure (BMVI) with its division “Digital Society” (BMVI 2018, own translation) is responsible for the “increasing digitalization of our infrastructures” (ibid., own translation). More concretely, the ministry notably fosters the expansion of broadband and digital mobility (ibid.). The Federal Ministry for Economic Affairs and Energy (BMWi) was traditionally in charge of all aspects of telecommunication and digital infrastructure policy (Rieger 2014:5). However, in the wake of the elections in 2013, the responsibility for broadband was attributed to BMVI and the division “Digital Society” was created (Rieger 2014:7–8). Overall, regarding the topic of this study, BMVI is not a very active discourse participant (see also I-11:119). However, BMVI is one of the ministries responsible for the Digital Agenda (D-61 BMWi 2014) from 2014; therefore, the ministry is listed as discourse participant.

3.2.7 Overview: Discourse Participants in Germany

After having identified and described the most important discourse participants and their roles and responsibilities regarding cybersecurity within the German executive, the following schematic representation (Figure 7) summarizes the findings presented above.

Figure 7: Discourse Participants in Germany



Source: Own compilation. Note: As in Figure 6, the different geometric forms indicate different types of institutional entities.

3.3 Comparison and Conclusion on Context Mapping

Overall, the above context mapping shows that cyber security policy is institutionally decentralized in the United States as well as in Germany. In both countries, several departments and agencies share responsibilities in this field. This is an indication for the crosscutting and complex character of the topic.

In the course of time, both countries have institutionalized their respective setting. The United States implemented it in a larger fashion in terms of personnel and financial resources (see for example I-11:128), whereas an interviewed German official characterizes Germany as a "small and poor country compared to the United States" (I-14:170, own translation) in the field of cybersecurity. BMI is the institutional lead player regarding cybersecurity in Germany, but there are only about 20 people working on the issue (I-11:122-123). In the United States, we find a highly differentiated structure with DHS emerging as a center of gravity and DoD with Cyber Command emerging as another striking component of the institutional set-up. As to Germany, we can identify a center of gravity around BMI and its subordinate agencies. Apart from these centers, we find numerous other institutional players with a broad range of responsibilities in the field of cybersecurity, so a complex structure.

The organization of the institutional structures and how to cooperate in the field of cybersecurity and digital policy more generally has been subject of numerous debates in both countries. As an example, it is illustrative to consider the German debate on three different models that were discussed in the wake of the election campaign of 2013 and the later coalition negotiations (Rieger 2014:3): The first model implied the creation of a new, central body, the so-called "Internet ministry" (ibid.:3, own translation). In contrast, the Federal Chancellery should fulfill a coordinating function according to the second proposal (ibid.). Finally, the joint leadership of three ministries was discussed in order to organize digital policy (ibid.). In the end, the Digital Agenda 2014-2017 (D-61 BMWi 2014) was realized under the joint leadership of BMWi, BMI, and BMVI because of the crosscutting character of the task (ibid.:2). So, a decentralized approach has been installed with the consequence, that much coordination is needed (ibid.:11).

As the institutional set-up in the United States as well as Germany shows, neither of those countries took a fundamentally new path in order to integrate cybersecurity policy into their executive structure. Rather, they added cybersecurity-related units and divisions to existing

departments, offices, and agencies – increasing the complexity and the need for coordination. In this sense, both countries stuck to established basic characteristics of their executive (see above section 2.2.5) such as the fragmented character and departments pursuing their own agenda in the United States (Lösche 2008b) and the strong autonomy of the departments in Germany (Rudzio 2006).

In the following discourse analysis, I will shed light on the communication of discourse participants in both countries and, when discussing the frames, also examine how institutional structures and discourses interact.

4 Discourse Analysis: Frames in the United States and Germany

In the following sub-chapter, the results of the discourse analysis are presented. I proceed as follows: First, I present results regarding the frame elements for the U.S. discourse and the German discourse (section 4.1). In a second part, overarching frames are identified for each country (section 4.2). Finally, in a third section, the results of both countries are compared and discussed (section 4.3).

4.1 Frame Elements in the U.S. and German Discourses

In the following sections, I present my findings for the U.S. and the German discourses regarding the four frame elements: cybersecurity risks, drivers and actors creating cybersecurity risks, evaluation, and solutions. In order to make the discourses as concrete as possible and to illustrate my findings, I use numerous quotations. The references in brackets refer to the list of documents I used for the discourse analysis (for the United States: texts U-01 to U-76, for Germany: texts D-01 to D-67).[36] Other than the text number, the references indicate the institutional actor, for example DHS, and the year of the publication of the text.

If not specified, findings refer to the complete data corpus of either the U.S. or the German discourse as a whole. Neither is it the goal of the study, nor is it possible with the applied research design to give exact numbers of appearance of a frame element in a discourse or other quantitative elements. However, in some cases it seems appropriate to give at least a rough impression of frequency with formulations such as “very prominent in the discourse” or “rarely”. In this way, a rough tendency is conveyed in order to better understand the findings.

Finally, it has to be noted that some of the aspects presented in the following sections are closely connected to each other. I nevertheless attribute them to specific frame elements or sub-sections of frame elements in order to look into the discourses in a structured and differentiated way. At the end, this proceeding allows outlining overarching frames for the executive discourses in both countries.

[36] The complete list can be found in the bibliography (sections 7.1 and 7.2).

4.1.1 Frame Elements in the U.S. Discourse

In the following sections, the frame elements in the U.S. discourse are presented starting with cybersecurity risks.

4.1.1.1 Cybersecurity Risks

4.1.1.1.1 Cybersecurity Risks in General

What is seen as cybersecurity risk in the U.S. discourse? In general, cybersecurity risks as articulated in the U.S. discourse include malicious cyber activity in the three basic forms of exploitation, disruption, destruction of data and information infrastructures: "Our nation is being challenged as never before to defend its interests and values in cyberspace. Adversaries increasingly seek to magnify their impact and extend their reach through cyber exploitation, disruption, and destruction" (U-64 DoD 2015:1).[37] The texts state a broad range of examples for each of the basic forms. The most common among them are the following cyber risks: digital identity theft, theft of intellectual property, cyber espionage, attacks on critical infrastructure, cyber means used in a military context, insider threats, and supply chain risks (U-37 DNI 2015:1; U-44 DHS 2014,:39; U-41 DHS 2011:3–4; U-29 DNI 2009:39).

I sort the cyber risks into three groups beginning with the focus category of this study, cybersecurity-related risks for critical infrastructure, followed by cyber risks within the military context and, finally, cybercrime risks. Within the discussion of each group, I address the following aspects:

- *Contents*: What does the risk consist of?
- *Evaluation*: How is the risk evaluated?
- *Time frame evolution*: How does the communication of this risk develop in the course of the observed time frame?
- *Speakers*: Who, i.e. which executive actor(s), talk(s) about this risk?

[37] Another basic classification brought up by the intelligence community is distinguishing between cyber attack and cyber espionage: "In the United States, we define cyber threats in terms of cyber attacks and cyber espionage. A cyber attack is a non-kinetic offensive operation intended to create physical effects or to manipulate, disrupt, or delete data. It might range from a denial-of-service operation that temporarily prevents access to a website, to an attack on a power turbine that causes physical damage and an outage lasting for days. Cyber espionage refers to intrusions into networks to access sensitive diplomatic, military, or economic information" (U-34 DNI 2013:1).

4.1.1.1.2 Cyber Risks for Critical Infrastructure

Contents and evaluation. One of the main risks articulated in the U.S. discourse clearly is cyber-related risk for critical infrastructure. In general, critical infrastructure is seen in a "complex and uncertain" (U-43 DHS 2013:8) risk environment with major changes such as the exposure to cyber risks being on the rise due to the "growing integration of information and communications technologies with critical infrastructure operations and an adversary focus on exploiting potential cyber vulnerabilities" (ibid.). The fact that critical infrastructure is IT-supported and thus "highly interconnected and interdependent" (U-39 DHS 2009:12) leads to more efficiency, but also higher vulnerability to cyber risks (ibid.). This vulnerability of critical infrastructure is exploited by malicious cyber activity with the result of "placing the Nation's security, economy, and public safety and health at risk" (U-69 Commerce 2014:1). All of this has to be seen against the background of the strong dependence of the United States on functioning critical infrastructure, which is frequently articulated during the discourse period analyzed (see for example U-69 Commerce 2014:1; U-39 DHS 2009:113).

Furthermore, it is important to note that cyber risks for critical infrastructure are assessed as *real*, *ongoing*, and *increasing*. Already in the 2009 National Infrastructure Protection Plan (NIPP), it is laid out that "malicious actors can and do conduct attacks against critical cyber infrastructure on an ongoing basis" (U-39 DHS 2009:113). Although the country has not experienced a catastrophic attack so far, President Obama points out the ongoing threat for critical infrastructure in 2012: "So far, no one has managed to seriously damage or disrupt our critical infrastructure networks. But foreign governments, criminal syndicates and lone individuals are probing our financial, energy and public safety systems every day" (U-12 WH 2012:1). Further strengthening the character of *ongoing*, he underlines that, "[c]omputer systems in critical sectors of our economy – including the nuclear and chemical industries – are being increasingly targeted" (ibid.). So, the risk for critical infrastructure is considered as *increasing*; this evaluation is also communicated in numerous other statements during all of the U.S. discourse (see for example U-44 DHS 2014:20; U-43 DHS 2013:8; U-39 DHS 2009:113). The observation that the risk is increasing holds true not only for critical infrastructure, but also for the other types of cyber risks discussed in this study. Moreover, all participants in the U.S. discourse basically share it. I anticipate this important evaluation at this point; more details follow in the respective sections below.

Which *effects* or *outcomes* of cyber risks for critical infrastructure do discourse participants imagine? How can or how might the risk unfold? The cyber-related risks for critical infrastructure, as articulated in the U.S. discourse, are imagined in many ways. In particular, actors fear a severe disruption of supply with vital services that could lead to dramatic consequences for the population (U-34 DNI 2013:1). More concretely, discourse participants imagine the potential effects of a severe cyber attack on critical infrastructure for example as financial crisis, as a standstill due to an electricity blackout or as a public health emergency due to non-functioning hospitals, a contaminated water supply or derailed trains transporting persons or lethal chemicals (U-12 WH 2012:1; U-60 DoD 2012:2). One of the most dramatic statements in this regard is then-Secretary of Defense Leon Panetta's[38] scenario of a "cyber Pearl Harbor" (U-60 DoD 2012:2): "The most destructive scenarios involve cyber actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack on our country. Attackers could also seek to disable or degrade critical military systems and communication networks. The collective result of these kinds of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability" (U-60 DoD 2012:2).

On top of the dramatic potential of cyber attacks on critical infrastructure, a strong sense of *immediacy* of the realization of a severe attack is regularly communicated – combined with a *call for action*. Leon Panetta compares the situation to 9/11 and stresses the indispensable need to act in order to not make the same mistakes again: "Before September 11, 2001, the warning signs were there. We weren't organized. We weren't ready and we suffered terribly for that lack of attention. We cannot let that happen again. This is a pre-9/11 moment. (…) The attackers are plotting. Our systems will never be impenetrable just like our physical defenses are not perfect, but more can be done to improve them" (U-60 DoD 2012:4). In a similar vein, William Lynn[39] points to realized achievements such as better network defenses, the establishment of U.S. Cyber Command, or improvements in critical infrastructure protection, but urges at the same time that "much remains to be done, and the window for doing it is short" (U-58 DoD 2011:1). The need to act is a more general topic of the U.S. discourse as will be seen in later parts of the analysis.

[38] Leon Panetta served as Secretary of Defense from 2011 to 2013.
[39] William J. Lynn III served as Deputy Secretary of Defense from 2009 to 2011.

To sum up the different elements I laid out above, the cyber risk for critical infrastructure is constructed in the discourse as real, ongoing, and increasing, and more severe scenarios are constructed as immediate and pending. From this assessment, an urgent need to act follows.

Time frame evolution. Regarding cyber risks for critical infrastructure in the course of the observed time frame, a certain peak in the risk articulation can be seen for the years 2012 and 2013. That is when Leon Panetta articulated the cyber Pearl Harbor scenario and the pre-9/11 moment (2012) and President Obama included cyber risks for critical infrastructure even in his state of the Union Address (2013), which is the only time he mentions cyber risks for critical infrastructure on this level: "America must also face the rapidly growing threat from cyber-attacks. (…) Now, we know hackers steal people's identities and infiltrate private emails. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy" (U-01 WH 2013). In this statement, the threat characterization as *real* and *immediate* becomes apparent again. Following this statement, Obama explains the importance of the *Executive Order 13636, Improving Critical Infrastructure Cybersecurity*, which he signed at the same day, and that Congress needs to pass comprehensive legislation. Towards the end of the analyzed time period, statements, notably those of the intelligence community, get more nuanced. For example, the director of national intelligence states in 2015 that there is the potential for espionage and disruption, but that "low-to-moderate level cyber attacks" (U-37 DNI 2015:1) are more likely than a catastrophic incident (ibid.).

Speakers. As follows from their competence within the U.S. government, risks for critical infrastructure are notably addressed by homeland security actors: "Safeguarding and securing cyberspace is a homeland security mission because the potential exists for wide-scale or high-consequence adverse cyber events, which could cause harm to critical functions and services across the public and private sectors and impact national security, economic vitality, and public health and safety" (U-41 DHS 2011:3). In consequence, DHS texts regularly address cyber risks for critical infrastructure as well as cyber risks in general (see for example U-39 DHS 2009; U-40 DHS 2010; U-43 DHS 2013; U-44 DHS 2014). However,

the possibility of a catastrophic cyber attack involving critical infrastructures is such an important and, in discursive terms, powerful scenario that is used by a wide range of other actors, too. President Obama invokes the scenario (U-12 WH 2012:1), DoD actors Leon Panetta and William Lynn (see examples above), and the intelligence community regularly assesses the risk of a potentially catastrophic attack on critical infrastructure (see for example U-37 DNI 2015:1; U-28 DNI 2008:15). Even an agency related to the Department of Commerce – the *National Institute of Standards and Technology* (NIST) – is concerned with the topic of cyber risks for critical infrastructure in its *Framework for Improving Critical Infrastructure Cybersecurity* (U-69 Commerce 2014).

4.1.1.1.3 Cyber Risks within the Military Context

Contents and evaluation. Cyber risks are an important topic in the military context. In remarks in 2009, President Obama qualifies the cyber attacks on websites of the Georgian government in 2008 as "a glimpse of the future face of war" (U-02 WH 2009:2). Also, cyber incidents with a disruptive character such as the ones in Estonia in 2007 and the aforementioned attacks in Georgia are assumed to occur regularly in future conflicts (U-29 DNI 2009:39). In general, DoD actors state that cyber attacks that could have "possible severe effects on both our military operations and our homeland" (U-59 DoD 2012:3).

Military actors' view on cyber risks is strongly influenced by their *own attack experiences*, the number and frequency of which grew "exponentially" (U-56 DoD 2010:97). Important examples are the 2008 attack with an USB drive[40] – "the most significant breach of U.S. military computers ever, and (…) an important wake-up call" (ibid.) – and attacks on the defense and other supporting industries leading to theft of intellectual property (U-63 DoD 2015:10). In consequence, foreign state actors "undercut the United States' strategic and technological advantage and (…) benefit[ted, K.U.] their own military and economic development" (ibid.).

[40] William Lynn describes the attack as follows: "In 2008, the U.S. Department of Defense suffered a significant compromise of its classified military computer networks. It began when an infected flash drive was inserted into a U.S. military laptop at a base in the Middle East. The flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the U.S. Central Command. That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control. It was a network administrator's worst fear: a rogue program operating silently, poised to deliver operational plans into the hands of an unknown adversary" (U-56 DoD 2010:97).

In its first cyber strategy, published in 2011, DoD puts the emphasis on "three areas of potential adversarial activity: theft or exploitation of data; disruption or denial of access or service that affects the availability of networks, information, or network-enabled resources; and destructive action including corruption, manipulation, or direct activity that threatens to destroy or degrade networks or connected systems" (U-57 DoD 2011:3). Because of the extremely large military network, "[t]he number of potential vulnerabilities (…) is staggering" (U-55 DoD 2010:37). Moreover, DoD admits the possibility of undetected attacks (U-57 DoD 2011:1). Also, in the view of DoD, different characteristics of cyber attacks such as anonymity, speed, or the easy availability of tools lead to the fact that cyber defense is harder than *offense* (U-55 DoD 2010:37). DoD actors stress the *far-reaching* character of cyber risks and that they "go well beyond military targets and affect all aspects of society" (U-57 DoD 2011:4). In this context, DoD again highlights the danger for civilian critical infrastructure underlining the strong dependence of the military on those civilian infrastructures (U-57 DoD 2011:4). Other topics for DoD are the potential dangers emanating from malicious insiders and supply chain risks, thus, the risk that IT products are tampered in manufacturing processes abroad (ibid.:3). Another risk is seen in the fact that modern information and communication technologies facilitate malicious actors' activities: "Increasing global connectivity is enabling radical groups to recruit and train new members, proliferate extremist ideologies, manage their finances, manipulate public opinion, and coordinate attacks" (U-29 DNI 2009:38).

But not only radical groups are expected to benefit from information and communication technologies, but also *foreign states* and their *militaries*. Already early on in the examined discourse period, foreign military cyber capabilities are seen as a danger: The "formalization" (U-32 DNI 2011:27) of such capabilities could give foreign countries an instrument to "undermine critical infrastructures that were previously assumed secure before or during conflict" (ibid.). Also, adversaries that are weaker in terms of conventional military capabilities could benefit from the asymmetric character of cyber means and use cyber attacks instead (U-12 WH 2012:1). Furthermore, it is worrying from a military perspective that cyber capabilities are increasingly *used* – given the fact that efforts to define commonly accepted rules and norms how to behave in cyberspace lag behind (U-34 DNI 2013:1). That increases "the chances for miscalculations and misunderstandings that could lead to unintended escalation" (ibid.).

Time frame evolution. In the course of time, a shift in the assessment of cyber risks within the military context can be observed in the sense that the assessment is more detailed and comprehensive in more recent documents. Also, the 2015 strategy is more than twice as long as the 2011 strategy in terms of pages. For example, DoD mentions specific hostile cyber actors – Russia, China, Iran, North Korea (U-63 DoD 2015:9,12) – and elaborates in some detail on its deterrence strategy (ibid.:10–12).

Speakers. Finally, it has to be noted that several speakers of the U.S. government contribute to the assessment of cyber risks within the military context: most prominently DoD, but also the White House and the Director of National Intelligence. The State Department is concerned with international cyberspace policy. It communicates in detail about other countries such as China and how they behave as cyber actors (see below section 4.1.1.2.5) as well as legal and normative issues (see below section 4.1.1.4.3). Regarding the more technical side of cyber risks, State refers back to the Intelligence Community (see for example U-53 State 2016:19–20).

4.1.1.1.4 Cybercrime Risks

Contents and evaluation. Regarding the cyber risks qualifying as cybercrime, we can distinguish two main categories that are addressed in the U.S. discourse: cybercrime that affects people on the *personal* level, such as the theft of credit card information (see for example U-42 DHS 2012:3), as well as cybercrime affecting *government entities* or *corporations*.

Regarding the institutional and corporate level, discourse mainly concentrates on two categories: On the one hand, on *large-scale intrusions*, where massive amounts of personal information or data are stolen or destroyed such as the case of the *Office of Personnel Management* (OPM)[41] in 2015 (U-25 WH 2016:2). On the other hand, the threat of cyber-enabled theft of *intellectual property* (IP) is broadly discussed. Already in 2011, DoJ pointed out that IP is increasingly targeted by cybercriminals (U-71 DoJ 2011:3). Also, IP theft in the military context is considered a particularly serious issue (see above section 4.1.1.1.3). William Lynn notes in 2010: "As military strength ultimately depends on economic vitality,

[41] The "unauthorized breach of the Office of Personnel Management's systems (…) resulted in the theft of approximately 22 million personnel files" (U-54 State 2016:6).

sustained intellectual property losses could erode both the United States' military effectiveness and its competitiveness in the global economy" (U-56 DoD 2010:100). Comparing different cyber risks, he stresses the pervasiveness of IP theft: "Although the threat to intellectual property is less dramatic than the threat to critical national infrastructure, it may be the most significant cyberthreat that the United States will face over the long term. Every year, an amount of intellectual property many times larger than all the intellectual property contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government agencies" (ibid.).
Moreover, the "global proliferation of malicious code or software" (U-63 DoD 2015:9) is seen in the discourse as a delicate problem: Malware and other hacking tools as well as IT expertise can be bought on a "dangerous and uncontrolled" black market (ibid.:10). U.S. discourse participants also note that the technological development allows for advantageous conditions for cybercrime activities (U-71 DoJ 2011:2) and that there is a growing involvement of international organized crime in cybercrime (U-06 WH 2010:49).

Time frame evolution. As to the evolution of communications on cybercrime risks in the course of time, two observations stand out: One the one hand, discourse participants constantly stress the growing professional organization and sophistication of cybercriminals and the attacks they launch, for example, they increasingly aim at corporate IP instead of personal credit card information (U-71 DoJ 2011:3). On the other hand, discourse participants state that less sophisticated forms of cybercrime risks and their financial impact increase, notably because access to the cybercriminal sector is easy and it is highly profitable (U-73 DoJ 2015:1). DoJ Assistant Attorney General Caldwell quotes a study estimating that "cyberattacks have cost the global economy at least $315 billion over the past twelve months" (ibid.).

Speakers. Because of the many different forms of cybercrime risks, it is a topic addressed by nearly all discourse participants examined in the study, although the extent of communications is varying. Detailed statements can notably be found in DoJ and FBI documents as well as the analyses of the director of national intelligence. However, it is interesting to note that in DHS communications, few detailed remarks on cybercrime risks are found despite the department's responsibility in the field.

4.1.1.2 Drivers and Actors Creating Cybersecurity Risks

In the following section, I elaborate on the drivers and actors creating cybersecurity risks as stated by the U.S. discourse participants.

As to the *drivers*, I find a network of aspects in the field of dependence and technology. They interact with each other and discourse participants combine them in various ways in their statements. Keeping this in mind, I single out the most prominent aspects – dependence, technology as an enabler, and the downside of innovation – to be able to understand the discourse in a more differentiated way. The underlying argumentative structure is that a driver, for example dependence, creates vulnerabilities to cyber risks. As to the *actors*, the documents analyzed show a twofold categorization: On the one hand, general groups of cyber actors are described, such as "cybercriminals"; on the other hand, the discourse participants identify distinct countries, such as China, at the origin of cyber risks.

4.1.1.2.1 Dependence

The first driver creating cyber risks is dependence in the sense of reliance on something indispensable. Actors articulate that there is a strong and growing dependence on digital infrastructure and, more broadly, critical infrastructure. Critical infrastructure in the U.S. discourse includes physical and virtual aspects: "America's critical infrastructure is complex and diverse, combining systems in both cyberspace and the physical world – from power plants, bridges, and interstates to Federal buildings and the massive electrical grids that power our Nation" (U-15 WH 2013:2). An outstanding metaphor that discourse participants use to illustrate the dependence is "backbone": "Over the last few decades, our Nation has grown increasingly dependent on critical infrastructure, the backbone of our national and economic security" (U-15 WH 2013:2). The metaphor is also used with regard to digital infrastructure – here combined with "national asset", another frequently used term to describe the meaning of infrastructure: "Digital infrastructure is increasingly the backbone of prosperous economies, vigorous research communities, strong militaries, transparent governments, and free societies. (…) These social and trade links have become indispensable to our daily lives. Critical life-sustaining infrastructures that deliver electricity and water, control air traffic, and support our financial system all depend on networked information systems. (…) The reach of networked technology is pervasive and global. For all nations, the underlying digital infrastructure is or will soon become a national asset" (U-09 WH 2011:3).

More directly linked to the risk context, President Obama points out in 2009 that "America's economic prosperity in the 21st century will depend on cybersecurity" (U-02 WH 2009:2). Discourse participants agree that, with growing use and the resulting dependence on the digital infrastructure, the vulnerabilities increase (U-28 DNI 2008:14–15) and so does the "importance and necessity of protecting" it (U-42 DHS 2012:2). Defense actors take a particular clear stance. They state that cyberspace has transformed military art and that "[n]o one today can exert or maintain national power without acute sensitivity to the digital networks that underpin the world's communications, prosperity, and security" (U-64 DoD 2015:2). Also, they frankly express their strong vulnerability and dependence. In 2011, DoD states that "[i]t is difficult to overstate this reliance" (U-57 DoD 2011:1). In 2015, DoD points out that its reliance "stands in stark contrast to the inadequacy of our cybersecurity" (U-63 DoD 2015:1). DHS with its responsibility for critical infrastructure points to the fact that critical infrastructure is more and more interconnected, including transnationally, and interdependent – especially the dependence on IT is strong; these factors heighten vulnerabilities to cyber attacks (U-43 DHS 2013:8; U-40 DHS 2010:8).

The aspect of strong and/or increasing dependence is omnipresent throughout all of the examined U.S. discourse and notably used by White House, DHS and DoD (see for other examples: U-26 WH 2016:2; U-63 DoD 2015:1; U-13 WH 2012:2; U-14 WH 2012:2; U-41 DHS 2011:4; U-05 WH 2009:2).

4.1.1.2.2 Technology as an Enabler

The second aspect is technology as enabler of cyber risks. In general, U.S. discourse participants regard technological development as an enabler of cybercrime (U-71 DoJ 2011:2–3). As the director of national intelligence explains for international organized crime: By the means of modern IT, old crimes such as fraud can be conducted more effectively, and new forms of computer crime have come into existence (U-31 DNI 2010:45). Many attributes of cyberspace support the realization of cyber attacks, in particular the cheap and easy availability of a variety of instruments and services, the speed, the high degree of anonymity, and the possibility to remotely attack a target (U-71 DoJ 2011:3; U-57 DoD 2011:3; U-55 DoD 2010:37). Furthermore, William Lynn underlines that "[i]n cyberspace, the offense has the upper hand" (U-56 DoD 2010:99), which is notably due to the fact that the Internet was not designed with security as main feature (ibid.). Moreover, Lynn mentions the asymmetric

nature of cyberwarfare and the difficulty of identifying attackers in cyberspace (ibid.). With a view on the examined period, the role of technology is a constant topic in the U.S. discourse. Especially actors from the defense and intelligence communities as well as the White House elaborate on this aspect. The White House stands out with a very prominent statement it uses repeatedly with only slight variations in wording: President Obama states in 2009 that "[i]t's the great irony of our Information Age – the very technologies that empower us to create and to build also empower those who would disrupt and destroy. And this paradox – seen and unseen – is something that we experience every day" (U-02 WH 2009:1). I give one further example from 2015 to show the continuity of this statement: "[I]t's one of the great paradoxes of our time that the very technologies that empower us to do great good can also be used to undermine us and inflict great harm" (U-21 WH 2015:4).

4.1.1.2.3 Downside of Innovation

Finally, I find an aspect linked to innovation that is relevant in creating cyber risks in the discourse participants' view. Being innovative is a very important trait in the U.S. discourse participants' self-conception, notably in matters of ICT. "[T]he nation that invented the Internet" (U-02 WH 2009:3) is also eager to use innovative products and technology: As President Obama puts it, there is a "thirst for computers, smartphones, and other digital solutions at work and at home" (U-05 WH 2009:2). However, innovation comes with a downside: In a market-driven environment, functionality is sometimes more important than security, which leads to cyber risks: "Owing to market incentives, innovation in functionality is outpacing innovation in security, and neither the public nor private sector has been successful at fully implementing existing best practices" (U-33 DNI 2012:7). Also, the following statement underlines that the speed of digitalization can cause problems: "In some cases, the world is applying digital technologies faster than our ability to understand the security implications and mitigate potential risks" (U-34 DNI 2013:1). The articulation of this downside of innovation is not dominant in the U.S. discourse, only few statements – notably from the intelligence community, which is not surprising – point to this implication (for an example other than the intelligence community see U-72 DoJ 2014:1).

As to the future development, the intelligence community estimates that the impact of the factors dependence and innovation "will probably be far greater in scope and impact than ever" (U-38 DNI 2016:1). Consequences notably consist in extensive vulnerabilities to cyber

risks (ibid.). Among the digitalization trends, the "Internet of Things" plays a particularly striking role for the future: It will "further transform the role of information technology in the global economy and create even further dependencies on it. The complexity and nature of these systems means that security and safety assurance are not guaranteed and that threat actors can easily cause security and/or safety problems in these systems" (U-35 DNI 2014:2).

4.1.1.2.4 General Actor Groups

An important question for discourse participants is: Who is at the origin of cyber risks? As pointed out at the beginning of the sub-chapter, the documents analyzed show a twofold categorization: On the one hand, general actor groups are described; on the other hand, discourse participants identify distinct countries at the origin of cyber risks. In the following, I shed light on the category of general actor groups.

As an FBI representative notes, "the range of actors who threaten our interests is as complex as it is varied" (U-75 FBI 2014:2). This variety is described in the discourse in numerous statements. Most of them simply list the range of actors that usually comprises three to five different actor types. An example can be found in the White House National Security Strategy from 2010: "The threats we face range from individual criminal hackers to organized criminal groups, from terrorist networks to advanced nation states" (U-06 WH 2010:27). In addition, a few statements contain more detailed typologies mentioning characteristic features for each type, such as the following example from an FBI document: "We face cyber terrorists, who aim to use our reliance upon and use of digital systems to advance their political or ideological goals. We face nation states, who aim to use the cyber world to conduct espionage, to make preparations for war, and who may even carry out acts of war through cyber means. We face ideology-driven criminals, who may use methods such as denial of service attacks, known as DDoS attacks, to further their own ideology or social cause. We face insider threats, whose legitimate access to sensitive information may be used for various illicit ends. Lastly, we face financially motivated groups and individuals, who use a range of methods to enrich themselves at others' expense" (U-75 FBI 2014:2).

As to the category of nation states, the intelligence community adds one more distinction regarding capabilities and intent: According to their assessment from 2015, there are "(1) nation states with highly sophisticated cyber programs (such as Russia or China), [and, K.U.]

(2) nations with lesser technical capabilities but possibly more disruptive intent (such as Iran or North Korea)" (U-37 DNI 2015:2). Apart from this, cybercriminals stand out in the discourse due to the "growing sophistication" (U-28 DNI 2008:15; U-29 DNI 2009:39; U-31 DNI 2010:2) regularly attributed to them. The intelligence community highlights this feature based on the high degree of organization, technical skills, and profit-maximizing orientation of cybercriminals (U-28 DNI 2008:15; U-29 DNI 2009:39; U-31 DNI 2010:2). DoD and FBI observe that terrorists currently employ the Internet for recruiting, propaganda, and communication purposes, but that they did not yet acquire intrusion capabilities (U-63 DoD 2015:9; U-76 FBI 2016:2). However, as FBI Director Comey puts it: "[L]ogic tells us that has to be the future of terrorism" (U-76 FBI 2016:2).

In general, the intelligence community assesses that the different actor types have "varying combinations of access, technical sophistication and intent" (U-31 DNI 2010:2). Also, there are various forms of collaboration and complicity between nation state actors and non-state actors, which makes distinguishing them a complicated endeavor (U-37 DNI 2015:2). Finally, it has to be noted, that the types of actors discussed in the discourse remain basically the same over the examined period.

4.1.1.2.5 Specific Actors

Beyond the basic typologies presented above, U.S. discourse participants make numerous remarks on some specific actors responsible for cyber risks, in particular China, Russia, Iran, and North Korea. Contributions in this regard notably come from the intelligence community and the State Department. Concerning the level of detail, I find a considerable increase in the intelligence community's documents over the examined time period. Whereas from 2008 to 2011, only a few short remarks are found, for instance on China and Russia (see for example U-31 DNI 2010:28), there is a clear increase in 2012 and 2013 (see for example U-33 DNI 2012:8). Even more detailed explanations are found in the statements from 2014 to 2016 (see for example U-37 DNI 2015:2–3). The State department gives very detailed statements on some key countries in 2015 and 2016 (see for example U-53 State 2016:16–19). In the following, I present the discourse participancts' characterization of China, Russia, Iran, and North Korea.

China and Russia are seen as advanced and aggressive cyber actors from the beginning of the observed period (U-31 DNI 2010:28; U-33 DNI 2012:7). Discourse actors notably blame entities within China and Russia for "extensive illicit intrusions into US computer networks and theft of US intellectual property" (U-33 DNI 2012:7). In 2014, the U.S. sanctioned such a case: It brought up an indictment against five Chinese military hackers because of economic espionage and further crimes (U-54 State 2016:3). In 2016, the director of national intelligence highlights that "cyber deception operations (…) to induce errors and miscalculation in decisionmaking" (U-38 DNI 2016:2) are part of China's military doctrine. Russia is equally described as an assertive actor in cyberspace using disinformation as a means of manipulation and establishing a military cyber entity (U-38 DNI 2016:2; U-37 DNI 2015:2–3). Also, Russian actors already proved their ability to remotely compromise industrial control systems (ICS) (U-37 DNI 2015:3). Moreover, China and Russia have visions of Internet Governance issues highly different from the United States: China champions a vision of cyberspace that is "government-controlled, with an absolutist conception of sovereignty over technology and content" (U-51 State 2015:3). In a similar vein, Russia attaches great importance to the "the maintenance of internal stability, as well as sovereignty over its 'information space'" (U-53 State 2016:18).

Interestingly, though, there is an evolution in the communication on China and Russia in the course of time as the U.S.-China relationship as well as the U.S.-Russia relationship deepen and get more cooperative. As a consequence, the picture of both countries gets more differentiated. In the view of U.S. discourse participants, the U.S.-China commitments from 2015 were an important milestone: One key commitment is that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property for commercial advantage" (U-54 State 2016:3). Moreover, new ways of collaborating on cybercrime and on rules for state conduct in cyberspace were agreed upon (ibid.). While the commitments "do not resolve all our challenges with China on cyber issues" (ibid., 4), the State Department appreciates them as progress and as an instrument "to hold Beijing accountable" (ibid.).

Similarly, Russia and the United States found "common ground" (U-54 State 2016:5). Both states agreed that international law is applicable to the behavior of states in cyberspace; moreover, they found a consensus on non-binding peacetime rules; finally, the United States

and Russia defined confidence building measures regarding cyberspace, the first of their kind, bilaterally between both countries as well as multilaterally within the OSCE (ibid.).

Iran is mentioned in the official U.S. discourse since 2012, when the intelligence community blames the country for espionage: "Iran's intelligence operations against the United States, including cyber capabilities, have dramatically increased in recent years in depth and complexity" (U-33 DNI 2012:8). In a more recent statement, specific cyber attacks against the United States between 2012 and 2014 were attributed to cyber actors from Iran, for example Distributed Denial of Service (DDoS) attacks directed at the finance sector (U-37 DNI 2015:3). In this case, indictments have been brought, too (U-76 FBI 2016:9).

North Korea is the fourth country I focus on in this section. Discourse participants mention North Korea as a cyber actor in 2014 for the first time qualifying it as "unpredictable" (U-35 DNI 2014:2). Shortly afterwards, North Korea was at the center of many discussions, as the country, according to U.S. investigations, had launched the large-scale cyber attack on Sony Pictures Entertainment (U-37 DNI 2015:3)[42]. DoD declared this attack as "one of the most destructive cyberattacks on a U.S. entity to date" (U-63 DoD 2015:2). It was accompanied by "coercion, intimidation, and the threat of terrorism" (ibid.). The United States reacted on this attack with publicly blaming North Korea and imposing sanctions (U-51 State 2015:3).

Overall, U.S. discourse participants observe high investments in cyber means by other actors and are aware of the attractiveness of such a "viable, plausibly deniable capability to target the U.S. homeland and damage U.S. interests" (U-63 DoD 2015:9). However, considering the four states discussed above, there are two striking differences emanating from the discourse: On the one hand, China's and Russia's cyber capabilities are assessed as much more advanced than the capabilities of Iran and North Korea (ibid.). On the other hand, discourse participants assess a strong difference in the mindset of the four states: Whereas Iran and North Korea are seen as "unpredictable" (U-35 DNI 2014:2) and showing "an overt level of hostile intent towards the United States and U.S. interests in cyberspace" (U-63 DoD 2015:9), China and Russia are evaluated as predictable. As the FBI director puts it, when

[42] In detail, DoD describes the attack as follows: "[I]n November, 2014, likely in retaliation for the planned release of a satirical film, North Korea conducted a cyberattack against Sony Pictures Entertainment, rendering thousands of Sony computers inoperable and breaching Sony's confidential business information. In addition to the destructive nature of the attacks, North Korea stole digital copies of a number of unreleased movies, as well as thousands of documents containing sensitive data regarding celebrities, Sony employees, and Sony's business operations" (U-63 DoD 2015:1–2).

discussing the success of negotiations with China and the impact of measures such as indictments: “They are serious people with whom you can have a conversation to explain this framework [of acceptable intelligence-gathering activities of a state, K.U.]” (U-76 FBI 2016:9–10). For the U.S., China and Russia are “unlikely to launch (…) a devastating attack against the United States outside of a military conflict or crisis that they believe threatens their vital interests” (U-34 DNI 2013:1).

4.1.1.3 Evaluation of Cybersecurity Risks

In the previous sections on cybersecurity risks and the drivers and actors triggering them, I already presented many elements that describe how discourse participants evaluate these risks. Overall, outstanding elements are the seriousness of the threat – in the words of the White House, cyber risks are “one of the most serious national security, public safety, and economic challenges we face as a nation” (U-06 WH 2010:27) – and the finding that the risks are “increasing in frequency, scale, sophistication, and severity” (U-53 State 2016:19). As was presented before, cyber risks in all variations are described as growing, basically throughout all of the U.S. discourse and in the communication of diverse discourse participants. What follows from this intensification is a permanently “[e]volving [t]hreat [l]andscape” (U-42 DHS 2012:3) in the view of discourse participants.

The evolution of the risk evaluation in the course of time is what I now shed light on in a more precise and chronological fashion. Therefore, I present highlights from a specific angle: the intelligence community’s annual threat assessment. I consider these assessments as a very helpful source as they contain the most comprehensive risk evaluation within the selected U.S. data corpus. Also, they are published every year, so changes during the time frame can be detected.

Interestingly, in the year 2007, cyber risks are not mentioned at all in the threat assessment. From 2008 onwards, cyber risks are a regular topic getting more comprehensive and differentiated every year. Notably, from 2013 onwards, the remarks are very detailed and nuanced. Often, the director of national intelligence distinguishes between the previously mentioned three basic forms of “exploitation, disruption, and destruction” (U-64 DoD 2015:1).

In 2008, the director of national intelligence states that “[o]ur information infrastructure (…) increasingly is being targeted for exploitation and potentially for disruption or destruction,

by a growing array of state and non-state adversaries" (U-28 DNI 2008:15). So, already the 2008 statement assesses the threat as *increasing*. Furthermore, it mentions the *potential* for disruption and destruction, whereas exploitation is assessed as already existing and ongoing. Moreover, the director of national intelligence states a *growth* in the number of threatening *actors*. The further analysis shows that these basic elements of assessing cyber risks are continued through all of the examined time period and that the overall judgment of the situation regularly gets more critical.

In the 2009 statement, the risk for critical infrastructure is highlighted due to the vulnerability of U.S. critical infrastructure and the increased connectivity: This connectivity "creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures" (U-29 DNI 2009:38). Attacks on critical infrastructures in other countries have already been observed (ibid.). Moreover, the intelligence community refers to the cyber attacks in Estonia 2007 and Georgia 2008 and expects "disruptive cyber activities to be the norm in future political or military conflicts" (U-29 DNI 2009:39).

In 2010, the intelligence community puts the emphasis on the "dangerous combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities, and a lack of comprehensive threat awareness" (U-31 DNI 2010:2). The latter points to the fact that the U.S. is not adequately prepared. Attacks occur "on an unprecedented scale with extraordinary sophistication" (U-31 DNI 2010:2) – an evaluation confirming previous assessments – and the logic of IT clearly favors the attackers (ibid.). Moreover, the discovery of a "formalization of military cyber capabilities" (U-32 DNI 2011:27) is mentioned as a new element in 2011, which creates a heightened risk for critical infrastructure (ibid.). In 2012, the director of national intelligence states that "innovation in functionality is outpacing innovation in security" (U-33 DNI 2012:7) and that this results in even more advanced cyber security attacks by a broader range of actors (ibid.).

The remarks from 2013 onwards continue in the described spirit. In the 2013 statement, the risk for critical infrastructure is especially prominent. The analysis concludes that there is a "remote chance of a major cyber attack against US critical infrastructure systems during the next two years that would result in long-term, wide-scale disruption of services, such as a regional power outage", but that "isolated state or nonstate actors might deploy less sophisticated cyber attacks as a form of retaliation or provocation" (U-34 DNI 2013:1). Under

certain circumstances, such attacks could result in "significant outcomes" (ibid.). So, not only vulnerabilities are outlined, but also damages are alluded to at this point. In the following year, the director of national intelligence highlights an increase in probability of a destructive attack notably due to the proliferation of attack tools and skills (U-35 DNI 2014:1). Because of its vulnerability, it is attractive to attack critical infrastructure, "particularly the Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems used in water management, oil and gas pipelines, electrical power distribution, and mass transit" (U-35 DNI 2014:2). The consequence could be "significant economic or human impact" (ibid.). Once more, enormous potential damages are articulated. In 2015, again, an overall increase in diverse dimensions of cyber attacks – impact, actors, methods, and victims – is stated (U-37 DNI 2015:1). However, a "'Cyber Armageddon' scenario that debilitates the entire US infrastructure" (ibid.) seems "remote" (ibid.). Instead, the intelligence community foresees "an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security" (ibid.). So, the intelligence community slightly refrains from the worst-case scenario, nevertheless underlining the high cost of cyber attacks. The conclusion of the 2015 assessment is that an elimination of cyber attacks is not possible; instead, "cyber risk must be managed" (ibid.), which is a clear hint that the U.S. has to get along with it and must act. A new element coming up in the 2015 statement is the assessment that attacks on the integrity of information[43] might be more frequent in the future (U-37 DNI 2015:3–4). In this type of attack the reliability or accuracy of information is targeted with the possible consequence that "[d]ecisionmaking by senior government officials (civilian and military), corporate executives, investors, or others will be impaired if they cannot trust the information they are receiving" (U-37 DNI 2015:3). Furthermore, attribution is a topic in this statement and an improvement becomes clear: Whereas in 2012, the detection and attribution of cyber threats was considered one of the "greatest strategic challenges" (U-33 DNI 2012:8), the Director of National Intelligence reports in 2015 that the capability of attributing cyber incidents has progressed significantly: "Although cyber operators can infiltrate or disrupt targeted ICT networks, most can no longer assume that their activities will remain undetected. Nor can they assume that if detected, they will be able to conceal

[43] Integrity is opposed to availability and confidentiality: "Most of the public discussion regarding cyber threats has focused on the confidentiality and availability of information; cyber espionage undermines confidentiality, whereas denial-of-service operations and data-deletion attacks undermine availability" (U-37 DNI 2015:3).

their identities" (U-37 DNI 2015:2). This statement can be seen in the U.S. tradition of openly demonstrating capabilities and power, in a certain sense, a sort of deterrence. Finally, an interesting conclusion emerges in the statement of 2016: On the one hand, innovations such as the Internet of Things and the dependence on ICT create more vulnerabilities to cyber attacks; on the other hand, new possibilities for the intelligence community emerge from this development, notably for the collection of intelligence (U-38 DNI 2016:1).

Concluding, it becomes apparent that, from 2008 onwards, the intelligence community champions a clear and consistent discourse in favor of a permanently aggravating cyber risk in diverse dimensions. It is based on the work of their enormous institutional apparatus and substantiated by numerous detailed examples. As the assessments are presented before Congress, they have a considerable public outreach. Moreover, it is interesting to note that the findings of the intelligence community are quoted in official documents of other government actors, for example the State Department (U-53 State 2016:19–20). All in all, the assessments can be considered a crucial and very influential pillar of the U.S. government's threat assessment and communication to the outside – thus, a very powerful source given the impact of the intelligence community's risk communication. As a consequence, the assessments help prepare the ground for the articulated solutions for cyber risks, which are the subject of the next section.

4.1.1.4 Solutions: Solving the Problem of Cybersecurity Risks

The section on solutions covers the articulated communications on the following aspects: actors responsible for solving the problem of cyber risks, goals of solutions, and concrete problem-solving measures.

