AIPA 2/2016

Arbeitspapiere zur Internationalen Politik
und Außenpolitik

Dominika Zedler

Zur strategischen Planung von Cyber Security in Deutschland

Lehrstuhl Internationale Politik
Universität zu Köln

ISSN 1611-0072

AIPA 2/2016

Arbeitspapiere zur Internationalen Politik
und Außenpolitik

Dominika Zedler

Zur strategischen Planung von Cyber Security in Deutschland

ISSN 1611-0072

Lehrstuhl Internationale Politik
Universität zu Köln, Gottfried-Keller-Str. 6, 50931 Köln

Redaktionelle Bearbeitung: Helena Fabricius und Mira Böing

Köln 2016

Abstract

In dieser Arbeit wird die strategische Planung der Cyber Security in Deutschland untersucht. Das hohe Gefahrenpotenzial für Staat, Wirtschaft und Gesellschaft durch kriminelle und terroristische Angriffe auf Kritische Infrastrukturen und durch Wirtschaftsspionage nimmt mit der fortschreitenden Digitalisierung weiter zu. Eine übergeordnete Strategie und eine effiziente Koordination der verantwortlichen politisch-institutionellen Akteure sind genauso wenig festzustellen wie exakte Definitionen und konkrete Maßnahmenkataloge, obgleich ein wachsendes Problembewusstsein und strategische Ansätze bei einzelnen Institutionen erkennbar sind. Während der Schutz vor Wirtschaftsspionage und die Zusammenarbeit zwischen Politik und Wirtschaft stark verbesserungswürdig scheinen, ist der Schutz Kritischer Infrastrukturen seit 2005 kontinuierlich ausgeweitet worden. Sowohl im Hinblick auf die politischen Rahmenbedingungen als auch personell und technisch ist ein Nachholbedarf zu konstatieren. Es wird angeregt, die Möglichkeit der Beseitigung der fragmentarischen Organisation der vielfältigen Verantwortlichkeiten durch die Schaffung einer zentralen Koordinierungsstelle zu erwägen.

Keywords: Cyber Security, Sicherheitspolitik, IT-Sicherheit, Wirtschaftsspionage, Cyberkriminalität, Cyberterrorismus, Kritische Infrastrukturen

Dominika Zedler

hat Politikwissenschaft an der Universität zu Köln studiert.

Kontakt: dominika.zedler@t-online.de

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AA	Auswärtiges Amt
ASW	Bundesverband Arbeitsgemeinschaft für Sicherheit in der Wirtschaft e. V.
BAAINBw	Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BDI	Bundesverband der Deutschen Industrie e. V.
BfV	Bundesamt für Verfassungsschutz
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
BKA	Bundeskriminalamt
BMI	Bundesministerium des Innern
BMVg	Bundesministerium der Verteidigung
BMVi	Bundesministerium für Verkehr und digitale Infrastruktur
BMWi	Bundesministerium für Wirtschaft und Energie
BND	Bundesnachrichtendienst
BSI	Bundesamt für Sicherheit in der Informationstechnik
CERT	Computer Emergency Response Team
CERT-Bund	Computer Emergency Response Team der Bundesverwaltung
CERTBw	Computer Emergency Response Team der Bundeswehr
Cyber-AZ	Cyber-Abwehrzentrum
Cyber-SR	Cyber-Sicherheitsrat
eco	Verband der deutschen Internetwirtschaft e. V.
EU	Europäische Union
GCHQ	Government Communications Headquarters
HP	Hewlett-Packard
IKT	Informations- und Kommunikationstechnologien
IT	Informationstechnik

KRITIS	Kritische Infrastrukturen
KSA	Kommando Strategische Aufklärung
MAD	Militärischer Abschirmdienst
NATO	North Atlantic Treaty Organization
NIFIS e. V.	Nationale Initiative für Informations- und Internet-Sicherheit
NPSI	Nationaler Plan zum Schutz der Informationsinfrastrukturen
NSA	National Security Agency
OECD	Organization for Economic Co-operation and Development
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
UP	Umsetzungsplan

Zur strategischen Planung von Cyber Security in Deutschland

1 Einleitung

In der Bundesrepublik Deutschland kommt es täglich zu Angriffen aus dem Cyberspace im privaten Bereich, in der Wirtschaft und in der öffentlichen Verwaltung (vgl. Bundesamt für Sicherheit in der Informationstechnik 2014, S. 11). Eine Studie von Kaspersky Lab zeigt, dass die Bundesrepublik Deutschland 2012 bis 2013 im globalen Vergleich eines der am häufigsten angegriffenen Staaten darstellte: Neben den USA mit 26,17 %, Russland mit 24,53 % und Großbritannien mit 17,8 % befindet sich die Bundesrepublik Deutschland mit 11,67 % aller verzeichneten Cyber-Attacken weltweit an vierter Stelle. Zwar schwankten die Zahlen über das Jahr, jedoch nicht die Rangfolge der Länder, die am häufigsten angegriffen wurden (vgl. Kaspersky Lab 2013). Wie aus Abbildung 1 hervorgeht, sind in den und gegen die genannten Staaten über 80 Prozent aller Cyber-Angriffe zu konstatieren. Somit steht fest, dass Deutschland einer massiven Bedrohung aus dem Cyberspace ausgesetzt ist.

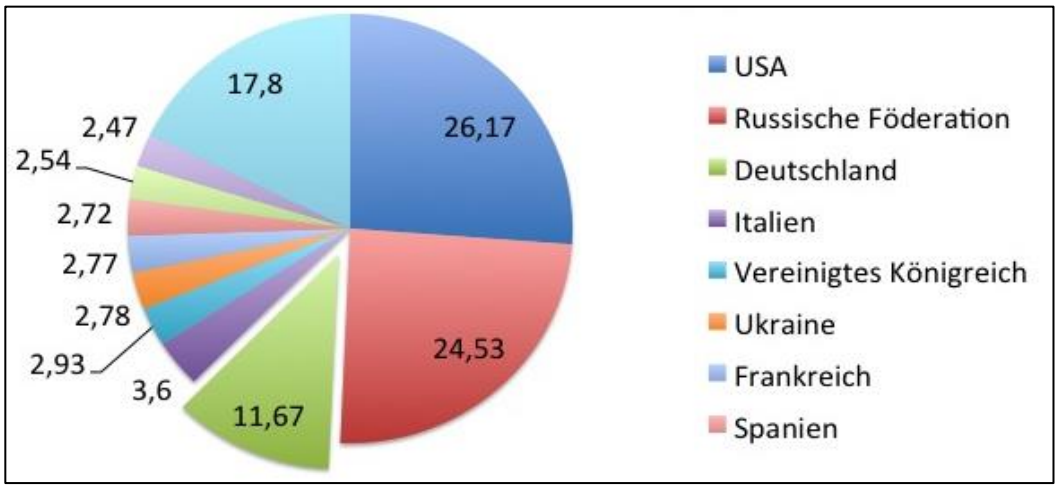

Abb. 1 Die am häufigsten attackierten Staaten 2012-2013 (Quelle: Kaspersky Lab, 2013)

Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nehmen die Möglichkeiten zur Durchführung von Cyber-Angriffen täglich zu. Mit der zunehmenden Digitalisierung von Staat, Wirtschaft und Gesellschaft gehen zugleich eine stetige Weiterentwicklung der Angriffsmethoden und eine effizientere Nutzung der vorhandenen Angriffsmittel einher. Das Internet als Angriffsplattform bietet einen weitgehend anonymen Raum. Inzwischen sind Cyber-Angriffe mit wenigen Mitteln möglich, es wird lediglich ein PC und Internet benötigt. Über das Internet können dann einfache Anleitungen bezogen werden, mit denen bereits kriminelle Handlungen durchgeführt werden können (vgl. Bundesamt für Sicherheit in der Informationstechnik 2014, S. 11).

Die Bedrohungslage und die damit verbundene Dringlichkeit der Stärkung der Cyber Security in Deutschland werden auch in den tagesaktuellen Nachrichten thematisiert, wie die Berichterstattung über den jüngsten Cyber-Angriff auf den Deutschen Bundestag (vgl. Wendt 2015) und der NSA-Skandal zeigen (vgl. faz.net 2015). Dadurch gewinnt Cyber Security weiterhin an Aufmerksamkeit. Im Juni 2015 wurde ein großer Cyber-Angriff auf den Deutschen Bundestag verübt, dabei konnten hochsensible Daten ausgespäht werden (vgl. Bewarder et al. 2015). Seit dem Whistleblower Edward Snowden ist auch in der breiten Öffentlichkeit bekannt, dass ausländische Nachrichtendienste Cyberspionage betreiben (vgl. Bendiek und Ulmer 2013, S. 1). Edward Snowden veröffentlichte mitunter Informationen zu den Programmen PRISM und TEMPORA, die von amerikanischen Nachrichtendiensten benutzt wurden, um deutsche Unternehmen auszuspähen (vgl. Corporate Trust Business Risk & Crisis Management GmbH 2014, S. 4-5). Hierdurch stellt sich nicht nur die Frage nach dem technischen Schutz vor Cyber-Angriffen, sondern Themen rund um Cyber Security und insbesondere Cyberspionage erhalten zusätzlich eine diplomatische Brisanz.

Die Bundesrepublik Deutschland ist fortwährend Ziel von nachrichtendienstlichen Cyber-Angriffen. Mit Cyberspionage bezwecken die Angreifer aus dem Netz einen informativen und strategischen und/oder finanziellen Vorteil (vgl.

Bundesamt für Sicherheit in der Informationstechnik 2014, S. 22). Die Innovationen und Entwicklungen der Unternehmen sind von Wirtschaftsspionage bereits betroffen, was finanzielle Schäden verursacht und die Wettbewerbsposition von Unternehmen und den Standort Deutschland schwächt (vgl. Corporate Trust Business Risk & Crisis Management GmbH 2014, S. 23; Bundesministerium des Innern 2009, S. 2). Somit ist davon auszugehen, dass aus Cyberangriffen nicht nur betriebs-, sondern auch größere volkswirtschaftliche Beeinträchtigungen resultieren. Die Systeme der Informationstechnik (IT) in Deutschland müssen besser geschützt werden, da sie von Cyber-Angriffen bedroht sind, wie der ‚Lagebericht der IT-Sicherheit in Deutschland 2014' des BSIs bestätigt: Darin wird die Gefährdungslage aufgrund des Angriffspotentials als kritisch eingestuft (vgl. Bundesamt für Sicherheit in der Informationstechnik 2014, S. 4). Auch wenn die Bedrohungslage für Kritische Infrastrukturen in Deutschland im internationalen Vergleich als gering eingeschätzt wird, so haben doch Cyber-Angriffe auf derartige Strukturen international zugenommen (vgl. Bundesamt für Sicherheit in der Informationstechnik 2014, S. 25).

1.1 Problemstellung und Forschungsfrage

Für den Wohlstand in Deutschland ist der Wirtschaftsschutz und insbesondere auch die Aufrechterhaltung der Kritischen Infrastrukturen unverzichtbar (vgl. Bundesministerium des Innern 2009, S. 2). Allerdings sind die Kritischen Infrastrukturen einer hohen Gefährdung ausgesetzt. Des Weiteren ist Deutschland als eines der führenden Industrienationen von Cyberspionage bedroht (vgl. Bundesministerium des Innern 2009, S. 2). Im Hinblick auf die zunehmende Digitalisierung wird das Gefährdungspotenzial weiterhin kritisch bleiben (vgl. Bundesamt für Sicherheit in der Informationstechnik 2014, S. 4, 10). Die Ursachen hierfür liegen in den Sicherheitslücken der IT-Systeme und den wachsenden Möglichkeiten, diese auszunutzen. Ein weiteres Problem ist die weltweite Anonymität im Internet, die es den TäterInnen erleichtert, unbekannt zu bleiben (vgl. Bundesamt für Sicherheit in der Informationstechnik 2014, S. 4).

In der Bundesrepublik Deutschland gibt es kein Bundesministerium für Cyber Security, die Zuständigkeiten sind auf mehrere Bundesministerien und Bundesämter aufgeteilt. Insofern ist eine gute Zusammenarbeit der zuständigen Bundesministerien und Bundesämter erforderlich. Eine weitere Rolle für Cyber Security in Deutschland spielt die Zusammenarbeit der Bundesministerien und Bundesämter mit den Unternehmen, die täglich der Gefahr von Cyber-Angriffen ausgesetzt sind (vgl. Bundesamt für Sicherheit in der Informationstechnik 2014, S. 11). Hierzu gehören auch die Kritischen Infrastrukturen, die in Deutschland überwiegend von privaten Betreibern betrieben werden.

Kritische Infrastrukturen werden vom Bundesministerium des Innern (BMI) als „[...] Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen“ definiert (Bundesministerium des Innern 2009, S. 3). Ein Ausfall oder eine Beeinträchtigung kann bereits „erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen“ nach sich ziehen (Bundesministerium des Innern 2009, S. 2-3). Bei einem Angriff können alle Bereiche der Gesellschaft, der Wirtschaft und der Politik betroffen sein (vgl. Bundesamt für Sicherheit in der Informationstechnik 2014, S. 4). Aus diesem Grund ist neben dem Wirtschaftsschutz der Schutz der Kritischen Infrastrukturen von besonders großer Bedeutung, sei es das Gesundheitswesen oder das Straßenverkehrsnetz. Inzwischen werden diese Infrastrukturen auch als „Cyber-Infrastrukturen“ bezeichnet (vgl. Schallbruch 2014, S. 1-2), um deren starke Vernetzung zu verdeutlichen. Vor diesem Hintergrund soll in der vorliegenden Ausarbeitung die folgende Forschungsfrage beantwortet werden: *Wie ist Cyber Security in Deutschland politisch und institutionell organisiert?*

Hieraus ergeben sich zwei Unterfragen, die ebenfalls beantwortet werden sollen:

- *Welche strategischen Planungen gibt es?*
- *Wie ist die Wirksamkeit von Cyber Security in Deutschland und welche Handlungsfelder bestehen für die Politik?*

Dazu sollen neben den bestehenden Dokumenten, wie der deutschen Cyber-Sicherheitsstrategie, die Bundesministerien und Bundesämter mit Aufgaben im Bereich Cyber Security näher analysiert werden und ausgewählte Unternehmen exemplarisch für die Wirtschaft einbezogen werden. Deutschland ist Mitglied der Europäischen Union (EU) und der North Atlantic Treaty Organization (NATO), weshalb die Zusammenarbeit auf der europäischen und der NATO-Ebene ebenfalls in die Analyse einfließen soll. Mit den gewonnenen Informationen sollen letztlich die Stärken, Schwächen, Chancen und Bedrohungen herausgearbeitet werden, um entsprechende Handlungsfelder aufzuzeigen.

1.2 Quellenauswahl und Stand der Forschung

In der Quellenlage zu dem Thema Cyber Security zeigt sich, dass der Forschungsstand noch einige Lücken aufweist (vgl. Kullik 2014, S. 22-28). Wie Jacob Kullik feststellt, ist das Thema Cyber Security noch sehr jung, was unter anderem ein Grund sein kann, dass neue Begriffe, wie Cyberterrorismus, noch nicht tiefgehend erforscht wurden. Auch gibt es noch keine empirisch gesicherte Datenlage, sondern lediglich „begrenzte Momentaufnahmen“ von Bundesministerien und Bundesämtern, Unternehmen oder Forschungsinstitutionen, die zum Teil nicht als neutrale Dokumente zu behandeln sind (vgl. Kullik 2014). Des Weiteren besteht ein „Dunkelfeld“ um Cyber-Kriminalität, das bisher nicht erfasst wird (vgl. Interview 7). So gibt es für viele Phänomene im Cyberspace bislang noch keine klar abgegrenzten Definitionen. Für die Forschung, Politik, Wirtschaft und Öffentlichkeit ist jedoch eine klare Definition der Begrifflichkeiten zur Bewertung der Bedrohungslage grundlegend (vgl. Grunert 2013, S. 107).

Um die Forschungsfrage beantworten zu können, wurden Experteninterviews geführt, da die vorhandene Quellenlage zur Analyse der Bundesministerien und Bundesämter nicht ausreichend war. Mit fast allen relevanten Bundesministerien und Bundesämtern, zu deren Aufgaben Cyber Security zählt, wurden Interviews geführt. Diese Interviews stellen die wichtigsten Quellen für die vorliegende

Arbeit dar. Weitere Interviews wurden mit exemplarisch ausgewählten Unternehmen geführt, um die Situation in der Wirtschaft und die Zusammenarbeit mit der Politik darzustellen.

Darüber hinaus wurden überwiegend Primärquellen und Internetauftritte der Bundesministerien und Bundesämter benutzt. Hierzu gehören beispielsweise die Cyber-Sicherheitsstrategie für Deutschland, die Digitale Agenda 2014-2017, Die Lage der IT-Sicherheit in Deutschland 2014 und das Cybercrime Bundeslagebild 2013 des Bundeskriminalamtes (BKA). Für weitere Informationen, insbesondere im Bereich der Wirtschaft, wurden auch Studien von Unternehmen herangezogen, wie die Studie e-crime. Computerkriminalität in der deutschen Wirtschaft mit Kennzahlen für Österreich und Schweiz der Unternehmensberatung KPMG.

Nur wenige Monographien und Sammelbände wurden verwendet, da zu dem Forschungsthema, insbesondere zur institutionellen Organisation von Cyber Security in Deutschland, noch keine große Auswahl zu finden ist. Hervorzuheben ist allerdings das Werk von Jakob Kullik mit dem Titel *Vernetzte (Un-)Sicherheit? Eine politisch rechtliche Analyse der deutschen Cybersicherheitspolitik*, in dem folgende Frage bearbeitet wird: „Besitzt Deutschland eine eigene, konsistente Cybersicherheitspolitik?“ (Kullik 2014, S. 20). Durch seine umfassende Politikfeldanalyse dient das Werk als zuverlässige Quelle zum Aufbau und zur Struktur der Cybersicherheitspolitik in Deutschland. Neben dem Werk von Kullik waren zur strategischen Planung von Cyber Security in Deutschland keine weiteren Monographien aufzufinden. Das Sammelwerk der Reihe *Studien zur Inneren Sicherheit* mit dem Titel *Cyber-Sicherheit* von Hans-Jürgen Lange und Astrid Bötticher enthält unter anderem einen Fachartikel der Herausgeberin Bötticher zur „Strukturlandschaft der Inneren Sicherheit der Bundesrepublik Deutschland“ (vgl. Bötticher 2015). Als weitere Sekundärquelle ist die Dissertation von Mischa Hansel *Internationale Beziehungen im Cyberspace: Macht, Institutionen und Wahrnehmung* als „ein Beitrag zur Theorie der internationalen Beziehungen im Cyberspace“ (Hansel 2013, S. 9) hervorzuheben.

Überdies wurden Fachartikel vorwiegend aus den Zeitschriften *Zeitschrift für Außen- und Sicherheitspolitik* (ZfAS) und *Internationale Politik* (IP) verwendet. Weitere wichtige Quellen sind die Studien und Aufsätze der ExpertInnen der Forschungseinrichtung Stiftung Wissenschaft und Politik (SWP). Für diese Arbeit wurden insbesondere die Beiträge von Annegret Bendiek benutzt, die als eine der führenden Expertinnen in Deutschland betrachtet wird und seit 2015 das Forschungsprojekt *Die Herausforderung der Digitalisierung für die deutsche Außen- und Sicherheitspolitik* leitet, mit einer Projektförderung des Planungsstabes des Auswärtigen Amtes (AA) (vgl. Stiftung Wissenschaft und Politik 2015). Ein weiterer Teil der Quellen besteht aus Zeitungsartikeln, die aufgrund der Aktualität des Themas für die Arbeit wichtig sind und beispielsweise Fakten über Cyber-Angriffe liefern, die zeitnah oder während der Entstehung dieser Arbeit vorgefallen sind, wie beispielsweise der Cyber-Angriff auf den Deutschen Bundestag (vgl. Biermann 2015).

1.3 Methodisches Vorgehen

Zur Beantwortung der Fragestellung sind konkrete Informationen erforderlich, zu denen nur in begrenztem Maße geeignete Literatur gefunden werden konnte. Als Methodik wurde daher das Fokusinterview mit einem stark strukturierten Leitfaden sowie mit offenen Fragen nach Helfferich ausgewählt (vgl. Helfferich 2014, S.571): Qualitative, leitfadengestützte Experteninterviews wurden mit VertreterInnen aus Bundesministerien, Bundesämtern und drei exemplarisch ausgewählten Unternehmen durchgeführt (vgl. Helfferich 2014, S. 559). Mithilfe der Experteninterviews kann auf Basis der bereits vorhandenen Quellen noch „Unbekanntes“ erforscht werden (vgl. Wassermann 2015, S. 58). Darüber hinaus lassen sich auch Expertenbewertungen erheben, die für die spätere Analyse hilfreich sind (vgl. Niederberger 2015, S. 42-43). Als ExpertInnen werden Personen bezeichnet, die über ein „detailliertes und spezialisiertes Wissen“ auf einem bestimmten Wissensgebiet verfügen (vgl. Wassermann 2015, S. 51).

Für die Experteninterviews wurden VertreterInnen aus den Bundesministerien und Bundesämtern ausgewählt, die im Bereich Cyber Security Aufgaben wahrnehmen. Da viele Bundesministerien und Bundesämter Aufgaben im Bereich Cyber Security wahrnehmen und aufgrund der Umfangsbeschränkung der vorliegenden Arbeit, konnten jedoch nicht alle Ressorts analysiert werden, darunter das Bundesministerium für Bildung und Forschung oder die Bundesnetzagentur; vielmehr wurden jene mit den meisten und wichtigsten Aufgaben im Bereich Cyber Security in Anlehnung an Jakob Kullik (2014) ausgewählt.

Das Thema und die Durchführung des Interviews wurden den Interviewpartnern bei der Kontaktaufnahme erläutert. Allen Interviewten wurde vorab eine anonymisierte Behandlung der Interviews zugesichert. Diese Vorgehensweise folgt den Empfehlungen zur Vorbereitung von qualitativen Interviews in der Sozialforschung von Niederberger (2015, S. 59). Daher wird der Zeitrahmen der Interviews nicht genannt, damit keine Rückschlüsse auf die InterviewpartnerInnen möglich sind. Ferner wurden alle Interviews persönlich („face to face“) durchgeführt – nur beim Bundesministerium für Wirtschaft und Energie (BMWi) war aus terminlichen Gründen lediglich ein Telefoninterview möglich.

Für qualitative Experteninterviews empfiehlt es sich, einen Leitfadenfragebogen zu entwickeln (vgl. Wassermann 2015, S. 57), der für diese Arbeit aus ca. 15 Frageblöcken bestand und mit weiteren Fragen untergliedert wurde, die unter anderem als sogenannte „Stimuli“ (vgl. Helfferich 2014, S. 571) dienen sollten. Da Bundesministerien bzw. -ämter und Unternehmen sich in ihren Aufgaben und Interessen unterscheiden, wurde ein Leitfaden für die Bundesministerien und Bundesämter entwickelt und ein weiterer für die Unternehmen. Des Weiteren wurden die Fragen den im Bereich Cyber Security wahrgenommenen Aufgaben der einzelnen Institutionen und Unternehmen angepasst. Der Leitfaden war so konzipiert, dass die Interviews jeweils etwa eine Stunde beanspruchten.

Für den Erfolg eines Interviews ist eine angenehme Gesprächssituation für den Interviewpartner entscheidend. Dazu ist es wichtig, „dass ein Experteninter-

view eine möglichst alltagsnahe Kommunikationssituation darstellt“ (Wassermann 2015, S. 60). Es wurde daher auf ein Tonbandgerät zur Aufzeichnung der Interviews verzichtet, um die InterviewpartnerInnen in die Lage zu versetzen, freier sprechen zu können. Nach den Interviews wurden stattdessen Gedächtnisprotokolle angefertigt.

Ein Nachteil der Experteninterviews ist die „subjektive, die Realität verzerrende Wahrnehmung des Experten“ (Wassermann 2015, S. 54), die in das Interview einfließt (vgl. Wassermann 2015, S. 54). In dieser Arbeit wurde zudem stellvertretend für die Bundesministerien, Bundesämter und Unternehmen jeweils nur eine Person interviewt. Auf die spätere Analyse wirkt sich dies nachteilhaft aus, da mit nur einem Vertreter auch nur jeweils eine subjektive Wahrnehmung wiedergegeben werden kann. Insbesondere bei den Bewertungen über die Zusammenarbeit mit anderen Institutionen ist dies zu beachten. Mit fast allen Bundesministerien und Bundesämtern konnte nichtsdestotrotz ein Interview geführt werden. Lediglich der Bundesnachrichtendienst (BND) und das Bundesamt für Verfassungsschutz (BfV) lehnten ein Interview ab.

Ferner ist anhand von drei exemplarisch ausgewählten Unternehmen keine ganzheitliche Analyse der Organisation der Cyber Security in der deutschen Wirtschaft möglich. Eine größere Anzahl von Unternehmen zu befragen, war jedoch im Rahmen dieser Arbeit nicht möglich und die gewählte Anzahl ist auch hinreichend, da die Interviews mit den Unternehmen zwar zusätzliche Faktoren offenbaren, der Fokus dieser Arbeit jedoch auf den Bundesministerien und Bundesämtern liegt.

In dieser Arbeit sollen die politische und institutionelle Organisation von Cyber Security in Deutschland, ihre strategische Planung und ihre Wirksamkeit untersucht und Handlungsfelder für die Politik identifiziert und bewertet werden. Darüber hinaus muss eine Zielrichtung definiert werden, die „relativ breit ausfallen [...] und mehrere Ziele umfassen“ (Wollny und Paul 2015, S. 200) kann. Demzufolge zielt die vorliegende Arbeit darauf, einen Beitrag zur Verbesserung der Cyber Security in Deutschland für Staat, Wirtschaft und Gesellschaft zu leisten: Aufbau-

end auf die Analyse und Bewertung der Ist-Situation soll der Handlungsbedarf in den identifizierten Handlungsfeldern aufgezeigt werden. Dabei wird als Handlungsfeld ein Wirkungsraum verstanden, auf den die politischen Akteure direkt oder indirekt einwirken können.

Um die Wirksamkeit von Cyber Security in Deutschland und den Handlungsbedarf für die Politik zu untersuchen, wird eine SWOT-Analyse durchgeführt. Mit der SWOT-Analyse (steht für Strengths, Weaknesses, Opportunities, Threats) können die internen Stärken und Schwächen sowie die externen Chancen und Bedrohungen dargestellt werden (vgl. Wollny und Paul 2015, S. 189-191, 200). Die SWOT-Analyse wurde in der Betriebswirtschaftslehre entwickelt und ermöglicht die ganzheitliche Bewertung der Unternehmenssituation und die Berücksichtigung von Trends und anderen Faktoren zur strategischen Zieldefinition (vgl. Wollny und Paul 2015, S. 189). Außerhalb der Betriebswirtschaftslehre können auch andere Organisationen und politische Gebilde an die Stelle der Unternehmen treten (vgl. Wollny und Paul 2015, S. 200). Die Analysemethode wird auch in anderen Sozialwissenschaften eingesetzt, den Autoren Volrad Wollny und Herbert Paul (2015) zufolge allerdings selten. Das mag an der Methodik liegen und daran, dass die SWOT-Analyse oftmals nicht ausreichend genutzt wird und im Nachhinein keine „Handlungsoptionen“ abgeleitet werden. Ein Vorteil dieser Analysemethode ist jedoch, dass sie sich an unterschiedliche Situationen und Zielsetzungen anpassen lässt (vgl. Wollny und Paul 2015, S. 189-191). In dieser Arbeit werden Stärken, Schwächen, Chancen und Bedrohungen als Handlungsfelder identifiziert und in einer SWOT-Matrix gegenübergestellt, um die strategische Bedeutung der Handlungsfelder oder des Handlungsbedarfs zu bewerten. Insofern werden in dieser SWOT-Analyse keine Strategien und somit auch kein Maßnahmenkatalog als Vorschlag ausgearbeitet, sondern die Methode wird in dieser Arbeit adaptiert, um lediglich Handlungsfelder der Politik strategisch nach der Dringlichkeit des Handlungsbedarfs zu gewichten. Dies soll der weiteren Forschung dazu dienen, auf Basis der Handlungsfelder Strategien und konkrete Maßnahmen abzuleiten.

Die Bewertung anhand der SWOT-Analyse erfolgt mit „verbal-argumentativen" Inhalten und nicht mit der „arithmetischen oder logischen Aggregation" (zur Erläuterung dieser Begriffe siehe Wollny und Paul 2015, S. 190). Die Durchführung ist somit zeit- und kostengünstig, jedoch ist ein Nachteil die „fehlende oder geringe Formalisierung" (Wollny und Paul 2015, S. 190), da die Bewertungskriterien beliebig oder mangelhaft ausgesucht sein können. Dadurch kann es zu Auswirklungen auf die Relevanz der Ergebnisse kommen. Darüber hinaus können Wissenslücken entstehen und die Interpretation kann Schwierigkeiten bereiten. Letztlich basiert die Analyse auf subjektiven Einschätzungen, die in dieser Arbeit durch die verwendeten Experteninterviews in der Analyse besonders stark sind (vgl. Wollny und Paul 2015, S. 190). Um diesen Schwächen der Analyse zu begegnen, wurde zuvor, den Empfehlungen von Wollny und Paul folgend, eine umfangreiche Literatur- und Internetrecherche durchgeführt (vgl. Wollny und Paul 2015, S. 190). Um weitere Informationen und Bewertungen zu erhalten, sind Experteninterviews eine gängige Methode im Vorfeld einer SWOT-Analyse. Hierbei wurde darauf geachtet, dass die ExpertInnen über ein sehr umfangreiches Wissen über die Thematik verfügen. Auch wenn diese subjektive Einschätzungen wiedergeben, kann zumindest davon ausgegangen werden, dass sie über ein hochqualifiziertes Expertenwissen über ihren Fachbereich und über Cyber Security verfügen. Letztlich erfolgt aus dem gesammelten Wissen die Identifizierung der internen und externen Faktoren (vgl. Wollny und Paul 2015, S. 201-202). Die internen Faktoren (Stärken und Schwächen) werden bei den Bundesministerien und Bundesämtern erfasst. Diese ergeben sich aus den „Vorgehensweisen", „spezifischen Benchmarks" und/oder einem „wünschenswerten Zustand" (vgl. Wollny und Paul 2015, S. 202). Die externen Faktoren (Chancen und Bedrohungen) für die politisch und institutionell organisierte Cyber Security in Deutschland sowie ihrer strategischen Planung bestehen „[…] aus erwarteten Umweltveränderungen und spezifischen Zielen, die von diesen Veränderungen tangiert werden" (Wollny und Paul 2015, S. 202). Zur Erhebung der externen Faktoren

wurden überwiegend Unternehmen einbezogen, da sie aus der Sicht der politisch-institutionellen Akteure einen wesentlichen Teil der Umwelt darstellen.

1.4 Aufbau

Der Aufbau dieser Arbeit orientiert sich an dem Werk von Jakob Kullik, der eine Politikfeldanalyse zur Cyber Security in Deutschland durchgeführt hat (siehe hierzu auch Kapitel 1.2). Die Institutionen wurden in seinem Werk in einer sinnvollen Kapitelfolge angeordnet, die zum Teil für diese Arbeit übernommen wurde (für Kapitel 2, 3 und 4).

Die vorliegende Ausarbeitung besteht insgesamt aus fünf Themenblöcken: In Kapitel 2 werden zunächst die Begriffe im Cyberspace definiert und die Bedrohungslage dargestellt, um im Anschluss die Bedeutung der Cyber Security und die Cybersicherheitspolitik zu erläutern (Kapitel 3). Im vierten Kapitel werden die einzelnen Bundesministerien und Bundesämter analysiert. Dieses Kapitel bildet den Schwerpunkt der vorliegenden Arbeit, da hier die wesentlichen Informationen für die spätere SWOT-Analyse erarbeitet werden. Anschließend wird im fünften Kapitel auf die Situation in der Wirtschaft eingegangen, indem die ausgewählten Unternehmen exemplarisch analysiert werden. Hieran schließt in Kapitel 6 die SWOT-Analyse an. Ein Fazit bildet den Abschluss der vorliegenden Arbeit (Kapitel 7).