4.1.1.4.1 Discourse on Responsibility

Who is responsible for solving the problem of cyber risks in the eyes of discourse participants? U.S. executive actors notably communicate two lines of argumentation in the discourse: On the one hand, a self-assertive stance and leadership claim as a country in the international perspective. On the other hand, the promotion of shared responsibility at the national level.

The United States as leading country in a digital world. As President Obama states in his Address to Joint Session of Congress in 2009, the United States is determined to use its alliances as well as "all elements of our national power" (U-01 WH 2009) in order to cope with cyber risks and other major challenges. This includes military means, which is detailed below in section 4.1.1.4.3. The imposition of sanctions as in the case of North Korea after the Sony attack is an example of using economic instruments (U-52 State 2015:7). What becomes apparent in statements of this kind is a self-assertive stance and a clear message of power. But the United States is not only ready "to defend our nation and our partners, our friends, our allies" (U-52 State 2015:7) against cyber risks, but also capable and willing to lead the world in the digital age: Indeed, "[a]s the birthplace of the Internet, the United States has a special responsibility to lead a networked world" (U-22 WH 2015:12). This leadership claim with regard to modern ICT is very strong and prominent in the U.S. discourse during all of the examined time frame (see for an early example U-02 WH 2009:3). Being innovative is key in order to maintain it: "So long as the United States (…) continues to be a pioneer in both technological innovation and cybersecurity, we will maintain our strength, resilience, and leadership in the 21st century" (U-08 WH 2010:3). President Obama emphasizes the innovative capabilities of the United States – "almost unique across the planet" (U-21 WH 2015:3) – as an important part of the country's self-conception. So, to be and to remain "on the cutting edge of this new technology" (U-60 DoD 2012:2) is one of the missions identified in the U.S. discourse against the background of the growing cyber risk.

Thus, the discourse of the digital leadership is very pronounced in the U.S. documents. However, it has also to be seen within the broader context of the leadership role as general topic in the U.S. self-conception: This stance manifests in the country's self-assigned value-based "moral leadership" (U-06 WH 2010:10), in the description of its economy as the "most dynamic economy in the world" (U-21 WH 2015:3), and the military as "the best-trained, best-led, best-equipped fighting force in history" (U-59 DoD 2012:preface). As the White House formulated in the 2015 National Security Strategy, "American global leadership remains indispensable" (U-22 WH 2015:preface). Having said that, the United States acknowledges that its "resources and influence are not infinite" (ibid.). It realizes that the international environment changes, that countries such as China and India gain influence and power and that the United States needs its allies and other partners (U-55 DoD 2010:iii). This aspect of the importance of international cooperation is also articulated in the context

of cyber risks and cybersecurity. With regard to shaping cyberspace according to the U.S. vision, the White House emphasizes that "international collaboration is more than a best practice; it is a first principle" (U-09 WH 2011:8).

Shared responsibility at the national level. The second line of argumentation regarding responsibility is the topic of shared responsibility in a domestic perspective. In communications of the discourse participants, it has got several meanings.

The *first* aspect of shared responsibility concerns the work of government: Here, a "whole-of-government approach" is strongly advocated by DHS (U-41 DHS 2011:3; U-40 DHS 2010:iv), DoD (U-57 DoD 2011:8) and State (U-48 State 2011:2), already early in the examined time frame. Such an approach aims at "work[ing, K.U.] closely with (…) interagency partners on new and innovative ways to increase national cybersecurity" (U-57 DoD 2011:8). As an example, DoD and DHS agreed on a cooperation memorandum in 2010 (ibid.). In consequence, military cyber means can be used to support civilian purposes in a civilian legal framework (U-58 DoD 2011:2). According to William Lynn, this type of cooperation "carries the long-standing tradition of military support for civilian authorities into the cyber domain" (ibid.). Later in the observed discourse period, in 2015, the DoD wording is even more pronounced regarding so-called "defend the nation operations" (U-63 DoD 2015:25): "DoD will work with FBI, CIA, DHS and other agencies to build relationships and integrate capabilities to provide the President with the widest range of options available to respond to a cyberattack of significant consequence to the United States" (ibid.). State implements the whole-of-government approach in bilateral cyber meetings by staffing the U.S. delegation with cyber experts from different departments (U-51 State 2015:8). Regarding cybercrime, the FBI underlines that government cooperation is vital as "no government agency, no matter how competent its agents and experts, can operate successfully on its own" (U-75 FBI 2014:6).

While discourse participants mention examples of successful government coordination, such as the investigation of the criminal online platform Silk Road 2.0 lead by the FBI and the DHS body HSI (DHS-Immigration and Customs Enforcement-Homeland Security Investigations, ICE-HSI) (U-75 FBI 2014:5–6), government still needs to improve: This concerns the knowledge of roles and responsibilities within government and the need to "minimize friction and duplicative efforts" (U-55 DoD 2010:104). Also, the White House acknowledges,

that, even in the year 2016, federal IT is not at the state of the art (U-25 WH 2016:2). Nevertheless, it has to be said that self-criticism is not very strong in the U.S. executive discourse. Rather, criticism towards Congress is a regular topic. Repeatedly during all of the observed discourse period, the president and other government actors urge Congress to act and to pass necessary cybersecurity legislation (see for example U-21 WH 2015:7; U-01 WH 2015 and 2013; U-17 WH 2014:2; U-12 WH 2012:2; U-42 DHS 2012:6–7). "[L]egislative and political gridlock" (U-60 DoD 2012:4) and "political dysfunction in Washington" (U-22 WH 2015:3) are seen as serious problems. Against this background, government actors stress that they do all that is possible within the framework of the available executive instruments, for example executive orders (U-17 WH 2014:2).

The *second* aspect of shared responsibility regards the shared responsibility of state and private sector in combating cyber risks. From the beginning of the examined discourse period, actors articulate that public-private partnerships are "critical" (U-02 WH 2009:3), notably with regard to the protection of critical infrastructure[44] given that, for the most part[45], infrastructure is owned and operated by the private sector. The White House emphasizes that the private sector "plays a vital role in preparing for and recovering from disasters" (U-06 WH 2010:19). This shows that the partnership is needed in the prevention of risks as well as response activities. A repeated message from the government, notably towards the end of the examined period, is that "all of us must work together to do what none of us can achieve alone" (U-23 WH 2015:2; see also U-46 DHS 2016:6; U-21 WH 2015:4; U-45 DHS 2015:2) and that "[w]e definitely need each other" (U-76 FBI 2016:16). So, discourse participants clearly articulate this need and also mention some positive examples of cooperation, for example the creation of the Cybersecurity Framework (U-17 WH 2014:2) or the dismantling of the botnet Gameover Zeus by the FBI and several companies in the field of computer security (U-74 DoJ 2016:2–3). However, the continuity of the topic throughout the period investigated shows that a successful partnership according to the

[44] In general, the public-private approach with regard to critical infrastructure includes a multitude of actors on diverse levels: "The community involved in managing risks to critical infrastructure is wide-ranging, composed of partnerships among owners and operators; Federal, State, local, tribal, and territorial governments; regional entities; non-profit organizations; and academia" (U-43 DHS 2013:1). The focus in this sub-section is the private sector.

[45] "The private sector owns and operates over ninety percent of all of the networks and infrastructure of cyberspace and is thus the first line of defense" (U-63 DoD 2015:5).

vision of the government is not easily implemented. As Commerce notes in 2011, there is low rate of adoption of protective measures by the private sector and individuals leading to an increased risk for economic and national security (U-68 Commerce 2011:1). Also, the director of national intelligence criticizes that there are actors from the private sector that do not take into account cyber risks from abroad or dangers emanating from the interdependent nature of critical infrastructure in their risk assessment (U-37 DNI 2015:1). The FBI points out another problem, this time regarding the response side: In case of an attack, most private sector actors do not contact law enforcement authorities; as a result, the latter cannot resolve the case or get access to information and evidence (U-76 FBI 2016:10). More generally, DHS states that public-private partnerships can be challenging because of "inherent differences in motivations and operational cultures, including risk tolerance, funding, and time horizons" (U-44 DHS 2014:60). One main difference in this regard is the government's responsibility for public safety and national security, whereas the private sector takes into account economic considerations (U-43 DHS 2013:1–2). As a consequence, the government has to encourage the private sector to go further and also "invest in the national interest" (ibid.:2). Against this background, discourse participants are eager to underline the shared interest and the benefits of a partnership, especially "access to knowledge and capabilities that would otherwise be unavailable" (ibid.:10), the primarily voluntary character (ibid.) and the trusted atmosphere (ibid:13).

In concluding on this aspect, the presented elements of the discourse show that public-private partnerships are essential for the government in order to fulfill its mandate. Much of the communication is oriented towards convincing the private sector from the benefits of a partnership and clarifying the respective roles and responsibilities. As one result of this clarification process at the end of the examined period, DoD points to the government's "limited and specific role" (U-63 DoD 2015:5). That means a division of labor taking into account the significance of attacks: "While the U.S. government must prepare to defend the country against the most dangerous attacks, the majority of intrusions can be stopped through relatively basic cybersecurity investments that companies can and must make themselves" (ibid.).

Finally, the *third* aspect of shared responsibility concerns all U.S. citizens. To call upon the individual responsibility is a very strong and continuous element in the examined discourse.

Commerce Secretary Gary Locke[46] expressed in an early statement of 2010: "Ultimately, effective cyber security is dependent on the vigilance of civil servants, of our military personnel, of citizens and of businesses. Everyone needs to understand how central cyber security is to the safety, security and prosperity of America" (U-66 Commerce 2010:3). Another typical statement is the following: "All Americans must recognize our shared responsibility and play an active role in securing the cyber networks we use every day" (U-08 WH 2010:2). The White House regularly articulates this message in the presidential proclamations regarding the annual *National Cybersecurity Awareness Month* and the annual *Critical Infrastructure Protection Month*, later on called *Critical Infrastructure Security and Resilience Month*[47]. In a similar vein, DHS underlines the importance of public awareness for collective cybersecurity: "[A]n aware and empowered public is our best defense against threats, and our greatest resource in building resilience and fostering innovation" (U-40 DHS 2010:57).

In conclusion, both lines of argumentation addressed in this section – the United States as leading country in a digital world and shared responsibility at the national level – are very stable across the examined time frame.

4.1.1.4.2 Discourse on Goals

The overall goal for the U.S. government is cybersecurity in a global sense. As President Obama already noted in 2009, the "digital infrastructure" (U-02 WH 2009:2) is a "strategic national asset" (ibid.) and its protection is seen as top priority: "We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage" (ibid.). So, again, the prevention and response side of cyber risks is included. The high priority of cybersecurity as a goal for the U.S. government is continuously emphasized in the examined discourse period (see for example U-16 WH 2013:2).

In order to better understand the DHS view on cybersecurity, it is useful to shed light on the *Quadrennial Homeland Security Reviews* (QHSR) published by DHS in 2010 and 2014. In its

[46] Gary Faye Locke served as Commerce Secretary from 2009 to 2011.

[47] There is an interesting change in the name of the *Critical Infrastructure Protection Month*: In 2012, it is called *Critical Infrastructure Protection and Resilience Month*, and from 2013 onwards *Critical Infrastructure Security and Resilience Month*. That shows the growing importance of the concept of resilience in the context of critical infrastructure.

first review from 2010, DHS defines "Safeguarding and Securing Cyberspace" (U-40 DHS 2010:30) as one out of five homeland security missions. It formulates two goals: "Create a Safe, Secure, and Resilient Cyber Environment" (ibid.) and "Promote Cybersecurity Knowledge and Innovation" (ibid.). Four years later, in the 2014 review, the overall mission "Safeguard and Secure Cyberspace" (U-44 DHS 2014:7) remains unchanged, however, its content is revised and refined. It now contains four goals: "Strengthen the Security and Resilience of Critical Infrastructure" (U-44 DHS 2014:78), "Secure the Federal Civilian Government Information Technology Enterprise" (ibid.), "Advance Law Enforcement, Incident Response, and Reporting Capabilities" (ibid.), and "Strengthen the Ecosystem" (ibid.). Besides the fact that the goals are formulated more concretely and more detailed in 2014, it is interesting to note that cyber risks for critical infrastructure strongly gained in importance. This is due to two major drivers of change identified by DHS: the pervasiveness of digitalization (U-44 DHS 2014:19–20) and the increasing degree of interdependence or "cyber-physical convergence" (U-44 DHS 2014:23) of critical infrastructure.

In the eyes of discourse participants, cybersecurity ultimately serves the higher purposes of national and economic security as well as public safety (see for example U-02 WH 2009:2). Other than the strong presence of national security as topic in the cybersecurity discourse, the aspect of economic security is especially important for the U.S. government. As the White House formulates in 2011, "[c]ybersecurity is not an end unto itself; it is instead an obligation that our governments and societies must take on willingly, to ensure that innovation continues to flourish, drive markets, and improve lives" (U-09 WH 2011:preface). So, cybersecurity is seen as a condition in order to realize the potential of digitalization: greater economic prosperity for the U.S. (ibid.). Of course, risks are seen and there is a strong element of preparedness in the discourse pointing to the responsibility to "stay a step ahead of our adversaries" (U-12 WH 2012:2). But overall, the potential of digitalization is communicated as something very positive in the U.S. discourse: According to President Obama, the "Internet Age" is still at the beginning and much more is to come in terms of innovation (U-21 WH 2015:9). From a U.S. point of view, even given the risks related to the Internet, there is no sense in restricting it: "[I]f we restricted all technology that could possibly be used for bad purposes, we'd have to revert to the Stone Age" (U-52 State 2015:7).

Finally, the goal of cybersecurity is also valid on the international level. The larger context of the international vision of the United States is a "free, open, and secure internet where universal human rights are respected, and which provides a space for greater progress and prosperity over the long run" (U-47 State 2011:5–6). Regarding the aspect of cybersecurity, the United States favors what it calls "international cyber stability" (U-51 State 2015:6): That means "a more peaceful environment where all states are able to enjoy the benefits of cyberspace; where there are benefits to state-to-state cooperation and avoiding conflict; and where there is little incentive for states to attack one another" (ibid.).

4.1.1.4.3 Discourse on Measures

In this section, I focus on concrete problem-solving measures regarding cybersecurity risks. I proceed by using the same overall structure as in the section on risks and present solutions in four groups: solutions for cybersecurity risks in general, for cyber risks for critical infrastructure, for cyber risks within the military context as well as solutions for cybercrime risks. It is neither possible nor helpful to exhaustively present all measures taken by the U.S. government and articulated in the discourse. Rather, I focus on a selection of essential and exemplary measures for each group.

Solutions for cybersecurity risks in general. To begin, I shed light on measures regarding cybersecurity risks in general. President Obama underlines that the topic of cybersecurity was taken up early in his administration (U-11 WH 2011:1) and that there is a "comprehensive strategy" (U-21 WH 2015:6) integrating prevention, response and recovery elements: "[A]s part of our comprehensive strategy, we've boosted our defenses in government, we're sharing more information with the private sector to help those companies defend themselves, we're working with industry to use what we call a Cybersecurity Framework to prevent, respond to, and recover from attacks when they happen" (U-21 WH 2015:6–7).

In order to get a more concrete idea what steps the U.S. government takes to cope with cyber risks, the so-called *Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise*, issued by DHS in 2011 (U-41 DHS 2011), is a good

example. On the one hand, the *Blueprint* wants to protect critical information infrastructure (U-41 DHS 2011:iii). Therefore, measures in four categories are proposed:

- "Reduce Exposure to Cyber Risk" (U-41 DHS 2011:13) by technical measures such as systems to prevent intrusions; collection, analysis, and sharing of information on cyber risks; identification and assessment of critical parts and vulnerabilities; implementation of security standards and monitoring activities; R&D and rapid implementation of security innovations (U-41 DHS 2011:13–15),
- "Ensure Priority Response and Recovery" (U-41 DHS 2011:16) by detection and analysis activities using the input of bodies such as the National Cybersecurity and Communications Integration Center (NCCIC) and responding in a coordinated and collaborative effort of public and private partners; plans for response and recovery; investigations of cyber risks; exercises and continuity planning to increase preparedness (U-41 DHS 2011:16–17),
- "Maintain Shared Situational Awareness" (U-41 DHS 2011:17) by fusing and distributing relevant information on cyber threats though the US-CERT and other entities; having in place strategies for risk communication; improving the knowledge base and training opportunities of cyber professionals (U-41 DHS 2011:17–19),
- "Increase Resilience" (U-41 DHS 2011:19) by integrating redundancies, diversity, and other techniques such that systems are able to continue basic operations even in case of cyber incidents (U-41 DHS 2011:19).

On the other hand, the *Blueprint* aims at "Building a Stronger Cyber Ecosystem for Tomorrow" (U-41 DHS 2011:iii). Therefore, measures in another four categories are proposed:

- "Empower Individuals and Organizations to Operate Securely" (U-41 DHS 2011:20) by improving education and career options in the field of cybersecurity; raising awareness and supporting individuals with information, tools and other resources (U-41 DHS 2011:20–21),
- "Make and Use More Trustworthy Cyber Protocols, Products, Services, Configurations and Architectures" (U-41 DHS 2011:21) by integrating security aspects in development and standard setting processes; supporting the widespread use of secure technology (U-41 DHS 2011:21–22),

- "Build Collaborative Communities" (U-41 DHS 2011:22) by using secure authentication systems; improving interoperability; using automated security mechanisms (U-41 DHS 2011:22–23),
- "Establish Transparent Processes" (U-41 DHS 2011:23) by broadly sharing information on cyber risks as well as on the efficacy of security measures among stakeholders; incentivizing the adoption of cybersecurity measures (U-41 DHS 2011:23–24).

What can be seen from this example is the wide range of measures for coping with cyber risks. They occur in different variations and with different areas of focus in many of the documents analyzed. The solutions proposed address the complete risk cycle: There are measures with a preventive character in order to avoid, or at least minimize, exposure to the risk, and there are response and recovery measures. There are measures on the political and legal level (such as strategies, plans, frameworks, agreements by the executive, law enforcement, legislation), on the technical level (such as research and development, standards), as well as measures regarding the public (such as awareness raising, education, training).

The *Cybersecurity National Action Plan* (CNAP) from 2016 is another example of a measure on the national political level. It is worth mentioning because it points to another important topic: the state of cybersecurity at the federal government, where many deficits can be found. As President Obama describes the urgent need to modernize federal IT: "It is no secret that too often government IT is like an Atari game in an Xbox world. The Social Security Administration uses systems and code from the 1960s. No successful business could operate this way" (U-25 WH 2016:2). Major elements of the CNAP are enormous investments in modern IT systems and cybersecurity education, the creation of a Federal Chief Information Security Officer, and the establishment of an expert commission, the Commission on Enhancing National Cybersecurity, elaborating long-term recommendations on cybersecurity for the public and private sector (U-27 WH 2016:2).

As to the *international* level, different measures and steps are articulated in the discourse in order to increase international cybersecurity. Primarily, the U.S. promotes its aforementioned "strategic framework of international cyber stability" (U-53 State 2016:12). Major goals of the framework are the "(1) global affirmation of the applicability of

international law to state behavior in cyberspace; (2) the development of international consensus on additional norms and principles of responsible state behavior in cyberspace that apply during peacetime; and (3) the development and implementation of practical CBMs, which can help ensure stability in cyberspace by reducing the risk of misperception and escalation" (ibid.:12–13). Another area, in which the U.S. is very active internationally, is "ensuring that nations perform their cybersecurity due diligence" (U-49 State 2014:3). Therefore, the U.S. collaborates with other states on diverse cybersecurity issues such as network defense or coping with attacks (ibid.). The U.S. also helps building capacity in states less developed in information and communication technology, for example by organizing cybersecurity trainings (ibid.). For these kinds of measures, the State Department works with DHS and other departments (ibid.).

In general, regarding international aspects, it is important to highlight the U.S. interest in the "primacy of interoperable and secure technical standards" (U-09 WH 2011:18) for products and services. Such standards are important preconditions for the operability and security of the global digital infrastructure and, ultimately, for trade and commerce (ibid.). As the U.S. wants to foster the success of its digital economy, Commerce Secretary Locke underlines that "for businesses (…) a more tailored approach to cyber security might be necessary" (U-66 Commerce 2010:2).

Measures regarding *people* present another prominent element in the discourse on measures. They basically include two elements: education and awareness raising in the field of cybersecurity. Early in his administration, President Obama underlined the forward-looking importance of this area of measures: "[W]e will begin a national campaign to promote cybersecurity awareness and digital literacy from our boardrooms to our classrooms, and to build a digital workforce for the 21st century. (…) Because it's not enough for our children and students to master today's technologies (…) – we need them to pioneer the technologies that will allow us to work effectively through these new media and allow us to prosper in the future" (U-02 WH 2009:3). Education implies cybersecurity education and training in a global sense and includes students of all ages as well as the cyber workforce. An important program in this regard is the National Initiative for Cybersecurity Education (NICE), which is led by the Department of Commerce's National Institute of Standards and

Technology (NIST).[48] Also, training and exercises in working environments where cyber risks can occur are regularly mentioned, for example in the *National Infrastructure Protection Plan* (U-43 DHS 2013:5) and the *Blueprint* mentioned above (U-41 DHS 2011:16–17). The second element is awareness raising to the general public. Therefore, the presidential proclamations regarding the annual *National Cybersecurity Awareness Month* and the annual *Critical Infrastructure Protection Month*, later on called *Critical Infrastructure Security and Resilience Month*, are important instruments. Moreover, specific campaigns are initiated to raise awareness. The most important one is the "Stop.Think.Connect." campaign launched by DHS in 2010 (U-42 DHS 2012:10) in order to "make basic cybersecurity practices as reflexive as putting on a seatbelt" (U-42 DHS 2012:10). A recent initiative of this campaign is called "Lock Down Your Login" and notably promotes stronger authentication (U-27 WH 2016:3).

Solutions for cyber risks for critical infrastructure. In this area, several national measures stand out, among them the *National Infrastructure Protection Plan* (NIPP) 2009, the NIPP 2013 (both discussed in section 4.1.1.4.4), and the *Cybersecurity Framework* from 2014. One main interest in these documents is to provide a useful framework for public-private cooperation in order to protect critical infrastructure from general and cyber-related risks. Another exemplary measure is the *National Cyber Incident Response Plan* (NCIRP) from 2016.

The *Cybersecurity Framework* from 2014 is based on *Executive Order 13636* from 2013 directing the government and the owners and operators of critical infrastructure "to improve cybersecurity information sharing and collaboratively develop and implement risk-based approaches to cybersecurity" (U-43 DHS 2013:9). More concretely, the framework shall notably help implement the use of "strong cybersecurity practices" (ibid.). It is a voluntary framework that was created with industry actors in a cooperative effort (U-69 Commerce 2014:3). I present and evaluate it in a more detailed way below in chapter 5.

[48] More details on NICE: "The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. (…) The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our Nation secure" (National Institute of Standards and Technology (NIST) 2018).

President Obama qualifies the framework as "turning point" (U-17 WH 2014:2) and evaluates the process of elaborating it as "a great example of how the private sector and government can, and should, work together to meet this shared challenge" (ibid.).

The *National Cyber Incident Response Plan* (NCIRP) follows *Presidential Policy Directive 41 (PPD-41), United States Cyber Incident Coordination*, and provides a plan articulating "the roles and responsibilities, capabilities, and coordinating structures that support how the Nation responds to and recovers from significant[49] cyber incidents posing risks to critical infrastructure" (U-46 DHS 2016:4). It is thus a solution concentrating on response and recovery. Because of its focus of looking at major organizational structures, the plan is intended as the "primary strategic framework" (U-46 DHS 2016:4). The basic idea of the NCIRP is to clarify that there are three lead agencies with their respective entities fulfilling different functions in case of a significant cyber incident: The Department of Justice (DOJ) through the Federal Bureau of Investigation (FBI) and the National Cyber Investigative Joint Task Force (NCIJTF) is responsible for the task of *threat response*; DHS through its National Cybersecurity and Communications Integration Center (NCCIC) takes care of *asset response*; and, finally, the Office of the Director of National Intelligence (ODNI) through the Cyber Threat Intelligence Integration Center (CTIIC) provides *intelligence support* (U-46 DHS 2016:11). An incident specific "Cyber Unified Coordination Group" is established in the case of a significant cyber incident and serves as "primary national operational coordination mechanism" (U-46 DHS 2016:31) between the actors involved in response activities.[50]

There is also an international component in the protection of critical infrastructure as IT and other infrastructures transcend borders. For this purpose, the United States cooperates with other governments and within multilateral organizations (U-39 DHS 2009:53–54). For example, there is a trilateral cooperation of the U.S., Canada, and Mexico to take care of overlapping issues of IT and cybersecurity (ibid.:56). In order to protect critical infrastructure on a global scale, international information sharing is an important aspect (U-26 WH 2016:2–3).

[49] Significant is defined as "likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people" (U-46 DHS 2016:8).

[50] The design of the NCIRP is oriented towards compatibility with other plans and systems such as NIST's Cybersecurity Framework and also aligns with the National Preparedness System (U-46 DHS 2016:7–9).

Solutions for cyber risks within the military context. In this area, the declaration of cyberspace as a military domain (U-56 DoD 2010:101) and the creation of U.S. Cyber Command (U.S. Department of Defense 2010:1) are important measures. Other elements concern DoD's infrastructure, forces and capabilities as well as research and development of military technology. As an important evolution in the course of the examined discourse period takes place, the measures in the military domain are discussed in detail below in section 4.1.1.4.4.

Solutions for cybercrime risks. The basic intention of the U.S. government is the prevention of cybercrime and, if prevention is not successful, investigation and prosecution (U-40 DHS 2010:56). This also serves the intention of deterrence (U-71 DoJ 2011:5). Discourse participants especially underline the need to bring together all available means, especially "coordinating and integrating robust counterintelligence, counterterrorism, intelligence, and law enforcement activities" (U-40 DHS 2010:56). Discourse participants express a very determined attitude regarding the fight against cybercrime: "[W]e want cyber criminals to feel the full force of American justice, because they are doing as much damage, if not more, these days as folks who are involved in more conventional crime" (U-20 WH 2015:4). In a similar vein, DHS underlines the necessity that "criminal organizations engaged in high-consequence or wide-scale cyber crime are aggressively investigated and disrupted, and their leaders arrested, indicted, and prosecuted" (U-40 DHS 2010:56).
FBI Director Comey highlights four different strategies: "[W]hether through indictment or prosecution or sanction or publicity, we are working very hard to make people at keyboards feel our breath on their necks and try to change that behavior. We've got to get to a point where we can reach them as easily as they can reach us, and change behavior by that reach-out" (U-76 FBI 2016:10). The strategies of indictment and publicity were used in the already mentioned cases of the Chinese hackers and Iran (see above section 4.1.1.2.5). Comey clearly pointed out that the U.S. goal was "to name and shame (…) who is doing this and exactly what they're doing" (U-76 FBI 2016:9). An example of sanctions in order to punish cybercrime is case of North Korea and the Sony hack (see above section 4.1.1.2.5). In the wake of this attack, *Executive Order 13694, Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*, and the *North Korea Sanctions*

and Policy Enhancement Act of 2016 were issued (U-53 State 2016:22).[51] For certain types of attack, a close collaboration between law enforcement and the private sector can help mitigate the risk: For example, in a case of a large-scale DDoS attack on the financial sector, the FBI provided companies with "classified threat briefings" (U-75 FBI 2014:4).

However, the most fundamental ways to cope with cybercrime are to investigate and prosecute criminal activities (U-71 DoJ 2011:5). The institutional "centerpiece" (U-74 DoJ 2016:2) in this regard is the *Computer Crime and Intellectual Property Section* (CCIPS) of the Department of Justice (DoJ).

While DoJ is proud of its successes in the fight against cybercrime – regularly achieved in cooperation with international and private sector partners (U-74 DoJ 2016:2) – discourse participants criticize that several law enforcement authorities are not up to date. Urgent updates are needed, for example, in the case of laws for combating spyware and botnets (U-73 DoJ 2015:4). An effective update could be reached in the case of the Rule 41 of the Federal Rules of Criminal Procedure[52], which is cited as a positive example in the discourse (U-74 DoJ 2016:4). More generally speaking, DoJ underlines that "[o]ur response to cyber threats requires revisiting laws that simply did not anticipate and cannot adjust to modern technology. We must (…) ensure that our laws protect Americans from criminals, and not the other way around" (ibid.).

Other obstacles in the fight against cybercrime are seen in "foreign-stored digital evidence" (U-74 DoJ 2016:5)[53] and encryption that is "warrant-proof" (U-74 DoJ 2016:6), that means it

[51] For more information see the text of the Executive Order (White House, Barack Obama 2015) and the blog post of White House Cybersecurity Coordinator Michael Daniel (Daniel 2015).

[52] The original version of the rule required that a search warrant had to be obtained in the district of the property that should be searched; however, in many cases of cybercrime, the actual location of a computer is not clear (U-74 DoJ 2016:3). The amendment of rule 41 corrected this difficulty: "The update to the Rule does not alter the probable cause or other standards we must meet to obtain a search warrant. What the Rule does change is that now, when criminals hide the location of their computers through anonymizing technology, we don't have to figure out in which federal district the computers are physically located before we can act to stop criminal activity. Likewise, when a criminal deploys a botnet that indiscriminately infects computers nationwide – as many botnets now do – we don't have to go to as many as 94 different judges" (ibid.).

[53] The issue with digital evidence is that "[i]ncreasingly, (…) American providers and other providers subject to the jurisdiction of the United States are storing such information outside the United States, and not always at rest and in the same location. The data can be partitioned and stored in multiple locations, or moved about on an ongoing basis, and some providers may not even know where all data relating to a particular user is at a given time" (U-74 DoJ 2016:5). In order to access foreign-stored data, authorities use cooperative mechanisms and legal assistance possibilities, but this proceeding often takes several months or even longer (ibid.). The problem got even worse in the wake of the "Microsoft Ireland" case (ibid.). As a consequence of the decision in this case, it became impossible "to compel a U.S. service provider, such as Microsoft, to produce data that it chooses to store for its own business purposes (and typically without the knowledge or input of its subscribers) outside the United States" (ibid.).

cannot be broken by law enforcement.[54] As DHS Secretary Johnson[55] puts it: "Our inability to access encrypted information poses public safety challenges. In fact, encryption is making it harder for your government to find criminal activity, and potential terrorist activity" (U-45 DHS 2015:8).

The vigorous stance of the United States communicated in the discourse on national cybercrime issues is also true for the international level: "We firmly believe that the battle against transnational cybercrime is one we can and will win" (U-49 State 2014:3). Accordingly, the United States is a strong supporter of the *Convention on Cybercrime* of the *Council of Europe* (CoE), the so-called *Budapest Convention*[56], and promotes its expansion (U-49 State 2014:3). The country is also eager to support other nations in the fight against cybercrime (U-09 WH 2011:22–23), which is done in the context of the already mentioned capacity building measures. The United States describes itself as a "global leader in the campaign against transnational cybercrime" (U-53 State 2016:5), which underlines the self-assertive stance of the country.[57]

4.1.1.4.4 Evolution of the Discourse regarding the Evaluation of Measures

In this section, the evolution of the discourse regarding the evaluation of measures shall be traced. In some areas, important changes can be observed in the course of the examined time period. Interesting evolutions can notably be observed in the area of cyber risks for critical infrastructure as well as in the military and international context.

[54] The FBI terms this problem "Going Dark" (U-76 FBI 2016:13). FBI Director Comey describes "Going Dark" as the "increasing inability with judicial authority to get access to information that sits on a device or that is traveling in real time – the challenge we face is that the advent of default ubiquitous strong encryption is making more and more of the room that we are charged to investigate dark" (U-76 FBI 2016:13).

[55] Jeh Charles Johnson served as Secretary of Homeland Security from 2013 to 2017.

[56] The Council of Europe *Convention on Cybercrime* (Budapest Convention) is the "first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception" (Council of Europe 2018). It entered into force in 2004; in 2018, it had got 56 signatories (Convention on Cybercrime 2018). The U.S. supports it because "[i]t identifies the three elements needed for effective cybercrime legislation, namely: (1) strong and harmonious substantive cybercrime laws; (2) comprehensive investigative tools for addressing high-tech crime and conducting digital forensics; and (3) effective mechanisms for both formal and informal international cooperation, like the G-8 24/7 Network" (U-49 State 2014:3).

[57] Another example of an international form of cooperation, in which the United States actively participates, is the cooperation among *Computer Security Incident Response Teams* (CSIRTs) (U-39 DHS 2009:56).

As *critical infrastructure* is in the focus of this study, it is important to note that already in the years before the period examined here, there were measures regarding the link between critical infrastructure and cyber risks. Important measures and documents were:

- the *Homeland Security Act of 2002* creating DHS and charging it with several missions, among them to "develop a comprehensive national plan for securing the CIKR [critical infrastructure and key resources, K.U.] of the United States, including power production, generation, and distribution systems; IT and telecommunications systems (including satellites); electronic financial and property record storage and transmission systems; emergency preparedness communications systems; and the physical and technological assets that support such systems" (U-39 DHS 2009:135),
- the *National Strategy to Secure Cyberspace* from 2003 dealing with the prevention of cyber risks and how to respond to it and serving as the "foundation for the cybersecurity component of CIKR" (U-39 DHS 2009:141), and
- *Homeland Security Presidential Directive* 7 (HSPD-7) from 2003 establishing a strengthened policy framework for protecting U.S. critical infrastructure and key resources (CIKR) notably by developing a *National Infrastructure Protection Plan* (NIPP) (U-39 DHS 2009:74).

On this basis, several plans and frameworks were adopted in the period examined in this study.[58] Among them are the *National Infrastructure Protection Plan* (NIPP) 2009 and the NIPP 2013. More specifically, the NIPP 2009 aims at providing an "overarching approach for integrating the Nation's many CIKR protection initiatives into a single national effort" (U-39 DHS 2009:i). This overall coordinating structure includes a "comprehensive risk management framework and clearly defined roles and responsibilities" (ibid.) for DHS and public and private partners on all levels. In general, the NIPP structure comprises two major coordination elements: On the one hand, there are Sector Coordinating Councils (SCC), the

[58] In this period in 2008, the Bush administration issued National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) launching the Comprehensive National Cybersecurity Initiative (CNCI) (U-39 DHS 2009:145). However, as the directive and the CNCI were classified at the time of their publication (Vijayan 2010), these documents are not part of the data corpus analyzed. A later version of the CNCI, partly declassified by the Obama administration (ibid.), is part of the data corpus (U-03 WH 2009). In a DNI document from 2009, the CNCI is described as follows: "The CNCI addresses current cybersecurity threats, anticipates future threats and technologies, and develops a framework for creating in partnership with the private sector an environment that no longer favors cyber intruders over defenders. The CNCI includes defensive, offensive, education, research and development, and counterintelligence elements, while remaining sensitive throughout to the requirements of protecting the privacy rights and civil liberties of US citizens" (U-29 DNI 2009:40).

members of which are private sector owners and operators of critical infrastructure (ibid.:4). On the other hand, Government Coordinating Councils (GCC) constitute the counterparts to the SCCs on the government side: They include members of the sector-specific and other agencies as well as government actors from diverse subnational levels (State, local, tribal, and territorial governments) (ibid.). The Sector-Specific Agencies (SSAs), that means specific federal departments or offices, develop Sector-Specific Plans (SSPs) under the NIPP framework in collaboration with partners from the respective sectors (ibid.:111).

In order to cope with cyber risks, the NIPP 2009 takes a twofold approach: On the one hand, it develops a "cross-sector cyber element that involves DHS, SSAs and Government Coordinating Councils (GCCs), and private sector owners and operators" (U-39 DHS 2009:12). On the other hand, it is the responsibility of the IT Sector and the Communications Sector (ibid.). A cornerstone of the plan is information sharing (ibid., 56). An important entity in this regard is the United States Computer Emergency Readiness Team (US-CERT) that provides a "single point of contact for cyberspace analysis, warning, information sharing, and incident response and recovery for CIKR partners" (ibid.:65). US-CERT is organized as public private partnership between DHS and partners (ibid.). The cross-sector cybersecurity element consists of numerous programs, for instance the *Critical Infrastructure Protection Cybersecurity* (CIP CS) *Program*, the *Control System Security Program*, or the *Standards and Best Practices Program* (ibid.:117–118).

The *National Infrastructure Protection Plan* (NIPP) 2013 basically continues the overall idea of the NIPP 2009 using risk management and public-private partnerships as key elements and the already mentioned coordinating bodies as structure (U-43 DHS 2013, 4). As an evolution from the NIPP 2009, the NIPP 2013 "[i]ntegrates cyber and physical security and resilience efforts into an enterprise approach to risk management" (ibid.). So, the NIPP acknowledges new risk developments since the last NIPP (ibid.:1) and routinely includes cyber elements in all considerations of the risk management framework[59] (ibid.:15). This integration can also be seen in the overall mission of the NIPP 2013: "Strengthen the security and resilience of the Nation's critical infrastructure, by managing physical and cyber risks

[59] The risk management framework is oriented towards the "five national preparedness mission areas of prevention, protection, mitigation, response, and recovery" (U-43 DHS 2013, 1) defined in Presidential Policy Directive 8 (PPD-8) on National Preparedness from 2011, which is another evolution compared to the NIPP 2009.

through the collaborative and integrated efforts of the critical infrastructure community" (ibid.:5).

Regarding cyber risks within the *military* context, the United States early on invoked a military dimension. So, cyberspace was declared a military domain: "As a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain of warfare. Although cyberspace is a man-made domain, it has become just as critical to military operations as land, sea, air, and space. As such, the military must be able to defend and operate within it" (U-56 DoD 2010:101). Given the assessment of cyber risks by the U.S. government and the overall leadership attitude of the country, this declaration is not surprising. The White House *International Strategy for Cyberspace* from 2011 formulates the implications of recognizing cyberspace as a military domain as follows: "When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means – diplomatic, informational, military, and economic – as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests" (U-09 WH 2011:14). This statement underlines the equivalence from hostile cyber threats to other forms of threats and the right to react appropriately – for the United States, this includes military means as ultimate option.[60]

Outside observers feared a militarization of cyberspace, which is a man-made civilian domain, and pointed out the dangers of this process (see for example Wallace 2013c). This was taken up in the official discourse at a relatively early point in time and DoD underlined its obligation to be able to defend this space (U-58 DoD 2011:3). Also, DoD stressed that a militarization is not intended; rather, DoD envisioned a "commitment to peace through preventive defense" (ibid.:4). Put in the words of William Lynn, "establishing robust cyberdefenses no more militarizes cyberspace than having a navy militarizes the ocean" (ibid.).

[60] The statement continues as follows: "In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible" (U-09 WH 2011:14).

With an eye on the examined time period, the years 2010 and 2011 can be considered a first phase of taking a strategic position and implementing important measures regarding how to handle cyber risks in the military context with a special emphasis on defense. Most notably, DoD creates the U.S. Cyber Command (USCYBERCOM). It is formally established in 2009 and ready to operate in May 2010 (U.S. Department of Defense 2010:1).[61] Other measures aim at implementing "new defense operating concepts to protect DoD networks and systems" (U-57 DoD 2011:6)[62], enhancing the IT acquisition process, above all by speeding it up (U-56 DoD 2010:107), as well as focusing governmental R&D on cybersecurity (ibid.:105). As an example, the *Defense Advanced Research Projects Agency* (DARPA) started the *National Cyber Range program* in order to do cyber simulations in a laboratory-like testing environment (ibid.:105–106). Moreover, the cyber workforce is a crucial topic for DoD. However, in the long run, there will be a shortage of qualified employees, as William Lynn points out: Despite the efforts of DoD and the U.S. government to employ more cybersecurity personnel in diverse areas, he states that "over the next 20 years, many countries, including China and India, will train more highly proficient computer scientists than will the United States" (U-56 DoD 2010:106). That is why, from his point of view, the United States has to "focus not on numbers but on superior technology and productivity" (ibid.:106–107). In the end, advanced technology – he mentions "[h]igh-speed sensors, advanced analytics, and automated systems" (ibid.:107) – must be the U.S. answer in order to compensate the shortage. But advanced technology is dependent on the continued success and innovative strength of the U.S. IT economy (ibid.).

A second phase follows towards the end of the examined time period around 2015, when DoD issues its second cyber strategy. In this strategy, the declaratory policy from the first phase is confirmed: "The United States will continue to respond to cyberattacks against U.S. interests at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power and in accordance with applicable law" (U-63 DoD 2015:11).

[61] Also regarding the creation of U.S. Cyber Command, the defense aspect was highlighted: "To facilitate operations in cyberspace, the Defense Department needs an appropriate organizational structure. For the past several years, the military's cyberdefense effort was run by a loose confederation of joint task forces dispersed both geographically and institutionally. In June 2009, recognizing that the scale of the effort to protect cyberspace had outgrown the military's existing structures, Defense Secretary Robert Gates ordered the consolidation of the task forces into a single four-star command, the U.S. Cyber Command, which began operations in May 2010 as part of the U.S. Strategic Command" (U-56 DoD 2010:101–102).

[62] A major element of this new approach is called "active defense" (U-56 DoD 2010:103): This technology tries to stop an intrusion before entering the targeted system; if it is still successful in entering it, active defense technology is able to capture the intruder within the targeted system (ibid.).

However, the overall communication of the military actors is much more transparent, which is a clear evolution from the first to the second phase. Also, more details are officially published. In particular, the offensive use of cyber means is now openly mentioned. Military experts had, for a long time, assumed that the United States builds such capabilities (Wallace 2013b). Now, the strategy openly states: "If directed by the President or the Secretary of Defense, the U.S. military may conduct cyber operations to counter an imminent or on-going attack against the U.S. homeland or U.S. interests in cyberspace" (U-63 DoD 2015:5).[63] Also, "DoD must be able to provide integrated cyber capabilities to support military operations and contingency plans" (ibid.:5). This could be, for instance, the disruption of military infrastructure by cyber means (ibid.). DoD underlines the importance of respecting the country's values and legal framework and making well-considered decisions before employing such cyber capabilities (ibid.:6). In line with the more transparent language, Michael Rogers, the Commander of U.S. Cyber Command, openly describes the Cyber Command as "the nation's warfighting arm in cyberspace" (U-64 DoD 2015:1). He also stresses that the "freedom and ability to operate in cyberspace is a goal in itself and also is a critical enabler for operations on land, in the air, at sea, and in space" (U-64 DoD 2015:8). This again shows the crucial importance of and dependence on information and communication technology especially in the U.S. military context. As a logic consequence, much has to be done in order to "preserve and extend America's cyber advantage" (U-64 DoD 2015:8).

While, in general, information technology in all areas enormously evolved between 2010 and 2015, the fundamental challenges for the U.S. military remain basically the same at the end of the examined period: It is still an essential task to defend DoD's digital infrastructure (U-63 DoD 2015:4) and to "build and maintain ready forces and capabilities to conduct cyberspace operations" (ibid.:7). As to forces, it has to be noted that the process of creating the *Cyber Mission Force* was started in 2012 and is still ongoing three years later (ibid.:6–7).[64] Moreover, there is still the topic of R&D as well as the necessity to "[b]uild bridges to

[63] This concerns "cyberattacks of significant consequence" (U-63 DoD 2015:5) that are defined as follows: "While cyberattacks are assessed on a case-by-case and fact-specific basis by the President and the U.S. national security team, significant consequences may include loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States" (ibid.).

[64] The *Cyber Mission Force* is organized as follows: "The Force includes Cyber Protection Forces that operate and defend the Department's networks and support military operations worldwide, Combat Mission Forces that support Combatant Commanders as they plan and execute military missions, and National Mission Forces

the private sector" (U-63 DoD 2015:3) in order to develop "leap-ahead technologies to defend U.S. interests in cyberspace" (ibid.:19). This is all the more important given that competitors threaten the U.S. advantage in the cyber domain and that "today much of the technical expertise necessary here resides outside government and often outside our nation" (U-64 DoD 2015:2).

With regard to *international* cooperation, the White House already noted in its 2011 strategy that it intends to "[b]uild and enhance existing military alliances to confront potential threats in cyberspace" (U-09 WH 2011:21). It notably aimed at increasing collective capacities for awareness, warning, defense, and deterrence (ibid.) as well as reducing "misperceptions about military activities and the potential for escalatory behavior" (ibid.) through a variety of mechanisms for coordination and exchange (ibid.). In 2014, the *North Atlantic Treaty Organization* (NATO) officially stated that "cyber defense is part of NATO's collective defense mission" (U-53 State 2016:4) – an important progress in the interest of the United States. Also, the United States is very active in diverse international fora and claims several achievements, that took place from 2013 onwards, as successes of its efforts. Major accomplishments could be reached in the *United Nations Group of Governmental Experts* (UN GGE)[65] in 2013 and 2015: There was notably an agreement that international law applies in cyberspace and a consensus on a set of voluntary rules during peacetime (ibid.:4). Also, within NATO and the *Group of 20* (G20), states affirmed in 2014 and 2015 that international law is valid in the cyber domain (ibid.:3–4). Agreements on confidence building measures (CBMs) in the *Organization for Security and Cooperation in Europe* (OSCE) in 2013 and 2016 constituted another success from an U.S. point of view (ibid.:4). The purpose of the CBMs is "to build trust and reduce the risk of escalation and misperception in the region" (ibid.). Moreover, the United States could reach bilateral agreements with China and Russia (see above section 4.1.1.2.5). The overall purpose that the United States intends with all these measures is a "shared understanding about norms of acceptable state behavior in cyberspace, which will help enhance stability, ground foreign and defense policies, guide

that counter cyberattacks against the United States. The Cyber Mission Force will be manned by 2016" (U-62 DoD 2014:33).

[65] Since 2004, several Groups of Governmental Experts (GGE) have been working on "existing and potential threats from the cyber-sphere and possible cooperative measures to address them" (United Nations Office for Disarmament Affairs (UNODA) 2015:1). The Groups are supported by the UN Office for Disarmament Affairs (United Nations Office for Disarmament Affairs (UNODA) 2015:2).

international partnerships, and help prevent the misunderstandings that lead to conflict" (U-49 State 2014:2).

4.1.1.5 Overview: Condensed Frame Elements in the U.S. Discourse

In order to conclude the presentation of the U.S. discourse, the following table (Figure 8) presents the most relevant frame elements in a condensed fashion.

Figure 8: Condensed Frame Elements in the U.S. Discourse

Cybersecurity Risks			
	Description/Evaluation	**Time Frame Evolution**	**Dominant Discourse Participants**
Cyber Risks in General	Malicious cyber activity in the form of exploitation, disruption, or destruction of data and information infrastructures		
Cyber Risks for Critical Infrastructure	Real, ongoing, increasing risk; immediate threat; potentially dramatic impact/consequences	Peak in 2012/2013	DHS, WH, DoD
Cyber Risks Within the Military Context	"glimpse of the future face of war"; possibly severe and far-reaching effects; threat to strategic and technological advantage; increasing risk	More differentiation in the course of time	DoD, WH, DNI
Cybercrime Risks	Threat on the individual level, for society, and economy; large-scale data/IP theft; increase of risks in sophistication and quantity	Constant (high) attention	DoJ, FBI

Drivers and Actors	
Drivers	Dependence ("backbone"); technology as enabler ("great irony of our Information Age"); downside of innovation
Actors	General: individual hackers, (organized) cybercriminals, terrorists, nation states; specific: China, Russia, Iran, North Korea

Evaluation	
Evaluation	Seriousness; permanently aggravating cyber risks in diverse dimensions ("increasing in frequency, scale, sophistication, and severity"); high potential for disruption and destruction; in the end: accepted permanence of cyber risks, above all "low-to-moderate level cyber attacks" → "cyber risk must be managed"

Solutions	
Responsibility	U.S. as leading country in a digital world; shared responsibility at the national level (whole-of-government approach, PPP, individual responsibility)
Goals	Comprehensive cybersecurity ("Safe, Secure, and Resilient" cyberspace) serving national and economic security; cybersecurity as condition in order to use potential of digitalization; international: "free, open, and secure internet"
Measures	Comprehensive set of people, technology and norms-oriented measures regarding prevention, response, and recovery at the national and international level; critical infrastructure: Cybersecurity Framework/Executive Order 13636; military: U.S. Cyber Command, cyberspace as military domain, offensive and defensive means; cybercrime: prevention, investigation, prosecution

Note: Own compilation. Quotations refer to the respective sections in chapter 4.1.1.

We now turn to the discourse of the German executive.

4.1.2 Frame Elements in the German Discourse

In the following sections, the frame elements in the German discourse are presented starting with cybersecurity risks.

4.1.2.1 Cybersecurity Risks

4.1.2.1.1 Cybersecurity Risks in General

What is seen as cybersecurity risk in the German government discourse? In order to find out, it is helpful to look at the definition of a cyber attack in the first *Cyber Security Strategy for Germany*, issued by the Federal Ministry of the Interior (BMI) in 2011: "A cyber attack is an IT attack in cyberspace directed against one or several other IT systems and aimed at damaging IT security. The aims of IT security, confidentiality, integrity and availability may all or individually be compromised. Cyber attacks directed against the confidentiality of an IT system, which are launched or managed by foreign intelligence services, are called cyber espionage. Cyber attacks against the integrity and availability of IT systems are termed cyber sabotage" (D-03 BMI 2011:14–15). From this definition, we can see that attacks impact confidentiality, integrity, and/or availability, in short: IT security. It is interesting to note that the term IT security – a term primarily used in the technical community – is used instead of cybersecurity. It holds true for large parts of the German discourse that IT security is a very prominent term, for example in the title of a regular publication of the Federal Office for Information Security (BSI).[66] The definition of cyber attack in the second cyber strategy from 2016 is quite similar to the one from 2011, and equally focuses on IT security: "A cyber attack is an impact on one or several other IT systems in or through cyberspace aiming at completely or partially compromising IT security by IT means" (D-04 BMI 2016:46, own translation).

There is a wide range of concrete examples of cybersecurity risks in the German discourse. They include, for instance, the theft of personal data (D-11 BSI 2013:5), "digital extortion" (D-36 BKA 2016:9, own translation), "electronic attacks" with the goal of espionage or sabotage (D-37 BfV 2013:377–378, own translation), the disruption of critical infrastructure

[66] "The IT Security Situation in Germany in 2007" (D-05 BSI 2007), equally in 2009 and 2011; the 2014 edition is called "The State of IT Security in Germany 2014" (D-12 BSI 2014), equally in 2015.

(D-29 BBK 2016:9; D-11 BSI 2013:5), or cyber attacks in the context of conflicts and war (D-58 BMVg 2016:37; D-50 AA 2014:1). BMI underlines the potential damages following cyber attacks, notably "a considerable negative impact on the performance of technology, businesses and the administration and hence on Germany's social lifelines" (D-03 BMI 2011:2). It is thus not surprising that the first cyber strategy states that cyberspace and IT security "have become vital questions of the 21st century" (ibid.).

I again sort the cyber risks into three groups: cybersecurity-related risks for critical infrastructure, cyber risks within the military context, and cybercrime risks. As in the section on the United States, I address the following aspects in the discussion of each group: contents, evaluation, time frame evolution, and speakers.

4.1.2.1.2 Cyber Risks for Critical Infrastructure

Contents and evaluation. Already in BMI's implementation plan for the protection of critical infrastructure (UP KRITIS) from 2007, "IT dangers" (D-01 BMI 2007:8, own translation) are listed as potential risks – in addition to terrorist threats and environmental dangers (ibid.). It is stated that a so-called "IT crisis" (ibid.:28, own translation) can trigger severe disruptions of supply and significant problems for public safety (ibid.). Therefore, the protection of critical infrastructure is considered an "important national mission" (ibid.:4, own translation) as "domestic security is increasingly influenced by IT security" (ibid.:4, own translation). In the *National Strategy for Critical Infrastructure Protection* (CIP Strategy) from 2009, the risk priorities are mentioned in a similar way. After discussing dangers emanating from terrorism and natural events, BMI states: "Of similar importance are the risks and threats to information infrastructure. Criminal acts, technical failure and/or human error or organizational shortcomings jeopardize the operability of this infrastructure since it is of vital importance to modern societies and their operational processes and its disruption or failure may, due to the existing interdependencies, have far-reaching consequences" (D-02 BMI 2009:10). So, BMI mentions different elements that can endanger the functioning of critical information infrastructure as well as its essential necessity for society.

A very prominent example discussed in the German discourse is the *Stuxnet*[67] case, a very advanced targeted attack on industrial control systems that occurred in 2010. Actors communicate it as wake-up call as it demonstrates a new level of attack sophistication that had existed only theoretically before the attack: The relevance of Stuxnet "lies in the fact that it clearly demonstrates the potential of attacks of this quality. It proves that there are people out there who will spare neither expense nor effort to attack what they perceive to be key targets and sabotage them unnoticed" (D-09 BSI 2011:16). Moreover, BSI admits that now, a new assessment of this kind of risk, which was previously classified as "residual" (ibid.), is necessary: "Whereas attacks on critical infrastructure and their process control systems have often been accepted as a residual risk in the past because of their presumed unlikelihood, this risk now has to be reevaluated" (ibid.). So, Stuxnet proves the actual vulnerability of critical infrastructure to cyber attacks in the eyes of discourse participants. A broad range of discourse participants comments on Stuxnet: BSI discusses it in various publications (see for example D-16 BSI 2016:3; D-11 BSI 2013:50–51; D-10 BSI 2011:31); BMI mentions it in the first cyber strategy (D-03 BMI 2011:3); the Federal Office of Civil Protection and Disaster Assistance (BBK) calls Stuxnet a "turning point in the perception" because of its destructive potential (D-29 BBK 2016:5, own translation). The Federal Ministry of Defence (BMVg) mentions Stuxnet as an example that highly sophisticated attacks are real (D-59 BMVg 2016:4).

Apart from highly sophisticated cyber attacks, BSI points out that "non-targeted attacks and rogue threats from stray malware are posing a growing risk" (D-10 BSI 2011:32). The worm *Conficker* is mentioned as example because of its disruptive capabilities (ibid.). Another example is a case of ransomware used in a cyber attack on a hospital[68] (D-14 BSI 2015:23,44). Towards the end of the examined period, BSI and the Federal Office for the Protection of the Constitution (BfV) highlight the risk of cyber sabotage. According to BSI,

[67] More details on Stuxnet: "It is a highly complex and thus development-costly piece of malware that targets industrial process control systems. As expert analyses have revealed, Stuxnet is programmed to sabotage a particular facility cofiguration [sic, K.U.] in a highly sophisticated and subtle way. It uses IT resources to target a specific process control technology and manipulates the processes by monitoring certain variables and changing control commands without the system operator noticing. A successful attack could render the product being processed unusable or even destroy the production systems" (D-10 BSI 2011:31).

[68] Details on the attack: "Criminals infect computers and encrypt data stored on them using the malicious Cryptowall (ransomware/cryptoware) software. The attackers then extort ransom money from the victim; when this ransom money is paid, the encryption is meant to be reversed. In April 2015, a system in a consortium of hospitals was affected by ransomware, which encrypted health data as well as medical reports and accounts" (D-14 BSI 2015:23).

"[t]hreats due to cyber-sabotage or terrorism are (…) distinct for critical infrastructures as the attackers' goal is disruption to availability or societal damage that is as great as possible" (D-14 BSI 2015:44). BSI qualifies the risk situation as "concerning" (ibid.) given the attack on the French television station TV5MONDE[69] in April 2015, which is evaluated as "example of successful cyber-sabotage" (ibid.). As to Germany, BfV communicates in 2014 that there is no immediate danger for cyber-sabotage (D-39 BfV 2014:23) – a statement that is not repeated in later communications. But even without an immediate danger, BfV emphasizes the "extraordinary potential of damage" (D-39 BfV 2014:23, own translation) of cyber sabotage and points out that "utmost vigilance and precaution" (ibid., own translation) is the order of the day. In 2015 and 2016, BfV mentions the possibility of electronic attacks on critical infrastructures that are unnoticed for years and then activated at a later point in time with the goal of disruption or destruction: The agency compares such attacks to a "silently ticking time bomb" (D-43 BfV 2016:248, own translation; D-42 BfV 2015:142–143).
In general, discourse participants characterize cyber attacks on critical infrastructure as "a reality" (D-58 BMVg 2016:37) and expect that the risk is growing (D-29 BBK 2016:9). Moreover, BSI underlines that companies – including owners and operators of critical infrastructure – are not adequately prepared for cyber risks (D-14 BSI 2015:44). Another problem is the fact that it is difficult or even impossible to realize hard- and software patches in numerous critical infrastructures (ibid.). Finally, the trend "Bring Your Own Device" strongly increases the risk for critical infrastructure according to BSI (ibid.).

Time frame evolution. In general, the protection of critical infrastructure and critical information infrastructure has been a topic in Germany for a long time. For example, the government published a *National Plan for Information Infrastructure Protection* (NPSI) (Bundesministerium des Innern 2005) in 2005, i.e. before the period considered in this study. The above-mentioned *CIP Implementation Plan* (UP KRITIS)[70] and *CIP Strategy* followed in 2007 and 2009 (D-01 BMI 2007, D-02 BMI 2009). Also, BSI already warned in 2007 against

[69] Details on the attack: "The French television broadcaster TV5MONDE became the victim of a massive cyber-attack in April 2015. The perpetrators sabotaged essential production and broadcast servers so that, for several hours, it was not possible to broadcast television programs. In parallel, the broadcaster's Twitter, Facebook and YouTube accounts were also taken over and misused to distribute propaganda messages" (D-14 BSI 2015:43).
[70] Complete title: *CIP Implementation Plan of the National Plan for Information Infrastructure Protection* (own translation of "Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen", D-01 BMI 2007).

the insecurity of SCADA (Supervisory Control and Data Acquisition) systems that are also used in critical infrastructure by emphasizing that "the risk potential is high" (D-05 BSI 2007:38). However, the overall communication on cyber risks for critical infrastructure was rather limited in the discourse – until Stuxnet happened in 2010 and "impressively demonstrated the real threat" (D-09 BSI 2011:16) according to BSI. Indeed, Stuxnet turns out to be a striking event in the context of the German discourse as was shown above. In consequence, the vulnerability of critical infrastructure, cyber attacks and their impact are much more prominent and discussed by a wide range of discourse participants (see for example D-58 BMVg 2016:37; D-51 AA 2015:1; D-45 AA 2013:2).

Speakers. It could be seen from the examples above that BMI and BSI are the leading actors in the German discourse regarding detailed communications on cyber risks for critical infrastructure. In the wake of Stuxnet, a broad range of actors takes up the topic in their respective communications. However, it is interesting to shed light on the Federal Office of Civil Protection and Disaster Assistance (BBK), as it has got special expertise and responsibility in the field of critical infrastructure. Therefore, one could expect that it would champion an early discourse on cyber risks. However, this is not the case. A special publication on critical infrastructure from 2010 (D-19 BBK 2010) does not explicitly consider cyber risks. The annual report of 2011 is the first to mention cyber risks at all and only very briefly states that "[i]n the foreseeable future we will have to concern ourselves with new technology" (D-22 BBK 2011:15) and "deal with threats which come from it" (ibid.). In another special publication, this time on cybersecurity, published in 2011, BBK admits that cyber risks should now be a top priority within the field of civil protection after having focused on physical risks in the past (D-21 BBK 2011:preface). Thus, BBK did not pioneer the topic, but only turned its attention to in the wake of Stuxnet and the first cybersecurity strategy from 2011 – as did the broad majority of the German government discourse. In subsequent BBK annual reports, cyber risks are mentioned, although not in a very detailed manner. It is only towards the end of the examined period, that BBK fully embraces the topic, which can be seen in special publications on critical infrastructure – including the cyber dimension – from 2014 (D-26 BBK 2014) and on cybersecurity from 2016 (D-29 BBK 2016). As can be read in the 2016 publication: "Meanwhile, the topic of cybersecurity,

specifically of critical infrastructure, has arrived in the domain of civil protection" (D-29 BBK 2016:5, own translation).

4.1.2.1.3 Cyber Risks within the Military Context

Contents and evaluation. Discourse participants in the German government discourse acknowledge the existence of cyber risks within the military context. State Secretary Ederer from the Federal Foreign Office (AA) qualifies cyberspace as "a potential new theatre of distrust and conflict" (D-50 AA 2014:1). In general, the risk situation is evaluated as unsettling as attacks can threaten international security (D-58 BMVg 2016:62; D-51 AA 2015:2). They also can lead to the "destabilization" (D-54 BMVg 2011:9, own translation) of Germany including "serious implications for national security" (ibid., own translation). The BMVg states in 2013 that activities in cyberspace will increasingly be part of military action (D-55 BMVg 2013:4). Norbert Riedel, then-special commissioner for cyber foreign policy, points out the delicate issue that cyber programs established by military actors "may sometimes include offensive aspects" (D-51 AA 2015:1). Thus, such programs can be construed as "offensive armament" (D-55 BMVg 2013:26, own translation). Regarding the situation of the German armed forces, BMVg articulates the risk of using commercial IT products, which is the case for the most part of the IT system of the armed forces (ibid.:10–11). Even in the case of critical applications, standard products are used (ibid.:9). The cyber incidents *Flame* and *Conficker* illustrate the vulnerability of BMVg and the armed forces (ibid.:9,11).

I find two major reasonings in the discourse on military cyber risks: On the one hand, actors worry about the development of military cyber capabilities given that "traditional political-military strategies are difficult to adjust to the cyber-space" (D-50 AA 2014:1) and because of the potential of escalation (D-50 AA 2014:2; D-44 AA 2011:2). Discourse participants mention several characteristics of cyberspace leading to this situation: cyber capabilities are advantageous for the offender (D-50 AA 2014:1) leading to a "new conundrum of offense and defense – or should I say lack of defense in the cyber space" (D-50 AA 2014:2); the impact of an attack can be enormous and be prepared with comparatively little effort (D-44 AA 2011:2); this impact "can cross domains and create real damage in the physical world" (D-51 AA 2015:1) as could be seen in the wake of the Sony attack (ibid.); the proliferation of attack tools is comparatively easy (D-59 BMVg 2016:3); the attribution of the attacker is highly difficult or even impossible (D-51 AA 2015:1; D-50 AA 2014:1; D-44 AA 2011:2); and

moreover, traditional deterrence strategies as used in the Cold War do not work (D-58 BMVg 2016:37; D-51 AA 2015:2). These attributes can provoke "serious misunderstandings or escalations" (D-44 AA 2011:2): Indeed, "cyber incidents can escalate into 'real-life' conflict or even war" (D-50 AA 2014:1) in the view of discourse participants.

On the other hand, I find a certain appeasing stance in the discourse in the sense that actors attach importance to the position that "an all-out 'cyber war' seems unlikely at present" (D-51 AA 2015:1). According to Rolf Nikel (AA), Leon Panetta's scenario of a cyber Pearl Harbor might be a little exaggerated; "strictly speaking, there was no cyber warfare between states so far. Stuxnet did not claim lives" (D-45 AA 2013:2, own translation). However, he also points out that this does not mean to play down the very worrying scenario of an attack on critical infrastructure (ibid.). It is important to note that German government actors criticize the term "cyber war" as "inadequate and misleading" (D-51 AA 2015:1) as it "implies an extensive, existential threat to a state solely through targeted attacks by other states on computer systems and IT networks, or through other actions in cyberspace. This seems unrealistic for the foreseeable future" (ibid.; similarly D-55 BMVg 2013:7). Overall, discourse participants expect a combination of cyber and traditional elements in warfare (D-51 AA 2015:1; D-55 BMVg 2013:4,7) and this combination can "pose a substantial threat" (D-51 AA 2015:1). This is all the more so as the easy availability of cyber means allows a diverse set of actors, including criminals and terrorists, the use of such means (ibid.). According to BMVg, cyber means and their special characteristics are already integrated in military thinking: Especially "the possibility to deny cyber attacks in the aftermath is already part of today's strategic calculation of a new, computer-based confrontation between states" (D-54 BMVg 2011:9, own translation). This results in situations of "serious asymmetric threats" (ibid., own translation). Another element making cyber attacks attractive for adversaries is the fact that cyber attacks may blur the lines between war and peace, as explained by BMVg: "The potential anonymity of attacks (…) and the cost-effective possibilities for asymmetric impact have made cyber attacks (…) an effective means – frequently, in order to achieve goals below the threshold of a military attack" (D-59 BMVg 2016:1, own translation). Finally, the risk of IT-enabled disinformation is briefly mentioned in 2011 (ibid.:8). Towards the end of the examined period, BMVg communicates on manipulative cyber activities in the context of

so-called "hybrid warfare"[71]: "A special challenge for open and pluralistic societies is 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" (D-58 BMVg 2016:37).

Time frame evolution and speakers. With regard to the German government, AA and BMVg are the most relevant discourse participants communicating on cyber risks within the military context. They both issue a communication including cyber aspects in 2011. However, these remarks are rather general and contain a certain hestitant stance. For example, Minister of State Werner Hoyer (AA) assesses in 2011 that "so far, the cyber threat in its new quality is not yet fully understood" (D-44 AA 2011:1, own translation). It is interesting to note that only from 2013 onwards, both AA and BMVg publish substantial in-depth communications on cyber risks. That means both discourse participants turn their attention to the topic of cyber risks at a rather late point in time.

4.1.2.1.4 Cybercrime Risks

Contents and evaluation. According to the Federal Criminal Police Office (BKA), the term cybercrime describes "crimes that are directed against the Internet, data networks, IT systems or the data within them (cybercrime in the narrow sense) or that are committed using IT" (D-36 BKA 2016:5, own translation). BSI points out the strong financial motivation behind cybercriminal activities (D-12 BSI 2014:23). The agency distinguishes between organized cybercrime, that means groups acting extremely professional and using a wide range of methods, and less advanced individual cybercriminals (ibid.). There are various forms of cybercrime mentioned in the discourse such as the "theft of digital identities and identity misuse" (D-36 BKA 2016:12, own translation), digital extortion, economic espionage, or IP theft (D-35 BKA 2015:13). From the BKA's point of view, identity theft in the context of online banking and extortion using so-called "ransomware" are the most important crimes (D-35 BKA 2015:7; D-33 BKA 2013:8). The Federal Office for the Protection of the

[71] More details on hybrid warfare: "Hybrid attacks can target all areas of society through cyber attacks and information operations (e.g. propaganda), economic and financial pressure, and attempts at political destabilisation. At the same time, irregular elements, covert special forces, subversion, and regular armed forces can be used. Hybrid warfare can be conducted by state and non-state actors alike. Hybrid tactics blur the boundaries between war and peace and can also constitute a breach of the general ban on the use of force. The roles of aggressor and conflict party are deliberately obscured" (D-58 BMVg 2016:39).

Constitution (BfV) concentrates more on espionage activities in the context of "electronic attacks" (D-37 BfV 2013:378, own translation), the goal of which is to get information, to compromise or even sabotage the targeted system (ibid.). According to the agency, there are targeted electronic attacks on political and economic actors since 2005, frequently in the context of high-level meetings (D-41 BfV 2014:312). Espionage activities in Germany notably target the areas research, armament, automotive industry, and air and space, and can lead to massive losses of IP (D-38 BfV 2014:23).

As to the evaluation of cybercrime, BSI strongly underlines the pervasiveness of the risk in the sense that every user can become a victim (D-12 BSI 2014:23). The agency also quotes a study saying that "cybercriminals are the attacker group that will pose the greatest threat over the coming years" (ibid.:24). BKA repeatedly states that the risk potential is high (D-33 BKA 2013:8; D-32 BKA 2012:18; D-31 BKA 2011:14). Moreover, the agency regularly forecasts that the threats will continue to rise (D-35 BKA 2015:12; D-34 BKA 2014:11; D-32 BKA 2012:18). A decisive factor for this development is the increase in attack opportunities, for example due to the rapid spread of mobile devices (D-35 BKA 2015:12; D-31 BKA 2011:14). Other technology trends such as the "Internet of Things" (D-35 BKA 2015:13, own translation) or "Bring Your Own Device" (BYOD) (ibid.) additionally facilitate cybercrime: More and more intelligent devices and applications are used, for example smart homes or smart cars, but many are insufficiently protected (ibid.). In a similar vein, often poorly protected private devices are used in the workplace (BYOD), which can endanger the security of corporate data and facilitate economic espionage or IP theft (ibid.). Another important observation articulated by BKA is the attackers' strong ability to adapt (D-34 BKA 2014:10; D-31 BKA 2011:14). This leads to a kind of technological race between users of IT applications and cybercriminals as can be seen in the case of phishing attacks in the context of online banking: A new security mechanism called "iTan" introduced in 2008 led to a decline in attacks; however, after a certain time, the criminals had adapted to it and found new ways to attack online bank accounts – in 2011, the number of attacks had tripled (D-31 BKA 2011:14). BKA reports a similar sequence of decline and increase of attacks for the years between 2012 and 2014 (D-36 BKA 2016:13). Furthermore, the structure of the cybercrime sector gets more and more professional: Various tools for committing cybercriminal acts, such as malware, stolen identities or cybercrime services, are offered online in what is called "underground economy" (D-35 BKA 2015:10; D-31 BKA 2011:7). This development greatly

extends the circle of potential cybercriminals to persons without specific IT knowledge (D-35 BKA 2015:14). The underground economy even includes a kind of (illegal) user support providing, for instance, malware updates, infections on demand, and mechanisms for more anonymity (ibid., 6). Overall, BKA observes an "increasing shift of crimes from the analogous into the digital world" (ibid.:10, own translation).

Finally, it is important to note that BKA admits that is hard to comprehensively describe and evaluate cybercrime notably due to the assumed high number of unreported crime (D-36 BKA 2016:19; D-31 BKA 2011:7,14). Crimes may not be reported intentionally, for example in order to protect the image of a company, or involuntarily because they are not detected by the victims (D-31 BKA 2011:7). Similarly, BfV assumes a high number of unreported electronic attacks notably due to the increasingly sophisticated and thus even more effective attacks (D-38 BfV 2014:19). Also, investigation is often difficult as cybercrime is international and attackers can easily conceal their identities (D-38 BfV 2014:15; D-33 BKA 2013:8). BfV adds the comparatively low cost of electronic attacks, the speed, and the high probability of success (D-38 BfV 2014:15). Concluding, BKA clearly communicates the growing importance of cybercrime in the police work (D-34 BKA 2014:11).

Time frame evolution and speakers. Due to the broad range of cybercriminal activities, basically all speakers mention the topic at some point. However, BKA and BfV are the most relevant speakers in the German discourse as they work and communicate on it in detail. Regarding the time frame, the discourse is quite homogenous and several key elements are communicated throughout all of the examined period: the high and increasing risk potential; the increasingly professional cybercrime sector and the strong ability of cybercriminals to adapt and innovate; the increasing opportunities for cybercriminal attacks created in the process of growing digitalization.

4.1.2.2 Drivers and Actors Creating Cybersecurity Risks

In the following section, I elaborate on the drivers and actors creating cybersecurity risks as stated by the German discourse participants. As to the *drivers*, I find dependence and connectivity, technology as enabler, and "digital carelessness" (D-12 BSI 2014:12). As to the *actors*, I find rather general remarks on general actor groups, on the one hand. On the other

hand, intelligence agencies play a major role in the German discourse and so, the last sub-section is devoted to this specific group of actors.

4.1.2.2.1 Dependence and Connectivity

German discourse participants articulate dependence and connectivity as important drivers of cyber risks. BMI notes in its CIP strategy the general high vulnerability of modern societies: "[S]ocieties using highly industrialized, very complex technologies and relying on specialized, sophisticated organizational structures are particularly vulnerable as a result" (D-02 BMI 2009:10). The notion of dependence and the resulting vulnerability is illustrated in the discourse with associations from the human body: Infrastructure, above all, critical infrastructure is seen as "the lifeblood of modern, efficient societies" (D-02 BMI 2009:3); digital infrastructure is compared to "the nervous system of modern societies" (D-45 AA 2013:5, own translation). More with a focus on the pervasiveness of IT and connectivity, BSI states in 2011: "As IT penetrates into all areas of our lives and networks become ever more interconnected, we depend on it operating flawlessly" (D-09 BSI 2011:22). A consequence is that there are "new hazards arising in parallel to this development, such as cyber attacks, attacks on mobile devices and attacks extending beyond conventional IT" (ibid.).

Connectivity basically means two things in the eyes of discourse participants: On the one hand the fact that infrastructures are more and more connected to each other, thus interdependent (D-21 BBK 2011:5); this includes transnational connections, for example of power and gas infrastructures (D-23 BBK 2012:93; D-19 BBK 2010:11). On the other hand, connectivity means the high degree of IT integrated in infrastructures, for example by using SCADA (Supervisory Control and Data Acquisition) systems in water supply or IT-controlled processes in diverse areas ranging from finance to intensive care units in hospitals, and their connection to the Internet (D-12 BSI 2014:7; D-21 BBK 2011:5). The latter leads to "new avenues of attack" (D-51 AA 2015:1). The growing connectivity of critical infrastructure is a risk notably due to the "increasing complexity of networks themselves and the use of standard software and standard protocols for networking" (D-14 BSI 2015:44).

BSI points out that incidents compromising the IT of critical infrastructure can limit or even disrupt normal operation (D-14 BSI 2015:42). The agency adds that "[d]ependencies between individual sectors or industries increase the risk of failures even further. Failures in one sector may lead to failures in other sectors, triggering a domino effect" (ibid.). For

example, such an effect could be triggered by a failure of power supply, which is described as especially critical by Norbert Riedel, then-special commissioner for cyber foreign policy: "One might think of a virus disrupting a country's power supply, which could have tremendous physical consequences in any advanced industrial society, both for the military and the society in general" (D-51 AA 2015:1; similarly D-14 BSI 2015:45).

Apart from critical infrastructure, private sector companies and the military are equally affected by dependence and connectivity. As BKA underlines, companies depend more and more on IT as diverse production, logistical and other processes are increasingly IT-controlled, interconnected and thus vulnerable (D-35 BKA 2015:13). Well-functioning IT is also a pre-condition for Germany's international economic activities (D-58 BMVg 2016:22). Regarding the situation of the military, BMVg states: "The increasingly connected military platforms and weapon systems rely on the unrestricted use of information and communication systems. Moreover, in the context of the armed forces' operation planning and accomplishment, the secure and timely availability of information is indispensable for military decision-making and issuing orders" (D-55 BMVg 2013:4, own translation).

Discourse participants outline several worst-case consequences of cyber risks given the IT dependence and connectivity: a complete paralysis of production and supply (D-29 BBK 2016:9); major economic losses (D-35 BKA 2015:13), the "destabilitzation" (D-54 BMVg 2011:9, own translation) of the country; serious conflicts in the physical world or, in the worst case, war (D-50 AA 2014:1). However, BSI also acknowledges that is very hard to forecast the vulnerability of a particular sector or possible effects of cyber risks (D-14 BSI 2015:45). In general, a sceptic comment summarizes that "[i]t would be naïve to assume that newly created digitally interconnected technologies will not also be exploited in the furtherance of disputes in economic, social and political arenas" (D-12 BSI 2014:4).

Finally, it has to be noted that dependence and connectivity are a continuous topic in the German discourse. BSI already notes in 2007 that "[t]he elevated dependence on modern communications technology in professional and private spheres automatically results in an increase in IT risks" (D-05 BSI 2007:5). In 2016, the overall assessment is still the same: BMI notes that digitalization increases a society's "vulnerability and the potential of misuse in cyberspace" (D-04 BMI 2016:7, own translation). The discursive continuity holds also true for the driver connectivity (see for example D-59 BMVg 2016:3; D-12 BSI 2014:7; D-01 BMI 2007:5). Moreover, discourse participants communicate their point of view that dependence

and connectivity are not about to disappear in the near future. To the contrary, BBK notes that dependence on infrastructure steadily increases (D-19 BBK 2010:7; see also D-58 BMVg 2016:22) and BSI forecasts that connectivity, above all in the context of critical infrastructure, "will remain a significant challenge beyond 2015" (D-14 BSI 2015:48). Growing dependence and connectivity also increase the "risk of unforeseeable cascade effects" (D-19 BBK 2010:7, own translation). As could be seen by the quotations used in this sub-section, basically all participants in the German executive discourse comment on dependence and connectivity as drivers of cyber risks (for a further example from the military see D-58 BMVg 2016:28; for an example of the BMWi see D-62 BMWi 2015:24).

4.1.2.2.2 Technology as an Enabler

The second driver occurring in the German discourse is technology as an enabler of cyber risks. Discussing the pervasiveness of IT, BfV states: "This development opened up new opportunities for espionage and sabotage" (D-40 BfV 2014:6, own translation). Many of the technological characteristics that facilitate cyber risks have already been mentioned in previous sub-sections. Therefore, they are only briefly summarized here. The most important characteristics, as articulated in the discourse, are the following: the difficulty of attributing the origin of cyber attacks; the advantageous situation for the offense compared to the difficult defense of cyber attacks; the lack of effective deterrence strategies; the relatively low cost and low level of technical skills needed to launch attacks; and the potentially enormous impact resulting from a cyber attack (see above sections 4.1.2.1.3 and 4.1.2.1.4).

Moreover, technology is communicated as enabler of cyber risks in another, more fundamental way: the lacking prioritization of security in the design of technology. On the one hand, BSI points to the imbalance in the design of the Internet that strongly prioritizes availability over integrity and confidentiality (D-13 BSI 2014:5). Its design was appropriate for the very small number of persons using the Internet at the beginning (ibid.). BSI explains: "The internet was mainly planned in terms of high availability. (…) Avoiding the use of cryptography has meant that data confidentiality and integrity continue to be insufficiently guarded. These design flaws are the reason for some of the most significant challenges to modern society and provide the methodological approach for many cyber attacks" (ibid.).

On the other hand, BSI criticizes that people – providers as well as users of IT – do not attach the same importance to IT security as they attach to functionality and commercial aspects (D-14 BSI 2015:6). Market pressure calls for quick, innovative and functional IT solutions – otherwise a provider may disappear from the market – whereas the demand for IT security is comparatively low (ibid.). As a consequence, from BSI's point of view, "the necessary level of security is not produced" (ibid.), which facilitates cyber attacks. BSI outlines some conflicts of goals, in which security loses ground against other aspects (ibid.:6–7). For example, there is the trend of "software-defined everything" (ibid.:6), which means highly dynamic and cost-efficient IT configurations based on software instead of hardware. However, this contradicts traditional ways of architecture, in which the "basic requirement of information security based on the separation of key processes and systems" (ibid.) is respected. The effectiveness of separation in a purely virtual environment is much lower than in conventional configurations (ibid.). Another conflict of goals is the strong increase in the use of mobile computing, which brings up difficult questions such as the protection of critical data of companies and secure ways of access when using mobile computing devices (ibid., 7).

The statement of the lacking prioritization of security in the design of technology is mainly found in more recent BSI communications. However, BMWi equally criticizes that IT security aspects are often left out during the design process and only integrated afterwards (D-62 BMWi 2015:24); "moreover, security risks of recent technology applications are not sufficiently taken into account" (ibid., own translation). Finally, already in 2010, BBK pointed to the effects of liberalization and privatization in areas of critical infrastructure: In a market-driven environment aiming at reducing costs, owners and operators increasingly evaluate investments in security from an economic perspective (D-19 BBK 2010:7).

4.1.2.2.3 "Digital carelessness"

A third driver of cyber risks I identify in the disourse regards the users themselves and their behavior: Following BSI, I call it "digital carelessness" (D-12 BSI 2014:12). Already in 2007, BSI states that "[u]nfortunately, the level of awareness of the importance of IT security among the various social groups is still far from adequate" (D-05 BSI 2007:11). For example, a user's computer can become a part of a botnet, unnoticed by the user, and thus be a risk for others (ibid.:7). Another challenge is seen in employees compromising a company's cybersecurity

"as a result of thoughtless behavior" (ibid.:8), for instance by not being careful when working with critical data or using private devices on company networks (D-05 BSI 2007:29–30). Later on, this trend is called "Bring Your Own Device" (BYOD) (D-14 BSI 2015:44; see also above section 4.1.2.1.4). Moreover, BSI criticizes in 2007 that regularly, the management level of companies shows a certain lack of interest in cybersecurity (D-05 BSI 2007:14) because cyber risks are considered as rather unlikely and seen "more as a technical problem" (ibid.). BSI quotes a study saying, "the human factor – i.e. the errors and negligence of the company's own employees – constitutes the greatest risk to IT security within a company" (D-05 BSI 2007:15). Similar observations are made in 2009, with a special emphasis on "the careless handling of data in the interactive Web 2.0 applications" (D-07 BSI 2009:5), above all social networks. In 2014, BSI notes that even the Snowden revelations did not have a major impact on actual user behavior, even if there was a clear decline in confidence in IT (D-12 BSI 2014:12). BSI states that existing protective measures "frequently do not meet user requirements in terms of convenience, intuitiveness and ease of operation" (ibid.).

The presented driver occurs on a regular basis throughout the examined discourse period and is almost exclusively articulated by BSI (for an example of the BKA see D-35 BKA 2015:12). However, it is interesting to note that in 2016, the topic enters BMI's second cyber strategy, thus a high-level strategic document: The strategy presents a measure called "Countering digital carelessness" (D-04 BMI 2016:14, own translation).

4.1.2.2.4 General Actor Groups

Who is responsible for cyber risks in the eyes of German discourse participants? As to the actors behind cyber risks, I find that the German discourse mainly concentrates on general actor groups, supplemented by rather few remarks on specific actors.

The typologies of actors used in the German discourse vary slightly. BSI, for example, distinguishes between "criminals, intelligence agencies and hacktivists, while malicious insiders [are, K.U.] forming a special category" (D-12 BSI 2014:23). The 2016 cyber strategy states: "Attackers frequently have a criminal, extremist/terrorist, military or intelligence service background" (D-04 BMI 2016:7, own translation). As attackers can act quite anonymously, it is especially hard to detect attacks and find out the attacker's background (D-04 BMI 2016:7; D-21 BBK 2011:2). As a result, it is hard to decide on how to appropriately

react to it (D-04 BMI 2016:7). The motivations of the different types of attackers mentioned include “financial interests, information procurement, sabotage, gaining of influence or the pursuit of political interests” (D-12 BSI 2014:23).

A continuous and very prominent observation in the discourse is the high sophistication of attackers and their professional behavior: Already in an early communication from 2007, BSI notes that “[t]he individual computer hackers who were spurred by ‘sporting’ ambition have almost all been replaced by professional criminals” (D-05 BSI 2007:7). In 2009, BSI describes that “attackers increasingly demonstrate psychological finesse” (D-07 BSI 2009:5), for example by using social engineering. In 2011, in the wake of Stuxnet, the agency reports “a new quality of specifically targeted attack” (D-09 BSI 2011:4), which is possible using zero-day-exploits; in 2015, the agency again states “an increasing professionalisation of the attackers, regardless whether they are attacking the state, businesses, the scientific community, or citizens and society” (D-14 BSI 2015:48).

Discourse participants communicate on several actor groups in the discourse: Other than cybercriminals that have been described above (see above section 4.1.2.1.4), participants briefly mention malicious insiders “who intentionally damage the company for reasons of revenge, envy or personal gain” (D-05 BSI 2007:30; see also D-12 BSI 2014:25) and hacktivists such as Anonymous using “computer systems and networks as a means of protest and in the furtherance of political or ideological objectives” (D-12 BSI 2014:24). Moreover, terrorists and extremists are discussed. Their use of cyberspace is mostly aimed at purposes of propaganda, coordinating activities, radicalization, and recruitment in the eyes of discourse participants (D-51 AA 2015:8; D-41 BfV 2014:59; D-54 BMVg 2011:8). BMVg underlines the “considerable intrinsic motivation” (D-55 BMVg 2013:12, own translation) these actors have got – in contrast to their limited technical capabilities (ibid.). Referring to these capabilities, BfV explains in 2014, that extremists are able to conduct so-called “low level actions” (D-41 BfV 2014:58, own translation) such as defacements of websites. However, the Federal Foreign Office is worried about a new type of attack in 2015: “The hacking attack on TV5 Monde in France this past April demonstrated that terrorists can use the internet as an attack tool. Not just a television station or a movie production firm can be targeted. Critical assets, systems and infrastructure become vulnerable when they are connected to the internet” (D-51 AA 2015:1). So, discourse participants state a rising threat level originating from this actor group.

4.1.2.2.5 Intelligence Agencies as Actors

The majority of comments on specific actors in the German discourse is centered on intelligence agencies. In 2014, BSI points out that it detected "strong and unambiguous evidence of cyber attacks by intelligence agencies against German infrastructure in the business, research and public administration spheres" (D-12 BSI 2014:22). The agency further states that intelligence agencies mainly conduct espionage activities targeting military and business information; sabotage can be another goal (D-12 BSI 2014:24). They are primarily interested in "furthering their own national interests or gaining advantages for national businesses on international markets" (ibid.). BSI emphasizes the power of intelligence agencies resulting from the partially enormous resources they have and their great variety of technological approaches and access possibilities including via national providers and manufacturers (ibid.). Moreover, intelligence agencies are in a position to "invest a great deal of money in the search for vulnerabilities to exploit. Given that (…) software packages will inevitably have a certain number of vulnerabilities, new gateways for cyber attacks are always open to them" (ibid.).

More specifically, China, Russia, and Iran are mentioned in communications of the German government as "detected attackers" (D-43 BfV 2016:249, own translation). According to BfV, China is responsible for the great majority of detected electronic attacks against Germany and is notably interested in information from the Federal Foreign Office and German embassies, the Ministry of Finance and the Ministry for Economic Affairs and Energy (D-41 BfV 2014:328). Other targets are private sector companies in the areas of defense and civil technology and engineering (ibid.). Regarding Russia, BfV describes that "all agencies are legally obliged to conduct economic espionage" (D-40 BfV 2014:8, own translation). The case of a large-scale cyber espionage attack called "Red October" that was active for several years was of special interest:[72] In Germany, the attack targeted information on Eastern Europe from federal ministries and German embassies (D-41 BfV 2014:322). For BfV, this case illustrated that the threat of cyber operations from Russia is real (ibid.). A third specific country mentioned in the discourse is Iran: In 2015, for the first time, Iranian attacks of espionage targeting science and research could be detected (D-43 BfV 2016:249,253).

[72] For more information see: https://www.heise.de/security/meldung/Kaspersky-gibt-weitere-Details-zu-Roter-Oktober-heraus-1786887.html (accessed July 27, 2019).

Regarding western intelligence agencies and especially the NSA, I find rather technical and cautious comments by BSI and BfV (see for example D-12 BSI 2014:22, D-40 BfV 2014:13). BSI could identify four attack vectors: the collection and analysis of large amounts of communication data; targeted attacks and surveillance of selected individuals or institutions; the manipulation of IT security mechanisms such as cryptography; and the manipulation of hardware, for example by integrating backdoors in IT equipment (ibid.). Michael Hange, President of the BSI from 2009 to 2015, also outlined the problem that cybercriminals could use the information revealed for own attacks (D-15 BSI 2015:41).

4.1.2.3 Evaluation of Cybersecurity Risks

The overall evaluation is that discourse participants worry about cyber risks, which is a permanent finding throughout all of the examined period. For example, in 2009, BSI points out that "the situation remains as critical as ever" (D-07 BSI 2009:4). In 2014, the evaluation is very similar: "The current IT landscape and the multifaceted nature of the security threats of today pose a permanent challenge for users of information technology. (…) In view of the overall attack potential posed by these threats, the state of IT security in Germany may be viewed as critical" (D-12 BSI 2014:25).

In addition, discourse participants regularly communicate an increasing risk (see for example D-04 BMI 2016:7; D-45 AA 2013:3; D-55 BMVg 2013:8; D-05 BSI 2007:5). That does not only concern the number of attacks – for example, in 2011, there were more than twice as many reported cybercrimes as in 2006 (D-55 BMVg 2013:8) – but also the quality (D-04 BMI 2016:7; D-59 BMVg 2016:4). BMVg illustrates the evolving character of cyber risks by stating that "[t]echnological advances – from simple viruses to complex attacks that are difficult to detect (advanced persistent threats) – represent a dramatic change in the nature of the threat situation" (D-58 BMVg 2016:36). The evolving character of attacks can also be seen in BSI's regular reports on cybersecurity: Whereas in 2007, the attention is notably drawn to broadly distributed malware such as worms and Trojan horses (D-05 BSI 2007:21), the top risk affecting government and private sector actors in 2014 is "[t]argeted espionage attacks on businesses, research bodies or the government" (D-12 BSI 2014:26).