2 Cyberbedrohungen und Cyber Security im Cyberspace

Die Bundesrepublik Deutschland ist eine „hochgradig vernetzte Gesellschaft“, die vor neuen Herausforderungen wie Cyberkrieg, Cyberkriminalität oder Cyberterrorismus steht, deren Bedeutung jedoch dem Großteil der deutschen Gesellschaft nicht bewusst ist (vgl. Alexander 2012, S. 39). Diese Bedrohungen gehen vom *Cyberspace* aus. Für den Schutz vor diesen Bedrohungen spielt Cyber Security eine zentra-

le Rolle. Nachfolgend sollen diese etablierten Begriffe definiert, erläutert und eingeordnet werden.

2.1 Cyberspace

Der Begriff Cyberspace existiert schon seit den Science Fiction-Werken von William Gibson, in den 80er Jahren (vgl. Hansel 2013 S. 33). Der Begriff wurde von Journalisten und Wissenschaftlern übernommen, „[...] um damit jenen Interaktionsraum zu benennen, der aus dem weltweiten Zusammenschluss von Computernetzen entstanden war“ (Hansel 2013, S. 33); er wird heute sehr weit gefasst und verwendet (vgl. Hansel 2013, S. 34).

In dieser Arbeit wird der Cyberspace verstanden als: „[…] ICT (information and communication technology) systems, networks and the information contained within these systems and networks, whether online or offline“ (Tessier-Stall 2011: S. 9). Die Informationstechnik hat sich in ihrer „leistungsfähigen und Nutzen schaffenden Fähigkeit“ (Bundesamt für Sicherheit in der Informationstechnik 2014, S. 7) weiterentwickelt, sodass sie mittlerweile in fast allen technischen Systemen integriert ist und einen wichtigen Faktor darstellt, der die Digitalisierung voran treibt (vgl. Bundesamt für Sicherheit in der Informationstechnik 2014, S. 7). Cyberspace ist eine Domäne, die durch die Verwendung von Elektronik und des elektromagnetischen Spektrums (zur Signalübertragung) gekennzeichnet ist, um Informationen über die vernetzten Informationssysteme zu speichern oder auszutauschen. Die vernetzten Informationssysteme benötigen hierzu eine physische Infrastruktur (vgl. Kuehl 2009, S. 26). Die Vernetzung kann dabei beispielsweise über Glasfaser oder Funk erfolgen, wobei derartige Netzwerke sowohl öffentlich als auch privat betrieben werden. Vor diesem Hintergrund ist der Cyberspace als ein „globaler Interaktionsraum“ zu verstehen (vgl. Hansel 2013 S. 34).

2.2 Cyberbedrohungen

Der Einsatz von Informations- und Kommunikationstechnologien (IKT) hat weltweit zugenommen, wodurch eine *Cyber-Abhängigkeit* der öffentlichen und privaten Nutzer von IKT-Systemen entstanden ist, die also mittlerweile eine zentrale Bedeutung für die Gesellschaft haben. Dadurch sind die IKT-Systeme zu attraktiven Zielen für Cyber-Angriffe geworden, mit denen diese Systeme gestört oder zerstört werden sollen. Aufgrund der Cyber-Abhängigkeit ist die Verwundbarkeit der IKT-Systeme als kritisches Risiko einzustufen, da Cyber-Angriffe auf diese Systeme große Schäden für die Sicherheit der Gesellschaft verursachen können. Die Cyber-Abhängigkeit wird in Zukunft noch weiter wachsen, wodurch auch Cyber-Angriffe zunehmen werden (vgl. Tessier-Stall 2011, S. 7). Cyber-Angriffe können sowohl staatliche als auch nicht-staatliche Akteure zum Ziel haben. Die Angriffe müssen aber nicht immer zielgerichtet sein, sondern können ihre Auswirkungen auch in der Breite entfalten (vgl. Bundesamt für Sicherheit in der Informationstechnik 2014, S. 15). Folglich unterscheiden sich Cyber-Angriffe auch in ihrer Art und Weise je nachdem, welches Ziel sie haben oder welche Auswirkungen von ihnen ausgehen. Das hängt mit den Interessensgruppen oder den EinzeltäterInnen zusammen, von denen sie ausgeführt werden. So kann es sich um Cyberaktivisten, Cyberterroristen, Cyberkriminelle oder ausländische Nachrichtendienste handeln (vgl. Tessier-Stall 2011, S. 9). Folglich kann die Auswirkung eines Cyber-Angriffes stark variieren – ob es sich nun um Cyberspionage ausländischer Nachrichtendienste auf Unternehmen handelt, wodurch längerfristig die Wettbewerbsfähigkeit der deutschen Unternehmen gefährdet und somit die gesamte Gesellschaft betroffen ist, oder ob Cyberkriminelle von einer privaten Einzelperson Kreditkartendaten stehlen, was keine Auswirkung auf die gesamte Gesellschaft hätte (vgl. Bundesamt für Sicherheit in der Informationstechnik 2012).

Cyber-Angriffe sind definiert als „ein IT-Angriff im Cyber-Raum, der sich gegen einen oder mehrere andere IT-Systeme richtet und zum Ziel hat, die IT-Sicherheit zu brechen“ (Bundesministerium des Innern 2011, S. 14). Cyberspionage,

Cyberkriminalität, Cybersabotage, Cyberterrorismus und Cyberkrieg gehören zu den Cyberbedrohungen im und aus dem Cyberspace, die signifikante Schäden verursachen können. Zu den Bedrohungen mit einem niedrigen Schadenspotenzial gehören hingegen Cyberaktivismus und Cybervandalismus (vgl. Kullik 2014, S. 43-69). Nachfolgend sollen die Cyberbedrohungen näher definiert werden.

Cyberkriminalität

„Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten, die mittels dieser Informationstechnik begangen werden“ (Bundeskriminalamt 2013, S. 5). Im Jahr 2013 wurden 64.426 Fälle von Cyberkriminalität erfasst, während im Vorjahr 63.959 Fälle verzeichnet wurden, wie aus dem Bundeslagebild zu Cybercrime des BKA’s hervorgeht (vgl. Bundeskriminalamt 2013, S. 5). Mittlerweile könne bereits von einer Industrie von Cyberkriminellen gesprochen werden, die auch deutsche Unternehmen angreifen (vgl. Sievers 2013). So waren im Jahr 2014 vier von zehn Unternehmen von Cyberkriminalität betroffen (vgl. KPMG 2014). Die Hackerangriffe konnten zurückgeführt werden auf organisierte Kriminalität, konkurrierende Unternehmen, aber auch ausländische Nachrichtendienste (vgl. Corporate Trust Business Risk & Crisis Management GmbH 2014, S. 3).

Cyberspionage

„Cyber-Angriffe, die sich gegen die Vertraulichkeit eines IT-Systems richten, werden, wenn sie von fremden Nachrichtendiensten ausgehen oder gesteuert werden, als Cyber-Spionage, ansonsten als Cyber-Ausspähung bezeichnet“ (Bundesministerium des Innern 2011, S. 15). Im Juni 2015 wurde ein großer Cyber-Angriff auf den Deutschen Bundestag verübt. Dabei konnten hochsensible Daten ausgespäht werden. Zum Zeitpunkt der Erstellung dieser Arbeit wird in den Medien berichtet, dass es sich dabei um Cyberspionage durch den russischen Nachrichtendienst FSB handeln könnte (vgl. Bewarder et al.2015). Diese Vermutung in den

Medien ist allerdings bislang noch nicht offiziell bestätigt worden und es liegen der Öffentlichkeit keine Beweise vor, dass dem tatsächlich so ist.
Von Cyberspionage ist aber auch die deutsche Wirtschaft stark betroffen. Dies hat zur Folge, dass die Innovationsvorsprünge der deutschen Industrie gefährdet sind (vgl. Schnaas 2014, S. 8). Die Innovationen der Industrie sind für Deutschland als ein führendes Industrieland unverzichtbar, da diese Wachstum, Wohlstand und Arbeitsplätze sichern. Bereits jetzt erleiden deutsche Unternehmen Schäden in Milliardenhöhe durch Industriespionage (vgl. Heeg 2015). In Kapitel 5 wird hierauf näher eingegangen.

Cybersabotage

„Cyber-Angriffe gegen die Integrität und Verfügbarkeit eines IT-Systems werden als Cyber-Sabotage bezeichnet" (Bundesministerium des Innern 2011, S. 15). Hierbei geht die größte Gefahr für die Gesellschaft von einem Angriff auf Kritische Infrastrukturen aus (vgl. Bundesamt für Sicherheit in der Informationstechnik 2014, S. 4), die in dieser Arbeit entsprechend ausführlicher behandelt werden. Cyberspionage und Cybersabotage sind meist miteinander verbunden. Sie sind Möglichkeiten, die beispielsweise von Terroristen genutzt werden können, um „terroristische IT-Anschläge" zu verüben (vgl. Kullik 2014, S. 67). Auf Cyberterrorismus wird im weiteren Verlauf noch näher eingegangen.

Cyberkrieg

Wie eingangs erwähnt (Kapitel 1.2), mangelt es an klar abgegrenzten Definitionen von Cyberbedrohungen (vgl. Bendiek und Ulmer 2013, S. 1). Folglich wird der Begriff Cyberkrieg in den Medien „[...] oft für jegliche Art von Vorfällen im Zusammenhang mit Computern, Computertechnik und dem Internet verwendet, ohne dabei klar von Cyberkriminalität abzugrenzen und festzustellen, dass Cyberkrieg eine Zustandsbeschreibung eines Krieges mit Cybermitteln meint, welcher so in der Realität [noch] nicht stattfindet" (Singer 2014, S. 17). Nach Tassilo Singer müsste der Begriff weiter gefasst werden unter *Cyberwarfare*, der Cyberoperationen umfasst,

womit „[...] die Nutzung von Cyberfähigkeiten mit dem Zweck, bestimmte Ziele durch die Nutzung des Cyberspace sowohl innerhalb als auch außerhalb desselben zu erreichen“ gemeint sind (Singer 2014, S. 17). In diesem Kontext wäre auch die internationale Rechtsordnung für die Kriegsführung zu überarbeiten (vgl. Singer 2014). Es bleibt indes umstritten, nach welchen Kriterien Cyberkrieg definiert wird, um diesen als bewaffneten Konflikt nach dem Völkerrecht einstufen zu können, und wie darauf rechtlich reagiert werden soll (vgl. Bendiek und Ulmer 2013, S. 1). Der Deutsche Bundestag hat 2011 erklärt, „dass ein Cyber-Angriff nur dann als bewaffneter Angriff im Sinne des Völkerrechts einzuordnen wäre, wenn dieser in seiner Wirkung die Schwelle zum bewaffneten Konflikt überschreiten würde und sich mit derjenigen herkömmlicher Waffen vergleichen ließe“ (Deutscher Bundestag 2011, S. 4). Doch auch diese Definition wirft Fragen auf, wie die Wirkung gemessen werden soll und wie diese sich mit herkömmlichen Waffen vergleichen ließe. Im Zuge des Cyber-Angriffes auf den Bundestag, der im Juni 2015 in den Medien bekannt wurde, gab es Berichterstattungen, in denen die Frage aufgeworfen wurde, ob der Vorfall den NATO-Bündnisfall nach Artikel 5 auslöste (vgl. Bewarder et al. 2015). Dies verdeutlicht eindringlich, dass die neuartigen Phänomene entsprechende Definitionen und Bewertungen benötigen. Festzustehen scheint jedoch, dass der Cyberspace mittlerweile als fünfte Domäne der Kriegsführung gilt nach Land, Luft, Wasser und Weltall (vgl. The Economist 2010).

Cyberkrieg ist eine Bedrohungsform, die auch die Bundesrepublik Deutschland betrifft; der Fall der Verteidigung von einem Cyber-Angriff ist allerdings noch nicht eingetroffen (vgl. Interview 5). Sollte dies der Fall sein, ist die Deutsche Bundeswehr für die Verteidigung zuständig. Hierzu gibt es unter anderem das Kommando Strategische Aufklärung (KSA), welches Fähigkeiten in der Cyberverteidigung besitzt, und den Militärischen Abschirmdienst (MAD), der als einer der deutschen Nachrichtendienste innerhalb der Bundeswehr für die Abwehr von Cyber-Angriffen zuständig ist (vgl. Kommando Streitkräftebasis 2015).

Cyberterrorismus

Cyber-Angriffe von terroristischen Gruppen erfolgen durch Spionage oder Sabotage im Cyberraum. Bisher wird davon ausgegangen, dass den Terroristen die nötigen finanziellen und technischen Mittel sowie das benötigte Know-how fehlen, um folgenschwere Terroranschläge im Cyberraum durchzuführen. Des Weiteren stellen die notwendigen Ressourcen und der Austausch von Fachwissen Gefahrenquellen für Terroristen dar, die zu ihrer Identifizierung führen können. Fest steht jedoch, dass Cyber-Angriffe zur Verstärkung der Wirkungskraft und Bedrohung durch terroristische Vereinigungen beitragen können (vgl. Kullik 2014, S. 67-68). Ferner ist anzunehmen, dass auch die Cyber-Fähigkeiten dieser Gruppen zunehmen werden. Wenn Terrorismus tatsächlich in den Cyberspace übergehen würde, könnten Staaten schwer getroffen werden und es wäre möglicherweise ein *9/11 im Cyberspace* zu befürchten (vgl. Kullik 2014, S. 67-68).

Auf dem internationalen Schwarzmarkt sind sogenannte *Cybersöldner* bereits von hohem Wert. Es bestünde die Möglichkeit, aus ihnen in Trainingslagern *Terror-Hacker* auszubilden. So könnten Cyberterroristen künftig Cyber-Anschläge auf IT-Systeme oder Kritische Infrastrukturen eines Staates verüben (vgl. Kullik 2014, S. 67-68). In der deutschen Verteidigungspolitik wird Deutschland als potenzielles Angriffsziel von Cyberterroristen betrachtet. Dies wurde beispielsweise auf einer Indienreise der Verteidigungsministerin Ursula von der Leyen thematisiert, die eine Kooperation mit Indien gegen Cyberterrorismus plant. Denn auch Cyberterrorismus kann nur auf internationaler Ebene wirksam bekämpft werden (vgl. heise online 2015).

Cyberaktivismus

Cyberaktivismus ist in der Wissenschaft noch weitestgehend unerforscht. Cyberaktivisten lassen sich bisher in drei Kategorien aufteilen: 1) mit positiv-konstruktiven Absichten, 2) mit negativ-destruktiven Absichten und 3) mit unklaren Absichten. Alle Gruppen haben ein breites IT-Fachwissen. Cyberaktivisten sind meist politisch

motiviert und verfolgen zum Teil liberale Ideale (vgl. Kullik 2014, S. 44). Sie verfolgen beispielsweise das Ziel der „Rede- und Informationsfreiheit des Individuums im Internet“ (Kullik 2014, S. 44). Darüber hinaus gibt es aber z. B. auch patriotische Cyberaktivisten.

Im Bürgerkrieg in Syrien ist zu beobachten, dass Anhänger Assads versuchen, global Informationen und Propaganda zu verbreiten, während die Opposition diese mit Unterstützung westlicher Netzaktivisten bekämpft. Dabei geht es auch um den Zugang zu Webseiten und Informationen innerhalb Syriens (vgl. Kullik 2014, S. 43-45).

Im Zuge der anhaltenden NSA-Affäre nimmt die Szene der Netzaktivisten auch in Deutschland zu, welche oftmals Druck auf politische Entscheidungsträger ausüben. Insofern sehen Politiker und Sicherheitsbehörden eine zunehmende Bedrohung im Netzaktivismus. Jakob Kullik geht davon aus, dass Cyberaktivismus in friedlicher oder aggressiver Art und Weise für die Zukunft eine Rolle spielen wird (vgl. Kullik 2014, S. 43-45).

Cybervandalismus

Beim Cybervandalismus wird nicht nur politisch protestiert, sondern es werden auch wahllos Webinhalte zerstört. Die TäterInnen sind in der Regel Jugendliche, die als *Script Kiddies* bezeichnet werden. Die TäterInnen nutzen das fehlende Sicherheitsbewusstsein der Anwender von IT-Systemen und System-Schwachstellen aus, wodurch sie IT-Systeme mit Viren infizieren und zerstören können (vgl. Kullik 2014, S. 46-47).

2.3 Cyber Security

Das Thema Cyber Security ist nicht neu, die Erfahrung der letzten 40 Jahre hat vielmehr gezeigt, dass die Fortschritte in den IKT-Systemen immer wieder neue Sicherheitsprobleme mit sich bringen, denen Endnutzer bzw. die Gesellschaft ausgesetzt sind. Die rasante Digitalisierung der letzten Jahrzehnte führte zu mehr Si-

cherheitslücken in der IKT (vgl. Luiijf 2014, S. 19-20). Dabei ist zu bedenken, dass Sicherheit ein relativer Begriff ist, Cyber Security ist somit der auf nationaler und globaler Ebene „anzustrebende Zustand der IT-Sicherheitslage, in welchem die Risiken des globalen Cyber-Raums auf ein tragbares Maß reduziert sind“ (Bundesministerium des Innern 2011, S. 15). Cyber Security bewirkt das uneingeschränkte Funktionieren der IT-Systeme (vgl. Tessier-Stall 2011, S. 9). Insofern bezweckt Cyber Security, Sicherheitslücken in IT-Systemen entgegenzuwirken und Cyber-Angriffe abzuwehren. Das bedeutet, es müssen Möglichkeiten geschaffen werden, durch die IKT-Systeme geschützt werden, damit diese möglichst störungsfrei und ohne die Gefahr, komplett zerstört zu werden, funktionieren können.

Es gibt verschiedene Maßnahmen, um den Herausforderungen von Cyber Security zu begegnen. Dazu gehören sowohl technische als auch institutionelle Mittel, die zur Prävention beitragen können. Institutionelle Mittel sind unter anderem die Sensibilisierung für Cyberbedrohungen sowie die Förderung der internationalen Zusammenarbeit. Die nationale Politik wird sich für die Zukunft aber auch die Frage stellen müssen, wie eine Balance zwischen defensiven und offensiven Cyber Security-Maßnahmen zu erreichen ist, um kein Cyber-Wettrüsten zwischen den Staaten hervorzurufen, wie es in der Wissenschaft des Öfteren bereits diskutiert wird (vgl. Lindstorm 2012, S. 6-7). Autoren wie Sandro Gaycken (2012) vertreten die Ansicht, dass das Wettrüsten bereits seit längerem begonnen hat (vgl. Gaycken 2012). Nachfolgend soll aufgezeigt werden, welche Pläne, Strategien und Maßnahmen zur Cyber Security in der Bundesrepublik Deutschland vorliegen.

3 Cybersicherheitspolitik auf Bundesebene

Bedrohungen durch Cyber-Angriffe sind in der Sicherheitspolitik neu, weshalb neue Lösungskonzepte benötigt werden (vgl. Tschersich 2011, S. 408). Cybersicherheit ist somit zu einer „facettenreichen politischen Herausforderung“ (Bendiek und

Ulmer 2013, S. 1) geworden, die in der Wissenschaft als ein neues Politikfeld der Außen- und Sicherheitspolitik beschrieben wird (vgl. Bundesministerium des Innern 2015d). So fand auch in der Politik Cyber Security in den letzten Jahren sowohl auf nationaler als auch auf internationaler Ebene immer mehr an Bedeutung. Es wurde beispielsweise auf EU-Ebene und für Deutschland eine Cyber-Sicherheitsstrategie festgelegt (vgl. Bendiek et al. 2012, S. 1; Bundesministerium des Innern 2015b). Auf die deutsche Cyber-Sicherheitsstrategie soll in Kapitel 3.2 näher eingegangen werden, die europäische Cyber-Sicherheitsstrategie wird in Kapitel 4.5.2 behandelt.

In Deutschland liegen die Zuständigkeiten für den Themenbereich Cyber Security beim BMI. So fordert der Bundesminister des Innern, Thomas de Maizière, „stärkere Vorsorgemaßnahmen“ (Bundesministerium des Innern 2015d). Die Zuständigkeiten liegen allerdings nicht nur beim BMI (Bundesministerium des Innern, 2015d); die Bundesregierung erstrebt beispielsweise mit ihrer Cyberaußenpolitik eine „Stärkung internationaler Normen“, um ein „verantwortungsvolles Miteinander der Staaten im Cyberspace“ zu ermöglichen (Bundesministerium des Innern, 2015d). Insbesondere mangelt es aber an international einheitlichen Definitionen von Straftatbeständen. Hierbei ergibt sich zunehmend das Problem der Klärung von Rechtsfragen bei nachrichtendienstlichen Aktivitäten im Cyberraum (vgl. Schaller 2014; Kapitel 4.5.3).

In den USA ist Cybersicherheit überwiegend im militärischen Bereich angesiedelt. Das mag auch daran liegen, dass die Fähigkeiten zu Cyberangriffen zu einem strategischen Instrument in zwischenstaatlichen Konflikten herangewachsen sind (vgl. Bendiek und Ulmer 2013, S. 1-2). Der interviewte Vertreter des Bundesministeriums der Verteidigung (BMVg) (Interview-partner 5 (BMVg)) führt in diesem Zusammenhang an, dass die USA als kinetisch-generische Weltmacht vorwiegend von Cyber-Angriffen auf militärische Einrichtungen bedroht seien, während Deutschland als eines der führenden Industrienationen und wirtschaftliche Groß-

macht vorrangig von Cyber-Angriffen auf Unternehmen bedroht sei (vgl. Interview 5).

Das Thema Cyber Security wurde in Deutschland überhaupt erst mit den Koalitionsverträgen von 2009 und 2013 von der Bundesregierung thematisiert (vgl. Kullik 2014, S. 82-85). Für den Schutz der Kritischen Infrastrukturen (KRITIS) wurde 2009 eine *Nationale Strategie zum Schutz Kritischer Infrastrukturen* (KRITIS-Strategie) beschlossen (vgl. Bundesministerium des Innern 2009). Danach wurde im Jahre 2011 die Cyber-Sicherheitsstrategie beschlossen, worauf die Digitale Agenda 2014 folgte (vgl. Bundesministerium des Innern 2011; Die Bundesregierung 2014b). Im Koalitionsvertrag von 2013 wurden insbesondere die Themen IT-Sicherheit und Wirtschaftsspionage aufgegriffen (vgl. Koalitionsvertrag zwischen CDU/CSU und SPD 2013, S. 140). Seitdem die Bundesregierung mit dem Koalitionsvertrag von 2013 das Thema IT-Sicherheit auf ihre Agenda gesetzt hat, gibt sie mit ihren festgelegten Grundsätzen der Digitalpolitik eine Richtung vor (vgl. Koalitionsvertrag zwischen CDU/CSU und SPD, 2013). Die Bundesregierung erklärt darin, dass „der digitale Wandel [...] zu einer der zentralen Gestaltungsaufgaben für Wirtschaft, Wissenschaft, Gesellschaft und Politik geworden [ist]“ (Die Bundesregierung 2015b). In den nachfolgenden Kapiteln soll nun auf die einzelnen Verträge, Strategien und Pläne eingegangen werden.

3.1 Cyber Security in den Koalitionsverträgen von 2009 und 2013

Das Thema Cyber Security wurde im Koalitionsvertrag von 2009 zwischen CDU, CSU und FDP zwar nicht als solche aufgenommen, es fand aber in einem Unterkapitel zur Innovation und Bildung Beachtung (vgl. Kullik 2014, S. 140, 146, 149). Mit dem Koalitionsvertrag von 2009 änderte sich die Wahrnehmung und es heißt, dass Deutschland „längst in der Informationsgesellschaft angekommen“ sei (Koalitionsvertrag zwischen CDU, CSU und FDP 2009, S. 100). Aus diesem Grund wird das Ziel gesetzt, dass alle Menschen Zugang zu Internet-Angeboten erhalten

sollen, wofür eine leistungsfähige Bereitbandversorgung notwendig ist (vgl. Kullik 2014, S. 86). Des Weiteren wird betont, dass „Recht und Gesetz im Internet schon heute und in Zukunft ebenso gelten wie überall sonst“ (Koalitionsvertrag zwischen CDU, CSU und FDP 2009, S. 101). Hierbei wird auch das Problem von Cyberkriminalität aufgegriffen und insbesondere der Datenmissbrauch hervorgehoben, weshalb zu dessen Bekämpfung das Datenschutzgesetz verbessert werden soll. Folglich wird im Vertrag festgehalten: „Die Sensibilität für den Schutz der eigenen Daten muss gestärkt, der Selbstdatenschutz erleichtert werden, um Datenmissbrauch vorzubeugen“ (Koalitionsvertrag zwischen CDU, CSU und FDP 2009, S. 101).

Zur weiteren Bekämpfung von Cyberkriminalität – mit Schwerpunkt auf Betrug und Identitätsdiebstahl – wird eine strafrechtliche Verfolgung in Zusammenarbeit mit den Bundesländern beschrieben. Die IT-Kompetenzen und speziell geschultes Personal in den Sicherheitsbehörden sollen mit dazu beitragen, eine bessere Strafverfolgung zu erzielen. Des Weiteren sollen Möglichkeiten einer sicheren Kommunikation mehr Beachtung finden. Um diesen Herausforderungen besser begegnen zu können, wird auch eine internationale Zusammenarbeit zur Bekämpfung von Cyberkriminalität angestrebt.

Die IT-Sicherheit (Cyber Security) soll im öffentlichen und nicht-öffentlichen Bereich erhöht werden. Insbesondere werden hier die IT-Systeme der Kritischen Infrastrukturen hervorgehoben, die besonderen Schutz erfordern. Dazu soll das BSI gestärkt werden. Zur Abwehr von Cyber-Angriffen sollen die Kompetenzen des Beauftragten der Bundesregierung für Informationstechnik gestärkt werden (vgl. Koalitionsvertrag zwischen CDU, CSU und FDP 2009, S. 101). Das BSI soll dabei unterstützend tätig sein, wozu es als „zentrale Cyber-Sicherheitsbehörde“ (Koalitionsvertrag zwischen CDU, CSU und FDP 2009 S. 103) weiter ausgebaut werden soll, um unter anderem als Koordinationsstelle zur Abwehr von Cyber-Angriffen zu fungieren (vgl. Koalitionsvertrag zwischen CDU, CSU und FDP 2009, S. 101-103).

Im Koalitionsvertrag von 2013 zwischen CDU, CSU und SPD wird das Thema Cyber Security bzw. IT-Sicherheit wieder aufgegriffen und unter neuen Gesichtspunkten eingehender behandelt (vgl. Koalitionsvertrag zwischen CDU, CSU und FDP 2009). So wird das Thema im Kapitel *Digitale Sicherheit und Datenschutz* ausführlicher behandelt als im Koalitionsvertrag zuvor – mit Konzentration auf Cyberkriminalität, IT-Infrastruktur und digitaler Datenschutz (vgl. Kullik 2014, S. 84). Auch hier wird die Gesetzeslage aufgegriffen und die Notwendigkeit einer Verbesserung des Strafrechts hervorgehoben (Koalitionsvertrag zwischen CDU, CSU und SPD 2013, S. 147).

Darüber hinaus wird im Koalitionsvertrag festgelegt, dass ein IT-Sicherheitsgesetz beschlossen werden soll. Unter dem Punkt *IT-Infrastruktur und digitaler Datenschutz* wird dies detaillierter behandelt (vgl. Koalitionsvertrag zwischen CDU, CSU und SPD 2013, S. 147). Das IT-Sicherheitsgesetz steht für die „verbindlichen Mindestanforderungen an die IT-Sicherheit für die Kritischen Infrastrukturen und der Verpflichtung zur Meldung erheblicher IT-Sicherheitsvorfälle“ durch die Betreiber der Kritischen Infrastrukturen (Koalitionsvertrag zwischen CDU, CSU und SPD 2013, S. 147). In Kapitel 3.5 wird näher auf das IT-Sicherheitsgesetz eingegangen.

Auf EU-Ebene wird eine europäische Cyber-Sicherheitsstrategie samt „Maßnahmen zur Rückgewinnung der technologischen Souveränität“ (Koalitionsvertrag zwischen CDU, CSU und SPD 2013, S. 147) angestrebt. Zudem soll so bald wie möglich eine verbesserte EU-Datenschutzgrundverordnung verabschiedet werden (vgl. Koalitionsvertrag zwischen CDU CSU und SPD 2013, S. 147). Auf institutioneller Ebene sind ein Ausbau des BSI und des Cyber-Abwehrzentrums (Cyber-AZ) sowie eine bessere „IT-Ausstattung der deutschen Sicherheitsbehörden“ vorgesehen (Koalitionsvertrag zwischen CDU, CSU und SPD 2013, S. 148). In dem Kapitel 3.5 wird mit Bezug auf das IT-Sicherheitsgesetz hierauf noch näher eingegangen.

Die NSA-Affäre wird in einem eigenen Kapitel thematisiert, mit dem Ziel, „ein rechtlich verbindliches Abkommen zum Schutz vor Spionage (zu) verabschie-

den“ (Koalitionsvertrag zwischen CDU, CSU und SPD 2013, S. 148), wodurch die Regierung sich wieder mehr Vertrauen von der Bevölkerung erhofft (vgl. Koalitionsvertrag zwischen CDU, CSU und SPD 2013, S. 148). Ein weiterer nennenswerter Punkt für den Themenbereich Cyber Security ist die Einführung einer „Digitalen Agenda“ für Deutschland. Mit der Digitalen Agenda sollen „Chancen für eine starke Wirtschaft, gerechte Bildung und ein freies und sicheres Internet“ (Koalitionsvertrag zwischen CDU, CSU und SPD 2013, S. 138) gestärkt werden. Zudem wird das Ziel formuliert, dass Deutschland zum „digitale[n] Wachstumsland Nr. 1 in Europa“ (Koalitionsvertrag zwischen CDU, CSU und SPD 2013, S. 138) wird. Auf die Digitale Agenda wird im gleichnamigen Kapitel 3.3 detaillierter eingegangen.

3.2 Der Schutz Kritischer Infrastrukturen

In diesem Kapitel sollen die Strategien und Pläne der Politik zum Schutz der Kritischen Infrastrukturen erläutert werden. Nachdem das Thema nach und nach in den Koalitionsverträgen aufgegriffen wurde, entstand 2005 der *Nationale Plan zum Schutz der Informationsinfrastrukturen* (NPSI), darauf folgte dann 2007 der *Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen*, 2009 die KRITIS-Strategie und 2014 der UP KRITIS, im Rahmen dessen auch ein UP KRITIS-Rat mit VertreterInnen aus Politik und Wirtschaft sowie der Umsetzungsplan Bund (UP Bund) gegründet wurde.

Der Schutz vor Cyberbedrohungen für die Kritischen Infrastrukturen fand erst nach und nach an Bedeutung in den Koalitionsverträgen (vgl. Kullik 2014, S. 82-85). Zunächst war das Thema in Arbeitsgruppen organisiert, worüber die Arbeitsgruppe KRITIS 1997 einen Bericht erstellte. Auftraggeber war das BMI. Inhaltlich wurden in diesem Bericht die möglichen Ausfälle der Anlagen, die durch IT-Systeme gesteuert wurden, und die potenziellen Folgen derartiger Ausfälle untersucht. Es wurde festgehalten, dass IT-Sicherheit in Zukunft eine höhere Relevanz erhalten soll (vgl. Kullik 2014, S. 86-88).

Nationaler Plan zum Schutz der Informationsinfrastrukturen

Ein strategischer Plan zum Schutz der Informationsinfrastrukturen wurde erst 2005 vom BMI mit dem NPSI vorgelegt (vgl. Bundesministerium des Innern 2005). Hier fand auch der Begriff IT-Sicherheit erstmals eine seiner Definitionen im Kontext der deutschen Politik: „IT-Sicherheit ist der Zustand, der die Verfügbarkeit, die Integrität, die Verbindlichkeit und die Vertraulichkeit von Informationen beim Einsatz von IT gewährleistet“ (Bundesministerium des Innern 2005, S. 20).

Die Informationsinfrastrukturen werden im NPSI als „das Nervensystem unseres Landes“ dargestellt (Bundesministerium des Innern 2005, S. 3). Es werden die Cyberbedrohungen für Informationsinfrastrukturen festgehalten, die ihren Ursprung nicht nur auf nationaler, sondern auch auf internationaler Ebene haben können. Das Täterbild hierbei ist kriminell oder terroristisch geprägt (vgl. Bundesministerium des Innern 2005, S. 3).

Folglich richtet sich ein größerer Teil des strategischen Plans an die Prävention zum Schutz Kritischer Infrastrukturen. Das BSI wird dabei eingebunden, IT-Systeme und Produkte für Unternehmen auf ihre Sicherheit hin zu zertifizieren. Dazu gehört auch die Verfügbarkeit von vertrauenswürdigen Kryptoprodukten, welche für eine sicherere Kommunikation ausgebaut werden soll. Insbesondere in Bezug auf Wirtschaftsspionage werden deutsche kryptografische Verfahren als essenziell betrachtet (vgl. Bundesministerium des Innern 2005, S. 10-11).

Eine Kooperation mit der Wirtschaft hielt die damalige Bundesregierung für notwendig, da Kritische Infrastrukturen häufig von privaten Unternehmen betrieben werden. So wird im NPSI festgehalten, dass mit Unternehmen und VertreterInnen aus der Wirtschaft ein Umsetzungsplan KRITIS erstellt werden soll. Zukünftig soll das BSI Unternehmen in ihrer Cyber Security in Form von Handlungsempfehlungen unterstützen (vgl. Bundesministerium des Innern 2005, S. 7-8).

Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen

Im Jahr 2007 folgte dem NPSI der *Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen* (vgl. Bundesministerium des Innern, 2007). Der neue Plan geht nicht nur auf die Informationsinfrastrukturen ein, sondern umfasst weitere Kritische Infrastrukturen. Das strategische Vorgehen, durch „Prävention", „Reaktion" und „Nachhaltigkeit" Kritische Infrastrukturen vor einer IT-Krise zu schützen, wird beibehalten (Bundesministerium des Innern 2007, S. 5-6). Eine IT-Krise wird im Umsetzungsplan KRITIS folgendermaßen definiert:

> Eine IT-Krise im Kontext des Umsetzungsplans KRITIS liegt vor, wenn mittelbar oder unmittelbar IT-bedingt ein Ausfall oder eine Beeinträchtigung von Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen mit nachhaltig wirkenden Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen eintritt beziehungsweise zu erwarten ist.
> (Bundesministerium des Innern 2007, S. 21)

Für diesen Fall werden im Umsetzungsplan KRITIS neben dem Schutz der Kritischen Infrastrukturen (unter dem Punkt ‚IT-Sicherheitslagefeststellung') Mechanismen und eine „IT-Krisenreaktion" vorgegeben, welche im Fall von Störungen in der Infrastruktur greifen sollen (vgl. Bundesministerium des Innern 2007, S. 21-22).

KRITIS-Strategie

Dem Umsetzungsplan KRITIS des Jahres 2007 folgte 2009 die KRITIS-Strategie (vgl. Bundesministerium des Innern 2009), in der nochmals die Bedeutsamkeit und Verantwortung des Schutzes Kritischer Infrastrukturen für Staat, Wirtschaft und Gesellschaft betont werden (vgl. Bundesministerium des Innern 2009, S. 3). Die einzelnen Sektoren der Kritischen Infrastrukturen werden in der KRITIS-Strategie unterteilt in *Technische Basisinfrastrukturen* und *Sozioökonomische Dienstleistungsinfrastrukturen*. Tabelle 1 gibt hierzu eine Übersicht.

Tab. 1: Übersicht über Kritische Infrastrukturen (Quelle: In Anlehnung an Bundesministerium des Inneren 2009, S. 5)

Technische Basisinfrastrukturen	**Sozioökonomische Dienstleistungsinfrastrukturen**
Energieversorgung	Gesundheitswesen, Ernährung
Informations- und Kommunikationstechnologie	Notfall- und Rettungswesen, Katastrophenschutz
Transport und Verkehr	Parlament, Regierung, öffentliche Verwaltung, Justizeinrichtungen
(Trink-)Wasser- und Abwasserversorgung	Finanz- und Versicherungswesen
	Medien und Kulturgüter

Von großer Bedeutung ist die gegenseitige Abhängigkeit zwischen Dienstleistungs- und Basisinfrastrukturen. So ist die Energieversorgung zur Aufrechterhaltung der Funktionen im sozioökonomischen Dienstleistungsbereich notwendig und die Sicherstellung der Energieversorgung wiederum beruht beispielsweise auf einem funktionierenden Rechtssystem. Durch diese wechselseitige Abhängigkeit können bei einem Ausfall mehrere Kritische Infrastrukturen betroffen sein. Folglich ist von einem Kritischen Infrastruktur-Netzwerk auszugehen, bei dem der Ausfall einzelner Elemente eine erhebliche Beeinträchtigung in mehreren Bereichen bedingen kann.

Von dem interviewten Vertreter des Bundesministeriums für Verkehr und digitale Infrastruktur (BMVi) (Interviewpartner 4 (BMVi)) wird bemängelt, dass es keine genaue Definition von Kritischen Infrastrukturen gebe. Insbesondere im Bereich von Transport und Logistik herrsche Unklarheit, ob beispielsweise die Logistik von Aldi als Kritische Infrastruktur zu werten sei (vgl. Interview 4). Klar voneinander abgegrenzte Definitionen sind notwendig, um Pläne und Strategien den Kritischen Infrastrukturen zuordnen zu können, für die sie geschaffen wurden. Die Problematik der unzureichenden Definitionen zeigt sich auch bei der Umsetzung des IT-Sicherheitsgesetzes, worauf in Kapitel 3.5 näher eingegangen wird.

UP KRITIS

Im Februar 2014 wurde der *UP KRITIS* beschlossen, der den *Umsetzungsplan KRITIS ablöste*. „Der UP KRITIS ist eine öffentlich-private Kooperation zwischen Betreibern

Kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen“ (Bundesamt für Sicherheit in der Informationstechnik und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2011-2013b).

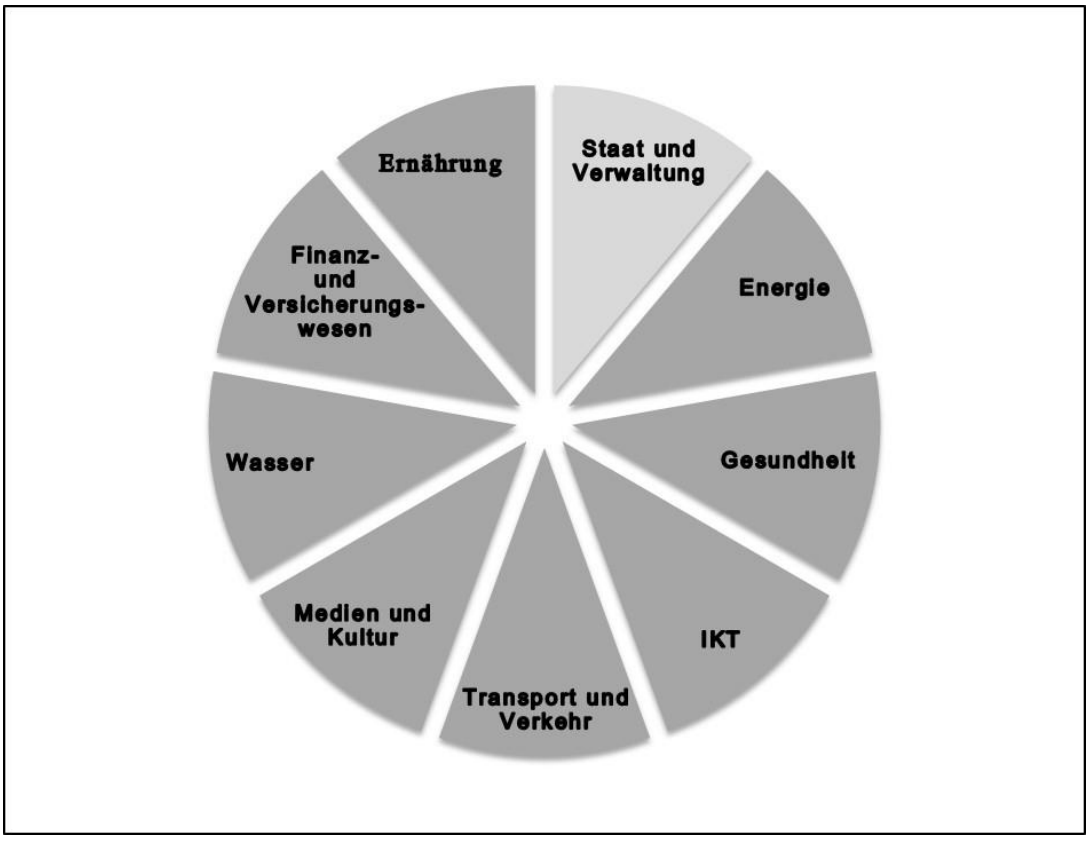

Abb. 2: Die Sektoren Kritischer Infrastrukturen in Deutschland (Quelle: Eigene Darstellung nach Daten des Bundesamtes für Sicherheit in der Informationstechnik und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2011-2013b)

Vom Plenum des UP KRITIS wurde das Dokument *UP KRITIS: Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen – Grundlagen und Ziele* beschlossen (vgl. Bundesamt für Sicherheit in der Informationstechnik und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2011-2013b). Darin wird nochmals betont, dass funktionierende Kritische Infrastrukturen für Staat, Wirtschaft und Gesellschaft unverzichtbar sind (vgl. UP KRITIS Themenarbeitskreis Fortschreibung 2014, S. 29). Wie in Abbildung 2 grafisch dargestellt, werden diese in neun Bereiche eingeteilt: 1) Energie, 2) Gesundheit, 3) IKT, 4) Transport und Verkehr, 5) Medien

und Kultur, 6) Wasser, 7) Finanz- und Versicherungswesen, 8) Ernährung sowie 9) Staat und Verwaltung (vgl. Bundesamt für Sicherheit in der Informationstechnik und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2011-2013b).

UP Bund

Der Sektor Staat und Verwaltung fällt nicht in den Zuständigkeitsbereich des UP KRITIS, hierzu wurde der UP Bund beschlossen. Aus dem UP Bund gehen einheitliche Mindestanforderungen an den Schutz der Informationsinfrastrukturen der Bundesverwaltung hervor (vgl. Bundesamt für Sicherheit in der Informationstechnik und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2011-2013b). Die Mindestanforderungen sind notwendig, da die Bundesverwaltung jährlich ca. drei Milliarden Euro in den Ausbau ihrer Informations- und Kommunikationsinfrastruktur investiert. Somit ergeben sich mehr Angriffsmöglichkeiten, wodurch ein hoher Schutz der IT-Systeme erforderlich wird (vgl. KPMG 2014, S. 6).

Die Maßnahmen aus dem UP BUND sind laut Interviewpartner 4 (BMVi) zufolge noch nicht flächendeckend umgesetzt worden. So bewertet er die Bundesministerien als gut geschützt, die Verwaltungsbehörden seien allerdings nicht ausreichend geschützt. Hier wird kritisiert, die Behördenleitungen hätten oftmals ein unzureichendes Problembewusstsein. Insofern fordert er, dass die Politik zunächst in ihren eigenen Einrichtungen mit gutem Beispiel vorangehen solle, bevor sie versuche, für Unternehmen Maßnahmen umzusetzen. Hierzu sei auch ein IT-Sicherheitskonzept für jede Behörde notwendig (vgl. Interview 4).

UP KRITIS-Rat

Beim Umsetzungsplan KRITIS verhalten sich laut dem interviewten Vertreter aus dem Bundesministerium des Innern (Interviewpartner 1 (BMI)) die Betreiber Kritischer Infrastrukturen hinsichtlich der Zusammenarbeit mit der Politik zurückhaltend. Mittlerweile habe sich diese Zusammenarbeit im UP KRITIS-Rat gut entwi-

ckelt. Eine bessere Zusammenarbeit sei dennoch nötig, wozu das IT-Sicherheitsgesetz beitragen solle. Bisher seien Versicherungen und Banken sowie die Betreiber in den Sektoren Telekommunikation und Energie gut aufgestellt. Mit dem IT-Sicherheitsgesetz möchte man nun insbesondere die nicht genannten Sektoren erreichen und mit gesetzlichen Mitteln eine Zusammenarbeit regeln (vgl. Interview 1). Generell wird jedoch angemerkt, dass es seit der Einführung des Umsetzungsplan KRITIS in der Politik und in den Unternehmen bereits mehr Diskussionen und Aufmerksamkeit in Bezug zur Cyber Security gibt (vgl. Interview 4).

Einige Bundesministerien und Bundesämter wünschen sich jedoch eine bessere Zusammenarbeit mit den Betreibern Kritischer Infrastrukturen (vgl. Interviews 1, 2, 3 und 8), andererseits äußern diesen Wunsch auch die Betreiber Kritischer Infrastrukturen (vgl. Interview 11). So kritisiert ein interviewter Vertreter von Open Grid Europe (Interviewpartner 11 (Open Grid Europe)) die Zusammenarbeit mit den politischen VertreterInnen im UP KRITIS-Rat und würde sich mit dem BSI nicht nur einen besseren Austausch über den UP KRITIS-Rat wünschen, sondern eine Plattform zum direkten Austausch mit dem Bundesamt (vgl. Interview 11). Der interviewte Vertreter der Deutschen Telekom AG (Interviewpartner 10 (Deutsche Telekom AG)) würde sich ebenfalls einen besseren Austausch mit der Politik im UP KRITIS wünschen (vgl. Interview 10).

Interviewpartner 4 (BMVi) kritisiert, dass sich seit dem UP KRITIS nicht viel verändert hätte (vgl. Interview 4). Das lässt auf die schlechte Zusammenarbeit im UP KRITIS-Rat schließen. Laut einem interviewten Vertreter des Bundesamtes für Sicherheit in der Informationstechnik (Interviewpartner 2 (BSI)) ermöglichte der UP KRITIS-Rat jedoch der Politik einen besseren Einblick in die Wirtschaft und ihre Herausforderungen beim Cyber-Schutz. Diese Zusammenarbeit sei für das BSI unbedingt notwendig, um bessere und umfangreichere Empfehlungen an die Unternehmen geben zu können (vgl. Interview 2). In diesem Zusammenhang bezeichnet der interviewte Vertreter des Bundesministeriums für Wirtschaft und Energie (BMWi) (Interviewpartner 3 (BMWi)) die Telekommunikationsbranche als sehr en-

gagiert und vorbildlich in Deutschland. Die Banken und der Energiesektor seien ebenfalls engagiert, während in der Zusammenarbeit mit der Wasserwirtschaft eine Optimierung nötig sei (vgl. Interview 3). In den einzelnen Kapiteln zu den Bundesministerien und Bundesämtern sowie zu den Betreibern Kritischer Infrastrukturen wird auf die Zusammenarbeit ausführlicher eingegangen.

In der KRITIS-Strategie, in dem Umsetzungsplan KRITIS, dem UP KRITIS und dem NPSI wird die Verantwortung für den Schutz der Kritischen Infrastrukturen immer wieder bei Staat, Wirtschaft und Gesellschaft gesehen (vgl. UP KRITIS Themenarbeitskreis Fortschreibung 2014, S. 29). Insofern bezieht die Politik die Betreiber Kritischer Infrastrukturen in die Verantwortung für Cyber Security stark mit ein.

3.3 Die deutsche Cyber-Sicherheitsstrategie

Die deutsche Cyber-Sicherheitsstrategie wurde 2011 vom Bundeskabinett beschlossen und kann als Weiterentwicklung des KRITIS Umsetzungsplans und des NPSI von 2005 betrachtet werden (vgl. Kullik 2014, S. 92). Sie umfasst mehrere Bereiche der Sicherheitspolitik, wie Cyberkriminalität oder Cyberterrorismus, die eine hohe Relevanz für Cyber Security aufweisen (vgl. Bundesministerium des Innern 2011, S. 3).

Die Formulierungen in der deutschen Cyber-Sicherheitsstrategie lassen erkennen, dass sie sich an den europäischen Sicherheitsstrategien und Dokumenten orientiert. Insbesondere lassen sich Gemeinsamkeiten zur europäischen Sicherheitsstrategie von 2003 erkennen. Letztlich hat aber erst 2010 die Sicherheitsstrategie der europäischen Politik dazu geführt, dass mehrere Mitgliedsländer nationale Cyber-Sicherheitsstrategien entwickelt haben, die es bis dahin nur in Estland, Großbritannien und Slowakei gegeben hatte (vgl. Berger 2013, S. 321). Während einige Mitgliedsländer der EU bereits eine Cyber-Sicherheitsstrategie hatten, ist erst 2013 eine gemeinsame europäische Strategie verabschiedet worden (vgl. Berger 2013, S. 307; Näheres hierzu siehe Kapitel 4.5.2). Die Cyber-Sicherheitsstrategie der Bundesre-

publik Deutschland umfasst insgesamt zehn strategische Ziele und Maßnahmen (vgl. hierzu Bundesministerium des Innern 2011, S. 6-12):

1. Schutz kritischer Informationsinfrastrukturen
2. Sichere IT-Systeme in Deutschland, bezogen auf die „IT-Systeme der Bürgerinnen und Bürger sowie der kleinen und mittelständischen Unternehmen“ (Bundesministerium des Innern 2011, S. 7)
3. Stärkung der IT-Sicherheit in der öffentlichen Verwaltung
4. Einrichtung eines Nationalen Cyber-Abwehrzentrums
5. Einrichtung eines Nationalen Cyber-Sicherheitsrats
6. Wirksame Bekämpfung von Cyberkriminalität
7. Effektives Zusammenwirken für Cyber-Sicherheit in Europa und weltweit
8. Einsatz verlässlicher und vertrauenswürdiger Informationstechnologie
9. Personalentwicklung der Bundesbehörden
10. „Ein mit den zuständigen staatlichen Stellen abgestimmtes und vollständiges Instrumentarium für die Abwehr von Angriffen im Cyber-Raum [...]“ (Bundesministerium des Innern 2011, S. 12).

Hierbei steht der Schutz Kritischer Infrastrukturen (1) im Mittelpunkt, d. h. die entsprechenden Branchen und nötigen Technologien müssen berücksichtigt werden. Um eine Zusammenarbeit innerhalb der Politik und mit der Wirtschaft erfolgreicher zu gestalten, sollen neben dem verbreiteten Einsatz von sicheren IT-Systemen (2) und einer erhöhten IT-Sicherheit in der öffentlichen Verwaltung (3) ein Cyber-Abwehrzentrum (Cyber-AZ) (4) und ein Cyber-Sicherheitsrat (Cyber-SR) (5) eingerichtet werden (vgl. Bundesministerium des Innern 2011, S. 6-10).

Aus Punkt 4 zum Cyber-AZ geht hervor, dass mit der Einrichtung eine bessere Zusammenarbeit mit Betreibern Kritischer Infrastrukturen geschaffen werden soll, zugleich sollen sie aber auch stärker in die Verantwortung für die Sicherheit der Kritischen Infrastrukturen einbezogen werden. Somit wird von den Betreibern gefordert, dass sie unter anderem sichere IT-Systeme einsetzen. (vgl. Bundesministerium des Innern 2011, S. 8-9).

Der Nationale Cyber-SR steht ebenfalls für eine bessere Zusammenarbeit auf institutioneller Ebene innerhalb der Bundesregierung, bezieht aber auch WirtschaftsvertreterInnen als *assoziierte Mitglieder* mit ein. Dabei versteht sich der Cyber-SR als Koordinationsstelle zwischen Staat und Wirtschaft (vgl. Bundesministerium des Innern 2011, S. 9-10). Näheres zu dem Cyber-AZ und dem Cyber-SR ist den Kapiteln 4.3.1 und 4.3.2 zu entnehmen.

Unter Punkt 6 wird in der Cyber-Sicherheitsstrategie die Bekämpfung der Cyberkriminalität nicht nur als national, sondern auch als international „wachsende Herausforderung" beschrieben (vgl. Bundesministerium des Innern 2011, S. 10). Hier ist eine „Harmonisierung" des Strafrechts auf internationaler Ebene anzustreben, um der internationalen Cyberkriminalität entgegenzuwirken (vgl. Bundesministerium des Innern 2011, S. 11). Auf europäischer Ebene bedeutet dies ein Übereinkommen des Strafrechts im Bereich Computerkriminalität. Auf internationaler Ebene soll geprüft werden, inwieweit eine Übereinkunft mit den Vereinten Nationen erforderlich ist.

Punkt 7 schließt daran an und widmet sich der internationalen Zusammenarbeit, die bei der Schaffung eines weltweit sicheren Cyber-Raums unverzichtbar ist. Hierunter fällt neben der Zusammenarbeit auf europäischer Ebene auch die Kooperation mit internationalen Bündnissen, wie mit den Vereinten Nationen oder der NATO (vgl. Bundesministerium des Innern 2011, S. 11). In den Kapiteln 4.5.2. und 4.5.3 wird die Zusammenarbeit auf EU- und NATO-Ebene eingehender erörtert.

Unter den letzten drei Punkten (8.-10.) wird die Notwendigkeit der Forschung für zuverlässige IT-Systeme und insbesondere für Kritische Infrastrukturen erwähnt. Die Entwicklungen der IT-Systeme sollen gestärkt werden, sowohl auf nationaler als auch auf europäischer Ebene sowie mit Verbündeten und Partnern. Auf nationaler Ebene werden die Bundesbehörden erwähnt, deren Kompetenzen und Ressourcen insbesondere im Bereich des Personals überprüft werden müssten. Zudem wird die Notwendigkeit von Kooperationen zwischen staatlichen Stellen auf Bundes- und Landesebene sowie mit Wirtschaftsunternehmen betont. Diese Koope-

rationen werden als ein „Instrumentarium“ zur Bekämpfung von Cyber-Angriffen verstanden (vgl. Bundesministerium des Innern 2011, S. 12).

3.4 Die deutsche Digitale Agenda

Im Koalitionsvertrag der 18. Legislaturperiode wurde das Vorhaben für eine Digitale Agenda festgelegt (vgl. Koalitionsvertrag zwischen CDU CSU und SPD 2013, S. 139), die dann im August 2014 vom Bundeskabinett verabschiedet wurde (vgl. Die Bundesregierung 2014a). Um den digitalen Wandel voranzutreiben, steht sie für die Umsetzung von „Netzausbau, Cybersicherheit und die Förderung der digitalen Wirtschaft“ (Die Bundesregierung 2014a). Die Digitale Agenda hat unter anderem die Ziele, Innovationen in Deutschland zu fördern, den flächendeckenden Ausbau von Hochgeschwindigkeitsnetzen voranzutreiben, um allen Menschen aus der Bevölkerung den Zugang zur Informationsinfrastruktur zu ermöglichen, sowie die Sicherheit von IT-Systemen zu erhöhen (vgl. Die Bundesregierung 2014a; Die Bundesregierung 2014b).

Aufgebaut ist die Digitale Agenda in sieben Handlungsfeldern, aus denen hervorgeht, dass das BMI besonders für die Bereiche „Innovativer Staat“, „Digitale Gesellschaft“ sowie „Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft“ (Die Bundesregierung 2014a) zuständig ist. Als besondere Stärke der deutschen Industrie wird die Industrie- und Produktionstechnik genannt (vgl. Die Bundesregierung 2014b, S. 2). Hier wird die Möglichkeit gesehen, die als „[...] Industrie 4.0 bezeichnete intelligente und maßgeschneiderte Produktion und Logistik fortzuentwickeln, sie um intelligente Dienste zu erweitern und somit für dauerhaftes Wachstum und anhaltend hohe Beschäftigung zu sorgen“ (Die Bundesregierung 2014b, S. 2). Obwohl mit Industrie 4.0 auch eine Rationalisierung einhergehen wird und dadurch möglicherweise Arbeitsplätze verloren gehen, werden hier auch neue Geschäftschancen und Wachstumsfelder gesehen, die wiederum für neue Beschäftigung sorgen und die Wettbewerbsfähigkeit der deutschen Industrie erhalten.

Mit Industrie 4.0 wird eine vierte industrielle Revolution beschrieben, die wirtschaftliche Möglichkeiten in der deutschen Forschung im Bereich Cyber Security mit sich bringt. IKT-Systeme werden in der Wirtschaft nicht mehr voneinander getrennt, wodurch vernetzte Produktionssysteme entstehen. Somit werden innerhalb des Unternehmens alle Bereiche vernetzt, aber auch mit den Zulieferern, deren Cyber Security von ebenso großer Bedeutung für die Unternehmen ist. Es werden also weitaus höhere Sicherheitsanforderungen notwendig, da mit der Vernetzung mehr Angriffsmöglichkeiten für Cyber-Angriffe entstehen. Somit entstehen auch ganz neue Wertschöpfungsketten mit IT-Diensten, wie bspw. Cloud-Computing. Die hochsensiblen Daten, bspw. aus der Produktion von Unternehmen, müssen trotz steigender Cyber-Angriffe geschützt werden können (vgl. Fraunhofer 2014, S. 13).

Die Welt ist mittlerweile in vielen Bereichen vernetzt, ob im privaten Bereich der BürgerInnen, in der Wirtschaft oder Politik. Dies erfordert einen Ausbau der digitalen Infrastrukturen. Die Bundesregierung möchte Rahmenbedingungen schaffen, die es ermöglichen, bis 2018 eine der weltweit besten leistungsfähigen Netze zu haben (vgl. Die Bundesregierung 2014b, S. 4).

Neben einigen weiteren Maßnahmen, die in der Wirtschaft umgesetzt werden sollen, wird die „Stärkung der deutschen digitalen Sicherheitswirtschaft“ erläutert (Die Bundesregierung 2014b, S. 13). In dem Kapitel Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft wird das Thema Cyber Security nochmal zentral behandelt, mit Konzentration auf die Sicherheit der digitalen Infrastrukturen, den Schutz der BürgerInnen, den Daten- und Verbraucherschutz sowie die Sicherheit im Cyberraum (vgl. Die Bundesregierung 2014b, S. 30-33). Hierbei sollen die „Sicherheit der Systeme und [der] Schutz der Daten“ (Die Bundesregierung 2014b, S. 13) in allen Punkten der Digitalen Agenda berücksichtigt werden. Im Vordergrund stehen also die Gesellschaft und die Wirtschaft (vgl. Die Bundesregierung 2014b, S. 31).

Die Digitale Agenda umfasst von Datenschutz bis hin zum Vorantreiben von Innovationen ein weites Spektrum an Aufgaben (vgl. Die Bundesregierung 2014b,

S. 31-33). Daher werden in der Digitalen Agenda die Aktivitäten der Bundesministerien gesammelt und letztlich als „gebündelte Kräfte“ in eine Agenda umgesetzt, die in den nächsten Jahren dem fortschreitenden Prozess der Digitalisierung eine Richtung vorgeben soll (vgl. Die Bundesregierung 2014b, S. 2). Um die Vorhaben umsetzen zu können, „[...] bedarf es einer strategischen Neuausrichtung der Cyber-Sicherheitsarchitektur ebenso wie einer besseren Ausstattung der Sicherheitsbehörden in technischer und personeller Hinsicht“ (Die Bundesregierung 2014b, S. 33).

3.5 Das deutsche IT-Sicherheitsgesetz

Das Vorhaben eines IT-Sicherheitsgesetzes wurde, wie in Kapitel 3.1 erwähnt, im Koalitionsvertrag von 2013 beschlossen (vgl. Koalitionsvertrag zwischen CDU, CSU und SPD 2013, S. 147). Am 12. Juni 2015 wurde dann vom Deutschen Bundestag der Gesetzentwurf zum IT-Sicherheitsgesetz (vgl. Deutscher Bundestag 2015c) mit einigen Änderungsanträgen von der Unions- und SPD-Fraktion (vgl. Deutscher Bundestag 2015a) für Deutschland beschlossen (vgl. Deutscher Bundestag 2015b). Federführend ist das BMI (vgl. Interview 1). Am 25. Juli 2015 ist das IT-Sicherheitsgesetz in Kraft getreten, die Rechtsverordnung war zum Zeitpunkt der Entstehung dieser Arbeit vom BMI noch in Bearbeitung (vgl. Bundesamt für Sicherheit in der Informationstechnik 2015c).

Die Notwendigkeit des IT-Sicherheitsgesetzes wird vor allem mit der weiterhin zunehmenden Nutzung der IT-Systeme durch Staat, Wirtschaft und Gesellschaft und der damit einhergehenden Digitalisierung und Vernetzung begründet (vgl. Bundesministerium des Innern 2014c, S. 1; Deutscher Bundestag 2015a, S. 12). Hierfür sind die Kritischen Infrastrukturen besonders wichtig, die mit dem Gesetz sicherer gemacht werden sollen. So müssen nach dem Inkrafttreten des Gesetzes die Betreiber Kritischer Infrastrukturen einen Mindeststandard an IT-Sicherheit erfüllen und Cyber-Angriffe an das BSI melden. Folglich soll mit dem IT-Sicherheitsgesetz die Zusammenarbeit zwischen Politik und Wirtschaft verbessert werden (vgl. Deutscher Bundestag 2015b). Mit dem Beschluss des IT-Sicherheitsgesetztes im Juni

2015 müssen derzeit nur Betreiber von Kernkraftwerken und Telekommunikationsunternehmen Cyber-Angriffe melden. Bis zum Inkrafttreten des IT-Sicherheitsgesetzes müssen in der Rechtsverordnung Kritische Infrastrukturen und deren Branchen eindeutig definiert werden, da ansonsten aus dem Gesetz nicht hervorgeht, auf welche Infrastrukturen sich die Verordnung bezieht, wie beispielsweise vom eco – Verband der deutschen Internetwirtschaft e. V. (eco) angemerkt wurde (vgl. eco – Verband der deutschen Internetwirtschaft e. V., 2015), aber auch von einer Vertreterin des Bundesverbandes der Deutschen Industrie (BDI) (vgl. Plöger 2015). In der Rechtsverordnung, die noch erarbeitet wird, soll dann klar definiert sein, welche Unternehmen dem Gesetz unterliegen (vgl. Bundesamt für Sicherheit in der Informationstechnik 2015c).

Eine Meldepflicht für Betreiber Kritischer Infrastrukturen bei Cyber-Angriffen forderte die EU bereits 2013 (vgl. Bendiek 2013, S. 1). Zunächst fand jedoch die Meldepflicht bei den europäischen Mitgliedsstaaten in Politik und Wirtschaft keinen Zuspruch. Daraufhin legte die EU den Mitgliedsstaaten einen Maßnahmenkatalog vor, der die Meldepflicht vorschrieb (vgl. Bundesministerium des Innern 2009). Dieser legte „eine europäische und internationale digitale Standortpolitik“ fest (Bundesministerium des Innern 2009), woraufhin im Dezember 2014 ein Gesetzentwurf des IT-Sicherheitsgesetzes der Bundesregierung (vgl. Bundesministerium des Innern 2014c) vom Bundesinnenminister vorgestellt wurde. Unter anderem erfolgte das Vorgehen mit der Begründung, dass „die IT-Systeme und digitalen Infrastrukturen Deutschlands [...] zu den sichersten weltweit werden [sollen]“ (Bundesministerium des Innern 2014c).

Bisher melden einige Unternehmen der deutschen Wirtschaft Cyber-Angriffe nicht. Mit dem IT-Sicherheitsgesetz sollen sie dazu gezwungen werden (vgl. Interview 1). Der Grund, weshalb Cyber-Angriffe nicht gemeldet werden, besteht laut einem interviewten Vertreter der Daimler AG (Interviewpartner 12 (Daimler AG)) darin, dass Unternehmen mit der Meldung die Kontrolle über diese Information abgeben und keinen Einfluss auf und kein zuverlässiges Wissen über ihre weitere

Verbreitung haben. Mit dem IT-Sicherheitsgesetz wird auch die Daimler AG dazu verpflichtet sein, Cyber-Angriffe zu melden, was bislang nicht der Fall ist, obwohl sie durch die Integration von Telekommunikationstechnik in ihren Fahrzeugen auch ein Anbieter in diesem Bereich ist (vgl. Interview 12). Den erwähnten Befürchtungen entgegnet Interviewpartner 1 (BMI), dass die Meldungen anonymisiert würden (vgl. Interview 1).