Many elements contribute to the presented assessment in the German discourse; most of them have been described in detail in previous sub-sections (see above sections 4.1.2.1 and 4.1.2.2): Among them are the "increasing complexity and vulnerability of information

infrastructures" (D-03 BMI 2011:3); the growing opportunities of attack due to the dependence, connectivity and pervasiveness of IT (see above section 4.1.2.2.1); the "continuous refinement and professionalisation of attackers and attack methods" (D-12 BSI 2014:25); and the technological particularities preventing the detection and prosecution of attackers (see above sections 4.1.2.1.3 and 4.1.2.1.4) – attribution is still characterized as "challenging and technically ambitious" (D-59 BMVg 2016:3, own translation) in 2016. Another element that discourse participants repeatedly observe is the blurring line between domestic and foreign affairs: "There are few areas where internal and external security are as closely intertwined as they are in cyber space" (D-58 BMVg 2016:38; similarly D-04 BMI 2016:27; D-18 BBK 2009:44).

What I would like to add to this evaluation section is the background against which the assessment in the German discourse is made, that is the overall communication of digitalization as a major transformative process in all areas of society. In its second cyber strategy, BMI states that digitalization "has fundamentally changed Germany in only few years" (D-04 BMI 2016:4, own translation). Discourse participants underline that IT is everywhere (D-07 BSI 2009:5) and that "intelligent systems and objects rule our daily life" (ibid.), which can be seen in cyber-physical systems or the permanent presence and utilization of smartphones (D-12 BSI 2014:8) and cloud services (ibid.:9), for example. In a summarizing fashion, BSI characterizes digitalization as "interconnected, complex, pervasive" (ibid.:7).

On the one hand, there are positive and welcoming comments on this process. For example, Federal Minister of the Interior de Mazière points out that the Internet "has changed how we communicate, process information and perform international business transactions profoundly – and for the better" (D-13 BSI 2014:8). Also, BMVg underlines the importance of seizing "the opportunities of future technologies" (D-59 BMVg 2016:3, own translation) for the benefit of the armed forces. Moreover, many communications of the Federal Foreign Office emphasize that the Internet allows for numerous opportunities "for economic growth and development, for good governance and democracy, as well as for social exchange between people around the world" (D-53 AA 2015:1).

However, on the other hand – and this is a very striking and prominent finding in the German discourse – there are many sceptic and doubting comments on digitalization

expressing doubts, uncertainty, or even fears. As a consequence of the omnipresence of IT, discourse participants observe that "the boundary between the physical and the virtual worlds will become increasingly blurred" (D-12 BSI 2014:9; similarly D-21 BBK 2011:preface) – which increases the relevance of cybersecurity questions (ibid.). As a result of the complexity of IT, the majority of users lacks transparency and understanding of how products and processes work (D-11 BSI 2013:29). Other than the opportunities, discourse participants refer to the "concerns regarding the repercussions [of digitalization, K.U.] on the living and working environment" (D-62 BMWi 2015:3, own translation), to "uncertainties and doubts" (ibid., own translation) and to many fundamental questions such as: "How do we tackle the digital transformation?" (D-63 BMWi 2015:6, own translation). As Federal Foreign Minister Steinmeier puts it: "The perspective of the digital revolution scares many people" (D-49 AA 2014:1 AA, own translation). Therefore, he points out the need and the challenge to find a new orientation in the "uncharted territory" (D-48 AA 2014:3, own translation) of the digital age. Everything is new and there is "no precedent" (ibid., own translation).

4.1.2.4 Solutions: Solving the Problem of Cybersecurity Risks

The section on solutions covers the articulated communications on the following aspects: actors responsible for solving the problem of cyber risks, goals of solutions, and concrete problem-solving measures.

4.1.2.4.1 Discourse on Responsibility

Who is responsible for solving the problem of cyber risks in the eyes of discourse participants? German executive actors notably communicate three aspects: First, they underline the responsibility of the state as problem-solver within the framework of its mandate. Second, they underline the shared responsibility with the private sector. Third, citizens need to do their part in handling cyber risks by acting responsibly.

Regarding the *first* aspect, discourse participants underline the mandate of the state to protect and to guarantee vital services including cybersecurity: "As in the offline world, the government also has a responsibility in the networked world to avert risks and criminality. We acknowledge this responsibility for public IT security and want to play our part in

protecting society and the economy in the digital age" (D-61 BMWi 2014:33). Two points are important in this regard in the eyes of discourse participants.

On the one hand, the protective responsibility of the state can only be successfully fulfilled in a whole-of-government fashion and in cooperation between the federal level and the level of the States (*Länder*) (D-04 BMI 2016:27; D-59 BMVg 2016:5). This is due to the crosscutting character of cybersecurity and the already mentioned blurring line between domestic and foreign affairs (D-04 BMI 2016:5; see also D-58 BMVg 2016:48; D-59 BMVg 2016:4). As pointed out in the cyber strategy from 2016, many agencies from different departments and from the federal as well as *Länder* level have to work together in order to prevent, investigate and defend cyber attacks (D-04 BMI 2016:27). It is a permanent and joint responsibility capitalizing on "synergies across federal structures, departments, agencies, and national borders" (ibid., own translation). However, all participating institutions have to comply with their respective legal mandates (ibid.).

On the other hand, it is important to note *how* the German government wants to fulfill its responsibility. Discourse participants clearly see the expectations of the citizens, their fears and concerns regarding digitalization (see above section 4.1.2.3). Therefore, government actors frequently communicate their intention to "take seriously these concerns" (D-49 AA 2014:1, own translation; similarly D-48 AA 2014:1) and to shape the process of digitalization in an "open and ongoing process that is inclusive of all relevant groups in our society" (D-61 BMWi 2014:2; see also D-62 BMWi 2015:3). As Federal Foreign Minister Steinmeier puts it speaking of the digital revolution: "We (…) have to give this revolution a human face" (D-48 AA 2014:2, own translation).

The *second* aspect highlighted in the discourse regards the shared responsibility of state and private sector. In addition to the "guarantee responsibility" (D-14 BSI 2015:41) of the state, there is the "operational responsibility" (ibid.) of the owners and operators of critical infrastructure. The need for cooperation between the state, the private sector, as well as society has already been advocated in the *National Plan for Information Infrastructure Protection* (NPSI) from 2005 (Bundesministerium des Innern 2005:7). It is thus a long-standing approach in the area of cybersecurity, but also the domain of critical infrastructure in general (D-02 BMI 2009:3; D-01 BMI 2007:4). The need for cooperation results from the afore-mentioned mandate of the state as well as the ownership structure in the area of

critical infrastructure (D-02 BMI 2009:8; see also D-18 BBK 2009:44). Ultimately, "neither the state nor the private sector is able to manage this task alone" (D-11 BSI 2013:20, own translation; similarly ibid.:11).

The shared responsibility is frequently emphasized throughout all of the examined period (see for example D-04 BMI 2016:21; D-14 BSI 2015:45; D-09 BSI 2011:22; D-01 BMI 2007:4). In the CIP strategy from 2009, the "principle of joint action by the state, society, and business and industry" (D-02 BMI 2009:3) is explained as follows: "The state co-operates, on a partnership basis, with other public and private actors in developing analyses and protection concepts. Either – primarily – as a moderator or – if required – by rule-making, the state regulates the measures for safeguarding and securing the overall system and the system procedural flows" (D-02 BMI 2009:3). The cooperation is described as "trusting and constructive" (ibid.) and notably the necessity of trust between the partners is repeatedly communicated in the discourse (D-04 BMI 2016:21; D-16 BSI 2016:19; D-38 BfV 2014:35; D-19 BBK 2010:3; D-02 BMI 2009:12).

Basically, the approach is intended as a voluntary one and, as pointed out by BMWi, guided by the norm that "self-regulation takes precedence over new legislation" (D-60 BMWi 2010:18, own translation). However, in case the voluntary approach does not work or does not achieve appropriate security results, the government "reserves (…) the right, within its jurisdiction, to optimize the protection of the respective infrastructures by amending existing legislation or enacting new legal regulations" (D-02 BMI 2009:15). An example for such a situation is the adoption of the so-called *IT Security Act* (*IT-Sicherheitsgesetz, ITSiG*) in 2015 (see below section 4.1.2.4.4).

Whereas in general, discourse participants evaluate the cooperation between state and private sector as working well (D-14 BSI 2015:41; D-02 BMI 2009:3), they also point out difficulties in collaborating due to different structures and specific ways of decision-making on each side as well as diverging goals – economic considerations, on the one hand, versus security interests, on the other hand (D-26 BBK 2014:2–3).

Finally, regarding the *third* aspect, discourse participants regularly underline the responsibility of society. In the first cyber strategy, the government underlined that the success of the strategy depends on "all players" (D-03 BMI 2011:4). The shared responsibility is repeated in the second cyber strategy (D-04 BMI 2016:9). It is also a constant topic for BSI

that already in 2007 called for the "personal responsibility" (D-05 BSI 2007:63) of users. In a communication of 2015, the agency states: "People are responsible for IT and information security, but are also often the weakest link in the defence chain. Alongside technical and organisational measures, sensitisation, awareness and a healthy degree of mistrust on the part of the user is essential for IT security" (D-14 BSI 2015:14). BMVg calls for more "'cyber hygiene' – that means increased 'cyber awareness' and 'cyber resilience'" (D-59 BMVg 2016:5, own translation) among all groups. The crucial importance of "preventive measures for self-protection" (D-36 BKA 2016:19, own translation) is also advocated by BKA. With regard to critical infrastructure in general, BBK regularly underlines the ability of citizens to help themselves and be prepared (see for example D-19 BBK 2010:preface; D-25 BBK 2013:9–10).

4.1.2.4.2 Discourse on Goals

The goals articulated in the German discourse refer to different components of cybersecurity. The following aspects are of particular importance to German discourse participants.

First of all, there is the goal of cybersecurity following from the mandate of the state "to ensure freedom and security (…) including in cyberspace" (D-04 BMI 2016:8, own translation). Discourse participants also note that "domestic security is increasingly influenced by IT security" (D-01 BMI 2007:4, own translation, similarly D-06 BSI 2008:2). In general, the protection of critical infrastructure constitutes an "important national task" (D-01 BMI 2007:4, own translation). This task "requires (…) an appropriate protection of information infrastructures" (D-01 BMI 2007:5, own translation). So, there is a close link between the protection of critical infrastructure and cybersecurity. In the cybersecurity strategy from 2011, this link is highlighted more clearly: "The protection of critical information infrastructures is the main priority of cyber security. They are a central component of nearly all critical infrastructures and become increasingly important" (D-03 BMI 2011:6). More precisely, three cybersecurity goals are defined in the German discourse at an early point in time: "prevention: appropriately protect information infrastructures; reaction: handle IT security incidents effectively; sustainability: strengthen German IT

security competence – set international standards" (D-01 BMI 2007:6, own translation).[73] The BMVg White Paper from 2016 defines cybersecurity as "the desired IT state in which the risks our country faces from cyber space are reduced to an acceptable and manageable level" (D-58 BMVg 2016:38). As can be seen from these examples, there is continuity in expressing the goal of cybersecurity.

Second, it is interesting to shed light on the way opportunities are communicated in the German discourse. In general, German discourse participants see numerous opportunities provided by digitalization: a digitally enabled economy leading to growth and more efficiency (D-62 BMWi 2015:3; D-63 BMWi 2015:6; D-46 AA 2014:2); innovations for major problems such as climate change (D-60 BMWi 2010:3); jobs (D-64 BMWi 2016:9; D-48 AA 2014:3); participation (D-46 AA 2014:2; D-47 AA 2014:2; D-61 BMWi 2014:2). However, rather than pure optimistism towards digitalization, discourse participants attach great importance to cybersecurity as a pre-condition for using the potential of digitalization, for example by underlining that the "security of information technology is the basis of any form of digitisation" (D-16 BSI 2016:18). In a similar way, the second cyber strategy emphasizes that making cyber risks manageable is the pre-condition for seizing the opportunities of digitalization (D-04 BMI 2016:8; similarly in the first cyber strategy D-03 BMI 2011:4). The following statement more concretely illustrates the major goal of "security, protection and trust within society and the economy" (D-61 BMWi 2014:30) advocated by the German government: "People will not trust new digital services and offerings unless their data is protected and they can operate with maximum security on the Internet. (…) Companies will not trust new business models unless they can be sure that the hardware and software used guarantees the confidentiality of their trade secrets and the integrity and availability of their IT systems" (ibid.:31). Thus, the creation of trust is a major topic in the discourse and mentioned repeatedly throughout the examined period and by different discourse participants (see for example D-04 BMI 2016:4; D-13 BSI 2014:8; D-50 AA 2014:2; D-60 BMWi 2010:18).

[73] These goals have been mentioned for the first time in the *National Plan for Information Infrastructure Protection* (NPSI) in 2005 (Bundesministerium des Innern 2005).

A *third* aspect is closely connected to the previous one and again shows the somewhat sceptic and reserved attitude in the German discourse: The communication of self-determination as high-ranking value (see for example D-61 BMWi 2014:4). That means, an important part of cybersecurity is creating the conditions that citizens "can act in a secure and self-determined way" (D-04 BMI 2016:13, own translation) in the digital age. In a similar way, BMWi defines the goal of "digital sovereignty" (D-63 BMWi 2015:49, own translation): It includes "trustworthy IT" (ibid., own translation), "mastering (…) digital key technologies and competences" (ibid., own translation), and creating an environment that allows for innovation but also helps protecting "our high standards for good work, data sovereignty, and a self-determined life" (ibid., own translation). The second of the three aforementioned elements is closely linked to the debate on how to strengthen "technological sovereignty" (D-11 BSI 2013:11, own translation) in Germany: Already in the first cyber strategy, the government points out that it "will strengthen Germany's technological sovereignty and economic capacity in the entire range of core strategic IT competences" (D-03 BMI 2011:11). With a view on the future development of digitalization, BSI reinforces the necessity of such competences: "Against the backdrop of increasing digitalization, the capability of being able to accurately assess security risks in an autonomous way and to define the necessary security measures by oneself will be decisive" (D-11 BSI 2013:11, own translation). We can summarize the aforementioned observations in a statement of BMWi: "We want digitalization with a sense of proportion" (D-63 BMWi 2015:49, own translation). In this way, a balance between progress and sovereignty shall be found (ibid.).

Finally, the goal of cybersecurity and connected aspects are also valid in the European and international context. German discourse participants regularly emphasize the importance of cybersecurity at the international level (D-55 BMVg 2013:26,33; D-03 BMI 2011:13), the protection of critical infrastructure across national borders (D-02 BMI 2009:18; D-01 BMI 2007:38), and the "continuing development of the global Internet as an open, safe and free space that protects diversity of opinion and the exchange of ideas" (D-61 BMWi 2014:2; similarly D-52 AA 2015:1; D-46 AA 2014:1; D-45 AA 2013:15; D-55 BMVg 2013:12). The government is aware of highly diverging views of other countries in this regard (D-55 BMVg 2013:29). In the first cyber strategy, discourse participants state that "[i]n global cyberspace security can be achieved only through coordinated tools at national and international level"

(D-03 BMI 2011:11). In a similar vein, the government communicates in the second cyber strategy that "close European and international coordination is (…) indispensable" (D-04 BMI:9, own translation), above all in view of transnational challenges like cyber attacks. In order to increase cybersecurity in Germany, discourse participants underline the necessity of European and international action, notably the creation of a "clear legal framework, confidence-building as well as greater resilience in Europe and worldwide" (D-04 BMI 2016:39, own translation).

4.1.2.4.3 Discourse on Measures

In this section, I focus on concrete problem-solving measures regarding cybersecurity risks. I proceed by using the same overall structure as in the section on risks and present solutions in four groups: solutions for cybersecurity risks in general, for cyber risks for critical infrastructure, for cyber risks within the military context as well as solutions for cybercrime risks. It is neither possible nor helpful to exhaustively present all measures taken by the German executive and articulated in the discourse. Rather, I focus on a selection of essential and exemplary measures for each group.

Solutions for cybersecurity risks in general. In general, BBK points out that *protection* of critical infrastructure, notably of IT infrastructure, is not enough; rather, *resilience* is needed, which is "the capability to deal with disruptions of varying extent, that means to withstand them, to resolve them, or to adapt to them" (D-26 BBK 2014:5, own translation). In a similar vein, BSI advocates the "'Assume the Breach' paradigm" (D-14 BSI 2015:49): "[P]revention and detection are no longer sufficient to deal with the current level of threat. Rather than simply defending against attacks, it should be part of an organisation's risk management activities to prepare itself for an IT security incident or a successful cyber-attack" (ibid.). The challenge in information and communication technology (ICT) is that ICT is "not only a hazard, but also (…) an endangered element that has to be protected" (D-29 BBK 2016:19–20, own translation). What measures are taken to tackle this challenge?

An important measure is the creation of a *Computer Emergency Response Team* (CERT) in 1994 (D-11 BSI 2013:14). The team initially works as internal body of BSI and is extended to a federal CERT, the so-called "CERT-Bund", in 2001 – in the wake of the so-called "year 2000

problem" (D-11 BSI 2013:14, own translation)[74] and the virus "I love you" (ibid.). Its main task is to be a "centralized point of contact for preventive and response measures" (D-07 BSI 2009:27), above all for federal IT. It is thus an operative body.

Moreover, the *National Cyber Response Centre* is established in 2011, "partly in response to the attacks on process control systems by the highly specialised Stuxnet malware" (D-16 BSI 2016:29). As defined in the first cyber strategy, the tasks of the center are to "optimize operational cooperation between all state authorities and improve the coordination of protection and response measures for IT incidents" (D-03 BMI 2011:8). The platform involves personnel from the main security-related agencies in Germany: "Staff from the BSI, the Federal Office for the Protection of the Constitution (BfV) and the Federal Office for Civil Protection and Disaster Assistance were recruited; since June 2011, the Federal Criminal Police Office (BKA), the Federal Police, the customs office, the Federal Intelligence Service (BND) and the Bundeswehr have been providing assistance as associated agencies" (D-16 BSI 2016:32). The main purpose of the center consists in continuously monitoring the cybersecurity situation (D-11 BSI 2013:17–18) and sharing information on vulnerabilities and attacks; moreover, it provides assessments and recommendations on cyber risks (D-03 BMI 2011:8). Despite the cooperative character of the platform, discourse participants strongly underline that authorities "participate in this centre within the framework of their statutory tasks and powers" (D-03 BMI 2011:8; see also D-15 BSI 2015:10; D-55 BMVg 2013:13).[75]

The measure of establishing a *National Cyber Security Council* is a measure on the strategic level and taken in the wake of the first cyber strategy (D-03 BMI 2011:9–10). The high-level

[74] The "year 2000 problem" (D-11 BSI 2013:14, own translation) describes the difficult IT situation at the turn of the year 1999/2000: Experts feared major IT disruptions as the date format had to change from two to four digits (ibid.). However, due to the preparations taken, a crisis could be prevented (ibid.).

[75] In more detail, BSI points out: "Special administrative agreements between the participating authorities provide the basis for these cooperative efforts to attain increased IT security. The agreements strictly respect the division of statutory responsibilities and respective powers of all the bodies involved. The principle of legality and the requirement for separation between the intelligence services and the police are particularly important here. Each authority appoints a contact person with individual responsibility as their staff member at the Cyber Response Centre, which is managed by the Federal Office for Information Security representative. The president of the Federal Office for Information Security is the spokesman for the Cyber Response Centre and thus its most senior representative. (...) It should be emphasised that although the participating authorities and institutions work together in close cooperation in the Cyber Response Centre, they carry out all operational tasks within their own remit and according to their individual areas of responsibility. However, their work is aided by the diversity of synergies that result, in particular from the regular transfer of knowledge within the Cyber Response Centre" (D-15 BSI 2015:10–11).

body is composed of the Federal Chancellery and State Secretaries from seven ministries[76], *Länder* officials, and, optionally, members of the academic and business communities (ibid., 9). The purpose of the council is to "coordinate preventive tools and the interdisciplinary cyber security approaches of the public and the private sector" (ibid., 9-10). This measure was aimed at creating visibility (ibid., 9); however, the council itself is not present in the discourse and there are hardly any comments on it. The second cyber strategy reaffirms the council's task as "strategic advisor of the federal government" (D-04 BMI 2016:45, own translation) and defines topics the council shall work on in order to give recommendations (ibid.).

Measures to raise *awareness* and promote *secure and trustworthy IT* represent another important and frequently articulated field of activity. The overall vision as formulated in the *Digital Agenda* authored by BMWi, BMI, and BMVI is: "IT is easy, transparent and safe to use" (D-61 BMWi 2014:3). Above all, BSI points out that it "works hard to improve awareness and understanding of IT security among private users" (D-10 BSI 2011:36). For example, the agency operates a website with "easy-to-understand, technically sound and neutral information" (D-10 BSI 2011:37) on cyber risks and solutions. In 2006, a CERT service is set up for citizens ("Bürger-CERT"); it issues "warnings on current viruses, worms and other malware which are updated on a daily basis" (D-06 BSI 2008:9). BSI also establishes a support service for victims of a botnet, the so-called "Anti-Botnet Initiative" (D-10 BSI 2011:15).[77] More generally, the federal government promotes measures for "digital education" (D-04 BMI 2016:14, own translation) for all user groups as well as "target group-specific sensitization" (ibid., own translation) on cybersecurity risks. An important cooperation partner of the government in this regard is the initiative "Deutschland sicher im Netz e.V."[78] ("Germany secure online") (ibid.).

[76] The council includes the following ministries: "The Federal Chancellery and a State Secretary from each the Federal Foreign Office, the Federal Ministry of the Interior, the Federal Ministry of Defence, the Federal Ministry for Economics and Technology, the Federal Ministry of Justice, the Federal Ministry of Finance, the Federal Ministry of Education and Resarch [sic, K.U.] and representatives of the federal Länder will participate. On specific occasions additional ministries will be included" (D-03 BMI 2011:9).

[77] More details on the initiative: "If a private PC is captured and used as a bot for criminal purposes despite all the precautions, the user can turn for help to the Anti-Botnet Initiative run by the eco-Association of the German Internet Industry, which the BSI initiated and supports, and in which ISPs provide support for affected customers" (D-10 BSI 2011:15).

[78] For more information see: https://www.sicher-im-netz.de/ (accessed July 10, 2018).

In general, the authors of the *Digital Agenda* underline the goal that Germany "remains one of the most secure digital locations in the world" (D-61 BMWi 2014:3; similarly D-64 BMWi 2016:10). Protection for all users is provided by "creating the conditions to ensure that every individual is in a position to protect themselves and their data online" (D-61 BMWi 2014:31). Measures in this regard mirror the overall goal of being empowered, such as "simple security technologies" (ibid.) and "secure infrastructures" (ibid.) for example, by using encryption. The German ambition is "to be the world's leading country in this area" (ibid.). Encryption by default and "De-Mail"[79] are important steps of implementation. Also, a major research programme called "Safe, secure and empowered in the digital world" (ibid.) is set up to support the measures.[80]

Given the risks of *economic espionage and cybercrime* threatening the economy, BMWi emphasizes the importance of cybersecurity as a "strategic factor for the development of our economy and our industry" (D-63 BMWi 2015:50, own translation). The agency initiates several measures to this end and has got a special focus on small and medium-sized enterprises (SMEs). For example, BMWi started the initiative "IT security in business" ("*IT-Sicherheit in der Wirtschaft"*) in the wake of the first cyber strategy (D-02 BMI 2011:7) in order to increase both awareness and cybersecurity in practical terms (D-63 BMWi 2015:51). The so-called "Alliance for Cyber Security" (*"Allianz für Cybersicherheit"*) is a platform for cooperation between the public and the private sector initiated by BSI and the *Federal Association for Information Technology, Telecommunications and New Media* (Bitkom) in 2012 (D-16 BSI 2016:29; D-11 BSI 2013:20). Its main goal is to assess and protect against cyber risks notably by the means of "distribution of information and exchange of experience" (D-11 BSI 2013:20, own translation). For example, participating companies can access information online or participate in regional or sector meetings (ibid.). BSI evaluates the initative as "successful" (D-13 BSI 2014:6). Promoting a "strong and innovative German

[79] De-Mail "will in future support both transport encryption and end-to-end encryption. Currently over 90 per cent of all e-mails are transmitted in unencrypted form. Furthermore, the two-factor-authentication process means that De-Mail offers security mechanisms against identity theft, which is often successful due to the fact that many providers use the standard software-supported password procedure" (D-12 BSI 2014:38).

[80] Interestingly, in contrast to the U.S. discourse, there is no debate on the use of encryption in the German discourse. Only once, the two sides of encryption are mentioned: In the second cyber strategy, the authors briefly point out that the German approach regarding encryption includes both: "security by encryption" (D-04 BMI 2016:15, own translation) as well as "security despite encryption" (ibid., own translation), that means that law enforcement authorities must be in a position to break encryption if necessary (ibid.).

IT economy" (D-04 BMI 2016:23, own translation) presents another pillar for enhancing cybersecurity. Also, the government has an interest in working with "trustworthy IT manufacturers" (ibid., own translation) in security and defense matters. In this regard it is interesting to note that a "roundtable 'security technology in the IT domain'" (Bundesregierung 2013, own translation) is created by the government in July 2013.[81] One topic of the roundtable is how to improve "national technological sovereignty" (D-11 BSI 2013:11, own translation).

Cybersecurity within institutions of the *federal government and administration* is another important topic, however with a limited presence in the examined discourse. Already the first cyber strategy points out that "[s]tate authorities have to serve as role models for data security" (D-03 BMI 2011:7). Relevant measures to improve federal cybersecurity are the creation of a "common, uniform and secure network infrastructure in the federal administration" (ibid.) and the implementation of the so-called *UP BUND*[82], which is the "first IT security policy for the federal administration which is being co-ordinated among all federal departments" (D-05 BSI 2007:17; see also D-03 BMI 2011:7–8).

Finally, I elaborate on the *European and international dimension* of German cybersecurity policy as articulated in the discourse. I begin with some examples of the European dimension, which is present throughout the examined period. Other than the *European Governmental CERTs Group* (EGC), which is considered as "particularly successful example of co-operation on a European level" (D-05 BSI 2007:209–212), discourse participants communicate active support and contributions to European programmes, such as the *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*[83] (D-45 AA 2013:11), the *EU Internal Security Strategy* (ISS)[84] and the *Digital Agenda*[85]*,* as well as

[81] The roundtable is created in the wake of the presentation of the so-called "Eight-Point Program for a better protection of privacy" (D-11 BSI 2013:11, own translation).
[82] *UP BUND* is the abbreviation of "Umsetzungsplan für die Gewährleistung der IT-Sicherheit in der Bundesverwaltung" (D-04 BMI 2015:35).
[83] For more information see: http://europa.eu/rapid/press-release_IP-13-94_en.htm (accessed July 15, 2018).
[84] For more information see: http://europa.eu/rapid/press-release_MEMO-10-598_en.htm (accessed July 2, 2018).
[85] For more information see: https://ec.europa.eu/digital-single-market/en/europe-2020-strategy (accessed July 2, 2018).

institutions such as the *European Network and Information Security Agency* (ENISA)[86] (D-03 BMI 2011:11; see also D-23 BBK 2012:93; D-19 BBK 2010:5–6) and Europol's *European Cybercrime Centre* (D-61 BMWi 2014:33). Regarding "core strategic IT competences" (D-03 BMI 2011:11), Germany intends to "pool our resources with those of our partners and allies, particularly in Europe" (ibid., 11-12) as stated in 2011. In the Digital Agenda from 2014, the authors underline that "[i]ssues like (…) the digital single market, (…), IT security and research funding involve not just German, but also important European considerations. We therefore act as advocates for the Digital Agenda for Germany on the relevant European committees and actively support the ongoing processes" (D-61 BMWi 2014:35). Moreover, Germany wants to "promote the use of German and European IT products and their manufacturers" (D-61 BMWi 2014:32).

As to the *international* level, numerous references are found throughout the examined discourse. In general, Germany is a strong advocate of a "regulatory framework" (D-64 BMWi 2016:9, own translation) and rules in international cyber policy (see for example D-04 BMI 2016:41), notably for "responsible state behavior in cyberspace" (ibid., own translation). Rolf Nikel (AA) points out: "Also in the case of cyber threats, it is important and possible to create more security by international rules and confidence-building" (D-45 AA 2013:2, own translation). Discourse participants appreciate the applicability of international law (D-50 AA 2014:2), allowing measures ranging from diplomatic means to self-defense (D-55 BMVg 2013:18). One main goal of German cyber policy is "to avoid escalation due to incidents in cyber space" (D-58 BMVg 2016:78). In this sense, discourse participants regularly communicate their active support for confidence-building measures, for example the ones negotiated within the OSCE (D-04 BMI 2016:41; D-45 AA 2013:13). Another example of confidence-building measures is exchanging documents in order to create transparency (D-45 AA 2013:10): Following this idea, Germany and Russia provided each other with their respective White Papers on cyber defense (ibid.:9). In the eyes of discourse participants, rules are also crucial in order "to protect (…) fundamental rights and civil liberties in the digital world" (D-61 BMWi 2014:36) as well as to technically manage the Internet itself (ibid., 35-36). Federal Foreign Minister Steinmeier emphasizes that "the internet is a free and open space. But it is not a legal vacuum! (…) We need reliable and transparent standards, and it is

[86] For more information see: https://www.enisa.europa.eu/ (accessed July 2, 2018).

states and international organizations who will have to coordinate and enforce them" (D-46 AA 2014:2–3). Finally, the German government highlights bilateral "cyber consultations" (D-04 BMI 2016:39; D-45 AA 2013:14, own translation) as important measure as well as helping other states to strengthen their digital capacities with security aspects playing a major role (cyber capacity building) (D-04 BMI 2016:42; D-61 BMWi 2014:36). Overall, Germany qualifies its approach as "pragmatic" (D-45 AA 2013:14, own translation) and inclusive of "all relevant actors – governments, private sector, civil society, the citizen" (ibid., own translation).

Solutions for cyber risks for critical infrastructure. The *CIP Strategy* is a general strategic document underlining the variety of risks for critical infrastructure and that this variety "must be included both in risk and threat analyses and in the selection of options for action (all-hazards approach)" (D-02 BMI 2009:9). Also, the document oulines roles and responsibilities for protecting critical infrastructure, however emphasizing that there is no absolute security (ibid., 11). BMI rather calls for a "new 'risk culture'" (ibid., 11) by promoting an "open risk communication" (ibid., 11) among all affected parties, a cooperative attitude and the commitment to play an active part in the protection of critical infrastructure (ibid., 11).

Other than the *CIP Strategy*, the *Civil Protection and Disaster Assistance Act* (*Zivilschutz- und Katastrophenhilfegesetz*, ZSKG) is adopted in 2009. By the ZSKG, the federal government has "to advise and support the *Länder* in the protection of critical infrastructure" (D-26 BBK 2014:preface, own translation), for example by developing guidelines (ibid.). BKK underlines that the adoption of the *CIP Strategy* and the ZSKG fill a gap by providing "a whole-of-government conception and a coordinated roadmap – in short: a roof" (D-19 BBK 2010:6, own translation).

Moreover, a series of exercises in crisis management exists since 2004, called LÜKEX ("*Länderübergreifende Krisenmanagement Exercise"*): The federal government, the Länder as well as invited companies take part in a common exercise in order to test and improve existing crisis management structures in a simulated major crisis event involving critical infrastructure (D-02 BMI 2009:6). The exercise takes place every two years and each LÜKEX edition presents a new crisis scenario (D-11 BSI 2013:15). In 2011, the scenario addresses cyber attacks with serious consequences for Germany (ibid.). Discourse participants

appreciate the exercises for their positive effects on cooperation: “These joint exercises have reinforced the trusting co-operation among the state and business and industry, based on the conviction that crisis management can only be achieved by joint action and effort” (D-02 BMI 2009:6). Other than the positive effects of exchange and networking, BBK underlines the increased awareness for high-risk situations (D-21 BBK 2011:8).

The so-called *UP KRITIS* recommends measures for cybersecurity more specifically and takes into account prevention, reaction, and sustainability (D-01 BMI 2007). The recommendations include measures on the company level, the sector level as well as cross-sector measures (ibid.:10). In the following, I list some exemplary measures for each of the goals:

- Prevention: conception and implementation of comprehensive, company-specific IT security measures; definition of roles and responsibilities regarding IT security; identification and special protection for critical processes; education and awareness measures; crisis simulation exercises (D-01 BMI 2007:11–20);
- Reaction: Assessment of an IT crisis following a pre-defined structure; alerting relevant parties; management of the crisis; having in place a monitoring system; analysis of monitoring data after a crisis (ibid.:20–23);
- Sustainability: Integration of IT security in curricula at schools and universities; cooperation between critical infrastructure companies and R&D institutions; cooperation within sectors and cross-sector cooperation (ibid.:24–27).

Moreover, a special focus is put on communication: It is recommended to improve and extend structures for reporting and sharing information in different situations (pre-, during, post-crisis) (ibid.:28–33), for example by establishing so-called “Single Points of Contact” (SPOCs) (ibid.:29). Overall, UP KRITIS works as a “model” (ibid.:40, own translation) for IT security.

Solutions for cyber risks within the military context. After a long period characterized by a reserved stance in military cybersecurity policy, BMVg announces the setup of a new division “Cyber/IT” in the ministry as well as creation of a new command “Cyber and Information Space” *(KdoCIR)* (D-57 BMVg 2016:1, own translation; see also D-56 BMVg 2015:1–2). The evolution of the discourse and the measures are presented in detail in section 4.1.2.4.4.

Solutions for cybercrime risks. In order to fight cybercrime, discourse participants mention three main measures throughout the examined discourse: strengthening the agencies dealing with the issue regarding their workforce and technical equipment; cooperating with the private sector as well as academic institutions; cooperating with institutions on the international level (see for example D-04 BMI 2016:22,30; D-61 BMWi 2014:33; D-55 BMVg 2013:27; D-03 BMI 2011:10).

Among the agencies to be strengthened, there are, for example, the Federal Criminal Police Office (BKA) and the Federal Police (D-61 BMWi 2014:33). The expansion of the BKA's *Cyber Crime Centre* is one measure (ibid.). Updating legal prescriptions that deal with cybercriminal activities is another measure (ibid.). Above all, the government intends to "close any loopholes in criminal law relating to the handling of stolen data" (ibid.). The Federal Office for the Protection of the Constitution (BfV) is also in the focus of the government: From 2013 onwards, different measures are implemented such as increasing personnel resources, improving cooperation with administrative and private sector partners, strengthening (cyber) counterintelligence (D-41 BfV 2014:4,22), and updating IT and infrastructure for investigation in order "to improve the analysis of existing data and to make communication patterns much more visible" (D-61 BMWi 2014:33; see also D-41 BfV 2014:22). BfV actively offers advice to companies in cases of cyber attacks such as espionage, underlining that its service is confidential (D-38 BfV 2014:25). In a similar vein, BKA emphasizes the importance of collaborating with the private sector (D-36 BKA 2016:19). An example for such a cooperation is the "German Competence Center against Cyber-Crime (G4C)"[87] (D-04 BMI 2016:22). Other than the defense against "cyber attacks with an extremist or terrorist background" (D-04 BMI 2016:31, own translation), counterintelligence in order to fight IT-enabled espionage attacks is qualified as important aspect by discourse participants (D-04 BMI 2016:31). Moreover, the government announces the development of an "early warning system against cyber attacks from abroad" (D-04 BMI 2016:32, own translation) by the Federal Intelligence Service (BND).

Finally, the importance of international cooperation is regularly highlighted in the discourse (see for example D-04 BMI 2016:30; D-55 BMVg 2013:27; D-03 BMI 2011:4). Germany is an advocate of the *Cyber Crime Convention* of the *Council of Europe* (CoE) (D-04 BMI 2016:43;

[87] For more information see: https://www.bka.de/SharedDocs/Pressemitteilungen/DE/Presse_2014/pm140121_Unterzeichnung_Kooperationsvertrag.pdf?__blob=publicationFile&v=1 (accessed July 28, 2018).

D-03 BMI 2011:10). Moreover, discourse participants mention the *European Network and Information Security Agency* (ENISA) as well as the *European Cybercrime Centre* by *Europol* as cooperation partners (D-61 BMWi 2014:33).

4.1.2.4.4 Evolution of the Discourse regarding the Evaluation of Measures

In this section, the evolution of the discourse regarding the evaluation of measures shall be traced. To begin with, I shed light on the *Computer Emergency Response Team* (CERT) and the evolution of measures that have been started with the first cyber strategy. Then, we turn to the area of critical (information) infrastructure protection. Finally, the most striking evolution can be observed in the military context.

As to the *Computer Emergency Response Team* (CERT), we see that the competences of CERT-Bund are continuously extended: In 2006, an "operations and analysis centre" (D-06 BSI 2008:19) is established within BSI, and in 2009, a new law[88] gives BSI the "right to issue public warnings against IT products and services" (D-11 BSI 2013:15, own translation). Moreover, CERT-Bund and other partners established a cooperation between German CERTs, on the one hand, and a European group called *European Governmental CERTs Group* (EGC), on the other hand (D-11 BSI 2013:14). Both initiatives are considered "very successful" (ibid., own translation, see also D-05 BSI 2007:58). Furthermore, CERT-Bund is a member of the international CERT association *Forum for Incident Response and Security Teams* (FIRST) and the *International Watch and Warning Network* (IWWN); both associations provide "valuable knowledge" (D-55 BMVg 2013:34, own translation). In the view of BSI, CERT-Bund has been able to establish a very positive standing notably based on trust, expertise and its position as "independent institution without commercial interests" (D-11 BSI 2013:15, own translation). The relevance of CERTs is still highlighted in the discourse in 2016: The second cyber strategy calls for "strengthening CERT structures in Germany" (D-04 BMI 2016:34, own translation). Therefore, BSI as Germany's "national CERT" (ibid., own translation) shall coordinate the enlargement of CERT structures and improve their cooperation (ibid.)

[88] BSI act from 2009, §7 (D-11 BSI 2013:15).

As to the *National Cyber Response Centre*, there is an interesting evolution: In the first years of cooperation, the partners had to handle "very different agency cultures as well as the different state of knowledge and experience" (D-11 BSI 2013:17, own translation). However, the creation of the platform is evaluated as a success: The center "has successfully transformed from a simple information hub to a central cooperation platform for institutions with responsibility for IT security in Germany" (D-15 BSI 2015:11). In a similar vein, BBK and BfV acknowledge its importance (D-29 BBK 2016:9; D-42 BfV 2015:143). Consequently, the digital agenda from 2014 and the second cyber strategy from 2016 strengthen the platform regarding its operational capabilities and organization (D-61 BMWi 2014:33; D-04 BMI 2016:28).

Secure and trustworthy IT is a goal communicated by the government in the first cyber strategy: "We want to provide specific incentives and funds for basic security functions certified by the state (…) to be used by the vast majority of citizens" (D-03 BMI 2011:7). These functions are developed and strongly promoted by BSI: Examples are the "new secure Digital ID card" [89] (D-10 BSI 2011:15) and the "De-Mail concept for secure e-mail communication" (ibid.). BSI notably highlights the importance of supporting a broad range of users in order to enhance cybersecurity: "Given that over 80 per cent of all cyber threats can be warded off simply by taking basic security measures, it is necessary to make basic technologies available to private individuals and SMEs" (D-12 BSI 2014:38). Finally, BSI is also very active regarding certification, creation and promotion of national and international standards for IT security; in projects such as smart metering, BSI collaborates with other stakeholders in order to develop common standards (D-16 BSI 2016:32; D-05 BSI 2007:54). In general, more certification notably regarding broadly used IT products is an important concern of the federal government (D-04 BMI 2016:17). Consequently, in the second cyber strategy, the government aims at creating a "quality label for IT security" (D-04 BMI 2016:17, own translation) for more transparency, consumer protection, and cybersecurity, and

[89] "Since November 2010 the new identity card has not only put citizens in possession of a picture ID in a new bank card format, it also provides additional electronic functions that significantly enhance security even on the internet. These include the electronic identity document and qualified electronic signatures" (D-16 BSI 2016:32).

promotes the international dissemination of common (international) standards for IT security (ibid.).[90]

As to the federal network infrastructure and the implementation of *UP BUND*, we observe that both measures are still relevant in 2016: According to the second cyber strategy, the infrastructure process is continued, and *UP BUND* will be updated (D-04 BMI 2016:35). Moreover, it is worth mentioning that BSI's role in federal IT gained in importance by the amendment of the BSI Act in 2009: The agency not only designs "mandatory security standards for the procurement and use of IT" (D-16 BSI 2016:29), but is also in charge of the protection of the administrative digital infrastructure (ibid.).

The measures with a European dimension are continuously present: In the 2016 cyber strategy, the authors state: "Security is a cornerstone of the common digital single market. Germany will make an effort that IT security is appropriately taken into account in all processes of digitalization" (D-04 BMI 2016:40, own translation). As to the international level, BMI rather generally notes in the first strategy that "German interests and ideas concerning cyber security are coordinated and pursued in international organizations, such as the United Nations, the OSCE, the Council of Europe, the OECD and NATO" (D-03 BMI 2011:11). From 2013 onwards, the international measures taken are articulated more concretely and in more detail in the discourse. For example, Germany communicates its support of the new NATO strategy from 2010 that deals with handling cyber risks (D-45 AA 2013:11). Regarding the alliance, the main concern of the German government is "the resilience of the alliance and the protection of NATO-owned networks" (D-04 BMI 2016:39, own translation). In the BMVg White Paper from 2016, the government states that it is "determined to (…) generate synergies with NATO (…) and intensify cooperation particularly in countering cyber and hybrid threats" (D-58 BMVg 2016:69–70). In the UN, Germany supports the work of the *United Nations Group of Governmental Experts* (UN GGE) (D-51 AA 2015:3; D-52 AA 2015:2; D-45 AA 2013:12).

Concluding and summarizing the evolution and implementation of measures in the course of the three big strategies (cybersecurity strategies from 2011 and 2016 (D-03 BMI 2011; D-04

[90] Examples for important international standards are *Common Criteria* and *ISO 27000* (D-04 BMI 2016:17).

BMI 2016), *Digital Agenda* from 2014 (D-61 BMWi 2014)), I find that important measures have been started in the first strategy such as highlighting the "protection of critical information infrastructures" (D-03 BMI 2011:6); raising awareness; maintaining and advancing the country's technological competences in secure IT; creating specific bodies to tackle cyber risks; strengthening cybersecurity-related authorities; improving federal cybersecurity; and relating German cybersecurity policy to European and international efforts (D-03 BMI 2011:6–12). This way has been continued and supported in the digital agenda and, much more concretely and differentiated, in the second strategy. On the one hand, there are several completely new aspects of the solution in the second cyber strategy, such as the creation of teams in BSI, BKA, and BfV that help manage cyber incidents on-site (D-04 BMI 2016:29)[91] or the creation of an office within BMI for "technical support of security and specialized authorities (…) regarding their operational cyber capabilities" (ibid., 32, own translation)[92]. On the other hand, it is important to note that existing instruments from the first strategy are adapted and strengthened, most notably the *National Cyber Response Centre* and the *National Cyber Security Council* (ibid.:28,45). The authors of the second strategy mention the idea of continuity from the first to the second cyber strategy regarding "strategic approaches and goals" (D-04 BMI 2016:5, own translation); at the same time, they also underline the necessity of a "new cross-departmental strategy" (ibid., own translation) in order to "holistically" (ibid., own translation) deal with cyber risks.

As to the protection of *critical infrastructure* in general, there are measures since the end of the 90s and they constitute a "key element of the state's security-related preparedness system" (D-02 BMI 2009:5). The already mentioned *CIP Strategy* was published in 2009 (D-02 BMI 2009).

Regarding the cyber domain more closely, we find that the protection of critical information infrastructure has been put on the agenda in 2005: Then, the *National Plan for Information Infrastructure Protection* (NPSI) (Bundesministerium des Innern 2005) was published. The *UP KRITIS* (D-01 BMI 2007) from 2007 is the implementation plan of the NPSI and is directed at the owners and operators of critical infrastructure (D-01 BMI 2007:8). The UP KRITIS

[91] The teams of the BSI are called "Mobile Incident Response Teams" (D-04 BMI 2016:29), the BKA establishes a "Quick Reaction Force" (ibid.), and the BfV sets up "Mobile Cyber-Teams" (ibid.).