Martin Schallbruch, IT-Beauftragter im BMI, begründet die Meldepflicht mit den täglich Tausenden von Sicherheitsvorfällen. Eine intakte Funktion der Kritischen Infrastrukturen könne nicht sichergestellt werden, wenn sicherheitskritische Vorfälle, die zum Ausfall der IT-Systeme führen können, nicht an die zuständigen Aufsichtsbehörden gemeldet würden. Darüber hinaus spricht er sich für die Mindestsicherheitsanforderungen für Unternehmen und insbesondere für alle Betreiber Kritischer Infrastrukturen aus. Dies sei bereits in einigen Branchen wie der Finanzwirtschaft üblich. Die Branche der Telekommunikations- und Telemediendienstanbieter sieht er verstärkt in der Verantwortung, denn diese stellten den Zugang zum Cyber-Raum bereit (vgl. Schallbruch 2014, S. 1-3). Beispielsweise werden Telekommunikationsunternehmen aufgefordert, mit dem aktuellen Stand der Technik ihre Kunden zu warnen, sollte es Sicherheitslücken in ihrem Botnetz geben (vgl. Bendiek 2013, S. 1). Ein Botnetz besteht aus zusammengeschalteten Bots. Ein Bot ist ein Computer, der kontrolliert werden kann. Wird die Kontrolle über ein Botnetz übernommen, ist es Angreifern möglich, alle Bots bspw. gleichzeitig auf einen Server oder Computer zugreifen zu lassen und somit die Dienste dieses Systems für die Nutzer zu blockieren oder das System zum Absturz zu bringen (Kullik 2014, S. 11).

Mit der Rechtsverordnung haben Betreiber Kritischer Infrastrukturen zwei Jahre Zeit, die geforderten IT-Mindeststandards umzusetzen. Die Pflicht zur Einhaltung des Gesetzes besteht somit erst nach zwei Jahren; das gilt auch für die Meldepflicht der Cyber-Angriffe. Sollte danach das Gesetz nicht eingehalten werden, können hohe Bußgelder verhängt werden (vgl. Bundesamt für Sicherheit in der Informationstechnik 2015c).

Im Gesetzentwurf des IT-Sicherheitsgesetztes ist unter Artikel 1 vorgesehen, dass die Aufgaben der Zuständigkeit für Informationssicherheit des BSIs erweitert werden soll (vgl. Bundesministerium des Innern 2014c, S. 1) Insgesamt soll das BSI gestärkt werden, um Cyber Security voranzutreiben (vgl. Bundesamt für Sicherheit in der Informationstechnik 2014; Bundesministerium des Innern 2014a). Hierfür sind im IT-Sicherheitsgesetz 215 bis max. 216,5 Planstellen/Stellen für das BSI vorgesehen, um die neuen Aufgaben erfüllen zu können. Weitere 9 bis max. 13 Planstellen sind auch für das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) vorgesehen; des Weiteren: für das BKA 48 bis max. 78 Planstellen, für die Bundesnetzagentur max. 28 Planstellen, für das BfV 26,5 bis max. 48,5 und für den BND max. 30 Planstellen/Stellen (vgl. Deutscher Bundestag 2015a, S. 5-6). Ob all diese Stellen letztlich besetzt werden, wird vom Interviewpartner 2 (BSI) bezweifelt (vgl. Interview 2). Zusätzlich erhalten die Bundesämter finanzielle Mittel für Sachkosten/Sachmittel (vgl. Deutscher Bundestag 2015a, S. 5-6).

Neben dem BSI wird auch das BKA durch das IT-Sicherheitsgesetz stärker einbezogen. So ist das BKA für die Ermittlung von Cyberkriminalität zuständig. Diese Kompetenz soll sich um Ermittlungen bei Cyber-Angriffen auf Einrichtungen des Bundes erweitern (vgl. Bundesamt für Sicherheit in der Informationstechnik 2014; Bundesministerium des Innern 2014a).

Das IT-Sicherheitsgesetz erhält auch einige Kritik von VertreterInnen der Wirtschaft, Wissenschaft und Vereinen. Beispielsweise forderte ein Vertreter der Deutschen Telekom AG im Rahmen des IT-Sicherheitsgesetzes eine angepasste Produkthaftungspflicht für Softwarehersteller, die nicht umgesetzt wurde. Dienstanbieter seien demnach dem Haftungsrisiko ausgesetzt, wenn die eingekaufte Software Sicherheitslücken enthält (vgl. Tschersich 2015). Dass die Produkthaftung für Softwarehersteller angepasst werden muss, wird auch von einem Vertreter aus der Wissenschaft kritisiert. Zudem konzentriere sich das Gesetz nur auf den Bereich der Kritischen Infrastrukturen; offen bliebe, wie mit den anderen Bereichen der Wirtschaft zu verfahren sei. Darüber hinaus würde die gesetzlich vorgeschriebene

Mindestanforderung an die IT-Sicherheit der Unternehmen die erwünschte IT-Sicherheit nicht bewirken, da die gesetzlich formulierte IT-Sicherheit nicht ausreichen würde. Jedoch sei dies ein erster Schritt zu mehr IT-Sicherheit (vgl. Schiller 2015). Eine Vertreterin der BDI merkt in ihrer Stellungnahme an, dass Doppelregulierungen zwischen bestehenden Rechtsvorschriften, wie dem Telekommunikationsgesetz, dem Bundesdatenschutzgesetz und dem Energiewirtschaftsgesetz, und dem IT-Sicherheitsgesetz entstehen können, insbesondere da die betroffenen Kritischen Infrastrukturen bisher nicht klar genannt werden (vgl. Plöger 2015).

3.6 IT-Planungsrat von Bund und Ländern

Der Vertrag zur Errichtung des IT-Planungsrats und die damit verbundenen Anforderungen traten am 1. April 2010 in Kraft. Die Mitglieder setzen sich aus der Beauftragten der Bundesregierung für Informationstechnik und den Verantwortlichen für Informationstechnik aus den Ländern zusammen. Darüber hinaus können beratend weitere VertreterInnen aus Wirtschaft und Politik teilnehmen (vgl. IT-Planungsrat 2014c).

„Wirksame IT-Sicherheit braucht starke Strukturen in allen Behörden der Bundesverwaltung“ (Bundesministerium des Innern 2011, S. 8), wie aus der Cyber-Sicherheitsstrategie für Deutschland hervorgeht. Hierin wird die Stärkung der „IT-Sicherheit in der öffentlichen Verwaltung“ (Bundesministerium des Innern 2011, S. 8) beschrieben. Diese Aufgabe wurde dem IT-Planungsrat von Bund und Ländern übertragen. Behörden sollen eine Vorbildfunktion bei der Datensicherheit einnehmen und einheitlich handeln. Hierzu müssen z. B. Ressourcen entsprechend verteilt und eingesetzt werden (vgl. Bundesministerium des Innern 2011, S. 8).

Im IT-Staatsvertrag werden unter anderem E-Government-Projekte zur Weiterentwicklung der Informationstechnik in der Verwaltung festgehalten (vgl. Informationstechnik 2015). Der IT-Planungsrat ist unter anderem zuständig für die Umsetzung der angedachten Projekte und der daraus resultierenden Zusammenarbeit von Bund und Ländern. Des Weiteren richtet sich der IT-Planungsrat an Bund

und Länder mit Fragen zu den IT-Sicherheitsstandards (vgl. IT-Planungsrat 2014c). Hierfür ist eine Zusammenarbeit zwischen Bund und Ländern unumgänglich. Die Verantwortung für die Zusammenarbeit wird dem IT-Planungsrat zugeschrieben.

Im Bereich der Informationssicherheit hat der IT-Planungsrat bisher die „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ (IT-Planungsrat 2014b) und den dazugehörigen Umsetzungsplan beschlossen. Der Plan wendet sich an das Informationsmanagement der öffentlichen Verwaltung (vgl. IT-Planungsrat 2014b). Seit 2015 hat Berlin mit dem Staatssekretär Andreas Statzkowski den Vorsitz im IT-Planungsrat inne (vgl. IT-Planungsrat 2014a). Er legt den Schwerpunkt auf den „Ausbau von Online-Transaktionen und Abbau von Schriftformerfordernissen“ (IT-Planungsrat 2014a); weiterhin soll aber auch die föderale IT-Kooperation entwickelt und intensiviert werden (vgl. IT-Planungsrat 2014a). Im Hinblick auf den Cyber-Angriff auf den Deutschen Bundestag (vgl. Bewarder et al. 2015) kann davon ausgegangen werden, dass für Cyber Security der IT-Systeme des Deutschen Bundestags noch ein großer Handlungsbedarf besteht und die bisher getroffenen Maßnahmen für die Bundesverwaltung, wozu auch die Bundestagsverwaltung zählt, noch nicht ausreichend sind oder umgesetzt wurden.

3.7 Zwischenfazit

Die genannten Dokumente stellen die Lage für Cyberbedrohungen dar und sehen überwiegend die Verantwortung für Cyber Security bei Staat, Wirtschaft und Gesellschaft (vgl. Bundesministerium des Innern 2005, S. 7; Bundesministerium des Innern 2007, S. 3; Bundesministerium des Innern 2011, S. 3; Die Bundesregierung 2014b, S. 27). Das Staat, Wirtschaft und Gesellschaft immer wieder im Fokus der hier behandelten Pläne und Strategien der Politik stehen, mag daran liegen, dass sie bei einem Ausfall der Kritischen Infrastrukturen durch einen Cyber-Angriff folgenschwer betroffen wären (vgl. KPMG 2014, S. 7) und die uneingeschränkte Funktionalität insofern unerlässlich ist (vgl. UP KRITIS Themenarbeitskreis Fortschreibung 2014, S. 29). Allerdings bleiben die Begriffe sehr allgemein gefasst und es wird nicht

konkret darauf eingegangen, was in Bezug auf die Verantwortung von Staat, Wirtschaft und Gesellschaft für Cyber Security gemeint ist.

Um Cyber Security in Deutschland zu stärken, wurde zunächst im Koalitionsvertrag von 2009 beschlossen, dass das BSI gestärkt werden und als Koordinationsstelle für Cyber-Angriffe dienen soll, und dass die IT-Kompetenzen des Personals ausgebaut werden sollen (vgl. Koalitionsvertrag zwischen CDU, CSU und FDP 2009, S. 101). Dieses Ziel verfolgt die Politik mit der Cyber-Sicherheitsstrategie weiter und errichtete 2011 das Cyber-AZ, dessen Federführung beim BSI liegt (vgl. Bundesministerium des Innern 2011, S. 8). Neben dem Cyber-AZ konnten aus der Cyber-Sicherheitsstrategie weitere Vorhaben umgesetzt werden, wie beispielsweise die Einrichtung des Cyber-SRs (vgl. Bundesministerium des Innern 2015a).

Das Ziel aus dem Koalitionsvertrag von 2013, eine Digitale Agenda für Deutschland zu verabschieden (vgl. Koalitionsvertrag zwischen CDU CSU und SPD 2013, S. 139), konnte ebenfalls umgesetzt werden (vgl. Die Bundesregierung 2014b). Übereinstimmend fordern die untersuchten Dokumente eine Kompetenzsteigerung des Personals, einen Personalausbau, eine bessere technische Ausstattung sowie eine Verbesserung der organisatorischen Struktur der Bundesministerien und Bundesämter im Bereich Cyber Security (vgl. z. B. Die Bundesregierung 2014, S. 33; Bundesministerium des Innern 2011, S. 12).

Darüber hinaus nennt die Digitale Agenda einige Ziele im Rahmen der weltweit zunehmenden Digitalisierung, deren Umsetzung die Innovationen der deutschen digitalen Wirtschaft fördern und den flächendeckenden Breitbandausbau bis 2018 vorantreiben sollen (vgl. Die Bundesregierung 2014a). Zudem wird in der Digitalen Agenda, wie auch in dem Koalitionsvertrag von 2013, das Ziel formuliert, Deutschland zum digitalen Wachstumsland Nr. 1 in Europa zu machen (vgl. Die Bundesregierung 2014b, S. 13; Koalitionsvertrag zwischen CDU, CSU und SPD 2013, S. 139).

Um Cyberbedrohungen Kritischer Infrastrukturen zu begegnen, ist unter anderem eine Kooperation zwischen Staat und Wirtschaft notwendig (vgl.

Bundesministerium des Innern 2005, S. 7-8), die bislang nicht ausreichend funktioniert hat und nun mit dem IT-Sicherheitsgesetz erzwungen werden soll (vgl. Interview 1). Das Vorhaben zu einem IT-Sicherheitsgesetz wurde bereits im Koalitionsvertrag 2013 festgelegt (vgl. Koalitionsvertrag zwischen CDU, CSU und SPD 2013, S. 147) und zwei Jahre später der Gesetzentwurf beschlossen (vgl. Bundesministerium des Innern 2014a). Mit dem IT-Sicherheitsgesetz möchte die Politik auch ein Vorbild sein, um die Gesetzgebung auf EU-Ebene zu fördern (vgl. Interview 1). Dies wurde bereits 2005 im NPSI als Ziel formuliert, international im Rahmen der Gesetzgebung zusammenzuarbeiten (vgl. Bundesministerium des Innern 2005, S. 3).

Mit dem IT-Sicherheitsgesetz werden zusätzliche Aufgaben auf das BSI zukommen, zu deren Bewältigung ein Stellenausbau vorgesehen ist (vgl. Deutscher Bundestag 2015a; Näheres hierzu siehe auch Kapitel 4.1.2). Ferner müssen für eine effiziente Umsetzung des IT-Sicherheitsgesetzes Kritische Infrastrukturen klar und konkret benannt werden (vgl. Kapitel 3.5). In der KRITIS-Strategie werden allerdings Kritische Infrastrukturen näher definiert und in Sektoren eingeteilt (vgl. Bundesministerium des Innern 2009, S. 5). Ob diese für das IT-Sicherheitsgesetz präziser formuliert werden, wird sich letztlich erst mit der Rechtsverordnung zeigen. Zusammenfassend wiederholen sich einige Ziele und Maßnahmen in den einzelnen Dokumenten, einige konnten aber auch bereits umgesetzt werden. Der Schwerpunkt der Politik liegt auf Kritischen Infrastrukturen und Wirtschaftsschutz.

4 Politische Institutionen im Bereich Cyber Security

In Deutschland sind die Aufgaben im Bereich Cyber Security auf unterschiedliche Bundesministerien und Bundesbehörden aufgeteilt. Die Aufgaben für Cyber Security ergeben sich für das BMI bereits aus der Verantwortung für die innere Sicherheit in Deutschland (vgl. Bundesministerium des Innern 2015c). Zu den Geschäftsbereichen des BMIs gehören auch die meisten Bundesämter, welche Aufgaben im Be-

reich Cyber Security wahrnehmen. Hierzu gehören das BSI, das BBK, das BKA und das BfV (vgl. Bundesministerium des Innern 2015e). Zusätzlich nehmen das BMWi, das BMVg, das BMVi und das Auswärtige Amt (AA) Aufgaben im Bereich Cyber Security wahr (vgl. Auswärtiges Amt 2014; Bundesministerium der Verteidigung 2015b; Bundesministerium für Wirtschaft und Energie 2015a). Das BMVg ist zudem die oberste Dienstbehörde für die Bundeswehr, deren Rolle bei der Cyberverteidigung im Folgenden beleuchtet wird (vgl. Bundesministerium der Verteidigung 2015a). Die genannten exekutierenden Bundesämter unterstützen die genannten Bundesministerien unter anderem im Bereich Cyber Security (vgl. Bundeskriminalamt 2015a; Bundesnachrichten-dienst 2015e).

Darüber hinaus wird in diesem Kapitel näher auf den nationalen Cyber-SR eingegangen, der für die Koordination der Zusammenarbeit innerhalb der Bundesregierung und für die Vermittlung zwischen Politik und Wirtschaft zuständig ist (vgl. Bundesministerium des Innern 2015a). Daneben soll auch das Cyber-AZ erläutert werden, dessen Aufgabe mitunter in der Organisation der Kooperation bei Fragen der Cybersicherheit zum einen zwischen Bundesbehörden und zum anderen zwischen diesen und Unternehmen besteht.

Das BMI und das BSI sind in Anlehnung an Jakob Kullik (2014) aufgrund ihrer Zuständigkeiten als zentrale Institutionen zu bezeichnen (Kapitel 4.1). Alle weiteren zu untersuchenden Bundesministerien werden aufgrund ihrer Aufgaben den flankierenden Institutionen zugeordnet (Kapitel 4.2) und die Bundesämter unter Kapitel 4.4 als exekutierende Institutionen bezeichnet (vgl. Kullik 2014) und nachfolgend erläutert. Zusätzlich wird auf die mit dem Bund kooperierenden Vereine und Organisationen sowie auf die Bedeutung der EU und der NATO für die Cyber Security in der Bundesrepublik Deutschland eingegangen (Kapitel 4.5).

4.1 Zentrale Institutionen auf Bundesebene

Dem BMI ist das BSI unterstellt (vgl. Bundesministerium des Innern 2015e). Zusammen sind diese Einrichtungen für die Cyber Security in Deutschland von größter Bedeutung, wie nachfolgend verdeutlicht werden soll.

4.1.1 Bundesministerium des Innern

Das BMI beschäftigt sich mit vielfältigen innenpolitischen Aufgaben. Die innere Sicherheit der Bundesrepublik Deutschland gehört zu den Aufgabenbereichen mit einem hohen Stellenwert, für die das BMI federführend zuständig ist (vgl. Bundesministerium des Innern 2015c).

Es beschäftigt insgesamt 1500 MitarbeiterInnen (vgl. Bundesministerium des Innern 2015c). Die Staatssekretärin des BMIs, Cornelia Rogall Grothe, ist Beauftrage der Bundesregierung für Informationstechnik. Ihr ist unter anderem die Abteilung ‚IT Informationstechnik, Digitale Gesellschaft und Cybersicherheit' unter der Leitung von Martin Schallbruch unterstellt, mit den Unterabteilungen ‚IT I (Digitale Gesellschaft, IT-Steuerung, IT-Strategie; Geschäftsstelle IT-Planungsrat)' mit sechs Referaten und der Stab ‚IT II (IT- und Cybersicherheit; sichere Informationstechnik)' mit vier Referaten (vgl. Bundesministerium des Innern 2015g). Die Bereiche wurden 2014 umstrukturiert, da die Aufgaben vielfältiger geworden sind. Die genannten Referate haben jeweils ca. sieben MitarbeiterInnen und verfügen über breit gestreute Kompetenzen aus den Bereichen Jura, Volkswirtschaftslehre, Politikwissenschaften und Informatik (vgl. Interview 1).

Die Zuständigkeit des BMI für die Sicherheit der Kritischen Infrastrukturen wurde bereits 2009 in der KRITIS-Strategie festgehalten: „Die zentralen bundesstaatlichen Maßnahmen zum Schutz Kritischer Infrastrukturen werden im Bundesministerium des Innern ressortübergreifend koordiniert" (Bundesministerium des Innern 2009, S. 3). Das BMI wird von anderen Bundesbörden beim Schutz der Kritischen Infrastrukturen in Form von Analysen, Gefährdungsbewertungen und Schutzkonzepten unterstützt (vgl. Kapitel 4; Bundesministerium des Innern 2009,

S. 3; Bundesministerium des Innern 2015e). Das BMI hat seit 2005 alle relevanten Strategien und Pläne zur Cybersicherheitspolitik herausgebracht, die in Kapitel 3 näher beschrieben wurden: den Nationalen Plan zum Schutz kritischer Infrastrukturen (2005), den Umsetzungsplan KRITIS (2007), die KRITIS-Strategie (2009), die Cyber-Sicherheitsstrategie (2011) und die Digitale Agenda (2014) (vgl. Bundesministerium des Innern 2005; 2007; 2009; 2011; 2014b). Das BMI hat signifikanten Einfluss auf die Gesetzgebung, aber auch auf die Umsetzung des IT-Sicherheitsgesetztes (vgl. Interview 1).

Die Zusammenarbeit mit den Bundesministerien, Bundesämtern und Organisationen wird von Interviewpartner 1 (BMI) generell als gut bewertet. Beispielsweise gibt es im Bereich der Wirtschaftsspionage eine enge Zusammenarbeit mit dem BMWi sowie mit der Allianz für Cyber-Sicherheit (siehe hierzu auch Kapitel 4.1.2) und dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) (siehe hierzu auch Kapitel 4.5.1; vgl. Interview 1). In enger Zusammenarbeit steht das BMI auch mit dem BSI, besonders bei Fragen der Cybersicherheit. Mit allen weiteren ihm untergeordneten Bundesbehörden besteht ebenfalls eine enge Zusammenarbeit (vgl. Interview 1).

Einen Informationsverlust gebe es durch die Aufteilung der Aufgaben im Bereich Cyber Security nicht, da unter anderem eine enge Verzahnung unter den Bundesbehörden durch das nationale Cyber-AZ bestehe; dennoch wird hier eine Verbesserungsmöglichkeit angemerkt (vgl. Interview 1). Interviewpartner 1 (BMI) vertritt die Auffassung, dass die Problematik der Zusammenarbeit und des Informationsverlustes durch die Fragmentierung von Cybersicherheitsaufgaben auf Bundesministerien und Bundesämter nicht aufgrund der Organisation bestehe, sondern abhängig vom Faktor Mensch sei (vgl. Interview 1). Er führt fort, dass insgesamt größere Aufmerksamkeit (Sensibilisierung, Problembewusstsein, „awareness“) notwendig wäre, weshalb sich das BMI beispielsweise für das IT-Sicherheitsgesetz eingesetzt habe (vgl. Interview 1).

Wie Interviewpartner 1 (BMI) angibt, könnten dem BSI zukünftig eventuell noch mehr gesetzliche Aufgaben zugesprochen werden. Die Möglichkeiten zur Umsetzung hängen allerdings von den zur Verfügung stehenden Haushaltsmitteln ab. Von der Wirtschaft wird hingegen erwartet, dass sie Produkte für Cyber Security entwickelt und Hersteller beispielsweise regelmäßig sichere Updates zur Verfügung stellen. Hierfür plant das BMI eine Begleitung der Digitalisierung durch Gesetze und Verordnungen. Denn durch die Digitalisierung entstehen Risiken, welche real eingeschätzt werden müssen. Die Politik fordert und fördert hierzu präventive Maßnahmen (vgl. Interview 1).

4.1.2 Bundesamt für Sicherheit in der Informationstechnik

Das BSI wurde im Jahr 1991 gegründet und gehört zu dem Geschäftsbereich des BMI (vgl. Bundesamt für Sicherheit in der Informationstechnik 2015f). Es ist „eine unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft“ (Bundesamt für Sicherheit in der Informationstechnik 2015f) und für die IT-Sicherheit des Bundes zuständig (vgl. Bundesamt für Sicherheit in der Informationstechnik 2015f; Hange 2015).

Demzufolge ist das BSI mit seinen 600 MitarbeiterInnen die nationale Sicherheitsbehörde für Cyber Security der Bundesrepublik Deutschland (vgl. Bundesamt für Sicherheit in der Informationstechnik 2015f; Hange 2015). Die MitarbeiterInnen sind überwiegend Juristen, Politikwissenschaftler und aus dem technisch-informatischen Bereich. Aufgrund der Aktualität des Themas Cyber Security und dem Fachkräftemangel ist es schwierig, zusätzliche MitarbeiterInnen in diesem Bereich zu finden. Interviewpartner 2 (BSI) argumentiert jedoch, dass dieses einen guten Ruf besitzt und so trotz des geringen Einkommens im Vergleich mit der freien Wirtschaft auf dem Arbeitsmarkt MitarbeiterInnen findet (vgl. Interview 2).

In seinen Zuständigkeiten ist das BSI federführend für das Cyber-AZ zuständig. In diesem Zusammenhang arbeitet es auch mit dem BKA, dem BfV und dem BBK zusammen. Die Zusammenarbeit wird insgesamt als gut bewertet, auch wenn bei fachlichen Fragen immer wieder unterschiedliche Interessen bestehen,

was auf die verschiedenen Faktoren zurückzuführen sei, die bei unterschiedlichen Behörden mitwirken. Generell gebe es aber einen guten Informationsaustausch mit den relevanten Behörden. Das BSI ist auch für die IT-Sicherheit der Bundesverwaltung zuständig, wobei die Zusammenarbeit gut wäre (vgl. Interview 2).

Ein Austausch mit VertreterInnen aus der Wirtschaft findet in Gremien statt, beispielsweise im Rahmen der Allianz für Cybersicherheit oder dem UP KRITIS-Rat (vgl. Interview 2), der mit dem 2014 beschlossenen UP KRITIS gegründet wurde (vgl. Bundesamt für Sicherheit in der Informationstechnik und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2011-2013b; siehe auch Kapitel 3.2). Das BSI initiierte die Allianz für Cyber-Sicherheit, die zusammen mit der BITKOM gegründet wurde. Die Allianz soll für seine Mitglieder zum Wissens- und Erfahrungsaustausch dienen. Mittlerweile hat die Allianz 1283 Institutionen als Mitglieder (vgl. Bundesamt für Sicherheit in der Informationstechnik 2015b). Die Teilnehmer sind sowohl Unternehmen aus der privaten Wirtschaft als auch aus dem öffentlichen Sektor. Jede teilnehmende Institution stellt einen Ansprechpartner (vgl. Bundesamt für Sicherheit in der Informationstechnik 2015a).

Für Unternehmen und BürgerInnen gibt das BSI zahlreiche Empfehlungen, Standards und Lageinformationen heraus. Die Zielgruppen sind 1) der Bund (operativ), 2) die Wirtschaft (kooperativ) und 3) die BürgerInnen (informativ). Die konkreten Aufgaben des BSIs liegen dabei in der Prävention (Täter abwehren), der Detektion (Täter direkt erkennen) und der Reaktion (reagieren und den Schaden begrenzen), wie von Interviewpartner 2 (BSI) angegeben wird (vgl. Interview 2).

Das BSI beriet das BMI beim Entwurf des IT-Sicherheitsgesetzes. Wie Interviewpartner 2 (BSI) angibt, wurden die Vorschläge nicht immer berücksichtigt, da oftmals weitere Faktoren eine Rolle spielten. Mit dem IT-Sicherheitsgesetz wird die Meldepflicht eingeführt (siehe Kapitel 3.5), allerdings erhält das BSI auch schon viele Meldungen über IT-Sicherheitsvorfälle von den Unternehmen, wie der Interviewte bestätigt. Die gemeldeten Fälle deckten jedoch bei weitem nicht die Zahl der Vorfälle ab. Das BSI sei aber in seiner Arbeit auf die Informationen der Unternehmen

angewiesen, um sich ein besseres Täterbild verschaffen zu können und Empfehlungen an die Unternehmen geben zu können. Wie der Befragte angibt, wäre an dieser Stelle eine bessere Zusammenarbeit mit den Unternehmen wünschenswert. Der interviewte Experte vertritt die Auffassung, dass das IT-Sicherheitsgesetz die Grundlagen für eine bessere Zusammenarbeit legt (vgl. Interview 2).

Durch das IT-Sicherheitsgesetz wird das BSI mehr Aufgaben erhalten, welche nur mit mehr Personal zu bewältigen sind, wie Interviewpartner 2 (BSI) angibt. Allerdings sei man sich hier unsicher, ob der gesetzlich vorgesehene Stellenausbau tatsächlich umgesetzt wird (vgl. Interview 2).

Aufgrund seiner Aufgaben führt das BSI mit einer großen Anzahl relevanter Bundesbehörden und Unternehmen eine Zusammenarbeit. Interviewpartner 2 (BSI) vertritt die Auffassung, dass die Zusammenlegung der Aufgaben der unterschiedlichen Bundesbehörden zu einem Ressort im Bereich Cyber Security nicht sinnvoll wäre. Die Bundesbehörden müssten so weit gestärkt werden, dass sie Cyber-Angriffe selbst abwehren könnten. Zur Stärkung der Unternehmen sei schon angedacht worden, dass MitarbeiterInnen des BSI zur Behebung von Sicherheitsvorfällen in die Unternehmen gehen würden. Durch das Vorgehen würde allerdings keine Neutralität mehr gewahrt werden, weshalb der Ansatz nicht weiter verfolgt wurde. Das BSI wünsche sich von den Unternehmen aber neben einer besseren Zusammenarbeit mehr Nachhaltigkeit, die durch Sensibilisierung des Managements geschaffen werden könnte (vgl. Interview 2).

Auf internationaler Ebene unterhält das BSI eine Zusammenarbeit mit dem AA. Des Weiteren ist das Bundesamt in Arbeitsgruppen und Gremien auf EU- und NATO-Ebene (sowie darüber hinaus) vertreten. Der Schwerpunkt der Zusammenarbeit liege aber auf der europäischen Ebene, wie Interviewpartner 2 (BSI) berichtet. Insbesondere mit Frankreich gebe es eine gute Zusammenarbeit, da die zuständige französische Bundesbehörde ähnlich wie das BSI organisiert sei (vgl. Interview 2).

Die Trendbeobachtung und das technische Monitoring des BSIs verzeichnet eine Fortentwicklung der IT-Sicherheit. Auch wenn dies schwer zu treffende Vor-

hersagen wären, sei kein Abschwung des Themas zu beobachten, wie Interviewpartner 2 (BSI) angibt. Somit sei das BSI durch die Geschwindigkeit der technischen Entwicklung und die damit einhergehenden Angriffsweisen der TäterInnen vor neuen Herausforderungen gestellt. Um diesen Herausforderungen begegnen zu können, müsse vermehrt auf automatisierte statt auf traditionelle Kommunikationsstrukturen zurückgegriffen werden und statische Schutzmaßnahmen müssten aufgelöst werden (vgl. Interview 2).

Für die Zukunft plant das BSI, den IT-Grundschutz zu reformieren (vgl. Interview 2). Mit dem IT-Grundschutz stellt das BSI Informationen und Standards zur Verfügung, die eine „Basis für Informationssicherheit" schaffen sollen (vgl. Bundesamt für Sicherheit in der Informationstechnik 2015d). Insbesondere kleinen und mittelständischen Unternehmen sollen hiermit Möglichkeiten mit einer niedrigen Einstiegsschwelle zu einer verbesserten IT-Sicherheit aufgezeigt werden. Aufgrund der schnellen technischen Entwicklungen sei aber eine Überarbeitung des IT-Grundschutzes erforderlich, wie Interviewpartner 2 (BSI) beurteilt. Eine Überarbeitung des IT-Grundschutzes sei allerdings eine große Herausforderung, da dies in Zusammenarbeit mit den Anwendern erfolgen müsste, welche noch verbessert werden sollte. Für die Umsetzung der Überarbeitung, aber auch der anderweitigen Aufgaben des BSI, wären daneben Beiträge aus der Forschung sehr wichtig, da das BSI nicht zur Cybersicherheit forscht (vgl. Interview 2).

4.2 Flankierende Institutionen auf Bundesebene

Neben den erwähnten (Kapitel 4.1) Institutionen nehmen auch weitere Bundesministerien Aufgaben im Bereich Cyber Security wahr (vgl. Bundesministerium des Innern 2015c). Hierzu zählen das BMWi, das sich für die IT-Sicherheit der Unternehmen einsetzt (vgl. Bundesministerium für Wirtschaft und Energie 2015a), das BMVi, das sich beispielsweise im Bereich der Kommunikationswirtschaft und der Breitbandstrategie engagiert (vgl. Bundesministerium für Verkehr und digitale Infrastruktur 2015a), das BMVg mit der obersten Befehls- und Kommandogewalt

über die Bundeswehr (Bundesministerium der Verteidigung 2015a), welche für die militärische Verteidigung von Cyber-Angriffen und für die militärische Cyberverteidigung zuständig ist (vgl. Interview 5), sowie das AA, welches die deutsche Cyber-Außenpolitik auf internationaler Ebene vertritt (vgl. Bundesministerium des Innern 2011, S. 11). Nachfolgend werden diese Institutionen näher analysiert.