[92] The German name of the office is "Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)" (D-04 BMI 2016:32).

recommends different measures along the NPSI goals prevention, reaction, and sustainability (ibid.). The UP KRITIS is updated in 2014 (D-26 BBK 2014:13), but nevertheless, it becomes clear in the eyes of the government that the voluntary cooperation model is "not sufficient to achieve an appropriate level of IT security in all critical infrastructure sectors" (D-14 BSI 2015:41). That is why a new mandatory measure is taken: In 2015, the so-called *IT Security Act* (*IT-Sicherheitsgesetz, ITSiG*) is adopted. It is directed at owners and operators of critical infrastructure and requires them "to maintain a minimum level of IT security and to report IT security incidents to the BSI" (D-16 BSI 2016:33). I present and evaluate the IT Security Act in a more detailed way below in chapter 5. BSI sees the act as a "boost" (D-16 BSI 2016:32) for the joint protection activities of the public and the private sectors regarding critical infrastructure. In a similar vein, BBK qualifies the act as a "milestone" (D-30 BBK 2016:11, own translation).

I also find references to the European and the international level focused on critical infrastructure protection. For example, UP KRITIS is communicated as "an essential contribution of Germany to the announced *European Programme for European Critical Infrastructure Protection* (EPCIP)" (D-01 BMI 2007:8), which shows the European orientation of German policy already early in the examined discourse. The support of the EPCIP[93] is also mentioned in the first German cyber strategy from 2011 (D-03 BMI 2011:11). In 2015, the EU *Directive on security of network and information systems* (NIS)[94] is qualified as "[i]mportant work" (D-51 AA 2015:4) notably because "[c]ritical infrastructure in particular will be protected through this measure" (ibid.) – an important German policy goal. As to the international level, it is interesting to note that the idea of a "minimum level of IT security in critical infrastructures on the international level, beginning in the European area" (D-01 BMI 2007:39) occurred already in 2007 in the German discourse. It re-occurred later, for example in 2013, when BMVg promoted the "obligation to protect critical information infrastructure" (D-55 BMVg 2013:27, own translation) as one of several basic principles for state behavior. In a similar vein, the Federal Foreign Office communicated in 2015, that "States must provide an adequate level of protection for IT infrastructure on their territory, with a view of

[93] For more information see: https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure (accessed July 2, 2018).
[94] This EU Directive, adopted in 2016, "is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU" (European Commission 2018b).

safeguarding the overall functionality and stability of the Internet" (D-51 AA 2015:3). As can be seen, the international dimension of critical infrastructure protection is a continuous concern of the German government.

Regarding Germany's approach towards cyber risks within the *military* context, I observe a major evolution: In the course of the examined period, there is an increase of both the presence of military aspects of cyber risks in the discourse as well as the measures implemented.

In the first cyber strategy, the military is only briefly mentioned: It has got a supplementary function given that the strategy "mainly focuses on civilian approaches and measures" (D-03 BMI 2011:5; see also D-55 BMVg 2013:12). In a 2013 document, BMVg states that "cybersecurity in the Bundeswehr is (…) part of a whole-of-government approach to security" (D-55 BMVg 2013:5, own translation). The agency emphasizes that actions of the armed forces always have to comply with German and international law: "A mission of the armed forces, including related to cybersecurity, always remains bound to existing constitutional requirements and requirements under international law" (D-55 BMVg 2013:5, own translation; similarly D-04 BMI 2016:33). Thus, the mentioned requirements would apply to a mission of the so-called "computer network operation forces of the Bundeswehr" (CNO) (D-55 BMVg 2013:17, own translation)[95]. Decisions have to be made on a case-by-case basis (ibid.). The CNO forces are able to conduct "targeted and coordinated measures to damage foreign information and communication systems as well as information processed therein" (D-55 BMVg 2013:6, own translation). The BMVg regards the CNO forces as necessary part of a "broad and flexible range of military capabilities" (D-54 BMVg 2011:27, own translation; see also D-55 BMVg 2013:5–6). However, according to a statement in 2013, the forces have not yet been used (D-55 BMVg 2013:24). In case of missions of computer network operation forces abroad, the Bundestag needs to be involved in decisions upon such missions according to the *Parliamentary Participation Act (Parlamentsbeteiligungsgesetz)* (D-55 BMVg 2013:19). Overall, BMVg discourse communications remain rather passive and reserved. For example, the agency states that "it is primarily the responsibility of the Federal Office for Information Security (BSI) as national

[95] BMVg dates the "initial enabling capability" (D-55 BMVg 2013:24, own translation) of the forces to the end of the year 2011 (ibid.).

IT security authority to advance IT security in Germany" (D-55 BMVg 2013:12, own translation).

The definition of cyberspace as a military domain is, of course, a topic in the German discourse. However, discourse participants do not pro-actively advocate and support the creation of this new military domain; it is rather a form of recognition of a commonly (e.g. by NATO) accepted fact in the course of time (D-59 BMVg 2016:1; D-56 BMVg 2015:1; D-55 BMVg 2013:6). This aligns well with a longstanding attitude in the German cyber discourse: Discouse participants highlight the "defensive approach" (D-45 AA 2013:10, own translation) of German cyber policy and warn against offensive cyber capabilities: "Regarding offensive cyber capabilities, we should be extremely cautious. Certainly, a reasonable defense strategy requires offensive knowledge. But using cyber instruments comparable to Stuxnet and Flame is a very double-edged sword" (ibid., own translation).

Discourse participants regularly attach great importance to measures that contribute to reducing the risk of misperceptions and (military) escalation in cyberspace (see above). For example, BMVg regularly conducts defence policy consultations with the United States, European countries as well as Russia and China (since 2012) (D-55 BMVg 2013:34). Also, discourse participants underline their opposition towards an arms race in cyberspace, for example in the Digital Agenda: "We are opposed to a 'cyber arms race' but instead favour a peaceful alignment of international cyber security policy" (D-61 BMWi 2014:35). Germany advocates the applicability of international humanitarian law – even if the matter is complex, as is articulated in a statement of the federal foreign office in 2015: "Discussing how international humanitarian law applies to cyberspace is highly controversial. Some argue that this encourages a militarization of this thus far civil resource; they refer to the threat of a new arms race. However, we believe that it would not be expedient to ignore reality: Cyber space is already being used by the military" (D-51 AA 2015:3).

A major change in terms of practical measures occurs in 2015: Then, BMVg announces the setup of a new division "Cyber/IT" in the ministry as well as creation of a new command "Cyber and Information Space" *(KdoCIR)* (D-57 BMVg 2016:1, own translation; see also D-56 BMVg 2015:1–2). The units shall start working in October 2016 and in April 2017 respectively

(D-57 BMVg 2016:1). The main motivation is to "bring together and strengthen" (D-56 BMVg 2015:1) responsibilities and military capabilities, that were scattered before (ibid.). The aspect of strengthening includes, for example, an expansion of the afore-mentioned CNO forces (D-59 BMVg 2016:28). Also, the reform initiates a structural improvement of military cybersecurity (D-04 BMI 2016:33). The overall goal of the reform is an "increasingly IT-driven modernization and the appreciation of the cyber and information space as military dimension" (D-59 BMVg 2016:2, own translation). Moreover, it is communicated as acknowledgement of the new cyber policies within NATO and the EU (ibid.).

Also, BMVg and BMI communicate a "common understanding" (D-59 BMVg 2016:5, own translation) of their respective responsibilities. This clarification process results in the statement that cybersecurity and the protection of critical infrastructure are joint national tasks whereas "defense aspects are original responsibilities of BMVg and Bundeswehr" (ibid., own translation; similarly D-04 BMI 2016:33). More concretely, this implies that the "Bundeswehr (…) has to ensure its own capacity to act in the cyber and information space (CIR) and has to provide an increasing contribution to the whole-of-government approach to security in the future" (D-59 BMVg 2016:5, own translation). With regard to the international context, the BMVg *White Paper* from 2016 lists the "fight against transnational terrorism, against threats from the cyber and information domain, and against new hybrid dangers" (D-58 BMVg 2016:92) as tasks of the armed forces. So overall, the roles of BMVg and Bundeswehr are strengthened and interpreted as more active. This change is also recognized and communicated in the second cyber strategy from 2016 (D-04 BMI 2016:33) and prepares the ground for a discussion on a more active use of cyber capabilities: Against the backdrop of "severe cyber attacks" (D-04 BMI 2016:29, own translation), the "federal government will (…) examine, which legal conditions would have to be met and which technological possibilities might be used by public authorities in order to conduct network operations in these cases" (ibid., own translation). Other than the new military role, BMVg also pursues a new strategy of gaining – urgently needed – workforce in order to better cope with cyber risks: Therefore, a "cyber reserve" (D-04 BMI 2016:37, own translation) including non-military staff is created. Overall, the *White Paper* formulates different measures for successful armed forces in the digital age: "[W]e must above all develop national capabilities, in other words promote a whole-of-government approach and cooperate with

research institutions, industry and partners; develop Bundeswehr cyber capabilities (…); make weapon systems, command posts, and armaments supply chains more robust by using (…) key national technologies; recruit the very best personnel (…) and bring together the various responsibilities and structures" (D-58 BMVg 2016:93). The importance of innovation is another point mentioned in the discourse, albeit less prominently. The White Paper states that "[c]onstant innovation is needed in order to deliver effective protection and ensure the superiority of armed forces" (D-58 BMVg 2016:131). However, BMVg also communicates its limited capabilities regarding innovation and the resulting need for cooperation against the background that "[m]any sources of forward-looking technological innovation exist outside the defence sector" (D-58 BMVg 2016:131).

Finally, it has to be mentioned that the Bundeswehr is allowed to provide support in case of severe domestic IT incidents and incidents affecting critical infrastructure under the authorities of "administrative assistance" (*Amtshilfe*) (D-04 BMI 2016:33, own translation; see also D-55 BMVg 2013:17; D-54 BMVg 2011:25), which is a longstanding option in German policy.

4.1.2.5 Overview: Condensed Frame Elements in the German Discourse

In order to conclude the presentation of the German discourse, the following table (Figure 9) presents the most relevant frame elements in a condensed fashion.

Figure 9: Condensed Frame Elements in the German Discourse

Cybersecurity Risks			
	Description/Evaluation	**Time Frame Evolution**	**Dominant Discourse Participants**
Cyber Risks in General	Attacks comprising IT security with the potential of a "considerable negative impact (…) on Germany's social lifelines" → "vital questions of the 21st century"		
Cyber Risks for Critical Infrastructure	"Criminal acts, technical failure and/or human error or organizational shortcomings" as causes; potentially "far-reaching consequences" for public safety; actual vulnerability of critical infrastructure demonstrated by Stuxnet → Worrying situation, growing and real risk	High attention since Stuxnet (2010)	BMI, BSI
Cyber Risks Within the Military Context	Worrying risk of military cyber capabilities; potential of escalation; combination of cyber and traditional means of warfare more likely than cyberwar	Higher attention since 2013	AA, BMVg
Cybercrime Risks	Financially motivated cybercrime, electronic attacks with the goal of espionage → Pervasive and high risk	Constant (high) attention	BKA, BfV

Drivers and Actors	
Drivers	Dependence and connectivity; technology as enabler; "digital carelessness"
Actors	General: criminals, terrorists, intelligence agencies, hacktivists, malicious insiders; specific: intelligence actors (China, Russia, Iran)

Evaluation	
Evaluation	"critical" situation; permanent challenge; high and evolving risk, growing in terms of quantity and quality; need for orientation in the "uncharted territory" of the digital age

Solutions	
Responsibility	State as problem-solver; shared responsibility in cooperation with the private sector; individual responsibility
Goals	Cybersecurity and protection of critical (information) infrastructure; "acceptable and manageable level" of cyber risks; cybersecurity as pre-condition for using the potential of digitalization; need of trust; technological and individual sovereignty (self-determined digitalization); European and international cybersecurity
Measures	Protection and resilience measures for critical (information) infrastructure in the areas of prevention, reaction and sustainability (CERTs, National Cyber Response Centre, National Cyber Security Council, promotion of awareness and secure, trustworthy IT, European and international cybersecurity efforts); critical infrastructure: UP KRITIS, IT Security Act; military: new cyber division in 2015; cybercrime: strengthening relevant agencies, increasing cooperation with private sector, academic, international partners

Note: Own compilation. Quotations refer to the respective sections in chapter 4.1.2.

4.2 Overarching Frames in both Countries

From the frame elements laid out above, two overarching frames can be concluded for each country. They are presented in the following sections and supported by my interview data.

4.2.1 Overarching Frames in the U.S. Discourse

Aggregating and interpreting the frame elements identified in the U.S. executive discourse, I find two overarching frames: a "homeland security frame" and a "technological leadership frame".

Both frames start from the common problem definition of serious, increasing, evolving, immediate cyber risks with a massive, if not existential, potential for harm. Cyber risks are seen as "one of the most serious national security, public safety, and economic challenges we face as a nation" (U-06 WH 2010:27) and evaluated as "increasing in frequency, scale, sophistication, and severity" (U-53 State 2016:19). The interview data confirms this assessment. For example, one expert formulates as follows: "We get briefed a lot on the risk and we know that over time, the risk has continued to escalate as more and more things are connected to the internet, there is greater, greater vulnerabilities that lie that could be used to hack into all sorts of things, banking systems, the industrial control systems that run gas pipelines in the electric sector. So, the cyber risk, as we see it, is growing. It is becoming more severe and the amount of vulnerabilities is increasing to tremendously" (I-04:36). Another expert highlights the implications of cyber risks for national security: "[T]hose threats that we are most concerned with, those national security threats, are probably the greatest cyber threats around these days. That kid in that high school or maybe even a teenage hacker, they can cause problems and inconvenience, but they cannot shut down a nation like China or like Iran aspires to do" (I-06:56).

4.2.1.1 The Homeland Security Frame

The *"homeland security frame"* highlights the threat by cybersecurity risks, often times seen as a potentially existential threat by discourse participants and described in dramatic scenarios (e.g. the scenario of a "cyber Pearl Harbor" (U-60 DoD 2012:2)), and the urgent need to act to counter this threat. Discourse participants find that the "nation is being

challenged as never before to defend its interests and values in cyberspace" (U-64 DoD 2015:1) and communicate that they are willing to take on this challenge – in a holistic manner, with a strong will, a diverse set of measures, and all relevant stakeholders. An interviewed expert from the field of homeland security emphasizes the changing character of cybersecurity risks from rather annoying incidents to incidents with possibly destructive effects notably with regard to critical infrastructure (I-04:36). He means attacks, "where you can actually blow things up. That is where we see the trend of the cyber risk in the long-term and where things are going and why we need to do more to help the security of such systems" (I-04:36). In a similar vein, another expert explains that "the protection of critical infrastructure and SCADA systems is extremely important and something that we need to find a way to incentivize" (I-03:28).

It is a characteristic feature of the homeland security frame that it takes a very pro-active stance. This is linked to at least two things: On the one hand, the pro-active stance is in line with the leadership attitude of the United States as described in the "technological leadership frame" (see below). On the other hand, discourse participants refer back to 9/11. Some perceive cyber risks as so dramatic that they qualify the current situation regarding cyber risks (notably until 2013) as "pre-9/11 moment" (U-60 DoD 2012:4). And they stress that it is crucial to not make the same mistakes again. It is a sort of anticipated fear of doing something wrong (again) that triggers the need to be prepared for any circumstances, and thus accepting partially strong measures. 9/11 is also important from an institutional point of view: It is the founding event for the Department of Homeland Security as an institution, and cybersecurity is one of its missions. The discourse shows that, from the beginning, the "homeland security enterprise" (U-40 DHS 2010:iii)[96] takes its mission and responsibility very seriously. The pro-active stance of the frame is also a topic in the interview data. A scientific expert critically judges official political action and assesses that "there is a strong emphasis on selling exigency through fear. (…) [T]hey say: Here are all these threats, and therefore, we need to do this, without actually explaining how their advocating will lead to a certain behavior" (I-02:22).

[96] "Homeland security enterprise" means "the Federal, State, local, tribal, territorial, nongovernmental, and private-sector entities, as well as individuals, families, and communities who share a common national interest in the safety and security of America and the American population" (U-40 DHS 2010:iii).

In the examined discourse, the executive emphasizes a "whole-of-government approach" (U-41 DHS 2011:3) that also includes the cooperation of homeland security and defense actors: Already in 2010, a cooperation memorandum in this sense is established and DoD highlights its intention and the necessity "to use military capabilities to support other departments' efforts to secure the networks that run the United States' critical infrastructure" (U-56 DoD 2010:108). Later in the observed discourse period, in 2015, the DoD wording is even more pronounced regarding so-called "defend the nation operations" (U-63 DoD 2015:25). So, from the beginning there is a significant military presence not only in the discourse, but also in the measures taken, notably with regard to critical infrastructure. The importance of the military is confirmed by the interview data. One interviewed expert notes that there "has been a very strong military push to engage in this" (I-02:23). In a similar vein, another expert explains that the military engagement lead to the 2010 article of William Lynn, Deputy Secretary of Defense, which was "declaring cyberspace to be the fifth domain in the Pentagon's planning" (I-07:67–68). This was "indicative of a trend that has consisted ever since of a growing role of the military in the U.S. policy making context" (I-07:68) in the expert's view. The expert analyzes that one of the reasons for this growing role is the strongly expanding use and importance of cyberspace: This "brought in the military more because more of its own infrastructure was tied to it, 90% of its traffic is exchanged through the public infrastructure, connected with the fact that the rest of the country gets more and more connected, so the question is, if you want to defend the country, how do you do that if everything becomes increasingly connected" (I-07:68). Another expert points to the specific characteristics of the cyber domain that can trigger military involvement: "cyber (…) challenges the traditional model of how you do security: The law enforcement dealt with domestic security, the military dealt with threats from overseas. Now you have the threats coming from overseas, but at a level below which the military's response is appropriate. And so, you have this gray area" (I-08:80). According to the expert, the attacks of 9/11 are a major reason that lead to "a militarization of U.S. security thinking" (I-08:83).

In the homeland security frame, a self-imposed imperative of being prepared is communicated to all actors on the inside and the outside environment highlighting the need to act ("We must be ready" (U-64 DoD 2015:11)). In consequence of the problem definition,

and the identified causes, responsibilities, and goals regarding cybersecurity, a wide range of measures is taken: They include the complete risk cycle and have the goal "to prevent, respond to, and recover from attacks when they happen" (U-21 WH 2015:6–7). The measures address people, for example awareness raising, they address technology, and they address the political and legal level (such as strategies, frameworks, law enforcement). However, legislation is difficult in times of a Congress caught in "political dysfunction" (U-22 WH 2015:3), which is regularly criticized by discourse participants. Nevertheless, the government wants to be active and stresses it does all that is possible within the framework of the available executive instruments, for example executive orders (U-17 WH 2014:2). The issue of political dysfunction is also addressed in the interviews with experts. One scientific expert notes the long time span of not passing legislation: "By my calculation, the last cybersecurity law was actually in 2002, so long time ago" (I-02:20, see also I-10:105). A committee-aide of the House Homeland Security Committee points out the difficulties at the example of two failed bills, one in each chamber: "Last Congress, you had the Lieberman-Collins Senate bill, which was a very comprehensive approach. It tried to tackle everything into one bill, and it became problematic because you had this mega-bill and you did not report out everything through the typical committee process. So, House tried this comprehensive approach last Congress, it did not work" (I-04:37). He especially sees the need to return to the "regular order" (ibid.) for a successful legislative process. Regarding the work across agencies and in Congress, a committee staffer of the House Intelligence Committee acknowledges that "there is always room for improvement" (I-06:59), but also that "[w]e are still learning a lot about cyber, and how that domain really works in practice" (ibid.). Finally, a policy expert puts forward the complexity of cyber issues: "There has been a period of time broadly post 9/11 where there has been an effort by Congress to try and deal with the cyber threat without really properly understanding what that threat is and what legislation is going to be most effective. One of the consequence of that desire to act in advance of fully understanding the problem is that various different people have had different perspectives about what is required, on the one hand, and what would work, on another hand" (I-08:85–86).

In the homeland security frame found in the discourse, participants are conscious of the fact that there is no absolute security, so they choose a "risk management approach that accepts

certain risks, reduces others, and concentrates on the most consequential" (U-40 DHS 2010:55). This is another link to the existential threat scenario invoked by discourse participants and also serves as justification for giving the military a strong role in line with the 9/11 experience mentioned above. As to the risk management approach, the interviewed experts have got differentiated views. Taking the example of cyber insurances, one expert illustrates the difficulty of risk management in the cyber domain: "How do you build actuarial tables, how do you acurately model the risk? It is definitely ever changing, the risks are very difficult to evaluate, very difficult to abstract away from an individualized context and model it on a broader abstract scale. Especially because not only are the vulnerabilites highly individualized, but the threat vectors are ever changing" (I-03:30). Another expert refers to Ralph Langner[97] and that "he argues strongly against risk management approaches in the cyber area, particularly in terms of industrial control systems, because he argues it is virtually impossible to measure the threat" (I-08:87). However, "risk management may work in the information technology's part of cyber security" (ibid.).

The character of the homeland security frame evolves in the course of time: It is rather dramatic and urgent in the years until 2013 and then transforms towards a more pragmatic homeland security approach. This more pragmatic approach implies a certain habituation and acceptance of the existence of cyber risks and sees coping with it and taking care of cybersecurity as a continuous, very important task ("cyber risk must be managed" (U-37 DNI 2015:1)). The more pragmatic point of view may also result from the fact that until now no cyber-related event comparable to 9/11 has taken place. So, homeland security is communicated as a permanent mission of all participating actors and the executive strongly points to everyone's responsibility. Of course, public-private partnerships can be challenging, as the government notes, because of different motivations and interests of involved parties. Many discourse participants use and drive the frame, most notably DHS, the White House, but also military actors. In this sense, the broadness of the homeland security frame serves all institutional actors for their joint, but also individual, purposes in the discourse.

[97] Ralph Langner is the cybersecurity expert who decoded the Stuxnet malware (see https://www.langner.com/stuxnet/ accessed January 25, 2020).

Cyber risks for critical infrastructure, their vulnerabilities, and potential damages are most strongly addressed in the homeland security frame, but it is valid for other cyber risks as well. The frame illustrates the broad meaning of the term (homeland) security for discourse participants. They closely link national (including military) security and economic security and both are threatened in the context of cyber risks: The "backbone of our national and economic security" (U-15 WH 2013:2) is threatened. So, cybersecurity in a global sense needs to be a top priority as it ultimately serves the higher purposes of national and economic security as well as public safety. One interviewed expert explains the government prioritization as "national security comes first, and then economic security" (I-07:71). In this view, the government hierarchy would be: First, the "continuation of government in case of a war" (ibid.) under a cyber attack; second, securing critical infrastructure that could lead to massive damage in case of a cyber attack, for example, an attack on a "chemical plant releasing toxic material in a highly densely populated area" (ibid.) or even "a coordinated timed attack in several locations" (ibid.); third, securing critical infrastructure like the financial sector against a "cyber attack that would only have consequences in the virtual world" (I-07:72). The latter includes aspects of both, national and economic security (ibid.).

Another element in the homeland security frame in order to support the need to act is defining a differentiation between 'we' and 'the others' and attributing who is responsible for cyber risks. Notably the DNI and State describe responsible states in a precise fashion; for example, China and Russia are seen as advanced and aggressive cyber actors, Iran and North Korea are seen as "unpredictable" (U-35 DNI 2014:2) in their behavior. Also, U.S. discourse participants directly point to actors that are culpable in their view: For example, the United States brings up an indictment against five Chinese military hackers in 2014 and blames North Korea for the large-scale cyber attack on Sony Pictures Entertainment. In the FBI discourse, an offensive nuance is partially added, for example, when speaking of the U.S. goal "to name and shame" (U-76 FBI 2016:9) responsible actors. In the interview data, I find confirmation for the emphasis on China. A committee staffer of the House Intelligence Committee exemplarily notes: "China is unable to innovate like our nations do and so they are tempting to shortcut that process by stealing innovation, by hacking into servers of companies to steal their designs, to steal their research, to steal their bid information, so they can undercut them in contracts, and for purchasing companies overseas. So, it is a

severe economic threat to countries like the U.S. or Canada or Western Europe" (I-06:56, see also I-01:6). In his view, China is seen as "our biggest problem right now" (I-06:57). While this view matches with the official political discourse, an interviewed policy expert observes that the threat from China is also instrumentalized for other purposes: "[T]he essential threat from the Chinese is one of economic espionage, but perceived as the best way to sort of bang the drum for this is hyping up the threat to physical destruction of the critical infrastructure" (I-08:89). So, there is the actual cyber risk with regard to China (see also I-09:93), but also the discursive use of the country as "bogeyman" (I-08:89): "China provides an enemy around which the U.S. has been able to organize its response to cyber threats" (ibid.).

In conclusion, the homeland security frame illustrates the overall U.S. intention "to make cyberspace safe so that its revolutionary innovations can enhance both the United States' national security and its economic security" (U-56 DoD 2010:108).

4.2.1.2 The Technological Leadership Frame

The *"technological leadership frame"* is the second frame found in the official U.S. discourse. It highlights and combines the importance of technology and leadership, both very dominant and continuous in the U.S. discourse. Regarding the technology aspect, on the one hand, technology is regarded as enabler of cyber risks: Many features of modern IT contribute to favoring cybercriminals compared to their prosecutors, and offense against defense. The vulnerability to cyber risks becomes also clear in the driver of dependence on information and communication technology in everyday U.S. life and particularly in the military domain. One interviewed policy expert with government experience highlights the aspect of military dependence: "The U.S. Department of Defense, they procure a lot of weapons and military systems, planes and all that. A lot of that is very technology-heavy, it is very sophisticated. So, from what I observe and working with them, they are very worried about compromised technology, whether it is counterfeit or it does not work well. So, the reason for the risk could be different. It could be intentional, it could be unintentional, but they are so worried about the product not working" (I-10:100).

On the other hand, U.S. discourse participants are convinced that technological problems can be countered with a better technological solution, at least in part. Numerous measures implemented in order to cope with cyber risks relate to the technical level, such as setting standards or looking for solutions in research and development. Moreover, discourse participants note that advances in information technology improve U.S. capabilities to detect and attribute cyber threats. Technological progress also enables new possibilities for the collection of intelligence. Overall, in the discourse, the role of information and communication technology is linked to a certain "irony" (U-02 WH 2009:1) and associated with the "paradox" (ibid.) of enabling chances and risks at the same time[98]: So, technology is communicated as the great point of vulnerability, but at the same time, the great strength of the United States.

In the end, however, the judgement of technology is very positive in the U.S. discourse. Overall, in the eyes of discourse participants, advantages by information and communication technology outweigh the disadvantages by far. In the United States, we find an open and positive attitude towards technology and digitalization more generally, even a "thirst for computers, smartphones, and other digital solutions at work and at home" (U-05 WH 2009:2). This is linked to a feeling of sovereignty based on the particular innovative spirit and technological power attributed to the nation. That is where the (technological) leadership element comes in: The United States is proud of being "the nation that invented the Internet" (U-02 WH 2009:3). Its innovative capabilities are an important part of the country's self-conception.

From a U.S. point of view, the "digital economy is the great engine of innovation and economic growth of the 21st century" (U-70 Commerce 2014:17) and so, a crucial driver of prosperity. And it is also a driver for cybersecurity, as stated in the interviews. One interviewed expert from the political sphere underlines the role of private corporations for innovation and for cybersecurity: "[T]hey have an incredibly powerful market incentive to innovate, both in terms of efficiency and bringing those services to market. But there is also a very powerful market for us to improve cyber security. I would say, there are lots of people

[98] President Obama states in 2009 that "[i]t's the great irony of our Information Age – the very technologies that empower us to create and to build also empower those who would disrupt and destroy. And this paradox – seen and unseen – is something that we experience every day" (U-02 WH 2009:1).

working very hard on this like Silicon Valley, trying to come up with ways to make our activities on the internet safer and more secure. (…) I have faith that market forces will bring us to a better place when it comes to security" (I-06:59).

The economic importance of information and communication technology is also mirrored by discourse communications highlighting the threat to intellectual property (IP) and competitiveness by cyber risks. The United States clearly communicates the claim to be capable and willing to lead the world in the digital age: Indeed, "[a]s the birthplace of the Internet, the United States has a special responsibility to lead a networked world" (U-22 WH 2015:12). This leadership claim with regard to modern ICT is very strong and prominent in the U.S. discourse during all of the examined time frame.

Also, creating U.S. Cyber Command and declaring cyberspace a military operational domain, both early in the examined time period, can be seen in the light of the technological leadership frame as it is another demonstration of power and American superiority in the military domain applied to the field of cyber risks and cybersecurity. It is combined with the unilateral doctrine to reserve "the right to use all necessary means" (U-09 WH 2011:14) to counter a severe cyber attack by an adversary. For the United States, this implies military means as the ultimate option. The leadership claim becomes also apparent in another area of international cybersecurity policy: The United States describes itself as a "global leader in the campaign against transnational cybercrime" (U-53 State 2016:5), which underlines the self-assertive stance of the country.

Whereas the homeland security frame illustrates the increasing articulation and practical importance of the military on the domestic side of cybersecurity, the military role towards the outside, in the world, is undisputed in the discourse from the beginning. Although the United States is interested in international cooperation and in a "shared understanding about norms of acceptable state behavior in cyberspace" (U-49 State 2014:2), it attributes itself a leading role. The military's strong role is articulated even more clearly and openly in the second military cyber strategy (2015) – that also mentions offensive cyber means – and thus also matches with the technological leadership frame.

U.S. discourse participants communicate a strong technological advantage compared to others. However, in order to be and to remain "on the cutting edge of this new technology" (U-60 DoD 2012:2), they also stress the absolute need to further advance in innovation. So, there is a strong pressure to "stay a step ahead of our adversaries" (U-12 WH 2012:2). As President Obama notes: "More than any other nation, America is defined by the spirit of innovation, and our dominance in the digital world gives us a competitive advantage in the global economy. However, our advantage is threatened by foreign governments, criminals and lone actors who are targeting our computer networks, stealing trade secrets from American companies and violating the privacy of the American people" (U-25 WH 2016:1). The mission of continued technological leadership is translated into a political responsibility to foster continued innovative power, but also to create the necessary cybersecurity workforce.

Finally, keeping technological leadership is communicated as condition for remaining in the (world) leadership position in a more general sense: "So long as the United States (…) continues to be a pioneer in both technological innovation and cybersecurity, we will maintain our strength, resilience, and leadership in the 21st century" (U-08 WH 2010:3). The technological leadership frame can be found throughout the examined discourse period and is basically acknowledged by all discourse participants with the White House and DoD being particular strong advocates.

In the interview data, there are statements confirming the technological leadership frame in the discourse analysis – even including the NSA: "[T]he U.S. is recognized as the innovative technical leader in the area: Internet built here, born here, the biggest commercial companies (…) are (…) mostly American. And even the NSA in its perverse way demonstrates the technological superiority of American know-how" (I-09:99). The policy expert adds his assessment that the United States was perceived as friendly and unquestioned rule-maker in the digital age, but that this could now be called into question: "For the first thirty years, people thought of the United States as a benign cyberspace despot. We set the rules, but we let everybody have all the freedom that they want. And now, we are probably going to have a giant contest over that" (I-09:99). Participants in this contest would be the authoritarian countries with their (different) model of Internet governance and the United States, either

united with Europe or alone and Europe as third party (I-09:99). So, this view confirms the technological leadership frame, but also acknowledges that the U.S. superiority in the digital domain is now seriously challenged.

4.2.2 Further Findings from Interview Data on the Background of the U.S. Discourse

In the following, I report some more findings from the interview data on the background of the official discourse. These findings cover topics "hidden" from the official discourse, most notably, policy experts' outside view on dynamics in the discourse, communication, and the relationship between executive actors.

One aspect regularly highlighted by interviewed U.S. scientific and policy experts and – obviously – barely visible in the examined official discourse is a certain "confusion about how to define the scope of what is the cyber risk from the government's perspective" (I-07:66) and the lack of a coherent government strategy (I-08:84, I-09:96). This is due to what one expert calls the "breakdown of the distinction between domestic and foreign spaces" (I-07:65) by the advent of cyberspace and the risks emerging from it. Against the background of a lacking government strategy, there is a stronger influence of the strategies of specific departments according to one expert's observations (I-08:84) and this leads to competence fights between different executive actors. As the policy expert notes, the lacking overall government perspective leads to the effect that "the more assertive departments [can, K.U.] be more assertive. DoD has far more resources and they just more can do" (I-08:82). It is also an issue of a civilian versus military vision of cybersecurity policy. Experts highlight the fight between DoD and DHS: "DHS has the authority, but not the capacity; DoD through the NSA does not have the authority but has the capacity" (I-07:70, similarly I-08:83–84).

DHS with its civilian, "bottom-up approach" (I-07:68) is perceived as weaker because it is a comparatively young agency (I-02:70), its institutional conception is doubted (I-02:25) and cyber attacks became more complex and sophisticated in the course of time – which pushed DoD regarding its perceived problem-solving capacity (I-02:70). Also, DoD and the NSA are perceived as very powerful actors (I-08:82, I-07:70) favoring a "top-down approach" (I-07:68). The expert evaluates the declaration of cyberspace as military domain as early sign of an increasing importance of the military (I-07:67-68). Also, regarding the creation U.S. Cyber Command, the expert emphasizes "the very deliberate choice to make it a dual-hatted

institution with the head of it being the director of the NSA and, at the same time, the commander of Cybercom" (I-07:68). Later, the civilian-military fight could, for example, be observed in the legislative debate on information-sharing in 2012 (I-07:70). In consequence of the legislative failure, Executive Order 13636 followed in 2013 (I-07:70–71). Apart from the DHS-DoD fight, one policy expert highlights the loss of influence of the Departments of Commerce and State compared to the strong position of DoD, the NSA and also the FBI (I-08:82) – headed by "the FBI Director who is now seen as an intelligence chief as much as he is seen as a policeman" (I-08:82–83), which also could be seen in the discourse examined in this study.

Experts also attribute the government "a poor job of discussing cyber risk" (I-09:95) towards the public and a communication strategy that is "informed more by tactical considerations than strategic ones" (I-08:84), i.e. oriented towards the purpose of funding or legislation: So, some political actors have been "hyping up the threat in order to scare Congress into passing the legislation" (I-08:84). This is confirmed by my findings. Regularly, discourse participants call on Congress to pass legislation. As to the funding, one expert notes the "dilemma" (I-07:72) of civilian agencies like DHS: They are "in a tougher position than DoD because they can raise the threat and will get more funding for it, whereas if you start pushing against that and you say that the threat is actually not as big, then you also get less money, which is not in your own self-interest" (I-07:72).

The institutional fights and the dynamics mentioned by the interviewed experts are an important finding with regard to the background of cybersecurity policy, 'hidden' from the official discourse. In the official discourse we can only detect that, from the beginning, actors started to figure out a good balance of roles and responsibilities and also tried to find models of cooperation. For example, already in 2010, a cooperation memorandum between DoD and DHS is mentioned. The example of the *National Cyber Incident Response Plan* (NCIRP, 2016), defining (again) the roles of DoJ/FBI, DHS, and the intelligence community, shows that this process was ongoing over the examined period and remained, at least in part, unresolved. The presented findings from the interview data give indications, why. In addition, it has to be mentioned that interviewed experts from the political sphere

acknowledge that cybersecurity risks constitute a challenge and they see themselves in a learning process (I-06:59).

4.2.3 Overarching Frames in the German Discourse

Aggregating and interpreting the frame elements identified in the German executive discourse, I find two overarching frames: a "security of supply frame" and a "moderation frame". Both frames start from the common problem definition that cyber risks are serious, increasing, and evolving risks with an – at least potentially – massive negative impact for society. In the interview data, policy and executive experts mention a broad range of different risks, ranging from hacktivism, cybercrime, attacks by state and non-state actors to (potential) cyber attacks on critical infrastructure (see for example I-12:132; I-15:183–184).

4.2.3.1 The Security of Supply Frame

The *"security of supply frame"* highlights the articulated need for a stable and continuous supply with services of critical (information) infrastructure. The protection of critical infrastructure in general is a longstanding, very important topic in the German discourse and on the political agenda since long time, which is documented by the *National Plan for Information Infrastructure Protection* (NPSI) from 2005 (Bundesministerium des Innern 2005). This is confirmed in the interview data. A BMI representative describes the NPSI as Germany's "first cybersecurity strategy" (I-14:169, own translation). The reason for major changes in Germany was an "attack on the federal administration in 2004 that constituted a wake-up call" (I-14:169, own translation) and that lead to a restructuring process in the administration regarding crisis management, exercises, and strategies (ibid.): "We have had the IT attack in 2004, we developed a strategy in 2005, we set up the implementation plans for critical infrastructure and the federal administration in 2006, we developed the respective papers, created coordination bodies in the federal administration et cetera. So, I can say that we took the very first occasion in order to improve ourselves without having had a major crisis" (I-14:169, own translation). The two implementation plans of the NPSI strategy – one for the federal government (*UP BUND*) and one for the critical infrastructure in general (*UP KRITIS*) – were finally published in 2007 (I-14:169). So, they can be seen as early political milestones confirming the security of supply frame.

Another aspect that the interviewed BMI expert mentions is the set-up of the exercise series on critical infrastructure (I-14:169), the so-called *LÜKEX* existing already since 2004. In 2011, the exercise focused on IT and the BMI official describes it as "the first nationwide IT exercise in Germany, in which the federal government, five *Länder* (…) as core countries as well as a number of critical infrastructure companies participated" (I-14:172, own translation). The IT Security Law is qualified as another important milestone (I-14:171), so that we can state a continuation of the security of supply frame during the examined time period.

Also, several interviewed policy experts accord a high importance to critical (information) infrastructure in Germany. One expert articulates: "I think, in this area – critical infrastructure protection, IT security, systems security – there is close cooperation in the sense of a public-private partnership. We are a highly developed country, an industry nation. In this regard, we are definitely well-positioned in comparison to others" (I-17:223, own translation). The importance of the topic is even recognized from outside observers: A U.S. expert states that Germany "has been very pro-active about investing in critical infrastructure protection, very German a view" (I-03:33).

In the security of supply frame, the overall goal is public safety and the state has got "a guarantee responsibility for critical infrastructures" (D-14 BSI 2015:41). So, the idea of security of supply is closely connected to the state and its agencies. Cybersecurity is perceived as key enabling piece for critical infrastructure. The state actively communicates its "responsibility for public IT security" (D-61 BMWi 2014:33) and that it wants to play its "part in protecting society and the economy in the digital age" (ibid.). This role of the state is confirmed by the interview data. One policy expert explains: "The federal government (…) has in mind Germany's welfare and security. And that is why the term critical infrastructure not only covers the federal government's IT applications and that their websites and servers (…) work, but also the critical infrastructure for the economy, transport, energy, banking and so on. In these areas, the state is responsible for defending against threats as well" (I-16:203, own translation).

In the examined official German discourse, Stuxnet is very prominent and perceived as dramatic event demonstrating the actual vulnerability of critical infrastructure. So, Stuxnet

works as wake-up call and triggers and advances a more proactive discourse and political action. I find confirmation in the interview data for the importance of Stuxnet (I-13:153; I-15:183). An interviewed BMVg official qualifies Stuxnet as "eye-opener with actual physical damages in the real world. So, it became clear that truly targeted attacks can cause such damage" (I-13:153, own translation). Also, the attacks in Estonia are mentioned by the expert as important event: The attacks constituted "a certain wake-up call not only for Estonia, but also for NATO: Attention, external influences on the networks can cause actual impacts. Of course, in theory, this was clear and tested before. But now, it became apparent that such things actually happen in the real world, even if consequences were not so dramatic, fortunately. But at least, it is possible that there can be dramatic consequences when you attack critical infrastructure. Just think about long-term blackouts for a large part of the population, that would have dramatic consequences, obviously. Certainly, this led to a change in NATO's thinking or to an accelerated thinking and higher awareness" (I-13:152–153, own translation). Moreover, the attacks in Georgia constituted an important event from a BMVg point of view because of the combination of a "conventional attack accompanied by activities in cyberspace" (ibid., own translation).

In the examined discourse, the drivers of dependence and connectivity are also prominently articulated in the context of critical (information) infrastructure: The "nervous system of modern societies" (D-45 AA 2013:5, own translation) is at stake and numerous scenarios illustrate the severe consequences of a disruption or failure in supply. The cyber attack on TV5Monde by terrorists is articulated as another worrying type of threat for critical infrastructure and the security of supply. In short, the "increasing complexity and vulnerability of information infrastructures" (D-03 BMI 2011:3) is seen as great threat. However, it is clear for discourse participants that there is no "100 percent protection" (D-29 BBK 2016:6, own translation), thus no absolute security. Rather, above all regarding IT, there needs to be a "risk culture accepting a small, but not inexistent probability of disruptions of tolerable extent" (ibid., own translation). This stance is confirmed by the interview data. There is a consensus among the interviewed experts that absolute (cyber)security is impossible and that the provision of different levels of cybersecurity is necessary depending on the respective protection purpose (I-13:149–150,155; I-14:165–166; I-15:185). As an official of BSI explains: "We always have to be aware of the fact, that there is no 100 percent

security – also in the digital realm. Sometimes, we think that we should have absolute security (…), especially in the digital realm. But that does not exist. Neither does it exist in the normal world. (…) Regarding IT, people sometimes tend to require that massive walls are stood up (…), in order to really protect things. What I want to say: There has to be graded security" (I-15:184–185, own translation). The BMVg official confirms this aspect and adds that too much security can come with a disadvantage, too: "There cannot be 100 percent security. You can try to improve IT security, so it corresponds to the state of the art. You do, what you can do. Too much does not only mean very high cost, but ultimately also limitations in operational capability, as you have to exchange data. That is the intention and purpose of networks" (I-13:149, own translation).

The state's mandate to protect citizens from cyber-related risks is presented as most important problem-solver in the security of supply frame, albeit in cooperation with the private sector and society in general. Regarding society, all have to do their part. Regarding the private sector, UP KRITIS is an important mechanism. Also, the goal of a strong national IT economy contributes to better cybersecurity and so, to improving the security of supply with essential services. However, despite the acknowledged necessity of the private sector in resolving cyber risk issues, the state is attributed a leading and controlling role. This aspect becomes especially clear in the creation of the IT security law, when the state uses its rule-making power and prescribes mandatory regulation. In a similar vein, other measures show that the state sees itself in a responsible and leading function: Regularly, strengthening and enlarging the respective agencies, most notbably BSI whose responsibilities are greatly extended during the considered period, or creating new institutions is presented as solution for coping with cyber risks. Among these bodies, there are the *National Cyber Response Centre* and the *National Cyber Security Council*. The interviewed experts from within the government evaluate both as useful and well-working bodies (I-13:155–156; I-14:169–170; similarly I-15:199). The BMVg representative evaluates the Cyber Security Council from his personal experience: "I repeatedly participated in meetings (…). I was very positively surprised about the concreteness of the exchanged information. (…) I have to say that the persons that regularly participate and contribute [to the Council, K.U.] have a pretty good level of knowledge. So, you can reach highly informed proposals, at least. On the other side, it is no operative body really taking decisions that apply to all. (…) But the fact is that we live

in a democracy with department roles and responsibilities, so there is no central governance that can simply decide about all the measures at this table and enforce them. That is not the way it works (…). Everyone has to take away things for his department and implement them. And everyone can contribute to improve the state of knowledge. I think, this body is good and important. Of course, time and again, there are new questions that have to be taken into account and discussed. But everyone can contribute to this, every department can co-determine the agenda" (I-13: 155–156, own translation). Regarding the Cyber Response Centre, the interviewed BMI official acknowledges that "it has got only ten employees, but there are (…) the liaison officers of the single sending agencies that, in turn, have the whole agency as back-office. So, we can pool the hundred experts in every single case. IT is so multifaceted that we cannot place all the experts in one huge center" (I-14:169–170, own translation). In contrast, interviewed policy experts are very critical: One expert explains that "substantially, not much happened" (I-12:135, own translation) in Germany's cybersecurity policy since 2007, and that the newly created bodies are "only paper, in the end" (ibid., own translation). Another expert finds that cooperation in the National Cyber Response Centre could be more effective (I-18:237).

In the examined discourse, in order to create cybersecurity, favored solutions not only address the protection of critical information infrastructure, but also its resilience in the event of an attack – which also confirms the problem definition that cyber risks are real. All in all, a holistic set of measures addressing prevention, reaction, and sustainability is implemented. The security of supply frame also applies to the European and international dimension of German cybersecurity policy, which can be seen for example in the German support for the *European Programme for European Critical Infrastructure Protection* (EPCIP) or the *Directive on security of network and information systems* (NIS).