4.2.1 Bundesministerium für Wirtschaft und Energie

Beim BMWi fällt Cyber Security in den Aufgabenbereich der Abteilung Digitale-Innovationspolitik VI, mit ihren drei Unterabteilungen und insgesamt 16 Referaten. Mit der IT-Sicherheit in der Wirtschaft beschäftigt sich das Referat VI A5 KT-Sicherheit, Notfallvorsorge, Initiative IT-Sicherheit in der Wirtschaft (vgl. Bundesministerium für Wirtschaft und Energie 2015b). Die Referate haben jeweils ca. 5-7 MitarbeiterInnen, welche über Kompetenzen aus den Bereichen Jura, Technik oder Wirtschaftsinformatik verfügen. Interviewpartner 3 (BMWi) gibt an, dass es wünschenswert wäre, mehr Fachkräfte für den Bereich zu erhalten, wie etwa InformatikerInnen mit einer speziellen Ausbildung in dem Bereich Cyber Security (vgl. Interview 3).

Auf die Gesetzgebung hat auch das BMWi Einfluss. Unter anderem hat es beim Telekommunikationsgesetz federführend mitgewirkt. Hierbei fand unter anderem eine Zusammenarbeit mit der Bundesnetzagentur statt, die zum Geschäftsbereich des BMWi gehört. Die Zusammenarbeit verläuft Interviewpartner 3 (BMWi) zufolge unkompliziert und vertrauensvoll. Das BMWi pflege einen regelmäßigen Austausch mit der Bundesnetzagentur, die über ihre Aufsicht über die Telekommunikationsunternehmen berichtet (vgl. Interview 3). Allerdings fällt hier eine unklare Aufgabenverteilung auf, da mit der Umbenennung des Bundesministeriums für Verkehr und digitale Infrastruktur dieses offiziell die Zuständigkeiten für das Telekommunikationsgesetz erhalten hat. Die Bundesnetzagentur müsste also somit an das Bundesministerium für Verkehr und digitale Infrastruktur berichten und nicht mehr an das Bundesministerium für Wirtschaft und Energie (vgl. Bundesministerium für Verkehr und digitale Infrastruktur 2015a). Eine weitere Zu-

sammenarbeit gibt es mit dem BSI. Diese würde gut funktionieren und die fachlichen Einschätzungen seien hilfreich, wie Interviewpartner 3 (BMWi) beurteilt. Mit dem nationalen Cyber-AZ könne dahingegen die Zusammenarbeit noch verbessert werden (vgl. Interview 3).

Zudem nimmt das BMWi am UP KRITIS-Rat teil, dessen interner Austausch Interviewpartner 3 (BWMi) als gut bewertet. Im UP KRITIS-Rat seien jedoch Sektoren vertreten, mit denen eine bessere Zusammenarbeit nötig wäre. Diese Sektoren hätten einen Nachholbedarf in ihrer IT-Sicherheit. Hierzu gehöre unter anderem eine verbesserte Zusammenarbeit mit Unternehmen der Wasserwirtschaft (vgl. Interview 3).

Um allgemein die Zusammenarbeit zu fördern, insbesondere mit mittelständischen Unternehmen, wurde die Task Force IT-Sicherheit in der Wirtschaft gegründet. Federführend für die Taskforce ist zwar das BMI, die Zuständigkeiten für mittelständische Unternehmen wurden aber dem BMWi zugetragen (vgl. Interview 3). Die Initiative soll dazu beitragen, die IT-Sicherheit in kleinen und mittelständischen Unternehmen zu verbessern (vgl. Bundesministerium für Wirtschaft und Energie 2015a). Dazu setzt sich das BMWi in der Initiative für Sensibilisierungsmaßnahmen ein. Hierzu werden zahlreiche Hilfsangebote, Posterkampagnen und Broschüren zur Verfügung gestellt. In diesem Rahmen gebe es auch eine gute Zusammenarbeit mit den Verbänden BITKOM und Deutschland sicher im Netz e. V., die sehr engagiert seien. Neben der nationalen Zusammenarbeit mit Bundesbehörden sei das BMWi auch auf internationale Ebene in verschiedenen Gremien vertreten (vgl. Interview 3).

Ein Informationsverlust durch die Aufteilung der Aufgaben auf zahlreiche Bundesbehörden wird laut Interviewpartner 3 (BMWi) nicht gesehen. Die Aufgabenaufteilung sei sehr gut, wobei auf die Anliegen der einzelnen Bundesbehörden intensiver als bisher eingegangen werden könnte, überwiegend in Prozessen, bei denen eine Lösung gefunden werden muss. Hier ist ein Widerspruch erkennbar, da zunächst die Aufgabenteilung als sehr gut beschrieben wird, dann aber doch einige

Kritikpunkte geäußert werden. Als ein Nachteil der Fragmentierung wird aber dennoch die Zersplitterung der Aufgaben genannt, die einen Überblick über die Zuständigkeiten erschwert. Andererseits heißt es aber auch, dass die vielfach verschiedenen Interessen der Bundesbehörden letztlich zu mehr Lösungsansätzen führen würden, die umgekehrt auch als positiv erachtet werden könnten (vgl. Interview 3). Hier lassen sich Argumente für und gegen eine Fragmentierung der Aufgaben im Bereich Cyber Security erkennen.

Für die Zukunft sind laut Interviewpartner 3 (BMWi) die vorgesehenen Maßnahmen zur Verbesserung der Zusammenarbeit bei der Umsetzung des IT-Sicherheitsgesetzes dringend erforderlich. Darüber hinaus plant das BMWi, mittelständische Unternehmen weiter zu unterstützen und im Dialog mit der Wirtschaft notwendige Maßnahmen festzulegen (vgl. Interview 3).

4.2.2 Bundesministerium für Verkehr und digitale Infrastruktur

Das BMVi ging infolge einer Umstrukturierung im Dezember 2013 aus dem Bundesministerium für Verkehr, Bau und Stadtentwicklung hervor (vgl. Bundesministerium für Verkehr und digitale Infrastruktur 2015a). Das BMVi beschäftigt insgesamt 1300 MitarbeiterInnen und ist in neun Abteilungen aufgeteilt. Hinzu kommen insgesamt 63 nachgeordnete Behörden (vgl. Bundesministerium für Verkehr und digitale Infrastruktur 2015b). Cyber Security wird im BMVi der Abteilung Digitale Gesellschaft zugeordnet. Hierunter befinden sich zwei Unterabteilungen: DG 1 Digitale Gesellschaft und Infrastruktur und DG 2 IKT im Verkehrsbereich. Der ersten Unterabteilung sind sechs Referate, der zweiten acht untergeordnet. Jedes Referat hat 10-12 MitarbeiterInnen. Überwiegend werden aber Aufgaben zur Cyber Security von den Referaten DG 20 IT-Strategie und IT-Steuerung des Ressorts, Dienstleistungszentrum-IT und DG 21 Betrieb der Informationstechnik (IT-Betrieb) wahrgenommen. Darüber hinaus ist speziell für die Cyber Security in der Logistik das Referat DG 25 Nationale/internationale zivile Notfallvorsorge, Gefahrenabwehr, Krisenmanagement, Lagezentrum zuständig. Die MitarbeiterInnen in

den genannten Referaten sind GeografInnen, InformatikerInnen, JuristInnen sowie aus technischen Berufen (vgl. Interview 4).

Mit der Umbenennung des BMVi erfolgte auch eine Umgestaltung der Aufgabengebiete, sodass nun auch Kommunikationswirtschaft und der Ausbau der digitalen Infrastruktur (Breitbandstrategie) hierzu zählen (vgl. Bundesministerium für Verkehr und digitale Infrastruktur 2015a). Daneben bestehen bisherige Aufgaben weiter, unter anderem in der Gesetzgebung im Bereich Verkehr und Logistik, im Ausbau des Schienen- und Straßenverkehrs. Um den neuen und bisherigen Aufgaben gerecht werden zu können, sei ein größeres Budget notwendig, da anderenfalls der Schienen- und Straßenverkehrsausbau bei einem Ausbau der digitalen Infrastruktur vernachlässigt werden könnte (vgl. Interview 4). Mit dem Ausbau der digitalen Infrastruktur soll bis 2018 eine flächendeckende Versorgung mit mindestens 50 Mbit/s realisiert werden (vgl. Bundesministerium für Verkehr und digitale Infrastruktur 2015d). Dieses Vorhaben geht auch aus der Digitalen Agenda hervor (vgl. Die Bundesregierung 2014b, S. 13; siehe hierzu auch Kapitel 3.4).

Die Zusammenarbeit mit anderen Bundesbehörden bei der Cyber Security ist auch für das BMVi essenziell. Diese wird von Interviewpartner 4 (BMVi) mit dem BMI und dem BSI gut bewertet, obwohl es eine bessere Zusammenarbeit mit dem Cyber-AZ geben müsse (vgl. Interview 4). Interviewpartner 4 (BMVi) vertritt die Auffassung, dass durch Änderungen der föderalen Struktur eine bessere Zusammenarbeit mit allen Bundesbehörden und dem Cyber-AZ zu erzielen wäre. Dadurch verringerte sich auch der Informationsverlust. Folglich wäre eine Zentralisierung der Aufgaben auf Bundesebene förderlich, mit der eine schnellere und vernünftige Dienstleistung erbracht werden könnte. Hieraus würde sich auch eine bessere Zusammenarbeit mit den Bundesländern und Kommunen ergeben (vgl. Interview 4).

Das BMVi arbeitet überwiegend mit Unternehmen aus der Logistikbranche zusammen. Dazu beschäftigt sich das Referat DG 25 im Bereich Cyber Security insbesondere mit den *kritischen Dienstleistungen*. Hierbei besteht in der Logistik die

Herausforderung, dass die Branche der kritischen Dienstleister aus vielen kleinen Unternehmen besteht. Eine weitere Problematik sei nach Interviewpartner 4 (BMVi) die unklare Definition von Kritischen Infrastrukturen im Bereich Transport und Logistik (vgl. Interview 4), wie schon in Kapitel 3.2 erwähnt.

Das BMVi erstellte im Oktober 2014 im Auftrag der Bundesregierung eine Sicherheitsstrategie für die Güter- verkehrs- und Logistikwirtschaft für den „Schutz kritischer Infrastrukturen und verkehrsträgerübergreifende Gefahrenabwehr" (Bundesministerium für Verkehr und digitale Infrastruktur, 2014). Diese Strategie soll vorbeugend wirken gegen „[...] schwerwiegende Unterbrechungen der Güterversorgung durch externe Einwirkungen und damit verbundene mögliche volkswirtschaftliche Schäden" (Bundesministerium für Verkehr und digitale Infrastruktur 2014, S. 2). Die Strategie ist so angelegt, dass sie keine harten Maßnahmen beinhaltet, sondern stattdessen auf Sensibilisierung setzt und Unternehmen Handlungsempfehlungen gibt, die die „[...] Wettbewerbsfähigkeit des Industrie-, Wirtschafts- und Logistikstandort Deutschlands [...]" sichern (Bundesministerium für Verkehr und digitale Infrastruktur 2014, S. 2). Zunächst sei aber in der Zusammenarbeit mit den Unternehmen nach Interviewpartner 4 (BMVi) erforderlich, dass diese Vorfälle melden und darüber hinaus präventive Maßnahmen ergreifen. Hierzu seien aber eine Sensibilisierung und Maßnahmen auf freiwilliger Basis notwendig (vgl. Interview 4). Dies steht im Kontrast zum IT-Sicherheitsgesetz und der Aussage des Interviewpartners 1 (BMI), der eine gesetzliche Vorschrift für notwendig hält, um letztlich die Zusammenarbeit mit den Unternehmen zu erzwingen (vgl. Interview 1).

Zum Schutz der Logistikunternehmen wird von Interviewpartner 4 (BMVi) angegeben, dass dezentrale Strukturen, wie in der Logistik vorzufinden, besser als zentrale, wie jene im Energiesektor, geschützt werden können. Wird jedoch ein kleines Unternehmen angegriffen, sind immer nur Teilbereiche der Kritischen Infrastrukturen betroffen. Dennoch bestehe durch einen schlechteren Schutz vor Cyber-Angriffen ein Nachteil für die kleinen Logistikunternehmen. Dieser sei in der Fi-

nanzierung der Sicherheitsmaßnahmen begründet, die für kleine Unternehmen kaum möglich seien (vgl. Interview 4). Für die Zukunft seien mehr Forschung und Entwicklung erstrebenswert, so Interviewpartner 4 (BMVi). Um die Systeme und Netze besser schützen zu können, seien weitere Investitionen notwendig. Des Weiteren seien zentrale Strukturen auch zukünftig für den Schutz der Kritischen Infrastrukturen erforderlich (vgl. Interview 4).

4.2.3 Bundesministerium der Verteidigung

Das BMVg ist in der Bundesrepublik Deutschland für die militärische Verteidigung zuständig, mit „[...]den Schwerpunkten Planung und Militärpolitik, der Obersten Kommandobehörde, der Obersten Dienstbehörde für die Bundeswehrverwaltung einschließlich des Rüstungsbereichs mit den Schwerpunkten Administration sowie Bedarfsdeckung für die Streitkräfte“ (Bundesministerium der Verteidigung 2015a). In dem Bereich Cyber Security nehmen 6-7 Referate Aufgaben wahr. In den anderen Referaten sind Beauftragte nebenamtlich mit für die Cybersicherheit relevanten Aufgaben beauftragt. Künftig ist in der internen Organisation im Bereich Cyber Security noch eine Verbesserung geplant (vgl. Interview 5). Insgesamt nehmen 20 MitarbeiterInnen aus dem BMVg Aufgaben zu Cyber Security wahr. Die MitarbeiterInnen verfügen über ein Studium in den Bereichen Technik (zum Teil mit dem Schwerpunkt Nachrichten- und Elektrotechnik), Wirtschaftswissenschaften und Politikwissenschaften. Laut Interviewpartner 5 (BMVg) ist es schwierig, MitarbeiterInnen mit den nötigen Kompetenzen in Cyber Security zu finden, sei es im technischen Bereich oder in den Sozialwissenschaften. Entsprechende MitarbeiterInnen werden jedoch dringend benötigt. Die bessere Bezahlung in der Wirtschaft für entsprechende Kompetenzen sei ein Grund hierfür. Ein weiteres Problem sei, dass die sogenannten *Klischee-Hacker* nicht in das System der Bundeswehr passen würden. Eine Anpassung an die Organisationsstrukturen wäre für entsprechende MitarbeiterInnen oft schwer (vgl. Interview 5).

Das BMVg verfüge laut Interviewpartner 5 (BMVg) im Bereich Cyber Security über ein großes Netzwerk mit anderen Bundesbehörden. Es sei eine zentrale An-

laufstelle und koordiniere Aufgaben mit anderen Bundesbehörden. So vertritt der Interviewte die Auffassung, dass die drei wichtigsten *Player* im Bereich Cyber Security aus dem BMI mit der gesamthaften staatlichen Führung, dem AA mit dem Schwerpunkt auf internationale Kooperationen mit anderen Staaten und dem BMVg mit Zuständigkeiten in der Verteidigung von Cyber-Angriffen, bestehen würden (vgl. Interview 5). Die Aussage, dass dem BMI die gesamthafte Verantwortung für Cyber Security obliegt, sollte infrage gestellt werden, da es z. B. keine Zuständigkeiten im Fall der Verteidigung von Cyber-Angriffen besitzt. Dennoch gibt es eine sehr enge Zusammenarbeit der drei Bundesministerien. Die Zusammenarbeit ist aus Sicht von Interviewpartner 5 (BMVg) intensiv und gut. Hingegen gebe es beispielsweise mit dem Cyber-AZ des BSIs keine gute Zusammenarbeit, was an deren vielfältigen Aufgaben begründet liege (siehe hierzu auch das Kapitel 4.3.1) und dem Personalmangel, um diesen nachkommen zu können. Hierzu macht der interviewte Experte den Vorschlag, eine ähnliche Institution nur mit zivilen MitarbeiterInnen zu gründen (vgl. Interview 5).

Für den Bereich Cyber Security ist auch die Deutsche Bundeswehr eine wichtige Institution, welche in den letzten Jahren in der nichtmilitärischen Informations- und Kommunikationstechnik eine Modernisierung erfahren hat. Hierzu wurde 2006 die BWI Informationstechnik GmbH gegründet, welche die Aufgaben im Rahmen des *Herkules- Projektes* übernommen hat (vgl. BWI Informationstechnik GmbH 2015b). Auf dieses Projekt wird in Kapitel 4.4.5 näher eingegangen.

Von Interviewpartner 5 (BMVg) wird die Zusammenarbeit mit der BWI Informationstechnik als gut bewertet (vgl. Interview 5), jedoch lässt das Interview vermuten, dass es auch Unstimmigkeiten in der Zusammenarbeit geben mag. Auf internationaler Ebene besteht eine Zusammenarbeit des BMVgs insbesondere auf militärischer Ebene mit der NATO und dem NATO Cooperative Cyber Defence Centre of Excellence (vgl. Interview 5), dies wird näher in Kapitel 4.5.3 beschrieben. Mit der EU arbeitet das BMVg im zivilen Bereich vorwiegend in der gemeinsamen Außen- und Sicherheitspolitik zusammen. Darüber hinaus arbeitet das BMVg auch

mit der European Defence Agency zusammen (vgl. Interview 5). In Kapitel 4.5.2 wird hierauf näher eingegangen.

Interviewpartner 5 (BMVg) sieht die gesamtstaatliche Verantwortung für Cyber Security beim BMI besser aufgehoben als beim BMVg (vgl. Interview 5). In den USA ist, wie bereits in Kapitel 3 erwähnt, Cyber Security überwiegend im militärischen Bereich angesiedelt (vgl. Bendiek und Ulmer 2013, S. 1-2). In Deutschland wird das Bedrohungspotenzial von Cyber-Angriffen für die Wirtschaft und Forschung als größer betrachtet als für das Militär. Im Fall eines Cyber-Angriffes sei das BMVg zuständig, wenn der Angreifer klar erkannt wurde. Bis der Angreifer festgestellt werden kann, dauert es aufgrund der Anonymität im Cyberspace oftmals einige Zeit. Die Ermittlung der Straftat obliegt dem BKA. Das BMVg würde erst im Verteidigungsfall mit einem Attributions-Nachweis eingreifen, also nicht ohne die Identifizierung des Täters und einem politischen Mandat (vgl. Interview 5).

Im Vergleich mit anderen Bundesministerien unterscheidet sich das BMVg besonders durch den Aufgabenbereich der Verteidigung von Cyber-Angriffen und der Cyberverteidigung. Mit der Verteidigung von Cyber-Angriffen ist hier die Verteidigung mit jeglichen militärischen Mitteln gemeint. Die Cyberverteidigung bedeutet hingegen, wenn das Militär zur Verteidigung digitale Mittel einsetzt, sei es zur Verteidigung von Cyber-Angriffen oder anderen Angriffen.

Für die Zukunft gibt Interviewpartner 5 (BMVg) an, dass beim BMVg noch Handlungsbedarf im Bereich Cyber Security besteht. Es bestehe ferner die Notwendigkeit, sich mit dem Cyberterrorismus intensiver auseinanderzusetzen und die Kompetenzen auf diesem Gebiet zu steigern (vgl. Interview 5). Insofern kann davon ausgegangen werden, dass Cyberterrorismus eine große Bedrohung für Deutschland darstellt, das BMVg zur Bekämpfung dieser Bedrohung aber noch vor großen Herausforderungen steht. Daraus lässt sich schließen, dass Deutschland gegenwärtig keinen ausreichenden Schutz vor Cyberterrorismus aufweist.

4.2.4 Auswärtiges Amt

Für die in der Cyber-Sicherheitsstrategie festgelegte Cyber-Außenpolitik der Bundesrepublik Deutschland hat das AA die Federführung innerhalb der Bundesregierung, das deutsche Interessen auf internationaler Ebene vertritt. Insbesondere sollen deutsche Interessen „[...] in internationalen Organisation wie den Vereinten Nationen, der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE), dem Europarat, der Organisation for Economic Co-operation and Development (OECD) und der NATO[...]“ vertreten werden (vgl. Bundesministerium des Innern 2011, S. 11). Das AA übernimmt diese Aufgaben auf institutioneller Ebene mit dem hierfür eingerichteten Koordinierungsstab für Cyber-Außenpolitik (vgl. Auswärtiges Amt 2015a). Gegründet wurde der Koordinierungsstab 2011 (vgl. Auswärtiges Amt 2015b), im gleichen Jahr wie die Herausgabe der deutschen Cyber-Sicherheitsstrategie (vgl. Bundesministerium des Innern 2011). Der Koordinierungsstab umfasst ca. 30 MitarbeiterInnen, die zum Großteil jedoch hauptsächlich mit anderen Aufgaben befasst sind. Hinzu kommen MitarbeiterInnen an bilateralen Vertretungen im Ausland und in den ständigen Vertretungen Deutschlands bei internationalen Organisationen wie EU, NATO und OSZE. Ein Kern von acht Personen führt das Tagesgeschäft. Die MitarbeiterInnen haben größtenteils eine Ausbildung im Höheren oder Gehobenen Dienst und ein Studium in den Politikwissenschaften, den Rechtswissenschaften oder der Volkswirtschaftslehre. Sie verfügen über gute Kompetenzen, dennoch werden auch ExpertInnen als Zeit- oder Fachkräfte zu bestimmten Themen hinzugezogen. Neben den MitarbeiterInnen im Koordinierungsstab gibt es weitere, die Aufgaben im Bereich der NATO, der europäischen Außen- und Sicherheitspolitik oder in der Abrüstung, aber auch speziell in der Cyber Security übernehmen (vgl. Interview 6).

Von August 2013 bis Juli 2014 gab es einen Sonderbeauftragten für Cyber-Außenpolitik, dessen Aufgaben für Cyber Security sich aus der Koordination der Cyber-Außenpolitik des AA ergeben haben. Denn das Thema Cyber Security kann „[...] nicht auf nationaler Ebene geregelt werden, sondern nur in internationaler Zu-

sammenarbeit“ (vgl. Auswärtiges Amt 2015b). Diese Aufgaben hat zwischenzeitlich im Rahmen einer umfassenden Reform des Auswärtigen Dienstes der Beauftragte für die Vereinten Nationen, Cyber-Außenpolitik und Terrorismusbekämpfung übernommen (vgl. Interview 6).

Das AA verfolgt einen dreifachen Ansatz, der das, was im Inland bereits geschaffen wurde, nach außen exportiert: erstens soll die Resilienz von Netzen und IT-Einrichtungen gestärkt werden, zweitens sollen eine internationale Stabilisierung verfolgt und bestimmte internationale Regeln für das Staatenverhalten vereinbart werden und drittens sollen mithilfe von formellen wie informellen Kontaktstrukturen sicherheits- und vertrauensbildende Maßnahmen geschaffen werden. Die größte Herausforderung besteht der Ansicht eines interviewten Vertreters des AAs (Interviewpartner 6 (AA)) nach darin, dass der Ursprung von Zwischenfällen im Cyberraum häufig nicht eindeutig zu erkennen sei. Daher seien sicherheits- und vertrauensbildende Maßnahmen notwendig: Bei einem auf Schaden ausgerichteten Cyber-Angriff können Staaten, mit denen eine gute Beziehung unterhalten wird, weitestgehend als Täter ausgeschlossen werden bzw. von diesen Staaten ist keine Störung oder Zerstörung von IT-Systemen zu erwarten. Folglich kann mit vielen guten diplomatischen Beziehungen der Gefahr der unkontrollierten Eskalation innerhalb von IT-Systemen nach einem Cyber-Angriff vorgebeugt werden (vgl. Interview 6). Mit einer unkontrollierten Eskalation ist hier gemeint, dass die Herkunft und die Ursache des Cyber-Angriffes nicht ermittelt werden können: etwaige Gegenmaßnahmen – sowohl im Netz als auch politischer oder sogar militärischer Art – könnten sich gegen den Falschen richten, was dann wiederum Gegenmaßnahmen dieser bislang unbeteiligten Seite hervorrufen könne. Es bestehe die Gefahr einer Eskalationsspirale.

Eine Zusammenarbeit findet vorwiegend mit dem BMI und dem BMVg sowie teilweise auch mit dem Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung statt. Das BSI unterstützt bei Bedarf vermittels des BMI und stellt dem AA gegebenenfalls auch Fachinformationen zur Verfügung (vgl. Interview 6).

In der Zusammenarbeit mit anderen Bundesministerien und Bundesämtern bewertet Interviewpartner 6 (AA) die Abstimmung untereinander gut (vgl. Interview 6), wobei hier die nicht strukturelle informelle Zusammenarbeit betont wird. Die Zusammenarbeit besteht überwiegend aus Ressortabstimmungen (vgl. Interview 6). Im Umkehrschluss kann dies als Andeutung interpretiert werden, dass die formelle Zusammenarbeit weniger gut funktioniert.

Auf EU-Ebene ist Cyber Security sehr vielschichtig mit einer Vielzahl an Gremien organisiert. So besteht eine Zusammenarbeit in vielen verschiedenen Gremien, in denen die Bundesregierung vertreten ist. Cyber- Sicherheitspolitik in EU, UN, OSZE und NATO wird vor allem in der informellen Gruppe Friends oft the Presidency on Cyber verfolgt, die das AA zusammen mit dem BMI wahrnimmt. Daneben gibt es weitere, stärker wirtschaftlich ausgerichtete Arbeitsgremien, wie z. B. eine EU-Ratsarbeitsgruppe Telekom (vgl. Interview 6). Der Aussage von Interviewpartner 6 (AA) zufolge erschwert die Vielzahl der EU-Gremien Entscheidungsprozesse. Eine Zusammenlegung könne sinnvoll sein (vgl. Interview 6).

Im Bereich der Wirtschaft arbeitet das AA unter anderem mit den deutschen Außenhandelskammern zusammen. Gemeinsam mit diesen unterstützt das AA die Unternehmen etwa im Kampf gegen die elektronische Wirtschaftsspionage. Hierzu müssten allerdings seitens der Unternehmen belastbare Hinweise vorgelegt werden; eine Unterstützung erfolge in Absprache mit den Unternehmen. Meist würde in vertraulichen Gesprächen nach Einzelfalllösungen gesucht, wie Interviewpartner 6 (AA) angibt (vgl. Interview 6).

Die Aufteilung der Aufgaben im Bereich Cyber Security auf verschiedene Bundesministerien und Bundesämter wird von Interviewpartner 6 (AA) nicht unbedingt negativ bewertet, da jedes Ressort eigene Schwerpunkte habe und Cyberbedrohungen vielfältig seien. Bei nur einem Ressort bestehe das Risiko, dass etwas übersehen werde. Die gegenwärtige Aufteilung erfordere aber eine Koordinierung und bei Meinungsverschiedenheiten fehle eine Instanz, die letztlich eine Entscheidung fällt. Ein Vorteil der föderalen Strukturen bestehe dahingegen in der Auftei-

lung der Aufgaben auf mehrere federführende Institutionen, die bei Sicherheitsvorfällen eine schnelle Reaktion ermöglichen. Ein Nachteil sei, dass bei Entscheidungsfindungen etwas übersehen werden könnte, da die einzelnen federführenden Institutionen nicht den gesamten Bereich betrachten können, sondern nur ihr Fachgebiet überblicken, allerdings wurden bislang hieraus resultierende Unstimmigkeiten schnell wieder eingefangen (vgl. Interview 6).

Für die Zukunft würden mehr SpezialistInnen im Bereich Cyber Security benötigt werden, wie Interviewpartner 6 (AA) angibt. Zudem müsse zu Cyber Security mehr Wissen geschaffen werden und für die Kritischen Infrastrukturen werden auch vom AA bestimmte Vorgaben als wichtig empfunden. Das AA wird künftig weiterhin auf sichere Netze im Cyberraum achten, um Cyber-Angriffen vorzubeugen. Hierzu stärkt es die diplomatischen Beziehungen zu den Drittländern (vgl. Interview 6).

4.3 Koordinierende Institutionen

Im Folgenden sollen die koordinierenden Institutionen, das nationale Cyber-AZ und der nationale Cyber-SR, erörtert werden. Das nationale Cyber-AZ koordiniert die Zusammenarbeit der Bundesministerien und Bundesämter untereinander und mit den Unternehmen (siehe hierzu Kapitel 4.3.1). Der nationale Cyber-SR wirkt koordinierend in der strategischen Planung von Cyber Security innerhalb der Bundesregierung und mit der Wirtschaft (siehe hierzu Kapitel 4.3.2). Anders als das Cyber-AZ arbeitet es auf strategischer Ebene und nicht operativ.

4.3.1 Nationales Cyber-Abwehrzentrum

Die Gründung des nationalen Cyber-AZs wurde mit der Cyber-Sicherheitsstrategie beschlossen und die Federführung an das BSI übertragen (vgl. Bundesministerium des Innern 2011, S. 8). Das Cyber-AZ ist im BSI dem Referat B 24 Internationale Beziehungen, Zusammenarbeit mit den Sicherheitsbehörden, Nationales Cyber-AZ zugeordnet (vgl. Bundesamt für Sicherheit in der Informationstechnik 2015f).

Neben dem BSI arbeitet das Cyber-AZ mit dem BfV und dem BBK zusammen. Die Aufgaben sind gesetzlich und in Kooperationsvereinbarungen festgelegt. Auch das BKA, die Bundespolizei, das Zollkriminalamt, der BND und die Bundeswehr bzw. das BMVg arbeiten mit dem Cyber-AZ zusammen (vgl. Bundesministerium des Innern 2011, S. 8; Interview 5). Darüber hinaus besteht eine Zusammenarbeit noch mit weiteren Bundesbehörden, welche die Betreiber Kritischer Infrastrukturen beaufsichtigen (vgl. Bundesministerium des Innern 2011, S. 8).

Das Cyber-AZ soll zur „[...] Optimierung der operativen Zusammenarbeit aller staatlichen Stellen und zur besseren Koordinierung von Schutz- und Abwehrmaßnahmen gegen IT-Vorfälle [...]“ (Bundesministerium des Innern 2011, S. 8) beitragen. Auf operativer Ebene bedeutet dies, „[...] IT-Vorfälle zu analysieren und abgestimmte Handlungsempfehlungen zu geben“ (Bundesministerium des Innern 2011, S. 8), wobei die Interessen der Wirtschaft berücksichtigt und Maßnahmenvorschläge der Bundesbehörden an die Unternehmen weitergeleitet werden sollen. Außerdem müssen dem nationalen Cyber-SR Empfehlungen gegeben und im Fall einer zu erwartenden Krise eine Meldung direkt an das BMI weitergeleitet werden (vgl. Bundesministerium des Innern 2011, S. 8-9). Demnach übernimmt das Cyber-AZ koordinierende Aufgaben zwischen den Bundesbehörden und der Wirtschaft. Zusammenfassend ist das Cyber-AZ eine *Informationsdrehscheibe* für die Bundesbehörden (vgl. Bundesministerium des Innern 2015f).