The security of supply frame is closely linked to and emphasizes the strong role of BMI and its subordinate agencies in the field cybersecurity policy. With a view on the examined period of time, it turns out as a continuous and very stable frame. The special role of BSI is also underlined by the interviewed policy experts. One expert notes that "BSI grows stronger and stronger" (I-12:135, own translation, similarly I-17:223). As to the ministries, BMI is clearly seen as the strongest player by the interviewed executive experts: It is called "a self-

assertive department" (I-11:119, own translation, similarly I-13:156–157; I-14:171). This is also due to the fact that the security agencies and, with regard to cybersecurity, most notably BSI, are in the realm of the Federal Ministry of the Interior (I-14:166–167,171).

4.2.3.2 The Moderation Frame

The *"moderation frame"* is the second overarching frame in the German discourse. It represents a strong and recurring frame regarding the communicated attitude and messages of discourse participants as well as political actions launched. It implies a reflected, reserved attitude and a defensive, passive or at least hesitant approach regarding political action. The moderation frame implies a cautious and critical stance towards cyber risks and digitalization in a more global sense. The problem definition of cyber risks in this frame is as outlined above (serious, increasing etc.). However, it is vey important to discourse participants to be moderate in the sense of being reflected, not to exaggerate, not to send signals of unnecessary alarm in their communications.

Manifestations of this frame can, for example, be found in statements where discourse participants articulate that a cyberwar is unlikely and that this term is misleading. Without underestimating cyber risks and their potential impact, discourse participants seek a certain appeasing stance. In the interviews this is taken up in the sense that several interviewed experts explicitly point to the near absence – "with very few exceptions" (I-12:132, own translation) – of large cyber attacks with effects in the physical world, for example on critical infrastructure (I-12:132; I-13:149) or attacks comparable to the ones in Estonia (I-15:189).

More with a view on political action, we find the moderation frame also in international cybersecurity policy as advanced in the discourse above all by BMVg and AA: These actors mainly want to avoid escalation and escalatory behavior in cyberspace – by others, and so they demonstrate their own peaceful attitude and behavior as good example. So, they promote confidence-building measures or exchange white papers on cybersecurity with Russia. For a long time in the examined period, discourse participants notably from BMVg and AA use a prudent discourse, emphasizing the civilian side of things and the importance of BSI's role, the "defensive approach" (D-45 AA 2013:10, own translation) of German cyber policy, they warn against offensive cyber capabilities and oppose an arms race in

cyberspace. Important overall goals confirming the moderation frame are creating trust, rules, and cooperation with (European and international) partners. These aspects are also supported by the interview data. The official of the Federal Foreign Office underlines the importance of trust and the multi-stakeholder model for an open and secure internet based on human rights (I-11:125–126): "When we talk about cybersecurity here, our focus is: We need to create trust. And we need to get all aboard. We as Foreign Office indeed have the mantra: Multi-stakeholder is key, therefore you need trust" (I-11:125, own translation). The official also unterlines the necessity to communicate with all parties, including those with diverging positions such as Russia or China (ibid.:115): "We basically talk to all. (…) Regarding the Internet, you cannot say: We do not talk to them now, because there might be a risk. Then, you precisely talk to them. So, we still communicate intensively with Russia or China, because you cannot simply close the channel and then, you do not know anymore what happens" (I-11:115, own translation). The representative of the Federal Ministry of Defence emphasizes the need for international cooperation and finding "global solutions" (I-13:157, own translation), for example regarding "responsible state behavior" (ibid.:152, own translation) in cyberspace. He also stresses Germany's de-escalatory intentions: "We try to be transparent and to encourage others to be transparent as well. Hopefully, this could at least limit severe state-sponsored attacks, for example in conflicts, because you do not even allow that an escalation or arms race can start" (I-13:157–158, own translation). These articulations support the moderation frame.

The representative of the Federal Ministry of Defence confirms the civilian character of the cybersecurity strategy (I-13:160) and sees "no special role [of the Bundeswehr, K.U.] for cybersecurity in Germany" (I-13:161, own translation) – as this is "the responsibility of the Ministry of the Interior, for example" (ibid., own translation). These assessments confirm the findings of the discourse analysis and the moderation frame.[99]

With a view on domestic cybersecurity policy, the moderation frame is found in many parts of the discourse where discourse participants communicate the need for reflection, rather than rushing things. It becomes apparent, for example, in the larger discourse on

[99] Until 2015, when BMVg took a stronger role. However, as the interview data is from 2014, the findings are consistent.

digitalization that accompanies the cybersecurity discourse: Frank-Walter Steinmeier uses the expression of "uncharted territory" (D-48 AA 2014:3, own translation) for describing the digital revolution and points to the need of orientation in order to find out how to get along with the internet in a more global sense, how to balance freedom and security in cyberspace. Also, discourse participants address the doubts, uncertainty, or even fears existing in Germany with regard to digitalization. They regularly emphasize to take serious the population's skepticism and concerns and to use an inclusive approach to shape digitalization. Creating trust in digitalization among the people and taking care of cybersecurity are important tasks in this regard. So, their goal is not a rapid and forced process or hectically pressing ahead with political action, but a reflected version of digitalization, as becomes clear, for example, in the statement of the "digitalization with a sense of proportion" (D-63 BMWi 2015:49, own translation).

Moreover, there is a strong presence of weighing chances and risks in the German discourse: On the one hand, there is skepticism towards digitalization as a whole and an emphasis on the downsides of connecting everything, for example by acknowledging cyber risks and the dependence on information and communication technologies aggravating the risks. So, there is a skeptical view of technology as risk-enabler. On the other hand, discourse participants underline the potential of digitalization and the role of cybersecurity for using this potential. The political goal following from this reflection process is finding a middle way of balancing chances and risks and of remaining sovereign and self-determined. The process of implementing a "balanced digitalization" (D-63 BMWi 2015:7, own translation) is lead by the state based on its political mandate (see also above) and acting in the role of a 'moderator'.

In practical political terms, the moderation frame partially implies a 'wait-and-see approach' embodied in a passive behavior by some executive actors. I find several examples of late action, notably with BBK, AA and BMVg that stay quiet in the discourse and in their actions for a comparatively long time. For example, BBK despite its special expertise and responsibility in the field of critical infrastructure takes up the topic of cyber risks for critical infrastructure only very late. The example of the Federal Foreign Office is also confirmed by the interview data. The official of the Foreign Office acknowledges that the department

started working on cybersecurity "comparatively late" (I-11:119, own translation). In addition, the moderation frame implies to accept things as they are to a certain extent. Regarding cyber risks, the interviewed BMVg representative explains that "you cannot avoid it, unless you would really withdraw from all the networking, as some suggest. But I think, that this is not realistic. So, you have to see that you do, what can be done, but you also have to live with the residual risk, because there is no 100 percent security. (…) If necessary, you have to adjust things, when you are taught a lesson by attacks. Otherwise you just have to live with it" (I-13:155, own translation).

The moderation frame is present in various dimensions during the examined discourse period as shown above. However, the changes initiated in 2015 regarding the military context – the creation of the new cyber division – show that discourse and political action leave the moderation frame at least in this specific area, as the roles of BMVg and Bundeswehr are strengthened and interpreted as more active.

4.2.4 Further Findings from Interview Data on the Background of the German Discourse

In the following, I report some more findings from the interview data on the background of the official discourse. The findings cover topics "hidden" from the official discourse, most notably, how involved executive experts as well as outside policy experts assess coordination, cooperation and communication efforts in the area of cybersecurity policy.

Internal views within the federal government with regard to the roles and responsibilities in the field of cybersecurity policy are diverging. An official of the Federal Foreign Office explains that roles and responsibilities are fragmented and that different ministries have the lead in different issues depending on the expertise (I-11:116). In general, every ministry brings in its view and expertise, for example, into a strategy like the Digital Agenda (I-11:118), and then, an intensive coordination and negotiation process follows between the departments in order to define the government's view (ibid.:120–121). However, this operating mode makes processes "a bit slow" (ibid.:116, own translation). In the official's view, the fragmented approach is "necessary, but frustrating, at the same time" (ibid.:117, own translation). In order to improve processes, a "coordination office in the chancellery" (ibid.:118, own translation) would be an appropriate solution according to the

representative (ibid.). The expert also points to the small number of persons dealing with cyber issues in the federal government – too small in this view (I-11:122–123). Other government representatives are less critical. An official of the Federal Ministry of the Interior emphasizes the close cooperation between the departments (I-14:170) and that "coordinations work very, very well" (I-14:170, own translation, similiarly I-13:155).

As to the question if there is an overarching executive cybersecurity strategy, there are diverging views. According to the representative of the Federal Foreign Office, there is "no holistic strategy" (I-11:118, own translation) from the government due to the fragmented responsibilities (ibid.). In contrast, the BMI representative sees an overarching strategy because of the close cooperation between the main departments and their basic consensus in key issues (I-14:170). Again, outside experts' views are very critical. One policy expert finds that the cybersecurity strategy from 2011 does not qualify as strategy, as there is a lack of prioritization, a lack of defining goals and means (I-12:134, similarly I-12:134, I-16:205 with regard to the Digital Agenda). Rather, he diagnoses a "fight between different departments on responsibilities" (ibid., own translation, similarly I-16:207). Also, experts perceive that all departments "have their own agenda" (I-18:248, own translation) and that there are conflicting goals within the government, for example a high level of cybersecurity vs. the interest of breaking encryption for security interests (I-17:222, I-18:249). In order to clarify roles and responsibilities as well as political priorities, one expert states that the "power of the chancellor to determine policy guidelines would be required" (I-12:136, own translation). However, Angela Merkel does not set cybersecurity proriorities in his view (I-12:136). In a similar vein, another policy expert assesses that unfortunately, cybersecurity policy is "not yet a matter for the boss" (I-16:206, own translation) in Germany: Angela Merkel does not take a particular strong stance on the topic (ibid.). Rather, she openly minimizes ambitions by speaking of the new character of digital topics and that there is the need to understand all these things, which was most famously articulated in the "unfortunate quote of the uncharted territory" [*"Neuland"*, K.U.] (I-16:206, own translation). Whereas he nevertheless acknowledges some progress in cybersecurity policy as "within departments, competencies are institutionalized" (I-16:206, own translation), another expert diagnoses a general lack of seriousness in dealing with cyber issues (I-17:224). Overall, these assessments correspond to the moderation frame as the observed passivity,

reservation, and lack of guidance can be interpreted in the sense of a 'wait-and-see attitude'.

To a certain extent, this is also mirrored in the government's communication, as interviewed policy experts note. A policy expert finds that "there is not much communication about cybersecurity in Germany" (I-12:144, own translation) and that the communication that is made, is "strongly fragmented along the particular interests of single political actors" (ibid., own translation). In a similar vein, another expert states that communication "remains a bit diffuse" (I-16:215, own translation), above all because of the already stated "lack of clear guidance" (ibid., own translation). In consequence of the weak strategic stance of the chancellor, he perceives "many different voices and a lot of unresolved interest conflicts" (ibid., own translation).

The presented findings support the assumption that cybersecurity policy still presents a big challenge in Germany and questions on departmental roles and responsibilities as well as strategic and communication issues are not yet perfectly resolved.

4.3 Comparison and Conclusion on Discourse Analysis

The discourse analysis resulted in numerous findings. Above all, two overarching frames were identified for each country: the homeland security frame and the technological leadership frame for the United States, and the security of supply frame and the moderation frame for Germany.

As to the discourse-related *expectations* formulated at the beginning of the study (section 2.3), I find the following results: For the United States, the importance of security associated with critical (information) infrastructure protection can be clearly confirmed for the examined discourse. This aspect is most notably mirrored in the homeland security frame and also prevails over economic aspects. Taking into account previous literature that examined the United States until 2008 (Dunn Cavelty 2008) and found that critical infrastructure threats turned out as particularly important topic (ibid.:132), we can extend this finding for the period until 2016. Also, the strong military component in the discourse as well as the measures taken can be confirmed. It is most visible in the creation of U.S. Cyber

Command and the declaration of cyberspace as military operational domain, but also in the second DoD cyber strategy and the military actors' continued aspirations within the executive branch for responsibilities in the cybersecurity domain as emphasized by the interview findings. The concept of exceptionalism is associated in literature with the superiority of the United States and their function as role model having the mandate to spread their values (Fluck 2016:19-20,23), among other things. Applied to our context, the expectation of exceptionalism is supported by the technological leadership frame, most notably in the self-perception of the United States as "the nation that invented the Internet" (U-02 WH 2009:3) having exceptional innovative powers as well as the self-proclaimed "special responsibility to lead a networked world" (U-22 WH 2015:12). These aspects are illustrative of exceptionalism as they express the superiority of the United States. Moreover, the international cybersecurity policy of the United States is an example, above all in the vision of a "free, open, and secure internet where universal human rights are respected, and which provides a space for greater progress and prosperity over the long run" (U-47 State 2011:5–6). By promoting this vision, the United States also spread their values internationally. Finally, "economic, technological and military superiority" (Fluck 2016:24, own translation) as well as an "orientation towards unilateralism" (ibid., own translation) have been associated with exceptionalism in literature. These elements can be found in the U.S. military cybersecurity discourse as presented above.

Regarding the expections for Germany, the strong presence of critical (information) infrastructure protection can be confirmed by the discourse analysis, above all in the result of the security of supply frame that clearly points into this direction. Moreover, the orientation towards European policy is given in the discourse. There are specific EU and European references, but very often European and international references are communicated together and attributed the same level of importance. The expectation that discourses – in both countries – get more specific and differentiated in the course of time is fulfilled. Indeed, later communications and documents are often much longer in terms of pages and show a much higher degree of specification and details. This can be seen, for example, when comparing the first and the second cybersecurity strategy in Germany or the first and the second cyber strategy of DoD in the United States.

Some further *comparative aspects* are presented in the following. Given the "breakdown of the distinction between domestic and foreign spaces" (I-07:65) by the advent of cyberspace and the risks emerging from it, both countries find themselves challenged by the new situation. There are similarities and differences in their respective reactions.

The United States takes a very pro-active and self-assertive stance in its discourse and actions. Assured by the faith in its innovative capabilities and its open and positive attitude towards technology and digization more generally, the United States is convinced to be able to stay "on the cutting edge of this new technology" (U-60 DoD 2012:2) and to defend its leadership. At the same time, the country develops a pragmatic approach in the course of time ("cyber risk must be managed" (U-37 DNI 2015:1)). However, for special situations, there must be special means for reaction: The United States is not hesitant in declaring what it will do in the case of a severe cyber attack by an adversary – it will react with "all necessary means" (U-09 WH 2011:14) including military ones as ultimate option. Also, the country is not hesitant in blaming and, if possible, sanctioning others for severe attacks on the United States such as in the case of North Korea. China is especially prominent in the U.S. focus. So, on the one hand, we find a cybersecurity discourse that is oriented towards the outside. That means, it is oriented towards cyber actors anywhere in the world and foreign countries – to let them know that the United States is ready and will act and, albeit less importantly, to encourage allies to cooperation. On the other hand, the cybersecurity discourse is directed to the domestic sphere. That means, towards Congress to pass legislation, but also towards the private sector, without which a successful cybersecurity policy is not possible, and towards the population at large in order to encourage citizens to do their part. The orientation towards the inside and the outside also mirrors the institutional competition between military and civilian actors. Nevertheless, it has to be noted that the military side successfully advocated its views in the examined discourse and, ultimately, could also leave its mark regarding measures.

For Germany, in contrast, we find a rather inward-looking perspective: The country has got a strong and longstanding focus on a stable and continuous supply with services of critical (information) infrastructure. The state presents itself in a leading position and willing to fulfill its "guarantee responsibility for critical infrastructures" (D-14 BSI 2015:41) and its "responsibility for public IT security" (D-61 BMWi 2014:33). At the same time, Germany is still in a process of finding its relation to digitalization in general. The "uncharted territory"

(D-48 AA 2014:3, own translation) needs to be explored and evaluated – at best, in an inclusive approach that integrates skepticism and fears of the population. The overall goal is to carefully balance chances and risks. Against the backdrop of this situation and the barely visible chancellor who does not use her guideline competency in the field of cybersecurity, the strong player on the side of domestic security – BMI – is well-positioned to push forward its policy. BMI is supported by a powerful set of four agencies working on different aspects of cybersecurity: on the technical-analytical side (BSI), on the side of investigation and law enforcement (BKA, BfV), and with a perspective on critical infrastructure (BBK). It is illustrative that both German cybersecurity strategies are published by BMI. However, despite a de facto institutional center of gravity at BMI, there are fragmented roles and responsibilities, coordination issues as well as institutional competition between the departments. As in the United States, the inward-looking perspective encourages the cooperation with the private sector. There is also a component of the cybersecurity discourse directed towards the outside, albeit not as prominent as the inward-looking part. It mainly advocates a de-escalatory, appeasing stance and is oriented towards confidence-building and encouraging cooperation with partners. Finally, it has to be noted that the discourse is not uniform: Some participants (BBK, AA, BMVg) remain passive for a comparatively long time. Another interesting evolution is the development towards a more active role of BMVg and the military in 2015 with the creation of a new cyber division.

Overall, the German approach proceeds in a rather moderate fashion in contrast to the United States' very pro-active stance. Striking differences between both countries are most notably found in their leadership (pro-active president vs. passive chancellor), their attitude towards information and communication technology as well as the behavior of the respective defense actors.

5 Analysis of Regulatory Examples in the United States and Germany

In the following chapter, we will turn to cybersecurity regulation in the United States and Germany, more precisely, a specific regulatory example in each country that represents a discourse effect in the analytical approach of this study. At first, I describe the selected regulatory examples. In a second step, I examine to which extent both examples match with the regulatory style expected for the respective country.

5.1 Overview on Selected Regulatory Examples

5.1.1 Executive Order 13636 and the Cybersecurity Framework in the United States

In February 2013, the Obama administration advanced its cybersecurity policy efforts by issuing two documents: On the one hand, the administration issued *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience* (PPD-21) (WH 2013a), and, on the other hand, *Executive Order 13636: Improving Critical Infrastructure Cybersecurity* (EO 13636) (WH 2013b). Both documents are an expression of the "need for holistic thinking about security and risk management" (DHS 2013). Whereas PPD-21 addresses critical infrastructure in general, the EO focuses on the aspect of cybersecurity, which is why it is especially interesting in the context of this study. The EO has got several provisions, among them information sharing between the government and the private sector (WH 2013b:2). However, most importantly in the context of the study, the EO directs the *National Institute of Standards and Technology* (NIST) to establish a "Baseline Framework to Reduce Cyber Risk to Critical Infrastructure" (ibid.). This framework initiated by the EO is what I shed light on as regulatory example or discourse effect in the United States. In the following, I use the abbreviation "CSF" for the cybersecurity framework.

Overall, the CSF "shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk" (ibid.:5). Therefore, the CSF has got the function to develop a "set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks" (ibid.:4). These standards shall be voluntary (ibid.).

The CSF is composed of three main parts: the “Framework Core”, the “Framework Implementation Tiers”, and the “Framework Profile” (Stine, Quill, and Witte 2014:2–3). The *Framework Core* comprises five functions: “Identify, Protect, Detect, Respond, Recover” (ibid.:2). For each function, contents are presented in an overview management fashion (“Category”) and in a more detailed technical outcome-oriented way (“Subcategory”) (U-69 Commerce 2014:19–36). Moreover, references of national and international standards are added to each section (ibid.). For example, regarding the function “Protect”, one category is called “Access Control” (ibid.:23–24). In this category, we find several specifying technical subcategories, such as “Identities and credentials are managed for authorized devices and users” (ibid.:23) or “Network integrity is protected, incorporating network segregation where appropriate” (ibid.:24). In addition, references of applicable standards (ISO/IEC, NIST etc.) are listed (ibid.:23–24).

The *Framework Implementation Tiers* can help an organization to classify the cyber risk assessment and management practices that are currently used (U-69 Commerce 2014:9). There are four different tiers (“Partial”, “Risk Informed”, “Repeatable”, “Adaptive”) describing risk management, cybersecurity awareness, and information sharing practices with external actors (ibid.:10–11). The tiers represent “a progression from informal, reactive responses to approaches that are agile and risk-informed” (Stine, Quill, and Witte 2014:3).

Finally, the *Framework Profile* shall help an organization to understand and improve its state of cybersecurity: By taking the elements of the Framework Core that are useful from the point of view of the individual organization’s situation, the purpose of this part of the CSF is “to identify opportunities for improving cybersecurity posture by comparing a ‘Current’ Profile (the ‘as is’ state) with a ‘Target’ Profile (the ‘to be’ state)” (Stine, Quill, and Witte 2014:3). In this way, gaps in cybersecurity can be identified and addressed (U-69 Commerce 2014:11).

Overall, the purpose of the framework is “to improve cybersecurity information sharing and collaboratively develop and implement risk-based approaches to cybersecurity” (U-43 DHS 2013:9). The framework shall notably help implement the use of “strong cybersecurity practices” (ibid.). It is a voluntary framework that was created with industry actors in a cooperative effort (U-69 Commerce 2014:3).

5.1.2 The IT Security Act in Germany

The Bundestag adopted the *IT Security Act* (ITSiG) in July 2015 (Bundestag 2015b). BSI sees the law as "another and more far-reaching expression of the responsibility to protect the state has got towards citizens, the economy and its own institutions and administrations" (BSI 2017:9, own translation). Moreover, the law represents a reaction on the perceived failure of the former approach regarding the protection of critical infrastructure that was based on voluntary participation (ibid.).

The IT Security Act stands for a "holistic framework for the cooperation between state and companies for more cybersecurity in critical infrastructures" (BSI 2017:11, own translation). More specifically, the IT Security Act contains two requirements: On the one hand, owners and operators of critical infrastructure have to "implement IT security according to the 'state of the art'" (BSI 2017:11, own translation). What exactly the state of the art consists of can be defined in "sector-specific security standards" (BSI 2017:25, own translation) by sector-specific working groups, the results of which are approved by BSI (ibid.). On the other hand, there is a reporting obligation for owners and operators of critical infrastructure: They have to "report significant IT security incidents to BSI" (BSI 2017:11, own translation). In order to clarify the applicability of the IT Security Act for different companies, the directive "BSIKritisV" from May 2016 (part 1) and spring 2017 (part 2) provides criteria such as the "degree of supply" (ibid.:16, own translation). If an operator supplies more than 500,000 people, his service is considered as "critical" in the sense of the law and the company is affected by the law (ibid.). Within two years, companies need to implement appropriate IT security measures; and within 6 months, a point of contact has to be established, so companies can report significant incidents (ibid.). There are specific criteria (in the BSI law) that help decide, if an incident has to be reported; this is notably the case for an "extraordinary IT incident" (BSI 2017:28, own translation). In case of an actual disruption of services as a result of the IT incident, the operator's name has to be reported (ibid.). Analyzing these and other sources of information, BSI develops a situation report (ibid.).

5.2 Analysis of Regulatory Examples

I shed light on three elements – 1) openness and control of the regulatory process, 2) procedural rules, and 3) orientation of policy-making and the role of science – in order to analyze if and to which extent both regulatory examples can be understood as examples

following the tradition of the country's regulatory style. Moreover, I reflect on the larger context of regulation regarding cybersecurity in both countries.

5.2.1 The Cybersecurity Framework and the Adversarial Style

Regarding the *openness and control of the regulatory process*, the process of developing the CSF can be described as very transparent and collaborative. This was explicitly mandated in the executive order: A consultative process with critical infrastructure stakeholders was required, such as owners and operators of critical infrastructure, *Sector-Specific Agencies* (SSAs) and the NSA (WH 2013b:5). Also, the *Critical Infrastructure Partnership Advisory Council* (CIPAC) and the *Sector Coordinating Councils* (SCCs) should be consulted (WH 2013b:4). According to NIST, the "Framework has been developed and promoted through ongoing engagement with, and input from, stakeholders in government, industry, and academia" (NIST 2018a). Part of this process was an initial *Request for Information* (RFI) in February 2013 (ibid.). NIST precisely described the methodology how it analyzed the responses to the RFI and presented detailed results in the form of important basic categories and topics, examples, and some statistical information on how many responses discussed a special topic (NIST 2013a). All responses were published online (NIST 2013b). The material was used in the further process (NIST 2013a:1). Moreover, five workshops were held between April and November 2013; they were public and took place in different places in the United States (NIST 2018a). Again, the workshop materials and protocols were published on the NIST website (ibid.). So, it can be stated that the CSF was indeed developed in an "open public review and comment process" (WH 2013b:5) as required by the executive order. The openness and transparency in the process correspond to the adversarial style. One interviewed expert appreciates that "[a] lot of people worked on the executive order, and there are parts in it that reflect different things that different parts of the U.S. government can do to help improve cyber security" (I-10:101). As a result, the executive order benefitted from this process and the interagency-work and contains "an excellent balance of security, but also commerce" (I-10:102) in the view of this expert.

The characteristic of openness was also perceived by participating stakeholders and experts as the interview data shows. One expert in industry notes: "We have a lot of opportunity of input. We are not always listened to, but overall, it is very much a collaborative approach" (I-10:111). The expert's organization was "very involved in the NIST framework" (I-10:106) and

notably provided input and expertise by making comments on draft reports and in meetings (I-10:106-107). According to this expert, NIST acted in the role of a "convener" (I-10:103). This included primarily to "bring together a lot of stakeholders to work on a tough issue" (ibid.) and "to push industry along" (ibid.). Another expert notes that the process for developing the CSF is more open compared to prior legislative initiatives in the field of cybersecurity (I-09:93) and that it is thus "far more likely to adopt general consensus-based standards" (ibid.). So, in this view, the open character of the process has got a positive impact on the overall result. The administrative side welcomed the overall process, too: In its statement for the release of the CSF, President Obama qualified the process of developing the framework as "a great example of how the private sector and government can, and should, work together to meet this shared challenge" (U-17 WH 2014:2).

In concluding on this first aspect of openness and transparency, the proceeding in the case of the CSF corresponds to the tradition of the adversarial style: the process is transparent, and third parties and the public are integrated, for example by the opportunity to comment. However, there is even more: The process is characterized by a strong emphasis on including diverse stakeholders and working together in a collaborative effort, by a very active cooperation with third parties, which is not typical for the adversarial style, but rather corresponds to the tradition of the corporatist style, thus an interesting finding.

As to the *procedural rules*, the EO mandated a very precise proceeding as already mentioned in part above: There was a clear mandate regarding the goal of the process – the development of a "Baseline Framework to Reduce Cyber Risk to Critical Infrastructure" (WH 2013b:2). Moreover, it was laid out whom to consult in what interest. Also, a precise timetable was presented beforehand: The preliminary version of the CSF shall be available 240 days after the EO; the deadline for the final CSF is one year after the EO (ibid.:5). In line with these provisions, NIST presented the final CSF in February 2014 (U-69 Commerce 2014). In this sense, the proceeding corresponds to the characteristic of the adversarial style of precise procedural rules. From the beginning, the intention was to create a voluntary framework and thus a rather soft way of regulation. Nevertheless, there were diverging positions on this endeavor, as can be seen in the initial RFI, for example (NIST 2013b), and those could be captured and integrated in the process. As one expert notes, "the framework

process is helping to drive people's understanding a little bit better" (I-08:87). As to this aspect, the CSF can be said to correspond to the adversarial style of regulation.

Orientation of policy-making and role of science. In general, in matters of cybersecurity and, particularly, in the context of the CSF, there are diverging views on the role of science. One observation is that there is a role for science in a rather specific sense: It is not science and evidence in a "classic" natural science perspective, such as in determining threshold values of hazardous substances. What plays a role is to understand technology: One expert points out that "engineers and scientists play many roles, one of which is trying to influence the policy, not in a political way, (…) but just in a reality-based way" (I-10:107). It is about giving input "about, technically, what is going on" (I-10:107). So, their function is to understand and explain technology (I-10:107). Moreover, their function is to draw attention to fields with significant need for research (I-10:107-108). One expert mentions that the formal inclusion of scientists in the domain of cybersecurity is done via "high-level advisory" (I-07:75) as in other policy fields. The *National Security Telecommunications Advisory Committee* (NSTAC) and the *National Infrastructure Assurance Council* (NIAC) are examples (ibid.). Other than certain requirements for scientific input, a lot of input is also "less formalized" (I-10:108), as one expert in industry notes.

Whereas several experts attribute "a critical role" (I-02:19) to academic research, one expert mentions the particularity of cybersecurity being a topic in the realm of national security and thus being "extremely over-classified" (I-03:31): According to this view, there is even a "brick wall in between of actual practioners and academics" (ibid.) hindering a debate. Another expert assumes that "the scientists' opinions are generally subsumed within the private sector, the private sector does not disregard those. I think, the idea of an independent science attitude is a bit of a myth" (I-09:95). Also, he adds that "in this space, there are not really scientific verities like the speed of light is x. There is no clearly effective perfect cybersecurity, it is a series of processes and people buy various products in proportion to their need, (…) – and that goes back to the risk: The financial networks have very different needs than the electric grid or the transportation grid or the agriculture grid (…). So, this is not one-size-fits-all, it is as diverse as the world" (I-09:95). Arguing in a similar vein and emphasizing the diversity of sectors, another expert criticizes the CSF as "too high-level and (…) too abstract to yield any meaning for results" (I-07:76-77).

As to the role of science, these views from the interview data show that there is a need for expert knowledge in a broad sense in the domain of information and communication technology, but also very applied context knowledge of critical infrastructure. So, IT and cybersecurity knowledge and a specific domain or sector knowledge have to come together. One expert underlines the importance of input of a variety of parties, from the national labs to the technology industry (I-06:60). A final aspect regarding sources of knowledge is the strong basis of "Informative References" (U-69 Commerce 2014:20-36) in the CSF to various very well known and established national and international standards of cybersecurity, above all the "ISO 27001" standard[100], which is illustrative of the importance and intent to bring in "pragmatic knowledge" (Renn 2001:408) and objectivity.

Bringing together these observations and concluding on the aspect of science, we can state that there definitely is a role for science, albeit no strict concentration on purely scientific knowledge, but rather on comprehensive technical expert knowledge and "pragmatic knowledge" (Renn 2001:408), which is due to the technological character of the policy field. Even with this restriction, it remains a strong orientation on knowledge, which is why I conclude that, in this aspect, the CSF corresponds to the characteristics of the adversarial style in large parts, although somewhat weaker than in the ideal adversarial model.

Conclusion. Taking into account the three aspects examined before – openness and control of the regulatory process, procedural rules, orientation of policy-making and role of science – I find some of the elements of the adversarial style in the United States as expected, most notably regarding transparency, openness, and procedural rules. The strong collaborative effort in the CSF, however, occurs as an interesting finding as this kind of proceeding is rather typical for the corporatist regulatory style. Also, the special role of technological knowledge in addition to strictly scientific knowledge is interesting to note. In the end, it can be stated that the examined example of the executive order and the cybersecurity framework follow the tradition of the adversarial style in many parts with interesting exceptions.

[100] The standard ISO 27001 provides "requirements for an information security management system (ISMS)" (ISO 2019). In general, the series of ISO/IEC 27000 standards have the purpose to "keep information assets secure" (ibid.), more specifically, they help an "organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties" (ibid.).

5.2.2 Discussion: Cybersecurity Regulation in the United States

In order to reflect on the above findings on the executive order and the cybersecurity framework in a larger context, I add some observations on regulation in the United States, in general, and on cybersecurity regulation, in particular.

Many of the interviewed experts explain that there is a general negative attitude towards regulation in the sense of mandatory requirements in the United States. This attitude is seen as a general attitude in the United States – one expert describes it as "a sort of cultural position" (I-08:87). Another expert notes that the "American approach is often adversarial because regulation is seen as such a strong step" (I-02:21) and also points to the fact that protective regulation, in certain cases, is not perceived as necessary because the United States is a "litigious society" (I-02:21), where the possibility of a lawsuit is seen as "an alternative way" (I-02:21). However, with a view on cybersecurity, tort law does not yet play much of a role, except for data breach cases in some states of the United States, according to experts (I-01:10; I-02:26; I-03:31).

It is interesting to note that the anti-regulation stance is especially powerful in the field of cybersecurity. One expert mentions that the "coalition of opinion from the business sector and the Internet community that makes a reasonably compelling argument that technology develops so quickly that if you try and regulate it you are just going to make life difficult for yourself" (I-08:87). In a similar vein, another expert unterlines that "[t]echnology changes constantly, the threats change constantly and then, business models change" (I-10:110). As a consequence, regulation cannot keep up with this constant change and so, it is "not a very effective approach to cybersecurity" (I-10:110, similarly I-04:39, I-06:58). These experts advocate for a voluntary model such as the CSF that contains "guidance on basic things" (I-04:39, similarly I-06:58) and a role for the government that is "[n]ot non-existent, but limited" (I-06:58). However, there is also the view that "almost nothing that the government can do will save us" (I-09:93) notably because of the speed of changes in technology and the distributed and interdependent character of critical infrastructure across country borders (ibid.:92-93). In contrast to the role of government, experts attribute a "uniquely important" (I-03:29) position to the private sector in the field of cybersecurity or even "the largest role" (I-06:59). Experts see another negative aspect of regulation, that is, companies are busy in complying with the regulation required from them; as a consequence, they are not in a position to innovate effective security mechanisms (I-10:110, I-06:58). As could be seen, the

anti-regulation stance in the field of cybersecurity is strong. Interestingly, experts from within the political sphere and experts from the outside share this critical view. It can also be found on the highest executive level. President Obama declared already in 2009: "My administration will not dictate security standards for private companies. On the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity" (U-02 2009 WH:3, similarly U-65 2010 Commerce:3). A minority of the interviewed experts mentions certain cases, in which regulation might be useful, and that there is a point for the perspective that "you need the specter of regulation to make the lighter touches work because they do require a certain amount of engagement by industry actors to agree to go along" (I-02:21).

In a final step, I want to bring together the CSF with the previous more general remarks on regulation. Therefore, it is useful to shed light on the circumstances of the creation of the CSF. It is important to mention that it came up as a reaction on the failure of legislation; the White House chose a different strategy, became active itself and brought up the EO (I-07:70-71; I-08:86). Before the CSF, there was a long period, in which several legislative proposals were brought up, but none did become law. Two experts note (in 2013) that the *Federal Information Security Management Act* (FISMA)[101], adopted in 2002, constitutes the most recent regulation in the field of cybersecurity (I-02:20, I-07:73). Among the bills under discussion, the so-called *Cyber Intelligence Sharing and Information Protection Act* (CISPA) of 2011 and the *Cyber Security Act* (CSA) of 2012 are particularly relevant. CISPA centered on information sharing[102], whereas CSA focused on the protection of critical infrastructure (I-08:86). One expert explains the main controversies as follows: "[O]ne was whether there should be mandatory legislation or not and the Republicans basically decided that they did not think there should be and there was a lot of politics involved as well. (…) The other side of it was, with whom the private sector should have the relationship within government. Essentially, many of the Republicans felt that they should have a relationship with the NSA. The democrats felt that, actually, it should be DHS that has that relationship" (I-08:86). In the end, both bills failed. The second aspect of the appropriate government point of contact

[101] FISMA "requires that Federal agencies develop a comprehensive information technology security program to ensure the effectiveness of information security controls over information resources that support Federal operations and assets" (U-39 DHS 2009:139).

[102] CISPA tried to introduce legislation for "sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities" (GovTrack 2019).

for information sharing is also an illustration of the more general debate in the United States on civilian vs. military dominance in cybersecurity policy (I-07:70-71).

On a more general level regarding the question of regulation or not, there are two, not equally strong camps in this debate (I-07:74), one side guided by the view that "cyber security is a national security issue and a classic case for the role of government" (ibid.) and the other side favoring a strongly private sector-centered approach (ibid.). Against this background, the EO works as a "kind of in-between-solution" (I-07:74), as one expert describes it. This observation has proven true in the sense that cybersecurity legislation has finally been passed in Congress afterwards in 2015 (Rosenzweig 2015).[103] On the other hand, CSF can still be considered a successful framework as regular updates followed continuously: In April 2018, version 1.1 was released (NIST 2018a). It also had a considerable impact on the international level: A German banking magazine points out that the NIST framework "has been recognized as de facto standard worldwide" (Abel and Leicht 2018:76, own translation).

5.2.3 The IT Security Act and the Corporatist Style

Regarding the *openness and control of the regulatory process* we can state that, in principle, the process of the ITSiG was as transparent and open as every standard legislative process in Germany: The ITSiG was not handled as classified matter, a draft of the ITSiG was put on the government website, and, theoretically, all interest groups were allowed to comment (I-14:176). However, it is striking to note that there was a strong focus of the government on certain interest groups and associations: The government sent the draft bill to selected associations, and it invited those selected associations for a non-public hearing (*"Verbändeanhörung"*) (I-14:176). According to an interviewed expert and participant, there was a broad range of representatives from different associations, but still it was a closed event upon invitation of the government (I-18:239). When the bill is discussed in committees of the Bundestag and in hearings of parliamentary groups, these sessions are also disclosed to the public (I-18:236, I-16:211). One expert perceives the closed character of the Bundestag as "fundamental problem going beyond the cyber topic" (I-16:211, own

[103] The so-called "Cybersecurity Act of 2015" introduces, among other things, regulations on cybersecurity information sharing between private sector entities and the government; the first government point of contact is DHS according to this law (Rosenzweig 2015).

translation), another notes that there is "no tradition" (I-12:144, own translation) of truly public consultations in Germany. While equally acknowledging that the Bundestag is a "quite closed" (I-18:236, own translation) institution towards the public, an expert from a business association notes that the "transparency (…) against the regulated" (ibid., own translation), in this case companies and not the public, is of key importance in his view (ibid.).

According to the government, it is important that processes such as the hearing of associations are kept in a non-public realm as conversations include partially critical security data and no one wants to risk that this knowledge is misused (I-14:176). And, above all, the non-public atmosphere is seen as essential precondition for a trustful relationship with private sector stakeholders (I-14:176). The idea and the benefits of the "cooperative approach" (I-14:176) are regularly articulated from different players in the process: An interviewed official of BMI underlines the necessity and the will of the government to proceed in a cooperative approach, as the IT knowledge and expertise sits in the private sector (I-14:179). The official adds that, in turn of offering a cooperative approach, the government expects that the companies will actively participate and contribute to the process (ibid.), for example by giving input on the question, which company size should be considered as critical and thus be regulated by the law (ibid.:175). At the same time, he is confident that the private sector will collaborate (ibid.:175,179). Interestingly, the business side is equally convinced that the process of cooperating turns out well: The expert from a business association articulates the feeling that the private sector is taken serious and adequately integrated in the process and that the ministry "has a real interest to say: We need to include the private sector" (I-18:242, own translation). Several interviewed experts speak of a longstanding culture of cooperation: "In Germany, we have got a certain culture, also thanks to the associations, so we frequently could resolve issues even if there were (…) diverging goals" (I-15:194, own translation, similarly I-16:210, I-14:175,178). The cooperative approach is also part of the official discourse in documents of authorities, for example in a BSI publication discussing the ITSiG: "The collaborative approach embodied in the law allows not only the government and the business community to benefit from each other's expertise, it also best serves the task of ensuring the highest possible level of IT security for society as a whole" (D-16 BSI 2016:32). Although the findings show that the involved parties appreciate the proceeding, it does not mean trust without limits: The representative of a business association emphasizes that "we get along well with BMI, but, in the end, we are

still on different sides of the river" (I-18:244, own translation) and that reservations of companies, compared to associations, against political actors are even stronger (I-18:244). Against this background, he assumes that a voluntary model of reporting cyber attacks on critical infrastructure is doomed to fail (ibid.). Other than the already described formal ways, the representative mentions informal ways of articulating the association's interests, such as meetings with representatives of the ministry (I-18:235,239).

Despite the non-public character of several elements in the actual legislative process, there is a high public visibility and attention on the debate in the case of the ITSiG. As the expert from a business association notes, in case the cooperative approach does not turn out as expected, journal articles are a favorite means for articulating criticism and bringing public attention to the topic (I-18:242). Another example for visibility is the publication of a study by the *German Federal Association for Information Technology, Telecommunications and New Media* (Bitkom) in 2014 (I-16:211, KPMG 2014). The study, conducted by KPMG, made an evaluation of the ITSiG and also pointed out the cost of the ITSiG for the private sector (I-16:211). By an interviewd policy analyst, Bitkom is seen as "the big player" (I-16:211, own translation) that, due to the study, presented itself as "opinion leader" (ibid., own translation). Moreover, the ITSiG was a topic on the international level: As the interviewed BMI official points out, there is high international interest on how Germany implements the ITSiG, for example in the context of the so-called Meridian conference, an intergovernmental meeting on critical infrastructure protection (I-14:173). The official states that more and more states tend to switch from a voluntary to an obligatory model and in this sense, he sees Germany as "leader of a movement" (I-14:173, own translation). These findings are in line with the characteristics the corporatist regulatory style proposes: The process is open to associations and there is "[l]imited public control, but high visibility" (Renn 2001:408).

As to the *procedural rules*, it has to be noted that the ITSiG is a standard law, so there are clearly defined procedural rules. Important steps of the proceeding notably include the following ones: The government drafts a first version of the law, which is sent to selected stakeholder associations so they can comment on it within a certain period of time (I-14:176; I-18:235), "mostly, way too short" according to an expert from a business association (I-18:235, own translation). The draft is also put on the website (I-14:176). Afterwards, there is

the already mentioned (non-public) hearing with invited stakeholder associations (I-18:235-236). Eventually, the draft is revised (I-14:177) and is then adopted in the cabinet (I-14:177). Then, the law goes through the process in parliament with several readings and discussions in the (non-public) committees and, eventually, in the parliamentary groups (I-14:177, I-18:236). During the process of the ITSiG, there was no doubt from the government side that it would succeed within the anticipated time frame "because of the stable majorities" (I-14:173, own translation) and due to the fact that it was written down in the coalition treaty from 2013 (I-14:177).

It is interesting to note that the history of the ITSiG already began several years ago: In 2012, there were several meetings between Minister of the Interior Friedrich and owners and operators of critical infrastructures from different sectors (I-14:173). The government's conclusion of these meetings was that there are different levels of how well sectors are prepared for cyber risks and so the necessity of a law was articulated (I-14:173, I-15:190). There was a first attempt of an ITSiG in 2013 that was not successful, due to the veto of the BMWi (I-18:238, I-16:205). Private sector interest groups saw this as a success of their work (I-18:238). Later in 2013, a second attempt was started with the coalition partners writing down their intention to "create an IT security law with binding minimum requirements for the IT security of critical infrastructure and the obligation to report significant IT security incidents" (CDU, CSU, SPD 2013:148, own translation) in the coalition treaty for the new government. An interviewed policy analyst notes that the political climate has significantly changed between the two attempts to establish an ITSiG because of the Snowden revelations (I-16:205). Whereas before the revelations, the failure in the passing of the ITSiG "did not cause high political cost for the political actors" (I-16:205, own translation), this is not the case anymore post Snowden (ibid.). The expert also noticed a different behavior of private sector actors: "Industry and economy have recognized that they cannot win this fight anymore post Snowden" (I-16:210, own translation). In consequence, their approach was more cooperative (ibid.). The expert from the business association sees the coalition treaty as a sort of turning point, in the wake of which the private sector decided to rather "participate in a constructive (…) way" (I-18:238, own translation) than trying a new strategy of blocking the law. For the policy analyst, this way of returning on a cooperative path shows "these processes (…) work out well" (I-16:210, own translation).

Finally, the law was adopted by the Bundestag in June 2015 (Bundestag 2015a) and entered into force in July 2015 (Bundestag 2015b). For the implementation of the law, a decree ("BSI-KritisV") was adopted (BSI 2017:16). Altogether, the process of the ITSiG took a long time, but, in the end, it followed clear and predetermined procedural rules, which brings me to the conclusion that, in this aspect, the ITSiG corresponds to the corporatist regulatory style.

Orientation of policy-making and role of science. As was discussed above, the element of trust between the government and the involved stakeholders is essential and, in this way, the process of the ITSiG corresponds to the idea of the corporatist regulatory style. As to the role of science, I find from my interview data that "classic science" is not at the center of attention in the process of the ITSiG. One expert describes that "science – except for the *Fraunhofer Institute* – is not much listened to" (I-17:224, own translation) by political actors. Making a link to the encryption debate, this expert states that computer scientists regularly show "how simple it would be to create more secure systems" (ibid., own translation), but that this is not in the interest of politicians who would like to create capabilities in security authorities to break encryption (I-17:222,224). Others underline that there is a role for science (I-14:178) and, again, that there is a close relationship and exchange between Fraunhofer and the political sphere (I-18:239). A representative of BSI emphasizes that Fraunhofer, compared to ten years ago, strongly expanded their research in the area of IT security (I-15:197). Another expert acknowledges that scientific knowledge is important for BMI, but with regard to the ITSiG, he attributes a higher relevance to concrete pragmatic knowledge, which, sometimes, is outside of the realm of abstract science (I-18:240). This points to the general importance of comprehensive technical expert knowledge in matters of cybersecurity regulation, which is a parallel to the U.S. example of the NIST Framework discussed above.