Hieran wird in der Wissenschaft Kritik geäußert. Diese bezieht sich auf die Zusammenarbeit im nationalen Cyber-AZ, da der BND, das BfV und das BKA dem deutschen Trennungsgebot unterliegen, aber im Cyber-AZ zusammen vertreten sind. „Aus Gründen der Rechtssicherheit soll die Arbeit von Polizei und Nachrichtendiensten in Deutschland organisatorisch, personell und informationell getrennt bleiben“ (Berger 2013, S. 232). Aufgrund der zusammenfließenden Informationen im Cyber-AZ wird dies nicht eingehalten. Es findet hier also ein Informationsaustausch der Bundesbehörden statt, die eigentlich dem Trennungsgebot unterliegen. Die Problematik besteht dann darin, dass die Erkenntnisse aus dem Cyber-AZ

durch Kooperationen des BSIs bis auf die europäische Ebene zur Europäischen Kommission weiterfließen können, die an strafverfolgenden Maßnahmen beteiligt sein kann. Da auch das BKA und der BND Informationen an europäische Sicherheitsbehörden weiterleiten, kann dies beispielsweise geschehen, indem das BSI an die ENISA berichtet, das BKA an EUROPOL und der BND an das Intelligence Analysis Centre. Somit entsteht ein Informationszusammenfluss auf europäischer Ebene. ENISA, EUROPOL und Intelligence Analysis Centre berichten wiederum an die Europäische Kommission und spätestens dann werden die Informationen nicht mehr getrennt behandelt. Kritisch daran ist letztlich, dass die Europäische Kommission an operativen und strafverfolgenden Maßnahmen beteiligt sein kann und hier ein Informationsfluss entstehen könnte, der auf gesetzlicher Ebene untersagt sein kann (vgl. Berger 2013, S. 323).

VertreterInnen aus der Politik gehen auf diese Thematik nicht ein. Interviewpartner 2 (BSI) bezeichnet die Zusammenarbeit mit den mitwirkenden Bundesbehörden im Cyber-AZ insgesamt als gut, wobei immer wieder fachliche Fragen aufkommen würden, bei denen es zu Meinungsverschiedenheiten kommen könne (vgl. Interview 2). Von den mitwirkenden Bundesbehörden im Cyber-AZ könnte unter anderem das BMWi seine Zusammenarbeit verbessern, wie Interviewpartner 2 (BSI) berichtet (vgl. Interview 2). Ein interviewter Vertreter aus dem BBK (Interviewpartner 8 (BBK)) kritisiert das Cyber-AZ nicht direkt, würde sich aber eine koordinierende Stelle wünschen, an der sich alle, die Aufgaben im Bereich Cyber Security wahrnehmen, wenden können. Diese Möglichkeit biete das Cyber-AZ nicht (vgl. Interview 8). So sei beispielsweise das AA am Cyber-AZ nicht beteiligt, für das es somit nur eine nachrangige Bedeutung hätte (vgl. Interview 6). VertreterInnen aus der Wirtschaft kritisieren unter anderem, dass Unternehmen und insbesondere Betreiber Kritischer Infrastrukturen nicht im Cyber-AZ vertreten sind (vgl. Interview 10).

Im Juni 2014 erhielt das Cyber-AZ auch in den Medien viel Kritik. Diese entstand durch einen Bericht des Bundesrechnungshofes, der den Nutzen des Cyber-

AZ infrage stellte. Kritisiert wird unter anderem, dass das Cyber-AZ Cyber-Angriffe nicht abwehrt, sondern lediglich strategische Handlungsempfehlungen mit dem BSI auf politischer Ebene herausgibt (vgl. Goetz und Leyendecker 2014). Die MitarbeiterInnen, die von den einzelnen Bundesbehörden dem Cyber-AZ gestellt werden, würden zudem nicht regelmäßig an den vorgesehenen Sitzungen teilnehmen (vgl. Biermann 2014). Vom Cyber-AZ wurde daraufhin eingeräumt, dass es in seiner Organisation und Arbeitsweise verbessert werden könnte (vgl. Goetz und Leyendecker 2014).

4.3.2 Nationaler Cyber-Sicherheitsrat

Die Aufgabe des Cyber-SR ist es, „[...] die Zusammenarbeit innerhalb der Bundesregierung sowie zwischen Staat und Wirtschaft unter Verantwortung der Beauftragten der Bundesregierung für Informationstechnik sichtbarer [zu] organisieren [...]“ (Bundesministerium des Innern 2011, S. 9). Daraus lässt sich schließen, dass die Zusammenarbeit bisher nicht optimal organisiert ist. Der nationale Cyber-SR wurde, wie auch das Cyber-AZ, auf der Grundlage der Cyber-Sicherheitsstrategie gegründet. Der Cyber-SR koordiniert die Zusammenarbeit und die strategische Planung von Cyber Security innerhalb der Bundesregierung und mit der Wirtschaft. Dementsprechend sind in dem Cyber-SR das Bundeskanzleramt, das AA, das BMI, das BMVg, das BMWi, das Bundesministerium der Justiz, das Bundesministerium der Finanzen und das Bundesministerium für Bildung und Forschung, aber auch die einzelnen Bundesländer vertreten. Die Mitwirkung von weiteren Ressorts kann je nach Notwendigkeit vom Cyber-SR eingefordert werden und anders als im Cyber-AZ können VertreterInnen aus der Wirtschaft hinzugezogen werden (vgl. Bundesministerium des Innern 2011, S. 9). Derzeit sind diese (u. a.) assoziierte WirtschaftsvertreterInnen des BDIs, BITKOM und der Deutschen Industrie- und Handelskammer (DIHK), der Übertragungsnetzbetreiber Amprion (vgl. Bundesministerium des Innern 2015a) und die Deutsche Telekom AG (vgl. Interview 10).

Der Cyber-SR tagt dreimal im Jahr unter dem Vorsitz der Beauftragten der Bundesregierung für die Informationstechnik, Frau Staatssekretärin Rogall-Grothe. Bei dringenden Anlässen kann auch außerplanmäßig getagt werden (vgl. Bundesministerium des Innern 2015a). So wurde beispielsweise im Juli 2013 eine Sondersitzung einberufen – aus dem Anlass „der öffentlichen Diskussion um die Überwachungsprogramme PRISM und Tempora“ (Bundesministerium des Innern 2015h). In dieser Zeit begannen nach den Enthüllungen von Edward Snowden die Berichterstattungen über die NSA-Affäre in den Medien (vgl. Spiegel Online 2013b).

Der Cyber-SR soll als „wichtiger Baustein“ der deutschen Cyber-Sicherheitsstrategie die Zusammenarbeit in der Bundesregierung sowie zwischen Politik und Wirtschaft verbessern (Bundesministerium des Innern 2015a). Während dabei ein politisch-strategischer Ansatz verfolgt wird, ist hingegen die Arbeit des Cyber-AZs eher operativ (vgl. Bundesministerium des Innern 2011, S. 9). Insofern werden im Cyber-SR „die präventiven Instrumente und die zwischen Staat und Wirtschaft übergreifenden Politikansätze für Cyber-Sicherheit koordiniert“ (Bundesministerium des Innern 2011, S. 9). Der Fokus lag bislang bei den Kritischen Infrastrukturen und der Cyber-Außenpolitik (vgl. Bundesministerium des Innern 2015a).

Interviewpartner 4 (BMVi) kritisiert, dass der Cyber-SR nur als Austauschgremium zwischen Verwaltung und Verbänden dient, aber wenig konkrete Maßnahmen unternimmt (vgl. Interview 4). Interviewpartner 6 (AA) berichtet hingegen positiv über den Cyber-SR und dass die Zusammenarbeit gut funktioniere (vgl. Interview 6). Interviewpartner 1 (BMI) zufolge erfülle der Cyber-SR zwar seine gesetzlichen Aufgaben, für die Zukunft könne jedoch darüber nachgedacht werden, ob der Cyber-SR noch weiterentwickelt werde (vgl. Interview 1).

4.4 Exekutierende Institutionen

Zu den exekutierenden Institutionen zählen hier die nachgeordneten Bundesbehörden der Bundesministerien, welche aufgrund ihrer Aufgaben im Bereich Cyber

Security für diese Arbeit relevant sind. Hierzu gehören die Bundesämter aus dem Geschäftsbereich des BMIs, das BBK, das BKA und das BfV (vgl. Bundesministerium des Innern 2015e). Hinzu kommen der BND, der seinen Auftrag von der Bundesregierung erhält (vgl. Bundesnachrichtendienst 2015b), sowie die Deutsche Bundeswehr, deren Befehls- und Kommandogewalt über die Streitkräfte im Frieden beim BMVg liegen (vgl. Bundesministerium der Verteidigung 2015a).

4.4.1 Bundeskriminalamt

Das BKA ist für die innere Sicherheit in Deutschland und somit auch für die Bekämpfung von Cyberkriminalität und für andere internetbasierte Deliktformen zuständig (vgl. Bundes-kriminalamt 2015b). Zur Durchführung dieser Aufgaben ist es „[...] die wichtigste und personell wie technisch am besten ausgestattete Polizeibehörde in der Bundesrepublik [...]“ (Kullik 2014, S. 140).

Insgesamt gibt es neun Abteilungen, wobei die Abteilung SO Schwere und Organisierte Kriminalität für die Bekämpfung von Cyberkriminalität zuständig ist. Das Thema Cyberkriminalität ist dort der Gruppe SO mit fünf Referaten (SO 41 bis SO 45) zugeordnet. Diese bestehen aus einem Referat zur Lage und Analyse von Cyberkriminalität, einem Referat für die Auswertung und Ermittlungsunterstützung und drei Referaten zur Ermittlung (vgl. Bundeskriminalamt 2015d). Das Personal in diesen Referaten wurde mit dem Anstieg der Cyberkriminalität in den letzten Jahren aufgestockt.

Das BKA beschäftigt über 5500 MitarbeiterInnen. Die Hälfte der MitarbeiterInnen sind KriminalbeamtInnen, die andere Hälfte besteht aus MitarbeiterInnen aus über 70 verschiedenen Berufsfeldern (vgl. Bundeskriminalamt 2015c). In den Referaten zur Bekämpfung von Cyberkriminalität arbeiten mittlerweile 100-120 MitarbeiterInnen. Von den KriminalbeamtInnen sind acht InformatikerInnen, alle weiteren haben ein Bachelor-Studium, sind Diplom-VerwaltungswirtInnen oder RechtswissenschaftlerInnen.

Ein interviewter Vertreter aus dem BKA (Interviewpartner 7 (BKA)) bestätigt, dass die Anzahl der Beschäftigten InformatikerInnen gering sei. Das BKA habe

aber Schwierigkeiten auf dem Arbeitsmarkt InformatikerInnen zu finden, denn die Besoldung und das Entgelt seien im öffentlichen Dienst wesentlich geringer als in der freien Wirtschaft. So sei es auch nicht möglich, InformatikerInnen mit einem Masterabschluss zu finden (vgl. Interview 7). Diese Aussage lässt sich kritisieren, da letztlich die Ursache für den Fachkräftemangel im BKA auf die Wirtschaft geschoben wird, mit ihrer besseren Bezahlung für InformatikerInnen. Hieran kann auch festgestellt werden, dass für die Sicherheit und Strafverfolgung von Cyberkriminalität zu wenig Geld ausgegeben wird.

Das BKA hat die Aufgabe, Cyberkriminalität zu reduzieren und somit die Sicherheitslage für die Wirtschaft und die BürgerInnen zu verbessern. Um dieser Aufgabe nachzukommen, ist die Strategie des BKAs die TäterInnen zu ermitteln und auch präventiv durch Repression vorzugehen. Dabei verfolgt das BKA drei Aufgaben: 1) Die Operative Auswertung von Cyberkriminalität, hierzu gehören die frühzeitige Erkennung von Cyber-Delikten und deren Auswertung zur Einleitung von Ermittlungsverfahren, 2) Internetrecherche in Datennetzen durch die Zentralstelle für anlassunabhängige Recherchen und 3) Einleitung und Durchführung von Ermittlungsverfahren (vgl. Interview 7).

Übergeordnet werden im Grundsatz des BKAs die Erlasse aus den Bundesministerien umgesetzt. Daneben finden Politikberatung und die Analyse von Straftaten statt, wozu unter anderem die Verfolgung elektronischer Spuren gehört. Insbesondere bei der Verfolgung von elektronischen Spuren zur Ermittlung von Straftaten und ihrer TäterInnen sei es nützlich, wenn auf gespeicherte Daten zurückgegriffen werden kann (vgl. Interview 7).

Ein weiterer Aufgabenbereich ist die Bekämpfung von Kinderpornografie. Die Ermittlung erfolgt überwiegend durch Internetrecherchen (vgl. Interview 7). Hierzu beschäftigt das BKA private Dienstleister aus dem IT-Sektor (vgl. Neue Osnabrücker Zeitung 2014). An dieser Stelle kann davon ausgegangen werden, dass private Dienstleister auch mit anderen Ermittlungsarbeiten beauftragt werden, da intern lediglich acht InformatikerInnen zur Verfügung stehen.

Neben den genannten Aufgaben bringt das BKA jährlich ein Bundeslagebericht zur Cyberkriminalität heraus (vgl. Bundeskriminalamt 2013) und hat sich auch beim IT-Sicherheitsgesetz mit Vorschlägen zur Erweiterung des Gesetzes des BKAs eingebracht (vgl. Interview 7). Die Zuständigkeiten des BKAs in der Strafverfolgung wurden mitunter um Datenausspähung und Computerbetrug erweitert (vgl. Deutscher Bundestag 2015c).

Bei der Erstellung der Cyber-Sicherheitsstrategie hat sich das BKA ebenfalls eingebracht. Es erstellte bereits 2009 eine Informations- und Kommunikationsstrategie und forderte eine nationale Cyber-Sicherheitsstrategie. In der heutigen Cyber-Sicherheitsstrategie, die erst 2011 verabschiedet wurde, sind Teile aus der Informations- und Kommunikationsstrategie des BKAs enthalten. Laut Interviewpartner 7 (BKA) sei die schnelle Verabschiedung dieser Strategie dem Bekanntwerden des Stuxnet-Angriffs geschuldet (vgl. Interview 7), der somit die Bundesregierung unter Druck gesetzt hat, sich stärker für Cyber Security einzusetzen und sichtbar Maßnahmen zu ergreifen, da der Angriff auch intensiv in den Medien diskutiert wurde. Stuxnet ist ein Computerwurm von bislang einmaliger Komplexität des Codes und des Angriffsziels, mit dem mutmaßlich amerikanische und/oder israelische Nachrichtendienste ein iranisches Atomkraftwerk angriffen, indem die Steuerung von Uranzentrifugen überdreht und Letztere dadurch zerstört wurden (vgl. Hansel 2012, S. 565). Der Vorfall hat international das Bewusstsein geschaffen, dass derartige Cyber-Angriffe möglich sind.

Wie Interviewpartner 7 (BKA) berichtet, findet auf nationaler Ebene mit den Landeskriminalämtern ein regelmäßiger und vertrauensvoller Austausch statt. Die Landeskriminalämter hätten aber eine heterogene Aufstellung in den Bundesländern, wodurch ein starkes Gefälle entstehe. Dies hat zur Folge, dass die großen Bundesländer, wie Niedersachsen, Bayern, Nordrhein-Westfalen und Baden-Württemberg, besser aufgestellt sind. Nicht so gut aufgestellt sind Stadtstaaten, wie z. B. Bremen, und kleinere Bundesländer, wie Saarland und Mecklenburg. Daher kann es anlassbezogen zu einem Zusammenschluss der Landeskriminalämter

kommen. Darüber hinaus ist das BKA zur Bekämpfung von Cyberkriminalität technisch besser ausgestattet als die Landeskriminalämter. So unterstützt es die Landeskriminalämter unter anderem in der Telekommunikationsüberwachung, der Datensammlung und der Forensik. Auch hierbei sei die Vorratsdatenspeicherung eine überaus wichtige Methode, um elektronische Spuren zur Ermittlung von Straftaten zurückverfolgen zu können (vgl. Interview 7). Derzeit wird die Vorratsdatenspeicherung anlässlich eines geplanten Gesetzes hierzu in der Politik und in den Medien viel diskutiert. Kritiker, wie der Bund Deutscher Kriminalbeamter, ein Vertreter aus dem deutschen Richterbund e.V. und ein Kriminalbeamter aus dem Bereich Organisierte Kriminalität sehen hierin keinen positiven Beitrag zur Strafverfolgung (vgl. Diehl 2015). Hätte es diesen Straftatbestand schon vor eineinhalb Jahren gegeben, so Peter Schaar (2015), „dann wären viele Berichte über die NSA-Affäre strafbar gewesen“ (Schaar 2015).

Neben weiteren deutschen Bundesministerien und Bundesbehörden arbeitet das BKA mit dem BMI und dem BSI zusammen. Die Zusammenarbeit mit der Fachaufsicht im BMI konnte in letzter Zeit verbessert werden. Mit dem BSI habe sich die Zusammenarbeit ebenfalls verbessert, so finde laut Interviewpartner 7 (BKA) fast täglich ein Austausch statt. Die Zusammenarbeit ist wichtig; so stelle das BKA den Anspruch an das BSI, über Cyber-Angriffe informiert zu werden. In den Erwartungen, die an sie gerichtet werden, würden sich die Bundesämter aber zum Teil unterscheiden. An das BSI würden größere Erwartungen gestellt als an das BKA (vgl. Interview 7).

Jede Bundesbehörde kämpfe um Ressourcen und habe ihre speziellen Aufgaben, mit denen sie sich von den anderen abgrenze, so Interviewpartner 7 (BKA). So unterscheidet sich das BKA bspw. vom Verfassungsschutz, indem es dem Legalitätsprinzip unterliegt. Somit ist die Aufgabe des BKAs die TäterInnen festzunehmen, während der Verfassungsschutz in dem Fall nur eine beratende Funktion einnehmen kann (vgl. Interview 7). Hieran wird jedoch deutlich, wie wichtig eine Zu-

sammenarbeit der Bundesbehörden zur erfolgreichen Bekämpfung von Cyberkriminalität ist.

Im Bereich der Kritischen Infrastrukturen arbeitet das BKA nur fallbezogen mit Betreibern zusammen, wie z. B. mit der Deutschen Telekom AG. Ansonsten gebe es aufgrund des Personalmangels keine regelmäßige Zusammenarbeit, wie Interviewpartner 7 (BKA) angibt. So gibt es auch keine BKA-Vertretung im UP KRITIS-Rat, sondern nur VerbindungsbeamtInnen im Cyber-AZ. Auf internationaler Ebene gibt es eine fallbezogene Zusammenarbeit mit Unternehmen, beispielsweise mit Facebook oder Google, deren Hauptsitz sich in den USA befindet (vgl. Interview 7).

Das BKA gründete einen Public Private Partnership, bei dem es mit Unternehmen aus dem Banksektor zusammenarbeitet. Hierüber erhofft das BKA sich einen Austausch mit den Unternehmen zu täglichen Bedrohungen, Sicherheitsmaßnahmen und taktisch wichtigen Informationen (vgl. Zierke 2013, S. 7). Dazu sollen den Unternehmen kompetente AnsprechpartnerInnen für einen persönlichen Austausch zur Verfügung gestellt und ein Grundverständnis für Cyber Security geschaffen werden. In dieser Zusammenarbeit soll auch der Austausch zwischen den Unternehmen gefördert werden (vgl. Interview 7).

Mittlerweile haben drei Banken aus dem Public Private Partnership den Verein „German Competence Center Against Cyber Crime“ gegründet. Unterstützt wird der Verein vom BKA und dem BSI (vgl. German Competence Center against Cyber Crime e. V. 2015).

Auf internationaler Ebene gibt es ebenfalls eine stark ausgeprägte Zusammenarbeit. Demzufolge nimmt das BKA beispielsweise bei der Kriminalitätsbekämpfung eine koordinierende Stellung ein. Dementsprechend fließen im BKA im Bereich Cyberkriminalität alle Informationen und Nachrichten sowohl aus dem In- und Ausland zusammen. Folglich ist das BKA für INTERPOL, EUROPOL und das Schengener Informationssystem die nationale Zentralstelle (vgl. Bundeskriminalamt 2015a).

Das BKA ist also weltweit vernetzt, denn „[...] für die weltumspannende Zusammenarbeit hat das Bundeskriminalamt einen gesetzlichen Auftrag, denn Staatsgrenzen dürfen den Kampf gegen Verbrecher nicht entscheidend behindern“ (Bundeskriminalamt 2015a). Zu diesem Zweck unterhält das BKA weltweit Kontakte zu VerbindungsbeamtInnen, woraus ein 60 Staaten überspannendes Netzwerk resultiert – mit einer schnellen Datensicherung und einer Rufbereitschaft, die wenn es notwendig ist, anlassbezogen genutzt werden kann. Bei zeitkritischen Vorfällen, die eine Datenerhebung erfordern, ermöglicht das weltweite Kontaktnetzwerk eine schnelle Reaktion (vgl. Interview 7).

Innerhalb Europas gebe es insbesondere eine gute Zusammenarbeit mit Großbritannien, Frankreich, Niederlande und der Ukraine, so Interviewpartner 7 (BKA). Mit den anderen europäischen Mitgliedsländern wird anlassbezogen zusammengearbeitet. Darüber hinaus besteht eine Zusammenarbeit mit EUROPOL, die sich verbessert habe, auch durch das eigens dafür eingerichtete Cyber Crime Center (siehe hierzu auch Kapitel 4.5.2). Außerhalb der europäischen Ebene nimmt die Zusammenarbeit mit INTERPOL im „Interpol global complex for information“ zu. Die Zusammenarbeit mit EUROPOL und INTERPOL wird positiv bewertet (vgl. Interview 7).

Darüber hinaus pflegt das BKA einen intensiven Austausch mit den USA und mit China. Mit den USA arbeitet das BKA über das FBI und dem Secret Service zusammen, die beide für Cyber Crime Delikte zuständig sind. Der Secret Service ist für den Schutz des Präsidenten, aber auch primär für Geldwäsche zuständig, die bei elektronischen Zahlungen als Cyberkriminalität zu betrachten ist. Für die gute Zusammenarbeit gibt es beim BKA sowohl beim FBI als auch beim Secret Service VerbindungsbeamtInnen (vgl. Interview 7).

China hat aus polizeilicher Sicht ähnliche Cyberkriminalität-Vorfälle zu verzeichnen wie Deutschland und auch eine gute Serverinfrastruktur, wie Interviewpartner 7 (BKA) berichtet. Jedoch sei die Todesstrafe in China für die Zusammenarbeit ein Problem. Denn bei schweren Delikten wird in China die Todesstrafe

verhängt. Hierzu zählen Cyber-Angriffe, wie das Ausspähen von Daten, insbesondere wenn es sich beim Angriffsziel um eine chinesische Behörde handelt. Für das BKA stelle sich insofern das Problem, dass bereits ein Informationsaustausch mit den chinesischen Behörden über Cyber-Angriffe für den Täter die Todesstrafe zur Folge haben kann. Denn wenn die chinesischen Behörden daraufhin herausfinden, dass der Täter auch chinesische Behörden angegriffen hat, kann dies die Todesstrafe für den Täter zur Folge haben. In diesem Fall darf eine deutsche Behörde nicht mitwirken (vgl. Interview 7). Das bedeutet für das BKA, dass die Strafverfolgung bei Cyber-Angriffen aus China erschwert ist. Das sollte kritisch betrachtet werden, da somit von China Cyber-Angriffe z. B. in Form von Wirtschaftsspionage durchgeführt werden können, ohne dass Konsequenzen einer Strafverfolgung befürchtet werden müssen. Cyber-Spionage, wie sie durch die chinesische Regierung in Auftrag gegeben wird (vgl. Fade 2014), kann hierdurch leicht geheim gehalten werden. Die Zusammenarbeit mit Russland ist hingegen aufgrund der aktuellen politischen Spannungen vollständig zum Erliegen gekommen. Allerdings befinden sich viele TäterInnen in Russland, wie Interviewpartner 7 (BKA) bestätigt (vgl. Interview 7).

Damit das BKA seinen Aufgaben besser nachkommen kann, wäre Interviewpartner 7 (BKA) zufolge, eine adäquate personelle Ausstattung nötig, sowie eine bessere IT- und Toolausstattung. Der Personalausbau, der im IT-Sicherheitsgesetz vorgesehen ist, sei nötig, da neben einer Erhöhung der IT-Sicherheit in Deutschland auch die TäterInnen im Rahmen der Strafverfolgung ermittelt werden müssten. Denn dem BKA fehle es an IT-SicherheitsexpertInnen und der Polizei an speziell ausgebildetem Personal. Mittlerweile weisen viele Delikte eine Überschneidung mit Cyberkriminalität auf, weshalb auf polizeilicher Ebene eine Fortbildung der BeamtInnen notwendig sei (vgl. Interview 7).

Das *Dunkelfeld* mit Fällen von Cyberkriminalität wächst stetig und die Professionalität, mit der Angriffe durchgeführt werden, nimmt zu. Hierdurch entstehe eine immer größere Erwartungshaltung an das BKA, die Quantität und die Qualität dieser Vorfälle zu analysieren, wie Interviewpartner 7 (BKA) berichtet. Dies kann

nur geschehen, wenn zwischen Wirtschaft und dem BKA mehr Transparenz über die Angriffe hergestellt werde. Eine vertrauensvolle Zusammenarbeit mit den Unternehmen sei auch im Hinblick auf das Legalitätsprinzip erforderlich (vgl. Interview 7).

Für die Zukunft plant das BKA, ein ganzheitliches Lagebild auf der EU-Ebene zu schaffen und die Effizienz des operativen Vorgehens gegen Cyberkriminalität zu steigern (vgl. Interview 7). Hierzu wurde beispielsweise vor vier Jahren der EU Policy Cycle – EMPACT mit EUROPOL beschlossen (vgl. EUROPOL 2015b). Das BKA plane in Zukunft, sich weiterhin fachlich qualitativ hochwertig in die Verbesserung der Cyber Security einzubringen, laut Interviewpartner 7 (BKA). Dazu sei eine Reihe von Tätigkeiten geplant, wie Einladungen herauszugeben, Vorträge zu halten oder sich für Hospitationen im Ausland und in der Aus- und Fortbildung einzusetzen (vgl. Interview 7).

4.4.2 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

Das BBK ist unter anderem für die Koordinierung des Schutzes kritischer Infrastrukturen zuständig und nimmt somit Aufgaben im Bereich der Cyber Security wahr. Es ist dabei dem BMI unterstellt (vgl. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2015a). Die Zuständigkeiten liegen beim Referat II.3 Strategie KRITIS, Cyber-Sicherheit KRITIS das zur Abteilung II Risikomanagement, Internationale Angelegenheiten gehört (vgl. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2014).

Für das BBK ist es schwer, geeignete MitarbeiterInnen zu finden, die eine hohe Affinität zur Cyber Security haben mit Kenntnissen im Bevölkerungsschutz und Katastrophenhilfe. Die MitarbeiterInnen bräuchten keine SystemanalytikerInnen oder KryptologInnen zu sein, es würden auch GeisteswissenschaftlerInnen und GeografInnen beschäftigt, wie von Interviewpartner 8 (BBK) mitgeteilt wird. Die Akquise geeigneter MitarbeiterInnen sei erschwert durch die attraktiveren und besser vergüteten Arbeitsplätze in der freien Wirtschaft (vgl. Interview 8).

In seinen Aufgaben versucht das BBK sich laut Interviewpartner 8 (BBK) vom BSI abzugrenzen und strategisch folgenorientiert und auswirkungsbezogen vorzugehen. Dazu wird unter anderem analysiert, was infolge von Cyber-Vorfällen geschieht oder geschehen könnte und wie die bedrohten Leistungen der Kritischen Infrastrukturen geschützt werden können. Daraufhin werden Empfehlungen an Betreiber Kritischer Infrastrukturen ausgesprochen. Hierbei weist das BBK auf die Probleme und Angriffsmöglichkeiten hin, die mit der Digitalisierung zunehmen. Auch für die Bundesverwaltung analysiert das BBK Möglichkeiten zur Senkung der potenziellen Verwundbarkeit. Hierunter fällt auch die Erarbeitung von Notfallplänen, die sich beispielsweise mit Szenarien beschäftigen, wie die Funktionsfähigkeit des Bundestages bei einer Störung erhalten werden kann (vgl. Interview 8). Diese Möglichkeiten bestehen noch nicht; denn bei dem Cyber-Angriff auf den Bundestag (siehe auch Kapitel 1.) war seine Arbeitsfähigkeit beeinträchtigt. So waren Abgeordnete beispielsweise durch das abgeschaltete Intranet zeitweise fast arbeitsunfähig und fühlten sich darüber hinaus über das weitere Vorgehen schlecht informiert (vgl. Wendt 2015). Hieraus lässt sich schließen, dass es für das BBK in diesem Bereich noch Handlungsbedarf gibt.

Eine Zusammenarbeit auf Behördenebene besteht mit dem BSI und dem BMI. Auf den Entwurf des IT-Sicherheitsgesetzes des BMI konnte das BBK durch Vorschläge Einfluss nehmen, die auch zum Teil aufgegriffen wurden. Ferner besteht eine Zusammenarbeit mit VertreterInnen der Sicherheitsbehörden durch das Cyber-AZ, dem IT-Planungsrat Bund und Länder und dem UP-KRITIS. Mit dem BSI bestehe seit elf Jahren eine gute Zusammenarbeit, insbesondere mit dem Referat C 22. Dennoch könne es vorkommen, dass Informationen verloren gehen, obgleich dies selten geschehe. Darüber hinaus habe sich mit dem Cyber-AZ der Informationsaustausch gut entwickelt (vgl. Interview 8).

Mit dem BMWi sei die Zusammenarbeit laut Interviewpartner 3 (BMWi) eher schwierig. Dieses versuche vorrangig, die Wirtschaft zu fördern, wobei Cyber Security ein Störfaktor sein könne (vgl. Interview 8). Als Störfaktor könnten hier die

Kosten gemeint sein, die für Cyber Security bei den Unternehmen entstehen würden. Langfristig betrachtet ist aber davon auszugehen, dass Unternehmen durch Wirtschaftsspionage oder Cyberkriminalität weiterhin hohe Schäden erleiden werden, wenn sie sich nicht schützen.

Das BBK nimmt am UP KRITIS-Rat teil, dadurch entsteht eine intensive Zusammenarbeit mit BranchenvertreterInnen der Kritischen Infrastrukturen. Interviewpartner 8 (BBK) bewertet die Zusammenarbeit mit Betreibern Kritischer Infrastrukturen, die neu hinzukommen, anfangs als schwierig. Mit Unternehmen, die bereits länger dem UP KRITIS-Rat angehören, wäre die Zusammenarbeit hingegen gut, wenn auch nicht konfliktfrei. Ein Vertrauensverhältnis, das sich über längere Zeit aufbaut, verbessere diese Zusammenarbeit, wobei die informelle Zusammenarbeit immer gut sei. Mit dem IT-Sicherheitsgesetz würde sich das BBK eine bessere Zusammenarbeit erhoffen, besonders mit den Branchen Ernährung, Wasser, Medizin, Transport und Verkehr. Für eine bessere Zusammenarbeit würde das BBK auch MitarbeiterInnen in die Unternehmen schicken, um die Prozesse besser zu verstehen (vgl. Interview 8).

Das BBK führt keine Zusammenarbeit auf europäischer oder internationaler Ebene, sondern beobachtet Auswirkungen auf den Zivilschutz passiv. Lediglich mit der Schweiz und mit Österreich gibt es eine direkte Kooperation, die aber nicht gestaltend ist (vgl. Interview 8).

Cyber Security betrifft noch viele weitere Fachbereiche, als die bisher genannten Bundesbehörden, mit denen das BBK zusammenarbeitet, so Interviewpartner 8 (BBK). Es wäre also eine koordinierende Stelle in Deutschland wünschenswert, in der sich alle politischen Institutionen und Unternehmen zusammenfinden würden, die Aufgaben im Bereich Cyber Security wahrnehmen. Das könnte im Rahmen eines institutionellen Arbeitskreises umgesetzt werden. Dadurch könnte auch der Informationsaustausch noch verbessert werden, um zu erfahren, was die anderen Bundesbehörden oder Unternehmen für ihre Arbeit benötigen würden. Im UP KRITIS-Rat würde sich eine solche Richtung bereits erkennen lassen. So entstehe

durch eine nicht ausreichende Zusammenarbeit hin und wieder auch ein Informationsverlust (vgl. Interview 8).