Conclusion. Altogether, the findings show that vital elements of the corporatist approach are fulfilled in the case of the ITSiG: Interest groups and experts are part of the process and are integrated in a cooperative way. The process follows strict procedural rules and, although the ITSiG was broadly debated in public, certain parts of the process are intentionally kept in a confidential, non-public atmosphere, so that public control is limited. Both the government as well as the business side underline the importance of trust, which finds its expression in

the cooperative approach. Against this background, the ITSiG is in line with the German tradition stated in the corporatist regulatory style albeit with limited findings regarding the role of science in the case of the ITSiG.

5.2.4 Discussion: Cybersecurity Regulation in Germany

Some additional remarks on cooperation and regulation in the field of cybersecurity policy in Germany shall be presented in the following. When asked if cybersecurity policy is different from other policy fields, the interviewed BMI official's point of view is that the proceeding is "quite different" (I-14:178, own translation) because of the close cooperation with stakeholders in issues of cybersecurity: The official states that "in the IT domain, we collaborate much closer with scientific institutions, with industry, with NGOs, for awareness campaigns, for voluntary collaboration for example in the CIP implementation plan. To my knowledge, such an approach was not taken anywhere else before over such a long period of time" (I-14:178, own translation). Another government official also observes a closer and more intense relationship between BMI and the private sector compared to the past (I-11:125; similarly I-17:221). There is also a practical need for this closer contact, as a policy analyst notes, as there is still a knowledge gap between the political sphere and the private sector regarding cybersecurity topics (I-16:218). The situation improved as the authorities learned and caught up, but there is still a gap (ibid.). In his view, it is also a question of sovereignty, in the end: Sovereignty in the sense that "the state itself defines what security is and prescribes it to other actors" (I-16:209, own translation). And despite limited or even lacking knowledge and resources in the cyber area, the state "wants to go back into the (…) driver's seat" (I-16:210, own translation), so the state wants to control and lead – which does not exclude exchanges with the private sector (I-16:209). Against this background, the ITSiG is a classic example of taking back control, of passing a law with mandatory requirements after the voluntary approach had failed in the perception of the government (see also I-14:172). This experience is not uncommon, when taking into account examples from other policy fields, as one expert notes: Regularly, voluntary approaches fail in the end, notably in areas of diverging interests – the state wants to guarantee security, whereas the private sector is led by economic considerations (I-12:142-143). This conflict regularly led to mandatory requirements as a result (ibid.:142).

The idea of the "driver's seat" (I-16:210) already became clear in the discourse analysis: For example, already in 2009, the government articulated in the context of the CIP strategy that it would use its regulatory powers in case of doubt (D-02 BMI 2009:15). Also, in the second cybersecurity strategy from 2016, in the section discussing the ITSiG, the government states that it "examines the extension of such obligations regarding prevention and reaction (…) to other companies of high societal relevance" (D-04 BMI 2016:22, own translation). Interestingly, the tendency towards regulation in Germany and in Europe is not surprising for outside observers: An interviewed U.S. expert states that "there is a fundamentally different approach to understand the role of the government, (…), there is the expectation that it will be handled in large part by the state" (I-02:24).

5.3 Comparison and Conclusion on the Analysis of Regulatory Examples

As could be seen, the selected regulatory approaches are centered on two main topics: Sharing information on cyber attacks with the government and finding ways to establish a high level of cybersecurity. Both countries found their ways in order to regulatorily implement these measures: the NIST Cybersecurity Framework and the IT Security Law. Comparing both regulatory processes, there is an interesting difference between the United States and Germany: While Germany, at first, used a voluntary approach with the "Alliance for Cyber Security", initiated by BSI and Bitkom, and then switched to mandatory regulation in the form of the IT Security Law, the process in the United States went in the opposite direction: At first, there was the strong and repeated ambition to adopt cybersecurity legislation. After different initiatives in this regard had failed, the White House acted per executive order and required that a voluntary model was developed and implemented.

With regard to the expectations formulated at the beginning of the study (section 2.3), we can state that confirming evidence was found for both countries. With the limitations described, the analysis shows that the United States as well as Germany proceeded in large parts as could be expected in view of their respective traditional regulatory style. In this sense, the selected examples can be seen as indication for a certain stability in the regulatory culture of both countries that also translates into the young policy field of cybersecurity policy.

6 Conclusion

The following sections present a short summary of the study as well as some concluding remarks and implications.

6.1 Summary

The study explored and analyzed political communication and regulatory processes related to cyber risks and cybersecurity in the United States and Germany in the time period from 2007 to 2016 in order to answer the overall research question: How do the executives of the United States and Germany address cybersecurity risks? In particular, what is the approach to cybersecurity-related risks for critical infrastructure? The study was based on Reiner Keller's Sociology of Knowledge Approach to Discourse (SKAD) that was innovatively adapted by integrating frames and regulatory styles.

The study proceeded in three steps: First, a context mapping revealed the roles and responsibilities in the area of cybersecurity policy in both countries. It could be shown that both countries created a complex and institutionally decentralized structure requiring high coordination efforts in order to integrate cybersecurity policy into their executive structure. Second, cybersecurity discourses in both countries were analyzed in detail in order to identify which frames the respective executive actors use in their official communication. For the United States, a *homeland security frame* and a *technological leadership frame* were found; for Germany, a *security of supply frame* as well as a *moderation frame* could be identified. Third, the study shed light on regulation in the field of cybersecurity, understood as discourse effect. Two examples of regulation were selected and examined in order to assess their consistency with the expected traditional regulatory style of each country. With certain limitations, evidence for the adversarial style in the United States was found for the example of the Cybersecurity Framework. Moreover, the example of the IT Security Law in Germany followed the corporatist regulatory style in large parts.

6.2 Implications of the Study and Venues for further Research

As Tessier Stall already noted in 2011, "[c]yberspace is both the playground and the battleground of the future" (Tessier Stall 2011:7). In this space, numerous risks occur and challenge today's societies. In consequence, cybersecurity is the order of the day in the digital age. In order to tackle the challenges and identify solutions, stakeholders negotiate the way forward in risk discourses. As Keller puts it, "risks and non-risks are discursive constructions with serious effects – depending on how they are defined, people feel safe or unsafe, technologies and industries are further developed or abandoned, socio-cultural and technological development paths of societies are oriented towards one or another direction" (Keller 2014:15, own translation).

The goal of the study was to analyze discursive constructions in the field of cyber risks and cybersecurity for the United States and Germany. It proceeded by means of a gradual research process from compiling frame elements to identifying frames and interpreting their implications, including examples of regulatory discourse effects as well as interactions with regard to the institutional structure in both countries.

What can be learned from the study? In the following, several contributions to scientific research as well as to practical cybersecurity policy are outlined.

As to the contributions to research, it has to be noted that the adopted Sociology of Knowledge Approach to Discourse (SKAD) proved to be an appropriate and helpful toolkit in order to clarify the meanings and messages intended by both governments, and generate new insights allowing an enhanced understanding of discursive processes. Not only did the collective actor conception and level of analysis of SKAD enable a differentiated analysis of the cybersecurity-relevant parts of the executives of both countries, but it also allowed for taking into account the whole picture. Another conclusion for future analyses of discourses is that the combined examination of discourse and discourse effects can be recommended, especially in the field of risks. Moreover, the study confirmed the adaptability of SKAD for special research interests. In the case of this study, the integration of regulatory styles provided an innovative theoretical supplement for SKAD as they worked as a concretization in the large area of discourse effects that is of special interest from a political sciences point of view. The results of the analysis of the selected regulatory examples can be seen as an

indication for a certain stability of the regulatory culture in the United States as well as in Germany that also translates into cybersecurity policy. More research analyzing regulations in the cyber domain is needed in order to confirm if this suggestion holds true more generally.

With a view on practical cybersecurity policy, the results of the study deliver insights into a formative period of cybersecurity policy. Cybersecurity issues evolved from a marginal issue to an essential topic on the political agendas in the United States as well as in Germany. The analysis of both executives' communications demonstrated, among other things, the crucial importance of critical infrastructure, framed differently in both countries. Another important finding was a strong military component in cybersecurity policy with regard to the United States. This aspect provides an especially illustrative example of how important it is to explore meaning constructions and their implications – also from a normative point of view. With Dunn Cavelty, we can emphasize that "[a]wareness of the power of threat representation and the preferences that come with them can help to understand that it is neither natural nor inevitable that cyber-security should be presented in terms of power-struggles, war-fighting, and military action, and that there are always different, and sometimes better options" (Dunn Cavelty 2013:119).

By the context mapping, we could learn that instead of radically changing the institutional landscape, gradual steps were taken in order to adapt the institutional setting. A decentralized structure prevailed in both countries. In consequence, time and strong coordination and communication efforts are necessary in order to advance cybersecurity policy. In the case of the *National Cyber Response Centre* in Germany, for example, the involved partners had to handle "very different agency cultures as well as the different state of knowledge and experience" (D-11 BSI 2013:17, own translation) when they started working together. At the same time, technology and thus, cybersecurity risks rapidly evolve and put even more pressure on the political system. In the end, bridging the gap between the established institutional and regulatory settings and the rapidly evolving field of cybersecurity turns out to be a crucial challenge. This challenge gets even more complicated when there are shortcomings in political guidance, as shown in the analysis for Germany, and competence fights as shown for both countries. The latter also point to more fundamental questions, for example, whether and to what extent the response to cyber risks

shall be characterized by military elements. It can be assumed that disputes on competences cannot be perfectly avoided in a young policy field. However, these aspects are problematic from my point of view, as they additionally complicate processes and reduce capacity for political action. In the interest of avoiding a dysfunctional system, in which policy advances are slowed down or even obstructed, it can be concluded for future cybersecurity policy, that it is highly important to have a clear and (more) visible strategic guidance in place, so that time-consuming political processes can be as efficient as possible. Moreover, the (remaining) uncertainties and disputes on competences in both countries should be settled in order to establish well-working mechanisms for day-to-day cooperation on the working level of the executive.

Persons involved in cybersecurity policy-making can benefit from the study as it examined a long time span and used a comparative approach that revealed and contrasted similarities and differences between the United States and Germany. The study can help practitioners to increase their knowledge and understanding of the other country's communication strategies and the country-specific political and institutional background in the cyber domain. A refined understanding of the long-term evolution of cybersecurity discourses and the awareness of nuances in the communication of both countries on similar topics – for example, the differences between the "homeland security" and "security of supply" frames – can contribute to pave the way for more reflected communication in the future and learning effects improving the political implementation of measures. This is all the more important as cybersecurity is an inherently international issue and countries need to cooperate. Also, best practices can be taken away, for example, the internationally recognized U.S. Cybersecurity Framework and the open and cooperative way of elaborating it. Finally, external observers may be interested in learning about the United States' and Germany's experiences in developing a cybersecurity policy and take away insights that enrich the perspective on their own cybersecurity policy context.

Further research should continue to deepen our understanding of discourses. The present study can be a starting point and provides preparatory work for further in-depth analyses. For example, an enlarged set of actors and more regulatory examples could be examined in order to explore if regular effects from frames to regulation – or from regulation into the

discourse – can be identified. Thus, a more systematic understanding of the relation between framing and regulation, between language and political practice could be provided. Also, further research with a more specific angle on the institutional centers of gravity identified in this study, such as BMI, could be carried out and help us learn more about internal framing processes within a specific institution.

Normatively, 'good' risk governance should be characterized by communication understood as a "two-way process" (Renn 2008:271). This study intended to contribute to a better understanding of one part of the equation: the side of political executives in the United States and Germany and their official communication. Further research can shed light on how receivers of this communication perceive and react to it, and more generally, what conditions have to be met in order to generate successful and inclusive cyber risk communication processes with all stakeholders involved.

A third venue for further research is deepening the normative implications of cybersecurity policies. Research in this regard is all the more relevant against the background of increasing digitalization that includes permanently evolving technologies such as currently artificial intelligence. The technological developments of the future will continue to open up the field for new (cybersecurity and other) risks and opportunities. Hopefully, they will be accompanied by fruitful risk discourses.

7 Literature

7.1 Data Corpus of U.S. Documents Used for the Frame Analysis

Note: All links in the following list have been accessed on August 5, 2018.

U-01 White House, Barack Obama. n.d. “Selections from the Address to Joint Session of Congress 2009 and the State of the Union Addresses 2010-2016.” https://obamawhitehouse.archives.gov/briefing-room/speeches-and-remarks.

U-02 White House, Barack Obama. 2009. “Remarks by the President on Securing Our Nation’s Cyber Infrastructure.” https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

U-03 White House, Executive Office of the President, National Science and Technology Council. 2009. “The Comprehensive National Cybersecurity Initiative.” https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative.

U-04 White House, Barack Obama. 2009. “Presidential Proclamation - Critical Infrastructure Protection Month.” https://obamawhitehouse.archives.gov/the-press-office/presidential-proclamation-critical-infrastructure-protection-month.

U-05 White House, Barack Obama. 2009. “Presidential Proclamation - National Cybersecurity Awareness Month.” https://obamawhitehouse.archives.gov/the-press-office/presidential-proclamation-national-cybersecurity-awareness-month.

U-06 White House. 2010. “National Security Strategy.” https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

U-07 White House, Barack Obama. 2010. “Presidential Proclamation - Critical Infrastructure Protection Month.” https://obamawhitehouse.archives.gov/the-press-office/2010/11/30/presidential-proclamation-critical-infrastructure-protection-month.

U-08 White House, Barack Obama. 2010. “Presidential Proclamation - National Cybersecurity Awareness Month.” https://obamawhitehouse.archives.gov/the-press-office/2010/10/01/presidential-proclamation-national-cybersecurity-awareness-month.

U-09 White House. 2011. “International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World.” https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

U-10 White House, Barack Obama. 2011. “Presidential Proclamation - Critical Infrastructure Protection Month, 2011.” https://obamawhitehouse.archives.gov/the-press-office/2011/11/30/presidential-proclamation-critical-infrastructure-protection-month-2011.

U-11 White House, Barack Obama. 2011. “Presidential Proclamation - National Cybersecurity Awareness Month.” https://obamawhitehouse.archives.gov/the-press-

office/2011/10/03/presidential-proclamation-national-cybersecurity-awareness-month.

U-12 White House, Barack Obama. 2012. “Taking the Cyberattack Threat Seriously.” *Wall Street Journal*, July 20, 2012.

U-13 White House, Barack Obama. 2012. “Presidential Proclamation - Critical Infrastructure Protection and Resilience Month, 2012.” https://obamawhitehouse.archives.gov/the-press-office/2012/11/30/presidential-proclamation-critical-infrastructure-protection-and-resilie.

U-14 White House, Barack Obama. 2012. “Presidential Proclamation - National Cybersecurity Awareness Month, 2012.” https://obamawhitehouse.archives.gov/the-press-office/2012/10/01/presidential-proclamation-national-cybersecurity-awareness-month-2012.

U-15 White House, Barack Obama. 2013. “Presidential Proclamation - Critical Infrastructure Security and Resilience Month, 2013.” https://obamawhitehouse.archives.gov/the-press-office/2013/10/31/presidential-proclamation-critical-infrastructure-security-and-resilienc.

U-16 White House, Barack Obama. 2013. “Presidential Proclamation - National Cybersecurity Awareness Month, 2013.” https://obamawhitehouse.archives.gov/the-press-office/2013/09/30/presidential-proclamation-national-cybersecurity-awareness-month-2013.

U-17 White House, Barack Obama. 2014. “Statement by the President on the Cybersecurity Framework.” https://obamawhitehouse.archives.gov/the-press-office/2014/02/12/statement-president-cybersecurity-framework.

U-18 White House, Barack Obama. 2014. “Presidential Proclamation - Critical Infrastructure Security and Resilience Month, 2014.” https://obamawhitehouse.archives.gov/the-press-office/2014/10/31/presidential-proclamation-critical-infrastructure-security-and-resilienc.

U-19 White House, Barack Obama. 2014. “Presidential Proclamation - National Cybersecurity Awareness Month, 2014.” https://obamawhitehouse.archives.gov/the-press-office/2014/09/30/presidential-proclamation-national-cybersecurity-awareness-month-2014.

U-20 White House, Barack Obama. 2015. “Remarks by the President at the National Cybersecurity Communications Integration Center.” https://obamawhitehouse.archives.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent.

U-21 White House, Barack Obama. 2015. “Remarks by the President at the Cybersecurity and Consumer Protection Summit.” https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.

U-22 White House. 2015. “National Security Strategy.” https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf.

U-23 White House, Barack Obama. 2015. “Presidential Proclamation - National Cybersecurity Awareness Month, 2015.” https://obamawhitehouse.archives.gov/the-press-office/2015/10/01/presidential-proclamation-national-cybersecurity-awareness-month-2015.

U-24 White House, Barack Obama. 2015. “Presidential Proclamation - Critical Infrastructure Security and Resilience Month, 2015.” https://obamawhitehouse.archives.gov/the-press-office/2015/10/29/presidential-proclamation-critical-infrastructure-security-and.

U-25 White House, Barack Obama. 2016. “Protecting U.S. Innovation From Cyberthreats.” *Wall Street Journal*, 2016, sec. Opinion. http://www.wsj.com/articles/protecting-u-s-innovation-from-cyberthreats-1455012003.

U-26 White House, Barack Obama. 2016. “Presidential Proclamation - Critical Infrastructure Security and Resilience Month, 2016.” https://obamawhitehouse.archives.gov/the-press-office/2016/10/31/presidential-proclamation-critical-infrastructure-security-and.

U-27 White House, Barack Obama. 2016. “Presidential Proclamation - National Cybersecurity Awareness Month, 2016.” https://obamawhitehouse.archives.gov/the-press-office/2016/09/30/presidential-proclamation-national-cybersecurity-awareness-month-2016.

U-28 Director of National Intelligence. 2008. “Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee.” https://www.dni.gov/files/documents/Newsroom/Testimonies/20080227_testimony.pdf.

U-29 Director of National Intelligence, Dennis C. Blair. 2009. “Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence.” https://www.dni.gov/files/documents/Newsroom/Testimonies/20090212_testimony.pdf.

U-30 Office of the Director of National Intelligence. 2009. “The National Intelligence Strategy of the United States of America.” https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2009_NIS.pdf.

U-31 Director of National Intelligence, Dennis C. Blair. 2010. “Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence.” https://www.dni.gov/files/documents/Newsroom/Testimonies/20100202_testimony.pdf.

U-32 Director of National Intelligence, James R. Clapper. 2011. “Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence.” https://www.dni.gov/files/documents/Newsroom/Testimonies/20110216_testimony_sfr.pdf.

U-33 Director of National Intelligence, James R. Clapper. 2012. “Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence.”

https://www.dni.gov/files/documents/Newsroom/Testimonies/20120131_testimony_ata.pdf.

U-34 Director of National Intelligence, James R. Clapper. 2013. “Statement for the Record. Worldwide Threat Assessment of the US Intelligence Community.” https://www.dni.gov/files/documents/Intelligence%20Reports/UNCLASS_2013%20ATA%20SFR%20FINAL%20for%20SASC%2018%20Apr%202013.pdf.

U-35 Director of National Intelligence, James R. Clapper. 2014. “Statement for the Record. Worldwide Threat Assessment of the US Intelligence Community.” http://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf.

U-36 Office of the Director of National Intelligence. 2014. “The National Intelligence Strategy of the United States of America.” https://www.dni.gov/files/documents/2014_NIS_Publication.pdf.

U-37 Director of National Intelligence, James R. Clapper. 2015. “Statement for the Record. Worldwide Threat Assessment of the US Intelligence Community.” https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.

U-38 Director of National Intelligence, James R. Clapper. 2016. “Statement for the Record. Worldwide Threat Assessment of the US Intelligence Community.” https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf.

U-39 U.S. Department of Homeland Security. 2009. “National Infrastructure Protection Plan. Partnering to Enhance Protection and Resiliency.” https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2009-508.pdf.

U-40 U.S. Department of Homeland Security. 2010. “Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland.” https://www.dhs.gov/sites/default/files/publications/2010-qhsr-report.pdf.

U-41 U.S. Department of Homeland Security. 2011. “Blueprint for a Secure Cyber Future. The Cybersecurity Strategy for the Homeland Security Enterprise.” http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf.

U-42 U.S. Department of Homeland Security, Janet Napolitano. 2012. “Remarks by Secretary Janet Napolitano at San Jose State University.” https://www.dhs.gov/news/2012/04/16/remarks-secretary-janet-napolitano-san-jose-state-university.

U-43 U.S. Department of Homeland Security. 2013. “NIPP 2013. Partnering for Critical Infrastructure Security and Resilience.” http://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf.

U-44 U.S. Department of Homeland Security. 2014. “The 2014 Quadrennial Homeland Security Review.” https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf.

U-45 U.S. Department of Homeland Security, Jeh Johnson. 2015. “Remarks by Secretary of Homeland Security Jeh Johnson at the RSA Conference 2015.”

https://www.dhs.gov/news/2015/04/21/remarks-secretary-homeland-security-jeh-johnson-rsa-conference-2015.

U-46 U.S. Department of Homeland Security. 2016. “National Cyber Incident Response Plan.” https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

U-47 U.S. Department of State, Hillary Rodham Clinton. 2011. “Internet Rights and Wrongs: Choices & Challenges in a Networked World.” https://2009-2017.state.gov/secretary/20092013clinton/rm/2011/02/156619.htm.

U-48 U.S. Department of State, Hillary Rodham Clinton. 2011. “Remarks on the Release of President Obama Administration’s International Strategy for Cyberspace.” https://2009-2017.state.gov/secretary/20092013clinton/rm/2011/05/163523.htm.

U-49 U.S. Department of State, Christopher Painter. 2014. “As Prepared Remarks at Georgetown University Institute for Law, Science and Global Security’s 2013 International Engagement on Cyber Conference.” https://2009-2017.state.gov/s/cyberissues/releasesandremarks/223075.htm.

U-50 U.S. Department of State, John Kerry. 2014. “Remarks to the Freedom Online Coalition Conference.” https://2009-2017.state.gov/secretary/remarks/2014/04/225290.htm.

U-51 U.S. Department of State, Christopher Painter. 2015. “Testimony Before Policy Hearing Titled: ‘Cybersecurity: Setting the Rules for Responsible Global Behavior.’” https://2009-2017.state.gov/s/cyberissues/releasesandremarks/243801.htm.

U-52 U.S. Department of State, John Kerry. 2015. “An Open and Secure Internet: We Must Have Both.” https://2009-2017.state.gov/secretary/remarks/2015/05/242553.htm.

U-53 U.S. Department of State. 2016. “Department of State International Cyberspace Policy Strategy.” https://2009-2017.state.gov/documents/organization/255732.pdf.

U-54 U.S. Department of State, Christopher Painter. 2016. “International Cybersecurity Strategy: Deterring Foreign Threats and Building Global Cyber Norms.” https://2009-2017.state.gov/s/cyberissues/releasesandremarks/257719.htm.

U-55 U.S. Department of Defense. 2010. “Quadrennial Defense Review Report.” https://www.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf.

U-56 U.S. Department of Defense, William J. Lynn III. 2010. “Defending a New Domain. The Pentagon’s Cyberstrategy.” *Foreign Affairs* 89 (5): 97–108.

U-57 U.S. Department of Defense. 2011. “Department of Defense Strategy for Operating in Cyberspace.” http://archive.defense.gov/home/features/2011/0411_cyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf.

U-58 U.S. Department of Defense, William J. Lynn III. 2011. “The Pentagon’s Cyberstrategy, One Year Later. Defending Against the Next Cyberattack.” *Foreign Affairs*. https://www.foreignaffairs.com/print/1070281.

U-59 U.S. Department of Defense. 2012. “Sustaining U.S. Global Leadership: Priorities for the 21st Century Defense.” http://www.defense.gov/news/Defense_Strategic_Guidance.pdf.

U-60 U.S. Department of Defense, Leon Panetta. 2012. “Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security.” http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

U-61 U.S. Department of Defense. 2013. “DoD Strategy for Defending Networks, Systems, and Data.” http://dodcio.defense.gov/Portals/0/Documents/DoD%20Strategy%20for%20Defending%20Network%20Systems%20and%20Data.pdf.

U-62 U.S. Department of Defense. 2014. “Quadrennial Defense Review 2014.” http://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf.

U-63 U.S. Department of Defense. 2015. “The DoD Cyber Strategy.” https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

U-64 U.S. Department of Defense, Michael S. Rogers. 2015. “Beyond the Build. Delivering Outcomes through Cyberspace. The Commander’s Vision and Guidance for US Cyber Command.” https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/US-Cyber-Command-Commanders-Vision.pdf.

U-65 U.S. Department of Commerce, Gary Locke. 2010. “Remarks at Business Software Alliance Cybersecurity Forum.” https://www.ntia.doc.gov/speechtestimony/2010/remarks-business-software-alliance-cybersecurity-forum.

U-66 U.S. Department of Commerce, Gary Locke. 2010. “Remarks at Cybersecurity and Innovation in the Information Economy.” https://www.ntia.doc.gov/speechtestimony/2010/remarks-cybersecurity-and-innovation-information-economy.

U-67 U.S. Department of Commerce, Gary Locke. 2010. “Remarks at Cybersecurity Forum, Georgetown University.” https://www.ntia.doc.gov/speechtestimony/2010/remarks-cybersecurity-forum-georgetown-university.

U-68 U.S. Department of Commerce, Internet Policy Task Force. 2011. “Cybersecurity, Innovation and the Internet Economy.” https://www.nist.gov/sites/default/files/documents/itl/Cybersecurity_Green-Paper_FinalVersion.pdf.

U-69 U.S. Department of Commerce, National Institute of Standards and Technology. 2014. “Framework for Improving Critical Infrastructure Cybersecurity. Version 1.0.” https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

U-70 U.S. Department of Commerce. 2014. “America Is Open for Business. Strategic Plan. Fiscal Years 2014-2018.” https://www.commerce.gov/sites/commerce.gov/files/media/files/2014/doc_fy2014-2018_strategic_plan.pdf.

U-71 U.S. Department of Justice, Jason Weinstein. 2011. “Cybersecurity: Responding to the Threat of Cyber Crime and Terrorism. Statement before the United States Senate, Committee on Judiciary, Crime and Terrorism Subcommittee.” https://www.judiciary.senate.gov/imo/media/doc/11-04-12%20Weinstein%20Testimony.pdf.

U-72 U.S. Department of Justice, Mythili Raman. 2014. “Remarks as Prepared for Delivery by Acting Assistant Attorney General Mythili Raman at the State of the Net Conference.” https://www.justice.gov/opa/speech/remarks-prepared-delivery-acting-assistant-attorney-general-mythili-raman-state-net.

U-73 U.S. Department of Justice, Leslie R. Caldwell. 2015. “Assistant Attorney General Leslie R. Caldwell Delivers Remarks at ‘Cybersecurity + Law Enforcement: The Cutting Edge’ Symposium.” https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-cybersecurity-law.

U-74 U.S. Department of Justice, Leslie R. Caldwell. 2016. “Assistant Attorney General Leslie R. Caldwell Delivers Remarks Highlighting Cybercrime Enforcement at Center for Strategic and International Studies.” https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-highlighting-cybercrime.

U-75 Federal Bureau of Investigation, Joseph M. Demarest. 2014. “Cyber Security: Enhancing Coordination to Protect the Financial Sector.” https://www.fbi.gov/news/testimony/cyber-security-enhancing-coordination-to-protect-the-financial-sector.

U-76 Federal Bureau of Investigation, James B. Comey. 2016. “The FBI’s Approach to the Cyber Threat.” https://www.fbi.gov/news/speeches/the-fbis-approach-to-the-cyber-threat.

7.2 Data Corpus of German Documents Used for the Frame Analysis

Note: All links in the following list have been accessed on September 6, 2018, except for three texts. The access date of these texts is indicated in the respective reference.

D-01 Bundesministerium des Innern. 2007. “Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen.” https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/umsetzungsplan-kritis.pdf?__blob=publicationFile&v=4.

D-02 Federal Ministry of the Interior. 2009. “National Strategy for Critical Infrastructure Protection (CIP Strategy).” https://www.bbk.bund.de/SharedDocs/Downloads/BBK/EN/CIP-Strategy.pdf?__blob=publicationFile.

D-03 Federal Government. 2011. “Cyber Security Strategy for Germany.” Edited by Federal Ministry of the Interior. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber_eng.pdf?__blob=publicationFile.

D-04 Bundesministerium des Innern. 2016. “Cyber-Sicherheitsstrategie für Deutschland 2016.” http://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/cybersicherheitsstrategie-2016.pdf;jsessionid=94EA9BF6FC504922A7E09FC5D27FF6C4.1_cid287?__blob=publicationFile&v=3.

D-05 Federal Office for Information Security. 2007. “The IT Security Situation in Germany in 2007.” https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2007.pdf?__blob=publicationFile&v=1.

D-06 Federal Office for Information Security. 2008. “Secure Information Technology for Our Society. Annual Report 2006-2007.” https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Annualreport/BSI_annual_report_2006-2007_pdf.pdf?__blob=publicationFile&v=2.

D-07 Federal Office for Information Security. 2009. “The IT Security Situation in Germany in 2009.” https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2009.pdf?__blob=publicationFile&v=1.

D-08 Federal Office for Information Security. 2010. “Improving IT Security. BSI Annual Report 2008/2009.” https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Annualreport/BSI_annual_report_2008-2009_pdf.pdf?__blob=publicationFile&v=2.

D-09 Federal Office for Information Security. 2011. “The IT Security Situation in Germany in 2011.” https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2011_bf.pdf?__blob=publicationFile&v=2.

D-10 Federal Office for Information Security. 2011. “Improving IT Security. BSI Annual Report 2010.” https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Annualreport/BSI_annual_report_2010_pdf.pdf?__blob=publicationFile&v=2.

D-11 Bundesamt für Sicherheit in der Informationstechnik. 2013. “Mit Sicherheit. BSI Jahresbericht 2011/2012.” https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Jahresberichte/BSI-Jahresbericht_2011-2012_pdf.pdf?__blob=publicationFile.

D-12 Federal Office for Information Security. 2014. “The State of IT Security in Germany 2014.” https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?__blob=publicationFile&v=3.

D-13 Federal Office for Information Security. 2014. “Security in Focus. BSI Magazine 2013/14.” https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2013-14.pdf?__blob=publicationFile&v=2.

D-14 Federal Office for Information Security. 2015. “The State of IT Security in Germany 2015.”

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2015.pdf?__blob=publicationFile&v=2.

D-15 Federal Office for Information Security. 2015. “Security in Focus. BSI Magazine 2015.” https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2015.pdf?__blob=publicationFile&v=3.

D-16 Federal Office for Information Security. 2016. “Security in Focus. BSI Magazine 2016/01.” https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2016-01.pdf?__blob=publicationFile&v=3.

D-17 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. 2008. “Global denken - lokal handeln. Jahresbericht 2007.” http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Jahresberichte/Jahresbericht_2007.pdf?__blob=publicationFile.

D-18 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. 2009. “Von Menschen für Menschen. Jahresbericht 2008.” http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Jahresberichte/Jahresbericht_2008.pdf?__blob=publicationFile.

D-19 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. 2010. “Bevölkerungsschutz 3/2010: Schutz Kritischer Infrastrukturen.” http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Publ_magazin/bsmag_3_10.pdf?__blob=publicationFile.

D-20 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. 2010. “Zukunft vielfältig gestalten. Jahresbericht 2009.” http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Jahresberichte/Jahresbericht_2009.pdf?__blob=publicationFile.

D-21 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. 2011. “Bevölkerungsschutz 4/2011: Cyber-Sicherheit.” http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Publ_magazin/bsmag_4_11.pdf?__blob=publicationFile.

D-22 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. 2011. “Bevölkerungsschutz hat viele Gesichter. Jahresbericht 2010.” http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Jahresberichte/Jahresbericht_2010.pdf?__blob=publicationFile.

D-23 Geier, Wolfram. 2012. “Der Schutz Kritischer Infrastrukturen - Gemeinschaftsaufgabe von Staat und Wirtschaft im Rahmen einer gesamtstaatlichen Notfallvorsorge.” In Nationales Krisenmanagement im Bevölkerungsschutz, edited by Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. Vol. 1. http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/Praxis_BS_Band1.pdf?__blob=publicationFile.

D-24 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. 2012. “Wir investieren in die Zukunft. Jahresbericht 2011.” https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Presse/Pressemeldung_2012/PM_BBK-Jahresbericht_2011.html.

D-25 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. 2013. “Wir wachsen mit den Herausforderungen. Jahresbericht 2012.” http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Jahresberichte/Jahresbericht_2012.pdf?__blob=publicationFile.

D-26 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. 2014. “Bevölkerungsschutz 4/2014: Kritische Infrastrukturen.” http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Publ_magazin/bsmag_4_14.pdf?__blob=publicationFile.

D-27 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. 2014. “Der Jahresbericht 2013.” http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Jahresberichte/Jahresbericht_2013.pdf?__blob=publicationFile.

D-28 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. 2015. “Der Jahresbericht 2014.” http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Jahresberichte/Jahresbericht_2014.pdf?__blob=publicationFile.

D-29 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. 2016. “Bevölkerungsschutz 2/2016: Cyber-Sicherheit.” http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Publ_magazin/bsmag_2_16.pdf?__blob=publicationFile.

D-30 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. 2016. “Der Jahresbericht 2015.” http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Jahresberichte/Jahresbericht_2015.pdf?__blob=publicationFile.

D-31 Bundeskriminalamt. 2011. “Bundeslagebild Cybercrime 2010.” https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2010.html;jsessionid=744699DCCE4CED222A0E17ABC82E26B0.live2302?nn=28110.

D-32 Bundeskriminalamt. 2012. “Bundeslagebild Cybercrime 2011.” https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2011.html?nn=28110.

D-33 Bundeskriminalamt. 2013. “Bundeslagebild Cybercrime 2012.” https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2012.html?nn=28110.

D-34 Bundeskriminalamt. 2014. “Bundeslagebild Cybercrime 2013.” https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2013.html?nn=28110.

D-35 Bundeskriminalamt. 2015. “Bundeslagebild Cybercrime 2014.” https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2014.html?nn=28110.

D-36 Bundeskriminalamt. 2016. “Bundeslagebild Cybercrime 2015.” https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2015.html?nn=28110.

D-37 Bundesamt für Verfassungsschutz. 2013. “Verfassungsschutzbericht 2012.”

D-38 Bundesamt für Verfassungsschutz. 2014. “Elektronische Angriffe mit nachrichtendienstlichem Hintergrund.” https://www.verfassungsschutz.de/embed/broschuere-2014-07-elektronische-angriffe-mit-nachrichtendienstlichem-hintergrund.pdf.

D-39 Bundesamt für Verfassungsschutz. 2014. “Spionage. Ihre Ziele. Ihre Methoden.” https://www.verfassungsschutz.de/embed/broschuere-2014-05-spionage-ihre-ziele-ihre-methoden.pdf.

D-40 Bundesamt für Verfassungsschutz. 2014. “Wirtschaftsspionage: Risiko für Unternehmen, Wissenschaft und Forschung.” https://www.verfassungsschutz.de/embed/broschuere-2014-07-wirtschaftsspionage.pdf.

D-41 Bundesamt für Verfassungsschutz. 2014. “Verfassungsschutzbericht 2013.” https://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/verfassungsschutzberichte/vsbericht-2013.

D-42 Bundesamt für Verfassungsschutz. 2015. “Verfassungsschutzbericht 2014.” https://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/verfassungsschutzberichte/vsbericht-2014.

D-43 Bundesamt für Verfassungsschutz. 2016. “Verfassungsschutzbericht 2015.” https://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/verfassungsschutzberichte/vsbericht-2015.

D-44 Auswärtiges Amt, Werner Hoyer. 2011. “Neue Herausforderungen für die europäische Sicherheit und Verteidigung, Rede von Staatsminister Werner Hoyer bei der 10. Berliner Sicherheitskonferenz am 8. November 2011.” http://www.auswaertiges-amt.de/DE/Infoservice/Presse/Reden/2011/111108_Hoyer_Berliner_Sicherheitskonferenz.html.

D-45 Auswärtiges Amt, Rolf Nikel. 2013. “Internationale Cybersicherheit und vertrauens- und sicherheitsbildende Maßnahmen.”

D-46 Auswärtiges Amt, Frank-Walter Steinmeier. 2014. “Rede von Außenminister Frank-Walter Steinmeier Beim 7th European Dialogue on Internet Governance: ‘Digital Society at Stake – Europe and the Future of the Internet.’” http://www.auswaertiges-amt.de/DE/Infoservice/Presse/Reden/2014/140612-BM_EuroDIG.html.

D-47 Auswärtiges Amt, Frank-Walter Steinmeier. 2014. “Rede von Außenminister Frank-Walter Steinmeier beim ‘Global Media Forum’ der Deutschen Welle am 01. Juli 2014 in Bonn.” http://www.auswaertiges-amt.de/DE/Infoservice/Presse/Reden/2014/140701_BM_GMF.html.

D-48 Auswärtiges Amt, Frank-Walter Steinmeier. 2014. “Rede von Außenminister Frank-Walter Steinmeier beim Transatlantischen Cyber-Dialog.” http://www.auswaertiges-amt.de/DE/Infoservice/Presse/Reden/2014/140627-BM_Cyber_Dialog.html.

D-49 Auswärtiges Amt, Frank-Walter Steinmeier. 2014. “Sicherheit und Freiheit im digitalen Zeitalter.” Handelsblatt, June 27, 2014. http://www.auswaertiges-amt.de/DE/Infoservice/Presse/Interviews/2014/140627-BM_Hbl.html.

D-50 Auswärtiges Amt, Markus Ederer. 2014. “Rede von Staatssekretär Markus Ederer Beim Cyber Cooperation Summit Am 4. Dezember 2014 in Berlin.” http://www.auswaertiges-amt.de/DE/Infoservice/Presse/Reden/2014/141204_STSE_Cyber.html.

D-51 Auswärtiges Amt, Norbert Riedel. 2015. “‘Cyber Security as a Dimension of Security Policy’ - Rede von Norbert Riedel, Sonderbeauftragter Für Cyber-Außenpolitik Im Auswärtigen Amt, Im Chatham House, London.” http://www.auswaertiges-amt.de/DE/Infoservice/Presse/Reden/2015/150518-CA-B-Chatham_House.html.

D-52 Auswärtiges Amt, Norbert Riedel. 2015. “‘Cyber-Außenpolitik’. Rede des Sonderbeauftragten für Cyber–Außenpolitik im Auswärtigen Amt, Norbert Riedel, beim Internet Governance Forum Deutschland.” http://www.auswaertiges-amt.de/DE/Infoservice/Presse/Reden/2015/150521-CA-B_International_Governance_Forum.html.

D-53 Auswärtiges Amt, Norbert Riedel. 2015. “Rede Des Beauftragten Für Cyber-Außenpolitik, Botschafter Dr. Norbert Riedel, Bei Der Tagung Der Freedom Online Coalition in Ulan Bator (Mongolei).” http://www.auswaertiges-amt.de/DE/Infoservice/Presse/Reden/2015/150504-Riedel_Freedom_Online_Coalition_Conference.html.

D-54 Bundesministerium der Verteidigung. 2011. “Verteidigungspolitische Richtlinien. Nationale Interessen wahren - Internationale Verantwortung übernehmen - Sicherheit gemeinsam gestalten.” https://www.bmvg.de/resource/blob/13568/28163bcaed9f30b27f7e3756d812c280/g-03-download-die-verteidigungspolitische-richtlinien-2011-data.pdf.

D-55 Bundesministerium der Verteidigung. 2013. “Bericht zum Themenkomplex Cyber-Verteidigung.”

D-56 Bundesministerium der Verteidigung, Ursula von der Leyen. 2015. “Tagesbefehl.” https://www.bmvg.de/portal/a/bmvg/start/journal/dossiers/cyber/!ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfIjo8zinSx8QnyMLI2MTA2CXA0cLQPNQ4INA40NAsz1wwkpiAJKG-AAjgb6wSmp-pFAM8xxmmFqqB-sH6UflZVYllihV5BfVJKTWqKXmAxyoX5kRmJeSk5qQH6yI0SgIDei3KDcUREAzgH1MA!!/dz/d5/L2dBISEvZ0FBIS9nQSEh/#Z7_B8LTL292250RE0A9Q7TS1Q3051, accessed April 7, 2017.

D-57 Bundesministerium der Verteidigung, Ursula von der Leyen. 2016. “Tagesbefehl.” https://www.bmvg.de/portal/a/bmvg/start/journal/dossiers/cyber/!ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfIjo8zinSx8QnyMLI2MTA2CXA0cLQPNQ4INA40NAsz1wwkpiAJKG-AAjgb6wSmp-pFAM8xxmmFqqB-sH6UflZVYllihV5BfVJKTWqKXmAxyoX5kRmJeSk5qQH6yI0SgIDei3KDcUREAzgH1MA!!/dz/d5/L2dBISEvZ0FBIS9nQSEh/#Z7_B8LTL292250RE0A9Q7TS1Q3051, accessed April 7, 2017.

D-58 Federal Government. 2016. “White Paper 2016 on German Security Policy and the Future of the Bundeswehr.” Edited by Federal Ministry of Defence. https://www.bmvg.de/portal/a/bmvg/start/weissbuch/downloads/!ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfIjo8zinSx8QnyMLI2MXNzNjQ0cAy2CHc1cjA3c3Uz0wwkpiAJKG-AAjgb6wSmp-pFAM8xxm2GsH6wfpR-

VlViWWKFXkF9UkpNaopeYDHKhfmRGYl5KTmpAfrIjRKAgN6LcoNxREQDBsD0r/dz/d5/L2dBISEvZ0FBIS9nQSEh/#Z7_B8LTL2922DG730AQ8SA6D30GF3.

D-59 Bundesministerium der Verteidigung. 2016. “Abschlussbericht Aufbaustab Cyber- und Informationsraum.” https://www.bmvg.de/resource/blob/11412/868d0f8c03b84846f6bb959618a5518f/c-26-04-16-download-auftrag-cyber-verteidigung-data.pdf.

D-60 Bundesministerium für Wirtschaft und Technologie. 2010. “IKT-Strategie der Bundesregierung ‘Deutschland Digital 2015.’” http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/ikt-strategie-der-bundesregierung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf, accessed September 19, 2016.

D-61 Federal Government. 2014. “Digital Agenda 2014-2017.” Edited by Federal Ministry for Economic Affairs and Energy, Federal Ministry of the Interior, and Federal Ministry of Transport and Digital Infrastructure. https://www.digitale-agenda.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda-engl.pdf?__blob=publicationFile&v=6.

D-62 Bundesregierung. 2015. “Strategie Intelligente Vernetzung.” Edited by Bundesministerium für Wirtschaft und Energie. http://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/Intelligente-Vernetzung/strategie-intelligente-vernetzung.pdf?__blob=publicationFile&v=3.

D-63 Bundesministerium für Wirtschaft und Energie. 2015. “Impulse für die Digitalisierung der deutschen Wirtschaft. Digitale Agenda des BMWi.” http://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/impulse-digitalisierung-deutsche-wirtschaft.pdf?__blob=publicationFile&v=7.

D-64 Bundesministerium für Wirtschaft und Energie. 2016. “Wirtschaft Digital - Erfolge und Ziele. Eine Bilanz zum IT-Gipfel 2016.” http://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/wirtschaft-digital-erfolge-und-ziele-bilanz-it-gipfel-2016.pdf?__blob=publicationFile&v=7.

D-65 Bundesministerium für Wirtschaft und Energie. 2016. “Digitale Strategie 2025.” http://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-strategie-2025.pdf?__blob=publicationFile&v=8.

7.3 General Literature

AA
2014 Cyber-Außenpolitik. http://www.auswaertiges-amt.de/DE/Aussenpolitik/GlobaleFragen/Cyber-Aussenpolitik/KS_Cyber-Aussenpolitik.html, accessed May 12, 2015.
2017 International Cyber Policy. https://www.auswaertiges-amt.de/en/aussenpolitik/themen/cyber-aussenpolitik, accessed September 9, 2018.