Im Allgemeinen wird von Interviewpartner 8 (BBK) das Bewusstsein für IT-Sicherheit in den Bundesbehörden als nicht ausreichend bewertet. So würden viele Bundesbehörden, die beispielsweise keine Sicherheitsbehörden sind, nicht erkennen, dass in ihrem Fachbereich Cyber Security eine wichtige Rolle einnimmt. Hier wird beispielsweise das Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit genannt, bei dem es gedauert hätte bis Cyber Security eine größere Bedeutung erhalten hat. Folglich müssten die Bundesressorts für die Thematik noch mehr sensibilisiert werden. Diese Ressorts würden im IT-Sicherheitsgesetz adressiert. Doch auch wenn die Aufgaben bereits auf die entsprechenden Bundesressorts gut verteilt sind, würden sie oftmals hin und her geschoben werden. Bei der klaren Aufteilung der Aufgaben müsse es noch eine Verbesserung geben. In der Aufgabenverteilung hätte man auch die Zuteilung der Aufgaben für digitale Infrastrukturen im BBK nicht beim Bundesministerium für Verkehr – jetzt auch für digitale Infrastruktur – erwartet, sondern beim Bundesministerium für Wirtschaft und Energie (vgl. Interview 8).

Für die Zukunft ist das „[...] Ziel des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe [...] ein proaktives Risikomanagement, um die Funktionsfähigkeit von Infrastrukturen zu erhalten." (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2015b). Hierfür bräuchte es laut Interviewpartner 8 (BBK) noch einen besseren Informationsaustausch, eine bessere Sensibilisierung sowohl in der Politik als auch in der Wirtschaft und eine digitale Zurückhaltung Deutschlands. Letztere adressiert die schnelle digitale Entwicklung. Umso schneller die Digitalisierung voranschreiten werde, desto größer sei die Verwundbarkeit der Systeme und damit des Staates, der Wirtschaft und der Gesellschaft. Mit mehr Resilienz könne dennoch dem Ziel, digitales Wachstumsland Nr. 1 in Europa zu werden, entgegen gesehen werden (vgl. Interview 8).

Auf die Probleme der schnellen digitalen Entwicklung weist das BBK hin, wie beispielsweise auf die dadurch entstandenen neuen Angriffsformen auf Staaten. Laut Interviewpartner 8 (BBK), sei die wissenschaftliche Erforschung der neuen internationalen Bedrohungsarten und deren Auswirkungen auf die Bevölkerung erst am Anfang. Die zukünftige Aufgabe für das BBK bestehe in der Analyse der Bedeutung von Cyber Security für den Bevölkerungsschutz. Für den Bereich Cyber Security müsse im Bevölkerungsschutz aber erst noch eine Strategie entwickelt werden (vgl. Interview 8). Das bedeutet, dass derzeit in Deutschland keine ausreichenden Kompetenzen und Strategien im Bereich Bevölkerungsschutz vor Cyber-Angriffen und deren Folgen vorhanden sind, die bei einer Katastrophe eine entsprechende Reaktion ermöglichen würden.

4.4.3 Bundesamt für Verfassungsschutz

Das BfV ist neben dem BND und dem MAD eines von drei Nachrichtendiensten in Deutschland. Der Verfassungsschutz ist als Inlandsnachrichtendienst tätig, dessen Federführung beim BMI liegt (vgl. Bundesamt für Verfassungsschutz 2015e).

Der Verfassungsschutz wird von den 16 Landesverfassungsschutzämtern in seinen Aufgaben unterstützt (vgl. Bundesverfassungsschutzgesetz vom 20. Dezember 1990 BGBl. I S. 2954, 1990). Er sammelt und wertet Informationen über Vorgänge aus, welche für die freiheitliche demokratische Grundordnung der Bundesrepublik eine Bedrohung darstellen könnte. Zu den Aufgaben des Verfassungsschutzes gehören auch die Bekämpfungen von Spionage- und Sabotagebedrohungen. Hierzu werden auch nachrichtendienstliche Mittel eingesetzt (vgl. Bundesamt für Verfassungsschutz 2015d).

In der Organisationsstruktur des BfV gibt es sechs Abteilungen, die dem Präsidenten und Vizepräsidenten unterstellt sind (vgl. Bundesamt für Verfassungsschutz 2015a). Die Abteilung 6 beschäftigt sich mit „Spionageabwehr, Geheim-, Sabotage- und Wirtschaftsschutz“ (Bundesamt für Verfassungsschutz 2015a). Ein weiterer Aufgabenbereich des BfVs ist die Bekämpfung von Terrorismus. Aufgrund der Bedrohungslage wurde dieser Aufgabenbereich in den letzten

Jahren ausgebaut und dabei mit der Abteilung Rechtsextremismus zusammengelegt. Durch die Zusammenlegung konnten diese Abteilungen Investitionen in moderne Kommunikationsmittel erhalten. Der Personalbestand wird flexibel angepasst (vgl. Bundesamt für Verfassungsschutz 2015a).

Von der Bundesregierung wurde Anfang 2015 im Hinblick auf die Zusammenarbeit mit den Landesverfassungsschutzämtern eine Gesetzesänderung verabschiedet. Demnach soll im Bereich der Bekämpfung des Extremismus der Verfassungsschutz eine zentralere Stellung einnehmen und die Informationen von den Landesämtern besser zusammenfassen (vgl. Schultz 2015). Hierbei wird deutlich, dass die Koordination der Landesämter und der Informationsfluss als verbesserungsfähig bewertet werden. Neu ist hierbei, dass die Behörden fusionieren dürfen, insofern könnten mehrere Bundesländer eine gemeinsame Behörde unterhalten (vgl. Schultz 2015).

Insbesondere im Bereich der Bekämpfung des Islamismus haben die Aufgaben des BfVs zugenommen. Hierzu gehört neben der Observation auch die Überwachung mithilfe des Internets, in Chats, E-Mails und sozialen Netzwerken (vgl. Flade 2014). Ferner beobachtet das Bundesamt die Cyber-Kriegsführung der Islamisten. So wurde der Cyber-Angriff auf den französischen TV-Sender TV5 Monde vom BfV als eine Form von Cyber-Krieg definiert (vgl. Severin 2015). Mit diesen zunehmenden und neuen Aufgaben im Bereich Cyberterrorismus ist ein Personalmangel entstanden (vgl. Flade 2014), der mit dem IT-Sicherheitsgesetz durch einen Stellenausbau auch im BfV behoben werden soll (vgl. Deutscher Bundestag 2015c).

Eine weitere besondere Herausforderung für den Verfassungsschutz ist die Abwehr der Spionageangriffe ausländischer Nachrichtendienste. Hierunter fällt auch der Bereich der Proliferation, wozu das BfV die Wirtschaft mit Aufklärungsarbeit sensibilisiert. Unter Proliferation wird die Verhinderung der Verbreitung von Massenvernichtungswaffen oder Ressourcen jeglicher Art zu deren Herstellung verstanden (vgl. Bundesamt für Verfassungsschutz 2015e).

Der Sabotageschutz ist insbesondere wichtig, da Terroranschläge mithilfe von Cyber-Sabotage durchgeführt werden könnten. Das BfV legt beim Sabotageschutz einen Schwerpunkt auf die Kritischen Infrastrukturen. Dabei stehen die Energieversorgung und die Telekommunikation sowie die Funktionsfähigkeit der Einrichtungen der Bundeswehr im Vordergrund (vgl. Bundesamt für Verfassungsschutz 2015c). Hierzu arbeitet das BfV unter anderem mit dem Cyber-AZ zusammen (vgl. Bundesamt für Verfassungsschutz 2015b).

Die Aufgaben des BfVs im Wirtschaftsschutz stehen in Zusammenhang mit Spionage durch ausländische Nachrichtendienste und Extremisten mit politischen Zielen. Das BfV verfolgt hierbei das Motto *Prävention durch Information* und leistet Aufklärungsarbeit für Unternehmen. Außerdem sieht sich das BfV als ein kompetenter und vertrauenswürdiger Ansprechpartner für Unternehmen im Bereich Wirtschaftsspionage (vgl. Bundesamt für Verfassungsschutz 2015f). Das BfV erklärt aber auch: „Grundsätzlich unterliegen Unternehmenssicherheit und Know-how-Schutz der Eigenverantwortlichkeit der Wirtschaft“ (Bundesamt für Verfassungsschutz 2015f). Dies schließt den Schutz vor Spionage durch ausländische Nachrichtendienste zunächst mit ein.

Auf seiner Internetseite erklärt das BfV, dass in letzter Zeit intensiv Angriffe auf Bundesbehörden und die Wirtschaft unternommen wurden (vgl. Bundesamt für Verfassungsschutz 2015b). Im Mai 2015 war, wie bereits in Kapitel 1.1 erwähnt, ein schwerer Angriff auf den Bundestag zu verzeichnen, bei dem die gesamte technische Infrastruktur des Bundestages betroffen war (vgl. Biermann 2015). Bei den zum Zeitpunkt der Erstellung dieser Arbeit laufenden Untersuchungen wird davon ausgegangen, dass der Spionageangriff von einem ausländischen Nachrichtendienst ausging. Das BfV ist für die Spionageabwehr verantwortlich, wie der Innenminister Thomas De Maizière erklärte. Da die gesetzliche Verantwortung bei dem BfV liegt, sprach er dem Bundestag die Hilfe des BfVs zu (vgl. sueddeutsche.de 2015).

Neben dem Personalmangel ist der BfV auch technisch mangelhaft ausgestattet, sodass eine Kooperation mit ausgewählten fremden Nachrichtendiensten

erfolgt. So berichtete *Spiegel Online* bereits 2013, zu Beginn der medial Aufsehen erregenden NSA-Affäre, über die Zusammenarbeit des Bundesamtes mit der NSA. Diese stellte dem BfV eine Spionagesoftware namens XKEYSCORE zur Verfügung. Während der BND die Installation der Software übernahm, ging der BfV im Gegenzug der NSA gegenüber eine sehr weitgehende Verpflichtung zur Informationsweitergabe ein: „To the maximum extent possible share all data relevant to NSA's mission" (Zeit Online 2015c). Die enge Zusammenarbeit zwischen der NSA und den deutschen Nachrichtendiensten besteht allerdings seit längerem und ist auch seit längerem bekannt (vgl. Pfister et al. 2013).

4.4.4 Bundesnachrichtendienst

Der BND ist der einzige deutsche Geheimdienst mit Zuständigkeiten im Bereich der wirtschaftlichen, politischen und militärischen Auslandsaufklärung. Den Auftrag dazu erhält er von der Bundesregierung (vgl. Bundesnachrichtendienst 2015b). Die Abteilung TA im BND ist speziell für „[...] die Informationsgewinnung mit technischen Mitteln [...]" zuständig, womit sie auch Aufgaben im Kampf gegen Cyber Bedrohungen und im Bereich der Cyber-Abwehr wahrnimmt (vgl. Bundesnachrichtendienst 2015a). Insgesamt hat der BND 6500 Mitarbeiter im In- und Ausland (vgl. Bundesnachrichtendienst 2015a). Hiervon hat sich die Anzahl der militärischen MitarbeiterInnen in den letzten Jahren von ca. 280 auf ca. 860 erhöht (vgl. Daun 2011, S. 183).

Als Dienstleister ist der BND gesetzlich dazu verpflichtet, die Bundesregierung, Ressorts und die Bundeswehr mit zuverlässigen Informationen zu allen politisch und gesellschaftlich relevanten Themen zu versorgen. Über Bedrohungen aus dem In- oder Ausland muss der BND die entsprechenden Ressorts informieren. Darüber hinaus unterstützt der BND die Regierung bei Entscheidungen in der Außen- und Sicherheitspolitik und die Bundeswehr bei ihren Auslandseinsätzen. Der BND bereitet aber nur Informationen auf und dient dabei nicht als operativer Geheimdienst auf militärischer Basis (vgl. Bundesnachrichtendienst 2015c).

„Im Rahmen der Cyber-Sicherheit sollen zum einen die Gefahren für und Angriffe auf deutsche Netzwerke und Computer rechtzeitig erkannt werden, aber auch Regeln zur Verhinderung von erfolgreichen Angriffen erarbeitet werden." (Bundesnachrichtendienst 2015d). Um diese Aufgaben zu erfüllen, arbeitet der BND auf nationaler und internationaler Ebene mit Sicherheitsbehörden zusammen. Dazu hat er die spezielle Befugnis und auch die „[...] technischen Möglichkeiten zur strategischen Erfassung internationaler Datenverkehre" (Bundesnachrichtendienst 2015d). Im Bereich Cyber-Sabotage legt auch der BND einen Fokus auf den Schutz Kritischer Infrastrukturen. Durch die Informationen des BNDs an die entsprechenden Ressorts können diese geeignete Abwehrmaßnahmen einleiten (vgl. Bundesnachrichtendienst 2015d).

Mit der Deutschen Telekom AG besteht eine Zusammenarbeit auf Basis des BND- und des Telekommunikationsgesetzes (§§ 110 ff. TKG). Die Gesetze verpflichten die Unternehmen der Telekommunikationsbranche unter bestimmten Voraussetzungen dazu, Auskünfte an die Bundesnachrichtendienste zu geben oder Überwachungsmaßnahmen zu ermöglichen (vgl. Deutsche Telekom AG 2015b). Die Zusammenarbeit mit anderen Sicherheitsbehörden und deutschen Nachrichtendiensten wird koordiniert vom Staatssekretär im Bundeskanzleramt, dem die Aufgabe des Beauftragten für die Nachrichtendienste des Bundes obliegt (vgl. Bundesnachrichtendienst 2015f). Wöchentlich gibt es eine Lagebesprechung im Bundeskanzleramt, an der die Präsidenten der Nachrichtendienste und des BKAs teilnehmen, sowie die zuständigen Staatssekretäre aus dem AA, dem BMI, dem BMVg, dem Bundesministerium der Justiz und der Leiter der Stabsabteilung II des Führungsstabes der Streitkräfte. Anlassbezogen nehmen auch der Generalbundesanwalt und VertreterInnen aus der Abteilung VI des Kanzleramtes teil. Zudem nehmen aus den Bundesministerien die ReferatsleiterInnen teil, welche mit den Tagesordnungspunkten befasst sind (vgl. Daun 2011, S. 177).

Der BND muss sich in seiner Zusammenarbeit mit der Polizei an das Trennungsgebot halten (siehe hierzu auch Kapitel 4.3.1). Erst wenn der BND einen kon-

kreten Verdacht auf eine Straftat hat, darf er die Strafverfolgungsbehörden einschalten (vgl. Berger 2013, S. 319). Bezüglich seiner Aufgaben arbeitet der BND aber anlassbezogen mit vielen weiteren Behörden aus dem In- und Ausland zusammen. So kann sich auf nationaler Ebene eine Zusammenarbeit mit jedem Ressort ergeben (vgl. Bundesnachrichtendienst 2015c). Tägliche Berichte des BNDs erfolgen jedoch nur an das Bundeskanzleramt und an die Ressorts AA, BMVg, BMWi und BMI sowie an die Sicherheits- und Nachrichtendienste (vgl. Daun 2011, S. 177). Neben den schriftlichen Berichten gibt es auch zunehmend einen mündlichen Austausch (vgl. Daun 2011, S. 177). So gibt es z. B. zwischen der Abteilung AT und dem Cyber-AZ einen direkten Kontakt zur Lagebeurteilung (vgl. Bundesnachrichtendienst 2015a).

Wie auch andere Bundesministerien oder Bundesämter legt der BND in seiner Arbeit einen Schwerpunkt auf die Bekämpfung des Terrorismus und der organisierten Kriminalität. Die Bundesministerien und Bundesämter arbeiten in diesem Bereich zusammen. Der Staatssekretär im Bundeskanzleramt, der zugleich auch Beauftragter für die Nachrichtendienste des Bundes ist, übernimmt hierbei die Koordination. Darüber hinaus ist der BND weltweit mit weiteren Sicherheitsbehörden vernetzt, die jeweils ihren eigenen nationalen Schwerpunkt haben (vgl. Bundesnachrichtendienst 2015f).

Die Arbeit des BNDs bleibt auf Grundlage des BND-Gesetzes meist im Verborgenen, sodass die Öffentlichkeit darüber keine Informationen erhält (vgl. Bundesnachrichtendienst 2015b). In den letzten Jahren steht der BND und mit ihm auch die beiden anderen deutschen Nachrichtendienste vermehrt in der Kritik der Medien. Zunächst richtete sich die Kritik danach, dass die Nachrichtendienste die Annexion der Krim durch Russland, den Vormarsch der IS oder die Aufstände des Arabischen Frühlings nicht vorausgesagt hatten (vgl. Neumann 2014). Zuletzt ist mit den Enthüllungen von Edward Snowden der BND in die Kritik geraten. Dem BND wird vorgeworfen, Kenntnisse über das Ausspähen sensibler Daten zu den europäischen Wirtschaftszielen und Rüstungsprojekten durch die NSA gehabt zu

haben. Der BND soll sogar bei der Ausspähung europäischer Unternehmen und Politiker mit der NSA kooperiert haben (vgl. Zeit Online 2015a).

Die Opposition wirft dem Bundeskanzleramt Kontrollverlust über den BND vor. Das Bundeskanzleramt hat daraufhin Defizite beim BND zugestanden und die Bundesregierung fordert eine Aufklärung (vgl. Zeit Online 2015b). Eine der Ursachen für die Unterstützung der NSA bei der Spionage und eines der Gründe, weshalb gegen die Spionage innerhalb Deutschlands nicht vorgegangen wurde, kann in der Abhängigkeit des BNDs gesehen werden: Damit konnten Geld und Personal gespart werden, wodurch sich Deutschland aber in eine Abhängigkeit von ausländischen Nachrichtendiensten gebracht hat (vgl. Neumann 2014, S. 12).

4.4.5 Deutsche Bundeswehr und der Militärische Abschirmdienst

Der deutschen Bundeswehr obliegt die Aufgabe, die auch aus den verteidigungspolitischen Richtlinien vom 18. Mai 2011 hervorgeht, die Landesverteidigung im Bündnisfall zum Schutz deutscher BürgerInnen und der Verbündeten. Auf internationaler Ebene soll sie zur Konfliktverhütung beitragen (vgl. Deutsche Bundeswehr 2015a). Zu Friedenszeiten hält, wie in Kapitel 4.2.3 erwähnt, die Bundesministerin der Verteidigung die Befehls- und Kommandogewalt über die Streitkräfte inne (vgl. Bundesministerium der Verteidigung 2015a).

Infolge neuer Bedrohungen, wie einem Cyberkrieg, steht auch die Bundeswehr vor neuen Herausforderungen. Denn gut ausgestattete ausländische Nachrichtendienste oder Militärs sind in der Lage, digitale Infrastrukturen vernetzter Gesellschaften anzugreifen; hierzu zählen insbesondere Industriestaaten wie Deutschland (vgl. Gaycken 2012, S. 12-13). Dies wird auch von Interviewpartner 5 (BMVg) bestätigt, dass in Deutschland das Bedrohungspotenzial für Angriffe auf die Wirtschaft sehr hoch sei und militärische Einrichtungen eher weniger betroffen seien (vgl. Interview 5). Weltweit gibt es bereits Länder mit weitaus größeren Armeen die Hackereinheiten besitzen, die zum Teil aus 500-1000 SoldatInnen bestehen. Es wird geschätzt, dass China sogar eine Truppe von 50.000-100.000 SoldatInnen hat. Die USA, Indien, Brasilien und Russland vergrößern ihre Truppen auf

mehrere Tausend, während europäische und kleine asiatische Staaten über Einheiten im dreistelligen Bereich verfügen. Deutschland verfügt über vergleichsweise kleine Einheiten (vgl. Gaycken 2012, S. 64), wozu das KSA mit lediglich 60 SoldatInnen zählt (vgl. Interview 5).

Innerhalb der Bundeswehr übernimmt der MAD mit ca. 1150 MitarbeiterInnen die Abwehr von Cyber-Angriffen in Form von Spionage oder Sabotage (vgl. Flade und Meyer 2013). Als einer der drei deutschen Nachrichtendienste nimmt der MDA Aufgaben des Verfassungsschutzes innerhalb der Bundeswehr wahr (vgl. Kommando Streitkräftebasis 2015). „Zu den gesetzlichen Aufgaben des MAD gehören die Informationssammlung und -auswertung zum Zwecke der Extremismus- und Terrorismusabwehr sowie der Spionage- und Sabotageabwehr“ (Kommando Streitkräftebasis 2015). Dabei ist die größte Herausforderung die Abwehr von Spionage bei internationalen Rüstungsprojekten (vgl. Kommando Streitkräftebasis 2015).

Der MAD führt aber auch die Sicherheitsprüfungen der Bundeswehr-MitarbeiterInnen und ihrer Angehörigen durch. Hierzu gibt es eine Zusammenarbeit mit dem nationalen Cyber-AZ (vgl. Flade und Meyer 2013) und diversen weiteren Bundesbehörden (vgl. Bundesministerium der Verteidigung 2015d). Seit 2004 geht der MAD auch seinen Aufgaben im Rahmen der Auslandseinsätze der Bundeswehr im Ausland nach (vgl. Daun 2011, S. 172). Zudem werden von ihm „Awareness Trainings“ angeboten, die sich an MitarbeiterInnen des BMVgs oder der Bundeswehr richten. Zusammengefasst hat er die Aufgabe der Abschirmung, also des Abwehrens und des Schutzes von Cyber-Angriffen und der *force protection*. Dies ist insbesondere notwendig zum Schutz hochrangiger MitarbeiterInnen der Bundeswehr und des BMVgs. Bei Hinweisen auf Cyber-Angriffen kann der MAD auch Gegenmaßnahmen einleiten (vgl. Interview 5).

Neben dem MAD hat das KSA eine wichtige Rolle bei der Cyber-Aufklärung und wäre im Verteidigungsfall für die Cyberverteidigung zuständig (vgl. Interview 5). Insofern ist das KSA auch für die Krisenfrüherkennung und die Informationsversorgung in Einsätzen zuständig. Hierzu verfolgt das KSA das Ziel, jederzeit

eine *actionable intelligence* bereitzustellen, das bedeutet die Truppen im In- und Ausland mit aktuellen Informationen und konkreten Handlungsempfehlungen zu versorgen. Dies erfolgt durch „Satellitengestützte Abbildende Aufklärung", „Fernmelde- und Elektronische Aufklärung", den „Elektronischen Kampf" sowie der „Objektanalyse" (Kommando Streitkräftebasis 2013). So würde bei einem Cyberkrieg das KSA die Truppen für den elektronischen Kampf stellen. Zur elektronischen Kampfführung stehen dem KSA vier Bataillone mit unterschiedlichen Fähigkeiten in diesem Bereich zur Verfügung (vgl. Kommando Streitkräftebasis 2013). Das KSA verfügt also über Cyber-Abwehrfähigkeiten und Cyber-Aufklärungsmöglichkeiten. Laut Interviewpartner 5 (BMVg) sind die Wirkungsmittel des Kommandos reversibel, das bedeutet, mit einer geringen Anzahl an SoldatInnen können bereits große Cyber-Angriffe ausgeführt werden (vgl. Interview 5), womit der Frage ausgewichen wurde, ob 60 SoldatInnen zur Cyber-Verteidigung ausreichen. Vergleicht man diese Zahl mit jenen von USA, China, Russland, Indien oder Brasilien (vgl. Gaycken 2012, S. 64), erscheint die Anzahl der SoldatInnen im KSA dennoch sehr gering, auch wenn die genannten Staaten größer als Deutschland sind.

Es kann aber davon ausgegangen werden, dass die Bundeswehr ihre Kompetenzen in der Cyber-Verteidigung weiter ausbauen wird. Ein Hinweis hierauf ist auch die Gründung des Forschungszentrums Cyber Defense an der Universität der Bundeswehr in München, zu der die Zunahme der Cyber-Angriffe beigetragen hat (vgl. Deutsche Bundeswehr 2013).

Für die IT-Ausrüstung der Bundeswehr mit *leistungsfähigem und sicherem Gerät* ist im Auftrag des BMVgs das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) zuständig. Das BAAINBw ist insofern der technische Dienstleister für die Bundeswehr (vgl. Deutsche Bundeswehr 2015b). Zu dem Geschäftsbereich des BAAINBw gehört auch das Zentrum für Informationstechnik mit seinen 85 militärischen und 117 zivilen Mitarbeitern, das „durch das Computer Emergency Response Team [der Bundeswehr] (CERTBw) als zentrale Stelle zur Überwachung, Aufrechterhaltung und Wiederherstellung der IT-

Sicherheit im IT-System der Bundeswehr“ (Bundesamtes für Ausrüstung Informationstechnik und Nutzung der Bundeswehr 2014) fungiert.

Bei einem Besuch der Verteidigungsministerien Ursula von der Leyen im BAAINBw, erklärte diese, dass neben der Verteidigung zu Land, zu Wasser und in der Luft auch mit der gleichen Priorität eine Verteidigung im Cyberraum aufgebaut werden müsse. Für die zukünftigen Konflikte geht sie davon aus, dass diese eine Cyberkomponente haben werden. Die nötigen Kompetenzen zur Verteidigung im Cyberraum seien im IT-Zentrum der Bundeswehr bereits vorhanden (vgl. Bundesministerium der Verteidigung 2015b). Dennoch lässt sich hieraus schließen, dass diese Kompetenzen noch weiter ausgebaut werden müssen.

Das IT-Zentrum arbeitet im Rahmen des Herkules-Projektes unter anderem auch mit der BWI Informationstechnik GmbH zusammen (vgl. BWI Informationstechnik GmbH 2015a). In der Organisationsstruktur des Bundesamtes für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr lässt sich die Abteilung Sonderorganisation HERKULES (H) wiederfinden (vgl. Deutsche Bundeswehr 2015c). Das Herkules-Projekt wurde 2006 zwischen der Bundeswehr, der IBM und Siemens zur Modernisierung der nichtmilitärischen Informations- und Kommunikationstechnik der Bundeswehr beschlossen. Die BWI Informationstechnik GmbH ist ein gemeinsames Unternehmen von Siemens, IBM und der Bundeswehr und hat diese Aufgabe für zehn Jahre übernommen (vgl. BWI Informationstechnik GmbH 2015b). Der Leistungsverbund, bestehend aus BWI Systeme GmbH und BWI Services GmbH ist eines der größten Public Privat Partnerships in Europa.

Im Rahmen des Herkules-Projektes wurden „140.000 Rechner, 300.000 Telefone und 12.000 Kilometer Datenkabel quer durch Deutschland“ in 1200 Liegenschaften der Bundeswehr modernisiert (BWI Informationstechnik GmbH 2015b) und eine Standardisierung der IT-Systeme geschaffen (vgl. BWI Informationstechnik GmbH 2015b). Zuvor gab es 3000 verschiedene Computertypen und 1000 Internetzugänge. Der Konsolidierungsprozess wurde von der Bun-

deswehr allerdings schlecht begleitet, wie eine interne Umfrage der Bundeswehr bestätigt, so ein interviewter Vertreter der BWI Informationstechnik (Interviewpartner 9 (BWI)) (vgl. Interview 9).

Die BWI Informationstechnik betreibt mit 3.000-4.000 MitarbeiterInnen die IT-Systeme der Bundeswehr und die dazugehörige IT-Sicherheit der Bundeswehr. Außerdem werden von 30 Weitverkehrsnetzen in Deutschland eines von der BWI Informationstechnik für die Bundeswehr betrieben, die restlichen von der Deutschen Telekom AG. Die Hälfte der MitarbeiterInnen der BWI Informationstechnik sind beurlaubte SoldatInnen von der Bundeswehr, die oftmals von der Bundeswehr im IT-Bereich selbst ausgebildet wurden. Es bestehe kein Problem, in der Bundeswehr geeignete MitarbeiterInnen zu finden, die auch ein hohes Bewusstsein für IT-Sicherheit hätten, so Interviewpartner 9 (BWI) (vgl. Interview 9).

Die allgemeine Zusammenarbeit im Rahmen des Herkules-Projektes mit der Bundeswehr wird von Interviewpartner 9 (BWI) als sehr gut bewertet. Mit dem Public Private Partnership war es möglich in der Bundeswehr eine gute Sicherheitsstruktur zu schaffen, so der Interviewte (vgl. Interview 9). Wie in Kapitel 4.2.3 erwähnt, wird die Zusammenarbeit von Interviewpartner 5 (BMVg) mit der BWI Informationstechnik ebenfalls als gut bewertet, jedoch ließ sich hier nach Lesart interpretieren, dass es dennoch Dinge geben mag, die in der Zusammenarbeit nicht funktionieren (vgl. Interview 5).

An dem BSI wird kritisiert, dass insbesondere die Zertifizierung von Produkten viel zu lange dauere. Eine Ursache hierfür seien die allzu strengen Regelungen, so Interviewpartner 9 (BWI). Die Bundeswehr könne in diesen Fällen selbst eine Genehmigung ausstellen, da ansonsten nur zertifizierte Produkte des BSIs benutzt werden dürften (vgl. Interview 9). Mit dem Herkules-Projekt sei die Bundeswehr in einigen Staaten zum Vorbild geworden, so berichtet Interviewpartner 9 (BWI). In anderen Staaten werden bislang nur Teilaufgaben an externe Dienstleister übertragen. Norwegen, Frankreich und Kroatien interessierten sich für die IT-Sicherheit der Bundeswehr, um diese bei sich ebenfalls umzusetzen. Die gleiche

Umsetzung einer Standardisierung der IT-Infrastruktur wäre aber auch für andere Ressorts der Bundesverwaltung möglich und notwendig (vgl. Interview 9). Mit der Beendigung des Herkules-Projektes wird die BWI Informationstechnik ab 2016 im Auftrag des BMVgs zur Inhouse-Gesellschaft der Bundeswehr werden. Auch Bereiche der Waffen-IT und Führungsinformationen sollen ab 2020 von der Inhouse-Gesellschaft betreut werden (vgl. Interview 9).

Insofern lässt sich hieraus schließen, dass die Zusammenarbeit mit der BWI Informationstechnik insgesamt gut ist. Ein Grund für die weitere Zusammenarbeit kann aber auch darin bestehen, dass die Bundeswehr Probleme hat, qualifizierte MitarbeiterInnen zu finden (vgl. Interview 5), während die BWI Informationstechnik angibt, keine derartigen Probleme zu haben (vgl. Interview 9). Die Hälfte der MitarbeiterInnen besteht jedoch aus beurlaubten SoldatInnen (vgl. Interview 5) und diese werden teilweise von der Bundeswehr ausgebildet (vgl. Interview 9). Der Leistungsverbund mit der IBM, Siemens und der Deutschen Bundeswehr könnte einen attraktiveren Arbeitgeber in der Wirtschaft darstellen als die Deutsche Bundeswehr oder eine Bundesbehörde der Bundesverwaltung.

Beim Schutz vor Cyber-Angriffen steht die Bundesregierung vor großen Herausforderungen, wie unter anderem der Cyber-Angriff auf den Deutschen Bundestag im Frühjahr 2015 verdeutlichte (vgl. Flade und Nagel 2015). Mit nur 60 SoldatInnen im KSA (vgl. Interview 5) ist davon auszugehen, dass auch hier noch große Herausforderungen für die Cyberverteidigung bestehen. Die Bundeswehr arbeitet bereits an einem Strategiepapier, um in der Cyberverteidigung besser gerüstet zu sein (vgl. Flade und Nagel 2015). Außerdem soll im neuen Weißbuch das 2016 erscheint und vom BMVg herausgegeben wird, die Cyberverteidigung eine größere Bedeutung erhalten (vgl. Flade und Nagel 2015), als es im Weißbuch von 2006 der Fall gewesen ist (vgl. Bundesministerium der Verteidigung 2006). Denn die Anzahl der 60 SoldatInnen, die zur Cyberverteidigung im Fall eines Cyberkrieges eingesetzt werden könnten (vgl. Flade und Nagel 2015), erscheint im Vergleich zu den Kapazitäten anderer Staaten zu gering.

4.5 Kooperationen der politischen Institutionen

Die Beschreibung der politisch-institutionellen Organisation der Cyber Security in Deutschland soll nachfolgend mit einer Betrachtung der Kooperationen mit Vereinen und Organisationen auf den Ebenen des Bundes, der EU und der NATO abgeschlossen werden.