Abel, Andreas, and Alfred Leicht
2018 Vernetzte Expertise. Bankinformation (BI) 5: 74–77.

Aberbach, Joel D., and Bert A. Rockman
2002 Conducting and Coding Elite Interviews. Political Science and Politics (PS) 35(4): 673–676.

Ballaschk, Cindy
2015 Tagungsbericht: Wissenssoziologische Diskursanalyse & angrenzende Perspektiven der Diskursforschung. Forum Qualitative Sozialforschung / Forum: Qualitative Social Research 16(3). http://www.qualitative-research.net/index.php/fqs/article/view/2399/3857#g31, accessed October 14, 2015.

Barnard-Wills, David, and Debi Ashenden
2012 Securing Virtual Space: Cyber War, Cyber Terror, and Risk. Space & Culture XX(X): 1–14.

Bayer, Martin
2019 Allianz Risk Barometer 2019 - die Angst vor Cyberangriffen wächst. Computerwoche(4–5): 8–9.

BBK
2018a About the Office. https://www.bbk.bund.de/EN/FederalOffice/Abouttheoffice/abouttheoffice_node.html, accessed August 31, 2018.
2018b Designation of the Sectors. https://www.bbk.bund.de/EN/Topics/CriticalInfrastructureProtection/GeneralInformation/generalinformation_node.html, accessed August 31, 2018.
2018c Information Technology and Telecommunications. https://www.bbk.bund.de/EN/Topics/CriticalInfrastructureProtection/GeneralInformation/02_IT-telecommunications/Information_technology_and_telecommunications_start.html, accessed August 31, 2018.

Benford, Robert D., and David A. Snow
2000 Framing Processes and Social Movements: An Overview and Assessment. Annual Review of Sociology 26: 611–639.

Berger, Peter, and Thomas Luckmann
1966 The Social Construction of Reality. Garden City, New York: Anchor Books.

BfV
2018 Bundesamt Für Verfassungsschutz - Welcome. https://www.verfassungsschutz.de/en/index-en.html, accessed August 31, 2018.

Bignami, Francesca
2011 Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy. American Journal of Comparative Law 59(2): 411–461.

BKA
2018 Cybercrime. https://www.bka.de/EN/OurTasks/AreasOfCrime/Cybercrime/cybercrime_node.html,

accessed August 30, 2018.

BMI
2016 Im Profil. Das Bundesministerium des Innern. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/multimedia/im-profil-2016.pdf?__blob=publicationFile&v=4, accessed August 30, 2018.
2017 Organization Chart. https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/ministry/organigramm.pdf?__blob=publicationFile&v=2, accessed August 30, 2018.
2018 Unsere Abteilungen und ihre Aufgaben. https://www.bmi.bund.de/DE/ministerium/das-bmi/abteilungen-und-aufgaben/abteilungen-und-aufgaben-node.html, accessed August 30, 2018.

BMJV
2019 Basic Law for the Federal Republic of Germany. https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html#p0304, accessed July 16, 2019.

BMVg
2018a Die Abteilungen. https://www.bmvg.de/de/ministerium/organisation/die-abteilungen, accessed September 9, 2018.
2018b Organisationsplan BMVg. https://www.bmvg.de/resource/blob/11902/4b96430ade25afd1e3a6ce6cfc757a59/a-03-download-organigramm-data.pdf, accessed September 9, 2018.

BMVI
2018 Aufgaben und Struktur. https://www.bmvi.de/DE/Ministerium/Aufgaben-Struktur/aufgaben-struktur.html, accessed September 9, 2018.

BMWi
2018a Taking Control of the Digital Transformation. https://www.bmwi.de/Redaktion/EN/Dossier/digitisation.html, accessed September 5, 2018.
2018b Organisationsplan BMWi. https://www.bmwi.de/Redaktion/DE/Downloads/M-O/organisationsplan-bmwi.pdf?__blob=publicationFile&v=166, accessed September 5, 2018.

BND
2018 Geschichte Des Bundesnachrichtendienstes Im Überblick. http://www.bnd.bund.de/DE/Organisation/Geschichte/Geschichte_Ueberblick/Timeline_node.html, accessed August 29, 2018.

Bogner, Alexander, Beate Littig, and Wolfgang Menz, eds.
2009 Experteninterviews. Theorien, Methoden, Anwendungsfelder. Wiesbaden: VS Verlag für Sozialwissenschaften.

Bogner, Alexander, and Wolfgang Menz
2009 Das Theoriegenerierende Experteninterview. Erkenntnisinteresse, Wissensformen, Interaktion. *In* Experteninterviews. Theorien, Methoden, Anwendungsfelder. Alexander Bogner, Beate Littig, and Wolfgang Menz, eds. Pp. 61–98. Wiesbaden: VS Verlag für

Sozialwissenschaften.

bpb
2016 Welt-Bruttoinlandsprodukt. bpb.de. http://www.bpb.de/nachschlagen/zahlen-und-fakten/globalisierung/52655/welt-bruttoinlandsprodukt, accessed July 14, 2019.

Brächer, Michael
2018 “Super-KIs werden wichtige Probleme lösen” - Interview mit Jürgen Schmidhuber. Handelsblatt, August 27: 29.

Brickman, Ronald, Sheila Jasanoff, and Thomas Ilgen
1985 Controlling Chemicals. The Politics of Regulation in Europe and the United States. Ithaca/London: Cornell University Press.

Brodowski, Dominik, and Felix C. Freiling
2011 Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft. Forschungsforum Öffentliche Sicherheit, Schriftenreihe Sicherheit 4. http://www.sicherheit-forschung.de/schriftenreihe/sr_v_v/sr_4.pdf.

BSI
2017 Schutz Kritischer Infrastrukturen durch das IT-Sicherheitsgesetz und UP KRITIS. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Schutz-Kritischer-Infrastrukturen-ITSig-u-UP-KRITIS.pdf?__blob=publicationFile&v=7, accessed July 16, 2019.
2018a Die Lage der IT-Sicherheit in Deutschland 2018. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=6, accessed July 18, 2019.
2018b Das Leitbild des Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/DE/DasBSI/Leitbild/leitbild_node.html, accessed August 30, 2018.
2018c CERT-Bund. https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/CERT-Bund/cert-bund_node.html, accessed August 30, 2018.
2018d IT Situation Centre. https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/IT-Situation-Centre/itsituationcentre_node.html, accessed August 30, 2018.
2018e IT Crisis Reaction Centre. https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/IT-Crisis-Reaction-Centre/itcrisisreactioncentre_node.html, accessed August 30, 2018.

Bundeskanzlerin
2018 Tasks of the Chancellor. https://www.bundeskanzlerin.de/Webs/BKin/EN/Chancellery/Tasks_of_the_Chancellor/tasks_of_the_chancellor_node.html, accessed August 27, 2018.

Bundesministerium des Innern
2005 Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI). http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/Nationaler_Plan_Schutz_Informationsinfrastrukturen.pdf?__blob=publicationFile.

Bundesregierung
2013 Acht-Punkte-Programm zum besseren Schutz der Privatsphäre. https://archiv.bundesregierung.de/archiv-de/acht-punkte-programm-zum-besseren-schutz-der-privatsphaere-333694, accessed July 27, 2019.
2018 Organisationsplan des Bundeskanzleramtes. https://www.bundesregierung.de/Content/DE/_Anlagen/druckversion-organigramm-bkamt.pdf?__blob=publicationFile&v=18, accessed August 29, 2018.

Bundestag
2010 Internet-Enquete eingesetzt. Deutscher Bundestag. https://www.bundestag.de/dokumente/textarchiv/2010/28851941_kw09_de_enquete-201096, accessed July 16, 2019.
2013 Schlussbericht der Enquete-Kommission „Internet und digitale Gesellschaft“. http://dipbt.bundestag.de/dip21/btd/17/125/1712550.pdf, accessed July 16, 2019.
2015a Bundestag beschließt das IT-Sicherheitsgesetz. Deutscher Bundestag. https://www.bundestag.de/dokumente/textarchiv/2015/kw24_de_it_sicherheit-377026, accessed July 26, 2019.
2015b Gesetz Zur Erhöhung Der Sicherheit Informationstechnischer Systeme (IT-Sicherheitsgesetz). Bundesgesetzblatt Teil I(31): 1324.

CDU, CSU, SPD
2013 Deutschlands Zukunft gestalten. Koalitionsvertrag zwischen CDU, CSU und SPD. 18. Legislaturperiode. Koalitionsvertrag 2013-2017.

Cebula, James J., and Lisa R. Young
2010 A Taxonomy of Operational Cyber Security Risks. Software Engineering Institute, Carnegie Mellon. http://resources.sei.cmu.edu/asset_files/TechnicalNote/2010_004_001_15200.pdf, accessed December 1, 2018.

Chong, Dennis, and James N. Druckman
2007 Framing Theory. Annual Review of Political Science 10(1): 103–126.

Cilluffo, Frank J., Sharon L. Cardash, and George C. Salmoiraghi
2012 A Blueprint for Cyber Deterrence: Building Stability through Strength. Military and Strategic Affairs 4(3): 3–23.

Convention on Cybercrime
2018 Wikipedia. https://en.wikipedia.org/w/index.php?title=Convention_on_Cybercrime&oldid=829834827, accessed March 27, 2018.

Council of Europe
2018 Details of Treaty No.185, Convention on Cybercrime. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse
2014 Defining Cybersecurity. Technology Innovation Management Review 4(10): 13–21.

Cull, Nicholas J.
2013 The Long Road to Public Diplomacy 2.0: The Internet in US Public Diplomacy. International Studies Review 15(1): 123–139.

Cyber Crime Center
2018 Department of Defense Cyber Crime Center. https://www.dc3.mil/.

Daase, Christopher
2002 Einleitung: Internationale Risikopolitik. Ein Forschungsprogramm für den sicherheitspolitischen Paradigmenwechsel. *In* Internationale Risikopolitik. Der Umgang mit neuen Gefahren in den internationalen Beziehungen. Susanne Feske, Ingo Peters, and Christopher Daase, eds. Pp. 9–35. Baden-Baden: Nomos.

Daniel, Michael
2015 Our Latest Tool to Combat Cyber Attacks: What You Need to Know. Whitehouse.Gov. https://obamawhitehouse.archives.gov/blog/2015/04/01/our-latest-tool-combat-cyber-attacks-what-you-need-know, accessed April 25, 2017.

DHS
2013 Factsheet Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience. https://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf, accessed October 20, 2018.
2018a Cybersecurity Overview. https://www.dhs.gov/cybersecurity-overview, accessed August 2, 2018.
2018b Protecting Critical Infrastructure. https://www.dhs.gov/topic/protecting-critical-infrastructure, accessed August 2, 2018.
2018c Combating Cyber Crime. https://www.dhs.gov/topic/combating-cyber-crime, accessed August 2, 2018.
2018d NPPD at a Glance. https://www.dhs.gov/sites/default/files/publications/nppd-at-a-glance-bifold-02132018-508.pdf.
2018e Office of Infrastructure Protection. https://www.dhs.gov/office-infrastructure-protection, accessed August 3, 2018.
2018f National Infrastructure Coordinating Center. https://www.dhs.gov/national-infrastructure-coordinating-center, accessed August 3, 2018.
2018g Office of Cybersecurity and Communications. https://www.dhs.gov/office-cybersecurity-and-communications, accessed August 4, 2018.
2018h National Cybersecurity & Communications Integration Center. https://www.dhs.gov/national-cybersecurity-and-communications-integration-center, accessed August 4, 2018.
2018i Office of Cyber and Infrastructure Analysis. https://www.dhs.gov/office-cyber-infrastructure-analysis, accessed August 4, 2018.
2018j Science and Technology. https://www.dhs.gov/science-and-technology/our-work, accessed August 4, 2018.
2018k Cyber Security Division. https://www.dhs.gov/science-and-technology/cyber-security-division, accessed August 4, 2018.
2019 Infrastructure Policy: Supporting Policy and Doctrine. Department of Homeland Security. https://www.dhs.gov/cisa/supporting-policy-and-doctrine, accessed July 16, 2019.

Di Camillo, Federica, and Valérie Miranda
2011 Ambiguous Definitions in the Cyber Domain: Costs, Risks and the Way Forward. Istituto Affari Internazionali (IAI), IAI Working Papers 1126. http://www.iai.it/pdf/DocIAI/iaiwp1126.pdf, accessed June 11, 2012.

DoD
2015 Fact Sheet: The Department of Defense (DoD) Cyber Strategy. https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Department_of_Defense_Cyber_Strategy_Fact_Sheet.pdf, accessed August 21, 2018.

DoJ
2018a Strategic Plan. Fiscal Years 2014-2018. https://www.justice.gov/sites/default/files/jmd/legacy/2014/02/28/doj-fy-2014-2018-strategic-plan.pdf#s4.
2018b About CCIPS. https://www.justice.gov/criminal-ccips/about-ccips, accessed August 23, 2018.
2018c Cybersecurity Unit. https://www.justice.gov/criminal-ccips/cybersecurity-unit, accessed August 23, 2018.

Donati, Paolo R.
2001 Die Rahmenanalyse Politischer Diskurse. *In* Handbuch Sozialwissenschaftliche Diskursanalyse. Band I: Theorien Und Methoden. Reiner Keller, Andreas Hirseland, Werner Schneider, and Willy Viehöver, eds. Pp. 145–175.

Dörner, Astrid
2018 “Künstliche Intelligenz ist nicht besser als die menschliche” - Interview mit Cathy Bessant. Handelsblatt, September 5.

Dresing, Thorsten, and Thorsten Pehl
2013 Praxisbuch Interview, Transkription & Analyse. Anleitungen und Regelsysteme für qualitativ Forschende. Marburg, 5. Auflage.

Druckman, James N.
2001 The Implications of Framing Effects for Citizen Competence. Political Behavior 23(3): 225–256.

Dunn Cavelty, Myriam
2008 Cyber-Security and Threat Politics. US Efforts to Secure the Information Age. London; New York: Routlegde.
2010 Cyber-Security. *In* The Routledge Handbook of New Security Studies. J. Peter Burgess, ed. Pp. 154–162. London; New York: Routlegde.
2013 From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. International Studies Review 15(1): 105–122.
2014 Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. Science and Engineering Ethics 20(3): 701–715.

Ebert, Christof, and Dominik Lieckfeldt
2017 Risk-Oriented Security Engineering. *In* Automotive – Safety & Security 2017. Sicherheit und Zuverlässigkeit für automobile Informationstechnik. Peter Dencker, Herbert Klenk, Hubert B. Keller, and Erhard Plödereder, eds. Lecture Notes in Informatics - Proceedings. Bonn: Gesellschaft für Informatik (GI). https://dl.gi.de/bitstream/handle/20.500.12116/144/lni-p-269-komplett.pdf?sequence=1&isAllowed=y, accessed March 9, 2019.

Ebert, Hannes, and Tim Maurer
2013 Contested Cyberspace and Rising Powers. Third World Quarterly 34(6): 1054–1074.

Entman, Robert M.
1993 Framing: Toward Clarification of a Fractured Paradigm. Journal of Communication 43(4): 51–58.

Ermisch, Steffen
2018 Gefährlicher Wildwuchs. Handelsblatt, October 8: 48–49.

European Commission
2018a International Digital Economy and Society Index 2018. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54991, accessed July 16, 2019.
2018b NIS Directive. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.
2019a The Digital Economy and Society Index (DESI). Text. Digital Single Market - European Commission. https://ec.europa.eu/digital-single-market/en/desi, accessed July 16, 2019.
2019b Digital Economy and Society Index (DESI) 2019 Country Report Germany. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=59893, accessed July 16, 2019.

FBI
2018a Cyber Crime. https://www.fbi.gov/investigate/cyber, accessed August 23, 2018.
2018b Addressing Threats to the Nation's Cybersecurity. https://www.fbi.gov/file-repository/addressing-threats-to-the-nations-cybersecurity-1.pdf/view, accessed August 23, 2018.
2018c Cyber Task Forces: Building Alliances to Improve the Nation's Cybersecurity. https://www.fbi.gov/file-repository/cyber-task-forces-fact-sheet.pdf/view, accessed August 23, 2018.
2018d National Cyber Investigative Joint Task Force. https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force, accessed August 23, 2018.

Fluck, Winfried
2004 Exzeptionalismus. *In* Länderbericht USA. Geschichte, Politik, Wirtschaft, Gesellschaft, Kultur. Peter Lösche and Hans Dietrich von Loeffelholz, eds. Pp. 705–706. Bonn: Bundeszentrale für politische Bildung.
2016 American Exceptionalism: Ein Schlüssel zum amerikanischen Selbstverständnis. *In* Handbuch Politik USA. Christian Lammert, Markus B. Siewert, and Boris Vormann, eds. Pp. 15–28. Wiesbaden: Springer.

Friedman, Allan A.
2013 Cyber Theft of Competitive Data: Asking the Right Questions. Brookings Institution, Center for Technology Innovation.
http://www.brookings.edu/~/media/research/files/papers/2013/09/25%20cyber%20theft%20competitive%20data%20friedman/brookingscybertech_revised.pdf.

Fuchs, Dieter, and Edeltraud Roller
2007 Politik. *In* Lexikon Politik. Hundert Grundbegriffe. Dieter Fuchs and Edeltraud Roller, eds. Pp. 205–209. Stuttgart: Philipp Reclam jun.

Goffman, Erving
1993 Rahmen-Analyse. Ein Versuch Über Die Organisation von Alltagserfahrungen. Frankurt am Main: Suhrkamp.

Goldstein, Kenneth
2002 Getting in the Door: Sampling and Completing Elite Interviews. Political Science and Politics (PS) 35(4): 669–672.

GovTrack
2019 Cyber Intelligence Sharing and Protection Act (2012 - H.R. 3523). GovTrack.Us. https://www.govtrack.us/congress/bills/112/hr3523, accessed January 12, 2019.

Grabosky, Peter
2013 Organised Crime and the Internet. The RUSI Journal 158(5): 18–25.

Gross Stein, Janice
2013 Threat Perception in International Relations. *In* The Oxford Handbook of Political Psychology. Leonie Huddy, David O. Sears, and Jack S. Levy, eds. Pp. 364–394. New York: Oxford University Press.

Guitton, Clement
2013 Cyber Insecurity as a National Threat: Overreaction from Germany, France and the UK? European Security 22(1): 21–35.

Hansen, Lene, and Helen Nissenbaum
2009 Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly 53: 1155–1175.

Herz, Carsten
2018 Der Feind aus der Datenleitung. Handelsblatt, November 1: 22–23.

Hitzler, Ronald, and Anne Honer
1997 Einleitung: Hermeneutik in der deutschsprachigen Soziologie heute. *In* Sozialwissenschaftliche Hermeneutik. Eine Einführung. Ronald Hitzler and Anne Honer, eds. Pp. 7–27. Opladen: Leske + Budrich.

Hofer, J., C. Kapalschinski, F. Kolf, and G. Weishaupt
2018 Übermacht Amazon. Handelsblatt, November 7: 4–5.

ICE
2018 Cyber Crimes Center. https://www.ice.gov/cyber-crimes, accessed August 4, 2018.

ISO
2019 ISO/IEC 27000 Family - Information Security Managment Systems. https://www.iso.org/isoiec-27001-information-security.html, accessed January 12, 2019.

Jansen, Jonas
2018 Warum sich der Chef um IT-Sicherheit kümmern muss. Frankfurter Allgemeine Zeitung, September 10. http://www.faz.net/aktuell/wirtschaft/cyber-schutz-warum-sich-der-chef-um-it-sicherheit-kuemmern-muss-15779358.html, accessed November 26, 2018.

Jarvis, Lee, Stuart Macdonald, and Andrew Whiting
2015 Constructing Cyberterrorism as a Security Threat: A Study of International News Media Coverage. Perspectives on Terrorism 9(1): 60–75.

Johanson, Derek
2013 The Evolving U.S. Cybersecurity Doctrine. Security Index: A Russian Journal on International Security 19(4): 37–50.

Johnston, Cameron
2015 Russia's Info-War: Theory and Practice. European Union Institute for Security Studies (EUISS), Issue Alert 22/2015. http://www.iss.europa.eu/uploads/media/Alert_22_Russia_s_info-war.pdf.

Keller, Reiner
1997a Müll - Die Gesellschaftliche Konstruktion Des Wertvollen. Ein Diskursanalytischer Vergleich Der Öffentlichen Diskussion Über Hausmüll in Deutschland Und Frankreich. Ph.D. Thesis, Technische Universität München.
1997b Diskursanalyse. *In* Sozialwissenschaftliche Hermeneutik. Eine Einführung. Ronald Hitzler and Anne Honer, eds. Pp. 309–333. Opladen: Leske + Budrich.
2003 Der Müll der Gesellschaft. Eine wissenssoziologische Diskursanalyse. *In* Handbuch Sozialwissenschaftliche Diskursanalyse. Band II: Forschungspraxis. Reiner Keller, Andreas Hirseland, Werner Schneider, and Willy Viehöver, eds. Pp. 197–232. Opladen: Leske + Budrich.
2004 Diskursforschung. Eine Einführung Für SozialwissenschaftlerInnen. Opladen: Leske + Budrich.
2011a Wissenssoziologische Diskursanalyse. Grundlegung eines Forschungsprogramms. Wiesbaden: VS Verlag für Sozialwissenschaften.
2011b The Sociology of Knowledge Approach to Discourse (SKAD). Human Studies 34(1): 43–65.
2014 Technikrisiken und wissenssoziologische Diskursforschung. Technikfolgenabschätzung – Theorie und Praxis 23(2): 15–21.

Keller, Reiner, Andreas Hirseland, Werner Schneider, and Willy Viehöver
2001 Zur Aktualität Sozialwissenschaftlicher Diskursanalyse - Eine Einführung. *In* Handbuch Sozialwissenschaftliche Diskursanalyse. Band I: Theorien Und Methoden. Reiner Keller, Andreas Hirseland, Werner Schneider, and Willy Viehöver, eds. Pp. 7–27. Opladen: Leske +

Budrich.
2003 Die Vielgestaltige Praxis Der Diskursforschung - Eine Einführung. *In* . Reiner Keller, Andreas Hirseland, Werner Schneider, and Willy Viehöver, eds. Pp. 7–18. Opladen: Leske + Budrich.

Kerkmann, Christof
2018 Ein mächtiger Fachidiot. Wie kann die Menschheit künstliche Intelligenz nutzen, ohne sich selbst überflüssig zu machen? Handelsblatt, October 29: 18–19.

Knitterscheidt, Kevin, and Georg Weishaupt
2018 Revolution auf leisen Sohlen. Handelsblatt, November 6: 18–19.

Kolton, Michael
2017 Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence. The Cyber Defense Review 2(1): 119–154.

KPMG
2014 IT-Sicherheit in Deutschland. Handlungsempfehlungen für eine zielorientierte Umsetzung des IT-Sicherheitsgesetzes.
https://www.bitkom.org/sites/default/files/file/import/Studie-IT-Sicherheit-in-Deutschland-BDI.pdf, accessed July 26, 2019.

Kruse, Jan
2011 Reader "Einführung in die Qualitative Interviewforschung." Freiburg.

Kullik, Jakob
2014 Vernetzte (Un-)Sicherheit? Eine politisch-rechtliche Analyse der deutschen Cybersicherheitspolitik. Chemnitzer Schriften zur europäischen und internationalen Politik, Band 7. Hamburg: Verlag Dr. Kovac.

Lawson, Sean
2013 Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats. Journal of Information Technology & Politics 10(1): 86–103.

Leech, Beth L.
2002 Asking Questions: Techniques for Semistructured Interviews. Political Science and Politics (PS) 35(4): 665–668.

Lewis, James A.
2014 National Perceptions of Cyber Threats. Strategic Analysis 38(4): 566–576.

Löfstedt, Ragnar E., and David Vogel
2001 The Changing Character of Regulation: A Comparison of Europe and the United States. Risk Analysis 21(3): 399–405.

Lord, Kristin M., and Travis Sharp
2011 America's Cyber Future. Security and Prosperity in the Information Age, Volume I. Center for a New American Security (CNAS).

https://s3.amazonaws.com/files.cnas.org/documents/CNAS_Cyber_Volume-I_0.pdf?mtime=20160906081238, accessed August 1, 2019.

Lösche, Peter
2008a Merkmale der Präsidialdemokratie. bpb.de. http://m.bpb.de/internationales/amerika/usa/10640/praesidialdemokratie, accessed July 14, 2019.
2008b Macht und Ohnmacht der Exekutive. bpb.de. http://m.bpb.de/internationales/amerika/usa/10643/exekutive, accessed July 14, 2019.

Louven, Sandra, and Johannes Steger
2018 Die große Mahnung aus Lissabon. Handelsblatt, November 7: 18.

Maaßen, Hans-Georg
2018 Rede von BfV-Präsident Dr. Maaßen auf der 6. Potsdamer Konferenz für Nationale CyberSicherheit am 21. Juni 2018: "Die Lage in Deutschland." https://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/vortraege/rede-maassen-20180621-potsdamer-konferenz-fuer-nationale-cybersicherheit, accessed August 31, 2018.

Matthes, Jörg, and Matthias Kohring
2008 The Content Analysis of Media Frames: Toward Improving Reliability and Validity. Journal of Communication 58: 258–279.

McCarthy, John D., Jackie Smith, and Mayer N. Zald
1996 Accessing Public, Media, Electoral, and Governmental Agendas. *In* Comparative Perspectives on Social Movements. Political Opportunities, Mobilizing Structures, and Cultural Framings. Doug McAdam, John D. McCarthy, and Mayer N. Zald, eds. Pp. 291–311. Cambridge, New York, Melbourne: Cambridge University Press.

Meiser, Ursula
2011 Die Konstruktion Europas in Der Elitendiskussion. Eine Frameanalyse Parlamentarischer Debatten in Deutschland Und Italien. Universität Stuttgart. http://elib.uni-stuttgart.de/opus/volltexte/2011/6284/pdf/Konstruktion_Europas.pdf.

Meyer, Christoph O.
2009 International Terrorism as a Force of Homogenization? A Constructivist Approach to Understanding Cross-National Threat Perceptions and Responses. Cambridge Review of International Affairs 22(4): 647–666.

Meyer, Christoph O., and Alister Miskimmon
2009 Perceptions and Responses to Threats: Introduction. Cambridge Review of International Affairs 22(4): 625–628.

National Institute of Standards and Technology (NIST)
2018 National Initiative for Cybersecurity Education (NICE). https://www.nist.gov/itl/applied-cybersecurity/nice/about.

NIST
2013a Initial Analysis of Cybersecurity Framework RFI Responses. https://www.nist.gov/sites/default/files/documents/2017/05/31/nist-initial-analysis-of-rfi-responses.pdf, accessed December 15, 2018.
2013b RFI - Framework for Reducing Cyber Risks to Critical Infrastructure. NIST. https://www.nist.gov/cyberframework/rfi-framework-reducing-cyber-risks-critical-infrastructure-2013, accessed December 25, 2018.
2018a Evolution of the Framework. NIST. https://www.nist.gov/cyberframework/evolution, accessed December 15, 2018.
2018b NIST General Information. https://www.nist.gov/director/pao/nist-general-information.
2018c Laboratories. https://www.nist.gov/labs-major-programs/laboratories.

NTIA
2018a About NTIA. https://www.ntia.doc.gov/about, accessed August 23, 2018.
2018b IANA Functions. https://www.ntia.doc.gov/category/iana-functions, accessed August 23, 2018.
2018c Eighth Quarterly Report on the Transition of the Stewardship of the Internet Assigned Numbers Authority (IANA) Functions. https://www.ntia.doc.gov/report/2016/eighth-quarterly-report-transition-stewardship-internet-assigned-numbers-authority-iana, accessed August 23, 2018.
2018d Internet Policy Task Force. https://www.ntia.doc.gov/category/internet-policy-task-force, accessed August 23, 2018.

Nye, Jr., Joseph S.
2010 Cyber Power. Harvard Kennedy School, Belfer Center for Science and International Affairs. http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf, accessed August 1, 2019.

ODNI
2017 ODNI Factsheet. https://www.dni.gov/files/documents/FACTSHEET_ODNI_History_and_Background_2_24-17.pdf, accessed August 18, 2018.
2018 Members of the IC. https://www.dni.gov/index.php/what-we-do/members-of-the-ic, accessed August 18, 2018.

O'Riordan, Timothy, and Brian Wynne
1987 Regulating Environmental Risks: A Comparative Perspective. *In* Insuring and Managing Hazardous Risks: From Seveso to Bhopal and Beyond. Paul R. Kleindorfer and Howard C. Kunreuther, eds. Pp. 389–410. Berlin, Heidelberg, New York, London, Paris, Tokyo: Springer.

Potthoff, Matthias
2012 Medien-Frames und ihre Entstehung. Wiesbaden: VS Verlag für Sozialwissenschaften.

Renn, Ortwin
2001 The Changing Character of Regulation: A Comparison of Europe and the United States. Commentary. Risk Analysis 21(3): 406–410.
2008 Risk Governance: Coping with Uncertainty in a Complex World. London; Sterling, VA:

Earthscan.

Rid, Thomas
2012 Cyber War Will Not Take Place. Journal of Strategic Studies 35(1): 5–32.

Rieger, Sebastian
2014 Wie verankert man Digitalpolitik in der Bundesregierung? Zuständigkeiten, Entstehungsprozess und Führungsmodell der digitalen Agenda. Stiftung Neue Verantwortung, Policy Brief. https://www.stiftung-nv.de/sites/default/files/policy_brief_digitale_agenda.pdf, accessed August 31, 2018.

Roberts, Sam
2017 Howard Schmidt, Cybersecurity Adviser to Two Presidents, Dies at 67. The New York Times, December 22. https://www.nytimes.com/2017/03/04/us/howard-schmidt-dead-white-house-cybersecurity-aide.html, accessed August 4, 2018.

Rosenzweig, Paul
2015 The Cybersecurity Act of 2015. https://www.lawfareblog.com/cybersecurity-act-2015, accessed January 12, 2019.

Rötzer, Florian
2007 DDoS-Angriffe auf estnische Server waren kein “Cyberwar.” heise online. https://www.heise.de/newsticker/meldung/DDoS-Angriffe-auf-estnische-Server-waren-kein-Cyberwar-138918.html, accessed August 5, 2019.

Rudzio, Wolfgang
2006 Das politische System der Bundesrepublik Deutschland. Wiesbaden: VS Verlag für Sozialwissenschaften.

Schaller, Christian
2014 Internationale Sicherheit und Völkerrecht im Cyberspace. Für klarere Regeln und mehr Verantwortung. SWP-Studie S 18, Stiftung Wissenschaft und Politik, Berlin. http://www.swp-berlin.org/fileadmin/contents/products/studien/2014_S18_slr.pdf, accessed August 5, 2019.

Schulze, Tillmann
2006 Bedingt abwehrbereit. Schutz kritischer Informations-Infrastrukturen in Deutschland und den USA. Wiesbaden: VS Verlag für Sozialwissenschaften.

Snow, David A.
2004 Framing Processes, Ideology, and Discursive Fields. *In* The Blackwell Companion to Social Movements. David A. Snow, Sarah A. Soule, and Hanspeter Kriesi, eds. Pp. 380–412. Blackwell Publishing Ltd.

Snow, David A., and Robert D. Benford
1992 Master Frames and Cycles of Protest. *In* Frontiers in Social Movement Theory. Aldon D. Morris and Carol M. Mueller, eds. Pp. 133–155. New Haven/London: Yale University Press.

State
2018 Office of the Coordinator for Cyber Issues. https://www.state.gov/s/cyberissues/index.htm, accessed August 22, 2018.

Steinharter, Hannah, and Michael Maisch
2018 Wenn Maschinen diskriminieren. Handelsblatt, August 27: 28.

Stevens, Tim
2018 Global Cybersecurity: New Directions in Theory and Methods. Politics and Governance 6(2): 1–4.

Stine, Kevin, Kim Quill, and Greg Witte
2014 Framework for Improving Critical Infrastructure Cybersecurity. NIST ITL Bulletin(2014–02).

Stone, John
2012 Cyber War Will Take Place! Journal of Strategic Studies 36(1): 101–108.

Teplinsky, Melanie J.
2013 Fiddling on the Roof: Recent Developments in Cybersecurity. American University Business Law Review 2(2): 225–322.

Tessier Stall, Sacha
2011 The Future of Cybersecurity. The Hague Centre for Strategic Studies and TNO, Paper No. 2011-4. http://www.inteltimes.net/wp-content/uploads/2012/09/The-Future-of-Cyber-Security.pdf, accessed June 22, 2012.

United Nations Office for Disarmament Affairs (UNODA)
2015 Fact Sheet - Developments in the Field of Information and Telecommunications in the Context of International Security. https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/07/Information-Security-Fact-Sheet-July2015.pdf.

U.S. Department of Defense
2010 U.S. Cyber Command Fact Sheet. http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf.

U.S. Secret Service
2018 Investigation. https://www.secretservice.gov/investigation/#field, accessed August 4, 2018.

Vijayan, Jaikumar
2010 Obama Administration Partially Lifts Secrecy on Classified Cybersecurity Project. Computerworld. https://www.computerworld.com/article/2520273/obama-administration-partially-lifts-secrecy-on-classified-cybersecurity-project.html, accessed May 1, 2019.

Vogel, David
1986 National Styles of Regulation. Environmental Policy in Great Britain and the United

States. Ithaca/London: Cornell University Press.
2003 The Hare and the Tortoise Revisited: The New Politics of Consumer and Environmental Regulation in Europe. British Journal of Political Science 33(04): 557–580.

Wallace, Ian
2013a Why the U.S. Is Not in a Cyber War. The Daily Beast. http://www.thedailybeast.com/articles/2013/03/10/why-the-u-s-is-not-in-a-cyber-war.html.
2013b Militarizing the Internet? The National Interest. http://nationalinterest.org/commentary/militarizing-the-internet-8734.
2013c Cyber Security: Why Military Forces Should Take a Back Seat. The Interpreter. http://www.lowyinterpreter.org/post/2013/10/21/Cyber-security-Why-military-forces-should-take-a-back-seat.aspx.

Weddeling, Britta
2018 Eine Branche zügelt sich selbst. Handelsblatt, October 18: 14–15.

Welchering, Peter
2018 Ein Sicherheitsschloss für die digitale Fabrik. Frankfurter Allgemeine Zeitung, September 25. http://www.faz.net/aktuell/technik-motor/digital/ein-sicherheitsschloss-fuer-die-digitale-fabrik-15803332.html?service=printPreview, accessed November 26, 2018.

WH
2013a Presidential Policy Directive - Critical Infrastructure Security and Resilience (PPD-21). https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, accessed October 20, 2018.
2013b Executive Order - Improving Critical Infrastructure Cybersecurity (EO 13636). https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity, accessed October 20, 2018.

White House
2018a Introducing the New Cybersecurity Coordinator. https://obamawhitehouse.archives.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator, accessed August 5, 2018.
2018b Michael Daniel. https://obamawhitehouse.archives.gov/blog/author/michael-daniel, accessed August 5, 2018.

White House, Barack Obama
2015 Executive Order 13694, Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities. https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf.

Wiener, Jonathan B.
2011 The Rhetoric of Precaution. *In* The Reality of Precaution: Comparing Risk Regulation in the United States and Europe. Jonathan B. Wiener, Michael D. Rogers, James K. Hammitt, and Peter H. Sand, eds. Pp. 3–35. Washington, D.C.; London: RFF Press.

Wiener, Jonathan B., and Michael D. Rogers
2002 Comparing Precaution in the United States and Europe. Journal of Risk Research 5(4):

317–349.

Ziegler, Peter-Michael
2007 In Estland wurde der Cyber-Krieg getestet. heise online.
https://www.heise.de/newsticker/meldung/In-Estland-wurde-der-Cyber-Krieg-getestet-133482.html, accessed August 5, 2019.

8 Appendices

8.1 Examples from the Text Inventory

In the following, two examples from the text inventory are presented referring to one exemplary text of each data corpus.

USA 2009 White House Obama Remarks on Securing Our Nations Cyber Infrastructure

1. Hauptinhalt:
   - Problembeschreibung: Digital infrastructure = backbone of economy, military, government. Dependence on cyberspace every day, it is woven in every aspect of life. Irony of Information Age/Paradox: Technologies that empower U.S. empower also those who would like to disrupt and destroy. Manifestations of paradox: privacy and economic security → privacy violations, economic competitiveness → theft of sensitive information, public safety and national security → military under constant attack, acts of terror with computers, cyber means in wars (Russia/Georgia).
   - Problembeschreibung/Analyse in Bezug auf Regierung: U.S. not as prepared as it should be, failed to invest in the security of digital infrastructure, federal government not well organized. Ergebnis: Status quo no longer acceptable, President directed review. Review process open and transparent.
   - Problemlösung: Administration will pursue a new approach to securing America's digital infrastructure. It will be treated as a strategic national asset, a national security priority. Networks shall be „secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage".
   - Problemlösung, konkrete Maßnahmen: Cybersecurity Coordinator at the White House → to ensure high-level focus and attention. Tasks u.a.: orchestrating and integrating all cybersecurity policies for the government.
   - Five key areas of action: 1) New comprehensive strategy, coordinated approach across government with Cybersecurity Coordinator, key management priority of President, milestones and performance metrics, 2) Work with all key players to be able to respond to future incidents in an organized and unified manner (plans, information sharing, warnings), 3) Strengthen public-private partnership, no dictation of security standards, 4) Invest in cutting-edge R&D, invest in infrastructure, 5) National campaign for awareness and literacy, digital workforce.
   - Cybersecurity policy will not include monitoring private sector networks or Internet traffic → protection of privacy and civil liberties, commitment to net neutrality.
   - Task of cybersecurity policy will not be easy (more and more people online, groups and governments sharpen cyber capabilities). Information Age only in its infancy. New world of greater security and prosperity is possible, if U.S. reaches for it and if it leads. U.S. = nation that invented the Internet, that launched information revolution.
2. Bezug KI:
   - ja (im Prinzip ganze Rede über critical information infrastructure, oft genannt digital infrastructure)
3. Text-Kategorie:
   - Problemlösung
4. Zu kodieren:
   - vollständig
5. Sonstiges/Gedanken:
   - Deutlich: Cyber als strategic asset, als national security priority, hochrangige Stellung unter Obama. Präsident geht voran in der Leitung dieses neuen Bereichs, neue umfassende Strategie.
   - Keine Gesetzgebung angekündigt (es werden keine Sicherheitsstandards diktiert)
   - Leadership-Anspruch der USA. Leadership sichert Dominanz.

D 2016 BMI Cybersicherheitsstrategie

1. Hauptinhalt:
    - Digitalisierung hat Deutschland verändert, Chancen und Risiken entstehen. Staat und Wirtschaft müssen Vertrauen herstellen. Sicherheit ist dafür sehr wichtig.
    - Text schreibt Strategie von 2011 weiter, aber Cybersicherheit wird verstärkt als gesamtstaatliche Aufgabe gesehen. Daher neue ressortübergreifende Strategie.
    - Hauptanliegen: Handlungsfähigkeit und Souveränität Deutschlands müssen gewährleistet sein, Chancen der Digitalisierung sollen genutzt werden, indem Risiken beherrschbar gemacht werden. Freiheit und Sicherheit auch im Cyber-Raum gewährleisten → zentrale Aufgabe des Staates.
    - Gemeinsame Verantwortung von Staat, Wirtschaft, Wissenschaft und Gesellschaft.
    - Vier Handlungsfelder mit Querschnittscharakter: 1) Sicheres und selbstbestimmtes Handeln (u.a. digitale Kompetenz der Anwender → Beurteilungskompetenz, sichere Kommunikation/elektronische Identitäten, Zertifizierung, IT-Sicherheitsforschung → vertrauenswürdige Technologie und Rahmenbedingungen), 2) Gemeinsamer Auftrag von Staat und Wirtschaft (CIP/kooperativer Ansatz mit ITSiG, Unternehmen schützen, IT-Wirtschaft stärken, Zusammenarbeit mit Providern, Informationsaustausch, Austausch von IT-Personal), 3) Gesamtstaatliche Cyber-Sicherheitsarchitektur (Staat muss Institutionen so aufstellen, dass er seinen Schutzauftrag erfüllen kann, NCAZ weiter entwickeln, Fähigkeiten zur Analyse und Reaktion vor Ort stärken (mobile Teams von BSI, BKA, BfV etc.), Strafverfolgung, Cyber-Spionage/Sabotage, BND-Frühwarnsystem, Verteidigungsaspekte, Bundesverwaltung sichern, Zusammenarbeit Bund-Länder, Personalentwicklung), 4) Internationales Handeln (europäische Cyber-Sicherheitspolitik, NATO, Capacity Building, internationale Strafverfolgung), Nationaler Cyber-Sicherheitsrat als ständiger Ratgeber der Bundesregierung
2. Bezug KI:
    - ja, allerdings nur ein Punkt unter vielen, erster Punkt unter 2)
3. Text-Kategorie:
    - Problemlösung, Mischung aus Strategie und Maßnahmen, Zweiteres stärker, relativ konkret, umfassend
4. Zu kodieren:
    - vollständig
5. Sonstiges/Gedanken:
    - Starke Betonung eines ganzheitlichen, gesamtstaatlichen Ansatzes.
    - Bedrohungslage sehr konkret beschrieben. Neuere Phänomene wie Desinformation aufgenommen.
    - “Digitaler Sorglosigkeit entgegenwirken” – negative Ausdrucksweise, Unterstellung von fehlendem Verantwortungsbewusstsein.
    - Viele konkrete Nennungen: z.B. Behörden müssen auch entschlüsseln können, Bundeswehr hat auch offensive Fähigkeiten
    - Text eher sicherheitsfokussiert; eher risiko-/gefährungs-/vorsicht-basierte Sprache
    - Vor allem im Bereich 3) wird massiv ausgebaut – neue Institutionen, Kooperationen, sehr viel offensiver/aktiver.
    - Insgesamt Weiterentwicklung, Verstärkung und Differenzierung der Strategie von 2011, “offensiver”/verteidigender Aspekt stärker → weniger passiv abwartend/zurückhaltend, mehr aktiv handelnd.

8.2 Coding System Used for the Frame Analysis

In the following, the coding system I used for the frame analysis is displayed.

Problem definition and evaluation of cybersecurity risks

- Cyber(security) Risks
  - Description, Causes
    - Particularities, Challenges of Cyberspace
    - Espionage, Electronic Attacks
    - Cybercrime Description and Evaluation
    - Internet Freedom Risks, Censorship, Surveillance
  - Evaluation
    - What is threatened?
    - Growing, Intensifying, Changing Threat
    - Other Evaluations
  - Other

Causes: Drivers and actors creating cybersecurity risks

- Dependence, Vulnerability
- Interconnectivity
- Domestic/Foreign Security (Policy)
- Transformative Character, Permanent Change, Chances & Risks
- Actors creating the problem
  - Variety of Actors, General Aspects
  - Special Actors

Articulating solutions: actors responsible for solving the problem of cyber risks, the goals of solutions and concrete problem-solving measures

- Responsibility
  - Role of the State, Self-Definition, Attitude
    - Demands towards Others, Criticism
    - Whole-of-Government, Interagency
  - Private Sector
  - Institutions
  - Shared Responsibility
    - State and Private Sector, PPP
    - International Cooperation
    - Variety of Responsible Actors
  - Other
- Goals
  - Create Cyber/IT Security, Resilience, C(I)P
  - Use Potential of Digitalization
  - Variety of Goals
  - Privacy, Data Protection
  - Other
- Measures
  - Cyber IT/Security, Resilience, CI(I)P, CERTs
  - Measures on the Political/Legal Level, Rules
    - National
      - Details CSF
    - International
    - Combat Cybercrime, Cyberespionage
  - Measures Regarding Technology

- Standards, Certification
- Trusted Identity
- Encryption

Information-Sharing, Communication
Strengthen the (IT) Economy
- Protect IP
- Global Economy, Open Markets

Innovation
R&D
Measures Regarding People
Cooperation, Interests
Military, Defense, Intelligence
Cyber Capacity Building
Federal Cyber Security
Combination of Measures
Other

Erklärung

Ich erkläre, dass ich, abgesehen von den ausdrücklich bezeichneten Hilfsmitteln, die Dissertation selbständig verfasst habe. Alle Stellen, die dem Wortlaut oder Sinn nach anderen Werken entnommen sind, wurden durch Angabe der Quellen als Entlehnung kenntlich gemacht.

17.05.2020

Kathrin Ulmer