4.5.1 Vereine und Organisationen auf Bundesebene

In Deutschland gibt es zahlreiche Vereine, Gremien und Initiativen, die mit den Unternehmen, Bundesministerien und Bundesämtern im Bereich der Cyber Security zusammenarbeiten, weshalb sie auch in dieser Arbeit exemplarisch erörtert werden sollen. Wie bereits in Kapitel 4.1.2 zum BSI erwähnt, gründete dieses mit der BITKOM die Allianz für Cyber-Sicherheit (vgl. Bundesamt für Sicherheit in der Informationstechnik 2015b). Die BITKOM wurde 1999 aus verschiedenen Branchen der Wirtschaft gegründet und beschäftigt sich als Digitalverband Deutschlands unter anderem mit dem Thema Cyber Security. Mittlerweile sind 2800 Unternehmen in der BITKOM vertreten, hierunter 1000 mittelständische und 300 Startup-Unternehmen sowie nahezu alle international tätigen deutschen Unternehmen, die sogenannten *Global Player*. BITKOM vertritt die Interessen der Unternehmen in der Politik und bietet Dienste rund um die Informationstechnologie an (vgl. BITKOM 2015). Die Nationale Initiative für Informations- und Internet-Sicherheit (NIFIS e. V.) wendet sich ebenfalls an Unternehmen, um diese unabhängig zu beraten und zu stärken. Gegründet wurde der Verein von VertreterInnen aus der Wissenschaft und Politik. Der NIFIS e.V. steht hauptsächlich für die Förderung und Sicherstellung der „Vertraulichkeit, Verfügbarkeit und Integrität von Daten in digitalen Netzwerken“ (Nationale Initiative für Informations- und Internet-Sicherheit (NIFIS e.V.) 2015).

Darüber hinaus gibt es weitere Vereine wie besipielsweise Deutschland Sicher im Netz e. V., der sich überwiegend an mittelständische Unternehmen und Verbraucher wendet. Die Schirmherrschaft hat mit der Gründung 2006 das BMI

übernommen. In einem Kooperationsvertrag verpflichtet sich dieser Verein dazu, das BMI bei der Umsetzung von Initiativen der Bundesregierung im Bereich Sicherheit in der Informationstechnik zu unterstützen (vgl. Deutschland sicher im Netz e. V. 2015). Aus der Digitalen Agenda geht hervor, dass die Zusammenarbeit mit dem Verein ausgebaut werden soll, insbesondere hinsichtlich des Schutzes der BürgerInnen (vgl. Die Bundesregierung 2014b, S. 33).

Weitere Interessenvertretungen der digitalen Wirtschaft sind beispielsweise der Bundesverband Arbeitsgemeinschaft für Sicherheit in der Wirtshaft e. V. (ASW) (vgl. ASW Bundesverband 2015) oder der Verband der deutschen Internetwirtschaft e. V. (vgl. eco- Verband der deutschen Internetwirtschaft e.V. 2015). Letzterer ist mit über 800 Mitgliedern der größte Verband der Internetwirtschaft in Europa und vertritt die Interessen seiner Mitglieder über die nationalen Grenzen hinaus (vgl. eco – Verband der deutschen Internetwirtschaft e. V. 2015). Des Weiteren engagiert sich der BDI für die Cyber Security-Interessen seiner Mitglieder in Gremien der Bundesregierung, dem nationalen Cybersicherheitsrat und der Allianz für Cyber-Sicherheit. Mit dem BMWi arbeitete er zusammen im Lenkungskreis zur Initiative „IT-Sicherheit in der Wirtschaft“ (vgl. Bundesverband der Deutschen Industrie e. V. 2015).

In den letzten Jahren ist aber auch eine zunehmende Präsenz des *Netzpolitik-Aktivismus* in Deutschland zu beobachten, wie beispielsweise vom Chaos Computer Club (vgl. Wendelin und Löblich 2013). Netzpolitik-Aktivisten sind durch die mediale Berichterstattung über ihre Proteste gegen die Vorratsdatenspeicherung in der Öffentlichkeit präsenter geworden. Zivilgesellschaftliche Akteure hatten bisher in dem digitalen Zeitalter keine große Rolle gespielt, mittlerweile hat insbesondere der Chaos Computer Club einige Erfolge durch seine Proteste erzielt (vgl. Wendelin und Löblich 2013). Neben der medialen Berichterstattung hat der Chaos Computer Club auch die Zusammenarbeit mit der Politik verstärkt und nahm beispielsweise an der Enquete-Kommission Internet und digitale Gesellschaft im Bundestag teil. Gegründet hat sich der Chaos Computer Club bereits vor 30 Jahren und ist mittler-

weile die größte europäische Hackervereinigung. Er ist aktiv unter anderem in der technischen Forschung, Politikberatung, Kampagnen, Veranstaltungen und Publikationen (vgl. Chaos Computer Club 2015).

In den USA werden BürgerInnen, Software-Entwickler und Unternehmen von der Politik aufgerufen, Daten und Software zu hacken, um Sicherheitslücken in den IT-Systemen zu entdecken. Diese Zusammenarbeit der Politik mit Hackern ist in Deutschland allerdings noch nicht üblich (vgl. heise online 2013). In den USA wird in der Politik generell weitaus mehr mit zivilen IT-SpezialistInnen zusammengearbeitet als in Deutschland. Das mag auch an der niedrigen Bezahlung der IT-SpezialistInnen innerhalb der Bundesverwaltung liegen, die hingegen in den USA der Privatwirtschaft entspricht (vgl. Kullik 2014). Von Interviewpartner 12 (Daimler AG) wird ein ähnliches Verfahren in Betracht gezogen, bei dem die Weltöffentlichkeit viel mehr genutzt wird, um Sicherheitslücken aufzudecken. Beispielsweise könnten Probleme bzw. Sicherheitslücken ins Internet gestellt und veröffentlicht werden, um dadurch international mit InformatikerInnen nach Lösungen zu suchen (vgl. Interview 12).

4.5.2 Kooperationen auf EU-Ebene

In der EU gibt es drei Säulen, die Aufgaben im Bereich Cyber Security wahrnehmen. Wie der Abbildung 3 zu entnehmen, sind diese Netzwerk- und Informationssicherheit, Strafverfolgung und Verteidigung. In der ersten Säule nimmt die Europäische Agentur für Netz- und Informationssicherheit (ENISA) eine wichtige Rolle ein. Der zweiten Säule ist EUROPOL zugeordnet, mit dem das BKA eine intensive Zusammenarbeit unterhält (vgl. Interview 7; Kapitel 4.4.2). Zur dritten Säule zählt die European Defence Agency. Mit allen drei Institutionen führt Deutschland eine intensive Zusammenarbeit (vgl. Kullik 2014, S. 174), auf die im Folgenden näher eingegangen wird.

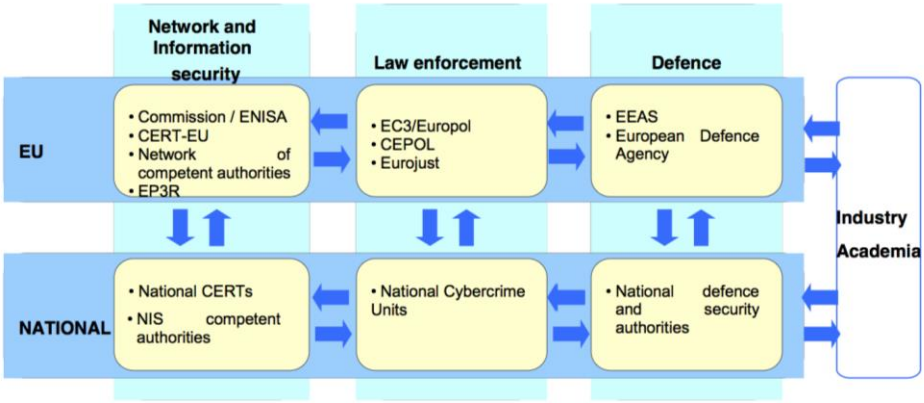

Abb. 3: Die drei Säulen der Europäischen Union im Bereich Cyber Security (Quelle: Europäische Kommission 2013a)

Die ENISA ist eine 2004 gegründete EU-Agentur, die „die Kapazitäten der Europäischen Union (EU), der EU-Mitgliedstaaten und der Unternehmen hinsichtlich der Verhütung, der Reaktion auf Probleme und deren Bewältigung im Bereich der Netz- und Informationssicherheit verstärken“ soll (Amtsblatt der Europäischen Union 2004). Für die ENISA ist zukünftig noch eine stärkere Zusammenarbeit mit dem Europol Cybercrime Center vorgesehen. Des Weiteren ist eine Unterstützung der europäischen Cybersicherheitspolitik vorgesehen, mit der Beratung auch im Hinblick auf die Gesetzgebung. Anhand von EU-Richtlinien soll auch die Forschung eine noch stärkere Gewichtung erhalten und unterstützend in der Früherkennung sowie der Prävention mitwirken. Die ENISA soll darüber hinaus auch eine beratende Funktion für europäische Mitgliedsstaaten und Institutionen übernehmen (vgl. ENISA 2013).

Die ENISA führt regelmäßig Übungen mit allen 29 Mitgliedsstaaten durch, „um Maßnahmen zur digitalen Gefahrenabwehr zu simulieren“ (ENISA 2014). An den Übungen nehmen unter anderem aus den Mitgliedsstaaten Computer Emergency Response Teams, Bundesministerien und Betreiber Kritischer Infrastrukturen teil. Die Übung Cyber Europe 2014 war bis dahin die größte durchgeführte Übung der ENISA (vgl. ENISA 2014). Eine engere Zusammenarbeit zwischen ENISA und Deutschland gibt es unter anderem mit dem BSI und dem CERT-Bund

sowie dem CERT der ENISA (vgl. Bundesamt für Sicherheit in der Informationstechnik 2015e).

Das Cybercrime Center wurde 2013 zur Bekämpfung von Cyberkriminalität innerhalb der europäischen Polizeibehörde EUROPOL gegründet. So wird auf europäischer Ebene Cyberkriminalität von organisierten Gruppen bekämpft, insbesondere bei schweren kriminellen Delikten wie dem Online-Betrug, Kinderpornografie und letztlich auch Cyber-Angriffe auf Kritische Infrastrukturen und Informationssysteme innerhalb der Europäischen Union (vgl. EUROPOL 2015a). Wie bereits in Kapitel 4.4.2 erwähnt, pflegt das BKA eine enge Zusammenarbeit mit EUROPOL, welche sich zwar aufgrund einer leistungsfähigen organisierten Struktur verbessert habe, die allerdings hinsichtlich der Personalstruktur Interviewpartner 7 (BKA) zufolge verbesserungswürdig sei (vgl. Interview 7).

Im Rahmen der gemeinsamen Sicherheits- und Verteidigungspolitik der Europäischen Union wurde die Europäische Verteidigungsagentur 2004 gegründet. Die Leitung obliegt dem Hohen Vertreter der gemeinsamen Außen- und Sicherheitspolitik. Bei der Cyber Security übernimmt die Europäische Verteidigungsagentur insbesondere die Aufgabe der Cyber Defence für die EU und arbeitet hierbei mit den nationalen Verteidigungsministerien zusammen (vgl. Fraunhofer INT 2014). Neben ENISA, EUROPOL und der Europäischen Verteidigungsagentur gibt es noch weitere Einrichtungen und Institutionen, die Aufgaben im Bereich Cyber Security wahrnehmen (vgl. OECD 2012), worauf aber nicht weiter eingegangen wird, da Deutschland auf europäischer Ebene in der Cyberkriminalitätsbekämpfung überwiegend mit ENISA und EUROPOL zusammen arbeitet (vgl. Interview 7).

Neben den genannten Institutionen sind auf Europäischer Ebene die europäische Cyber-Sicherheitsstrategie, die europäische Digitale Agenda und die NIS-Richtlinie (Netz- und Informationssicherheit) für die Cyber Security ausschlaggebend. Die Digitale Agenda für Europa ist eine der Leitlinien der Strategie 2020, welche die Europäische Kommission in Anbetracht der Wirtschaftskrise und den damit verbundenen Herausforderungen 2010 vorstellte. Hierin ist es das Ziel, die Wirt-

schaft zu fördern und dabei auch der Informations- und Kommunikationstechnologie eine größere Rolle zukommen zu lassen. Die Strategie gibt sieben Leitinitiativen vor, eine davon ist die Digitale Agenda für Europa (vgl. Europäische Kommission 2010).

Die Digitale Agenda wird jährlich anhand eines Fortschrittanzeigers hinsichtlich der Erreichung der Ziele überprüft (vgl. Europäische Kommission 2014, S. 3). Die Digitale Agenda für Europa soll „die Wirtschaft Europas durch die aus dem digitalen Binnenmarkt erwachsenden positiven Impulse ankurbeln" (Europäische Kommission 2014, S. 3). Mittlerweile wächst die europäische digitale Wirtschaft um 12 % jährlich. Der Fortschrittsanzeiger von 2014 hat gezeigt, dass die Breitbandversorgung innerhalb der EU, insbesondere in ländlichen Gebieten, nicht ausreichend ist. Darüber hinaus mangelt es vielen BürgerInnen an der erforderlichen digitalen Kompetenz, um die digitalen Angebote nutzen zu können (vgl. Europäische Kommission 2014, S. 3).

Der Digitalen Agenda für Europa folgte 2013 die europäische Cyber-Sicherheitsstrategie. Die Strategie steht für einen „Open, Safe and Secure Cyberspace" (vgl. Europäische Kommission 2013a). Hierzu werden fünf Prioritäten festgelegt: 1) Die Resilienz gegenüber Cyberangriffen stärken, 2) Die Cyberkriminalität stärker reduzieren, 3) Im Rahmen der gemeinsamen Außen- und Sicherheitspolitik auch eine gemeinsame Cybersicherheitspolitik verfolgen, insbesondere in der Cyberverteidigung, 4) Die Förderung der Entwicklung von Ressourcen für die Cyber Security und 5) Eine Cyberstrategie der Europäischen Union zu entwickeln, die sie auf internationaler Ebene vertritt (vgl. Europäische Kommission 2013b).

Parallel zur europäischen Cyber-Sicherheitsstrategie wurde die NIS-Richtlinie festgelegt, die dazu beitragen soll, die „Netzwerk- und Informationssystemsicherheit (NIS) in der EU zu verbessern" (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und Bundesamt für Sicherheit in der Informationstechnik 2011-2013). Diese Richtlinie legt fest, dass öffentliche und private Betreiber der Kritischen Infrastrukturen ein Mindestmaß an IT-Sicherheit erfüllen müssen und An-

griffe an dafür vom Staat eingerichtete Meldestellen gemeldet werden müssen. Diese sollen wiederum miteinander vernetzt sein und sich über Vorfälle austauschen und diese an die ENISA berichten (vgl. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und Bundesamt für Sicherheit in der Informationstechnik 2011-2013). In Deutschland wurde mit dem Beschluss zum IT-Sicherheitsgesetz die Meldepflicht und die Pflicht zur Einhaltung von IT-Mindeststandards eingeführt (vgl. Die Bundesregierung 2015c).

4.5.3 Kooperationen auf NATO-Ebene

Auf internationaler Ebene unterstützt Deutschland unter anderem die NATO Cyber-Abwehr, die vor neuen Herausforderungen steht (vgl. Varwick und Schmid 2012). Die NATO beschloss erstmals 2008 ihre Cybersicherheitspolitik als Reaktion auf einen Cyber-Angriff in Estland (vgl. NATO 2015). 2011 folgte die NATO Policy on Cyber Defence, verabschiedet von den Verteidigungsministern des Bündnisses (vgl. NATO 2011). Seitdem ist die Cyberverteidigung zu einer der Kernaufgaben der kollektiven Verteidigung der NATO geworden.

Darüber hinaus ist durch die wachsende Komplexität der Cyber-Angriffe eine der wichtigsten Aufgaben der NATO der Schutz der Kommunikations- und Informationssysteme ihrer Bündnisländer. Die NATO ist für ihre Kommunikationsnetze selbst verantwortlich, wie auch ihre Bündnisländer jeweils für ihre Kommunikationsnetze, die mit denen der NATO kompatibel sein müssen (vgl. NATO 2015). Für den Schutz sind in Deutschland unter anderem das BMVi, BMVg, das BSI und das BBK sowie die Telekommunikationsunternehmen zuständig (vgl. Bundesamt für Sicherheit in der Informationstechnik und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2011-2013a; Bundesministerium der Verteidigung 2015c; Bundesministerium für Verkehr und digitale Infrastruktur 2015c).

Ferner hat die NATO sich zum Ziel gesetzt den Informationsaustausch mit den Bündnisländern und deren gegenseitige Unterstützung bei der Prävention und dem Schutz vor Cyberangriffen zu stärken. Ihre Fähigkeiten sollen durch die Cyber-

Ausbildung in Form von Trainings und Übungen erweitert werden (vgl. NATO 2015). Deutlich wird auch der Bedarf an Forschung in diesem Themengebiet durch das eigens dafür errichtete NATO Cooperative Cyber Defence Centre of Excellence nach dem Angriff auf Estland. Das Forschungs- und Ausbildungsinstitut steht für Bildung, Beratung, Lehre, Forschung und Entwicklung auf dem Gebiet der Cyber Security (vgl. NATO Cooperative Cyber Defence Centre of Excellence 2015).

Auf internationaler Ebene stellt sich das Problem der „[...] Schaffung von Rechtssicherheit bei der Abwehr von Cyberbedrohungen [...]“ (Schaller 2014, S. 5). Deutschland setzt sich hier, wie bereits erwähnt, für Normen ein, die „[...] ein verantwortungsvolles Miteinander der Staaten im Cyberspace gewährleisten sollen[...]“ ein (Schaller 2014, S. 5). International ist aber eine Debatte entstanden, wann Staaten bei einem Cyberangriff ihr Recht auf Selbstverteidigung nach Artikel 51 der UN-Charta anwenden dürfen. Den Rahmenbedingungen des Völkerrechtes zufolge sind Cyberoperationen der bewaffneten Kriegsführung gleichgestellt. Hierzu wurden mit der Budapester Konvention bereits 2001 spezielle Normen im Völkerrecht für den Kampf im Cyberspace aufgenommen. Völkerrechtliche Regelungen sind von großer Bedeutung angesichts der wachsenden Bedrohungen für Staaten im Cyberraum, z. B. durch Cyber-Angriffe von Terrororganisation. Durch einheitliche Regelungen wie in der Budapester Konvention können Cyberangriffe gegen die Mitgliedsstaaten gezielter bekämpft werden (vgl. Schaller 2014, S. 5-10). Für die NATO stellt sich die Frage, wann der Bündnisfall nach Artikel 5 im Fall eines Cyberangriffes ausgerufen werden kann und wie darauf zu reagieren ist. Angesichts des Cyberangriffes auf den Deutschen Bundestag wurde diese Debatte auch in den Medien aufgegriffen (vgl. Clauß 2015).

„Ein grundsätzliches Problem für die Zusammenarbeit mit der NATO im Bereich der Cyber-Abwehr sind die verzweigten Kompetenzen innerhalb Deutschlands.“ (Varwick und Schmid 2012). Insofern ist eine Kooperation Deutschlands mit der NATO durch die verschiedenen Zuständigkeiten der Bundesbehörden innerhalb Deutschlands erschwert. Eine Kooperation erfolgt unter anderem durch das

Cyber-AZ, das wiederum dem BSI untergeordnet ist; die Federführung des Bundesamtes liegt aber letztlich beim BMI.

Daneben gibt es, wie bereits erwähnt, den nationalen Cyber-SR, in dem alle wichtigen Entscheidungsträger im Bereich der Cyber Security vertreten sind (vgl. Varwick und Schmid 2012), um „übergreifende Politikansätze für Cyber-Sicherheit" (Bundesministerium des Innern 2015b, S. 10) zu koordinieren.

Deutschland ist aber auch in internationalen Gremien der NATO vertreten, beispielsweise durch das AA (vgl. Interview 6), und kommt damit seiner selbstgesetzten Aufgabe aus der Cyber-Sicherheitsstrategie nach, die als „effektives Zusammenwirken für Cyber-Sicherheit in Europa und weltweit" (Bundesministerium des Innern 2015b, S. 11) festgelegt wird.

In Zukunft wird es für die NATO angesichts der wachsenden Bedrohungslage von Cyber-Angriffen auf die Mitgliedsstaaten erforderlich sein, im Bereich der Cyberverteidigung stärker zu werden. Denn es ist davon auszugehen, dass die NATO-Mitgliedsstaaten infolge der Wirtschafts- und Schuldenkrise immer weniger in die Verteidigung investieren werden. Bei Investitionen komme es jedoch weniger auf die „harten militärischen Kapazitäten" an, sondern auf die Koordination zwischen den Mitgliedsstaaten. Vor diesem Hintergrund ist die vielfältige Aufgabenteilung unter Bundesministerien und Bundesämter eine Herausforderung für die Zusammenarbeit der Bundesrepublik Deutschland mit der NATO (vgl. Varwick und Schmid 2012).

4.6 Zwischenfazit

Aus den hier dargestellten Informationen ergibt sich der Eindruck, dass Cyber Security in der Bundesrepublik Deutschland stark fragmentiert ist. Die Aufgaben sind auf unterschiedlichste Bundesministerien und nachgeordnete Bundesämter verteilt. Dadurch ergibt sich eine Vielzahl an Kompetenzen, die aber nicht zentral organisiert sind. Das bedeutet, es gibt keine zentral koordinierende Institution auf

Ebene der Bundesverwaltung, welche die gesamthafte Verantwortung für Cyber Security übernimmt.

An den hier behandelten Bundesministerien und Bundesämtern und ihren Aufgaben lässt sich erkennen, dass die Politik die Bedrohung durch Cyber-Angriffe wahrnimmt. Die Bedeutung von Cyber Security hat dabei nicht nur auf nationaler, sondern auch auf internationaler Ebene zugenommen. So hat die Thematik Cyber Security mittlerweile viele Bereiche von Staat, Wirtschaft und Gesellschaft erreicht. Die Aufgaben zu Cyber Security sind auf Bundesebene auf eine Vielzahl von Bundesministerien und Bundesämter aufgeteilt, woraus hervorgeht, dass Cyber Security in vielen Fachbereichen der Bundesministerien und Bundesämter wahrgenommen wird und von Relevanz ist. Hieraus ergeben sich einige Aspekte, die nachfolgend zusammenfassend dargelegt werden sollen.

Nationale Zusammenarbeit der Bundesministerien und Bundesämter

Interviewpartner 1 (BMI) vertritt die Meinung, dass die Qualität der Zusammenarbeit ausschließlich vom Faktor Mensch abhinge (vgl. Interview 1), während Interviewpartner 7 (BKA) die Auffassung vertritt, dass die Zusammenarbeit mit ihrer Organisation zusammen hängt und ein ganzheitlicher Ansatz dadurch nicht verwirklicht werden kann (vgl. Interview 7). Somit erkennen VertreterInnen des BMIs und auch des BSIs die Problematik der schlechten Zusammenarbeit von Bundesbehörden mit dem Cyber-AZ nicht (vgl. Interview 2; 1). Von einer engen Verzahnung mit anderen Bundesbehörden durch das Cyber-AZ (vgl. Interview 1), kann aber nur teilweise ausgegangen werden.

Letztlich erfüllt das Cyber-AZ seine Aufgabe der Kooperation zwischen den Bundesministerien und Bundesämter nur teilweise, da nicht zwischen allen eine gute Zusammenarbeit besteht (vgl. Bundesministerium des Innern 2011, S. 8). Die Federführung obliegt dem BSI, dessen Zusammenarbeit mit einigen Bundesbehörden allerdings verbessert werden konnte (vgl. Interview 3; 4; 7; 8).

Nichtsdestotrotz gibt es auch hier Verbesserungsmöglichkeiten. So müssten Cyber-Angriffe vom BSI an das BKA zuverlässiger gemeldet werden. Nur so könne

mehr Transparenz geschaffen und eine Strafverfolgung aufgenommen werden (vgl. Interview 7).

Mit dem IT-Sicherheitsgesetz erhält das BSI bereits mehr Aufgaben, die aber auch nur mit einem Personalausbau zu bewältigen sind (vgl. Interview 2). Seitens des BMI könnte ein weiterer Ausbau der Aufgaben des BSIs und dem Cyber-AZ für die Zukunft angedacht werden (vgl. Interview 1). Das würde sicherlich auch die Zusammenarbeit mit Unternehmen und Bundesbehörden stärken. Aufgrund der Vielzahl der beteiligten Bundesbehörden, Vereinen und Arbeitsgruppen besteht zudem das Problem, dass bei Unternehmen Unsicherheit über die AnsprechpartnerInnen besteht (vgl. Interview 7; Kapitel 4).

Eine weitere Zusammenarbeit findet auf europäischer und internationaler Ebene statt, insbesondere durch das AA und das BKA, die auf europäischer Ebene vom BSI unterstützt werden. Zur Bekämpfung von Cyber Security sind für Deutschland die Kooperationen auf EU- und NATO-Ebene von Bedeutung, die nachfolgend erörtert werden.

Internationale Zusammenarbeit

Auf EU-Ebene ist unter anderem die ENISA für Cyber Security bedeutend, da sie als Agentur für Netz- und Informationssicherheit innerhalb Europas zuständig ist, wobei sie vorwiegend eine beratende Funktion besitzt. Die Agentur soll weiterhin in ihrer Rolle gestärkt werden, indem sie vermehrt Aufgaben wahrnimmt: 1) in der Beratung und Unterstützung des Europol Cybercrime Centers, 2) zur europäischen Cybersicherheitspolitik, 3) zur Forschung und 4) bei der Beratung von europäischen Mitgliedsstaaten (vgl. ENISA 2013). In Anbetracht der zunehmenden Cyberbedrohungen und der Tatsache, dass diese nicht nur auf nationaler Ebene bekämpft werden können, scheint es sinnvoll, eine europäische Institution wie die ENISA zu stärken, um die Zusammenarbeit der europäischen Mitgliedsstaaten auf diesem Gebiet zu fördern. Denn auf europäischer Ebene sollte über eine Verbesserung der Zusammenarbeit nachgedacht werden, wie auch Interviewpartner 6 (AA) bestätigt. So wäre beispielsweise eine Zusammenlegung einiger Arbeitsgruppen auf EU-Ebene

effektiver (vgl. Interview 6). Hier lässt sich vermuten, dass mit der Zusammenlegung eventuell auch die Zusammenarbeit einfacher gestaltet werden könnte.

Eine gute internationale Zusammenarbeit umfasst auch die Strafverfolgung. TäterInnen nutzen die Anonymität aus, wodurch die Strafverfolgung erheblich erschwert wird (vgl. Bundesamt für Sicherheit in der Informationstechnik 2014, S. 4). Zur Strafverfolgung ist die Zusammenarbeit mit EUROPOL auf europäischer und mit INTERPOL auf internationaler Ebene und dem BKA sichergestellt. Zudem verfügt das BKA über ein weltweites Netzwerk und kann bei Cyber-Angriffen schnell reagieren (vgl. Interview 7).

Auch auf NATO-Ebene ist die Zusammenarbeit durch die beschriebene Fragmentierung bei einer nicht immer klaren Aufgabenteilung beeinträchtigt (vgl. Varwick und Schmid 2012). Deutschland setzt sich international für Rechtsstaatlichkeit im Cyberraum ein (vgl. Schaller 2014, S. 5), wozu eine Zusammenarbeit mit der NATO wichtig ist. Zudem erfordert die Thematik internationale Rahmenbedingungen in Anbetracht der Anonymität im Cyberspace. Laut Interviewpartner 6 (AA) ist zwar die informelle internationale Zusammenarbeit gut (vgl. Interview 6), daraus lässt sich aber schließen, dass die formelle Zusammenarbeit verbessert werden könnte. Die diplomatische Zusammenarbeit über das AA ist insbesondere wichtig, da im Fall eines Cyber-Angriffes Staaten mit guten nachbarschaftlichen Beziehungen als Täter in der Regel ausgeschlossen werden können. Aufgrund der politischen Spannungen mit Russland, hervorgerufen durch die Ukraine-Krise, besteht derzeit im Bereich der Bekämpfung von Cyberkriminalität keine Zusammenarbeit mehr (vgl. Interview 6). Russland besitzt allerdings eine große Tätergruppe (vgl. Interview 7).

Bei dem Cyber-Angriff auf den Bundestag vermuten einige ExpertInnen einen Cyber-Angriff von Hackern aus Russland bzw. des russischen Geheimdienstes (vgl. Baumgärtner et al. 2015; Bewarder et al. 2015). Dies zeigt, wie wichtig eine gute Zusammenarbeit auch zwischen den Staaten ist. So hätte man in dem Fall mit Russland zur Strafverfolgung zusammen arbeiten oder ausschließen können, dass die

Hacker von der Regierung beauftragt werden, falls dies tatsächlich der Fall gewesen sein sollte.

Um den Aufgaben der internationalen aber auch der nationalen Zusammenarbeit nachzugehen, bedarf es einer angemessenen personellen Ausstattung der Bundesministerien und Bundesämter. Hier konnten jedoch einige personelle Ressourcenmängel festgestellt werden, auf die nun eingegangen werden soll.

Personeller Ressourcenmangel

Eine weitere Herausforderung neben der nationalen und internationalen Zusammenarbeit ist der Personalmangel in den Bundesministerien und Bundesämtern (vgl. Interview 2; 3; 7; Flade 2014). Mit dem IT-Sicherheitsgesetz werden noch weitere Aufgaben auf die Bundesbehörden zukommen, weshalb im Rahmen des Gesetzes auch ein Stellenausbau in einigen Bundesbehörden geplant ist (vgl. Interview 2; 7; 8). Jedoch erhalten nicht alle Bundesbehörden einen Personalausbau und es wird teilweise auch bezweifelt, ob der Stellenausbau tatsächlich mit in Kraft treten des IT-Sicherheitsgesetztes zeitnah umgesetzt wird (vgl. Interview 2).

Darüber hinaus ist es laut VertreterInnen der Bundesbehörden schwierig, Mitarbeiter mit den benötigten Kompetenzen zu akquirieren (vgl. Interview 5; 6; 7; 8). Es werden vor allem InformatikerInnen, aber auch GeisteswissenschaftlerInnen gesucht, die in ihrem Fachgebiet einen Schwerpunkt auf Cyber Security nachweisen können (vgl. 7; 8). Einer der Gründe für den Mangel an geeignetem Fachpersonal ist die geringe Bezahlung in der Bundesverwaltung im Vergleich zur Wirtschaft (vgl. Interview 5; 7; 8). Dies wird am deutlichsten im BKA, das 120 MitarbeiterInnen im Bereich Cyber Security beschäftigt, hiervon sind nur acht InformatikerInnen und diese haben einen Bachelorabschluss, da keine Masterabsolventen mit einer entsprechenden Bezahlung eingestellt werden können (vgl. Interview 7).

Die Kompetenzen im BKA, in den Landeskriminalämtern und der Polizei müssten für die Strafverfolgung im Cyberraum gestärkt werden. Das BKA erhält zwar mit dem IT-Sicherheitsgesetz einen Stellenausbau, aber es werden auch mehr Aufgaben entstehen. So werden aufgrund der gesetzlichen Verpflichtung durch das

IT-Sicherheitsgesetz mehr Betreiber Kritischer Infrastrukturen Cyber-Angriffe melden. Diese müssen letztlich aber auch strafrechtlich verfolgt werden, um langfristig Erfolge im Kampf gegen Cyberkriminalität zu erzielen (vgl. Interview 7).

Bei der Polizei wird bereits deutlich, dass Polizisten eine bessere Ausbildung in dem Bereich benötigen (vgl. Interview 7). Es kann davon ausgegangen werden, dass mit unzureichend ausgebildetem Sicherheitspersonal keine angemessene Strafverfolgung erfolgen kann. Diese Problematik kann unter anderem als Grund für die hohe Dunkelziffer im Bereich Cyberkriminalität betrachtet werden.

Auch die Fähigkeiten der Deutschen Bundeswehr müssen ausgebaut werden, insbesondere im Bereich des Cyberterrorismus (vgl. Interview 5). Im Vergleich mit anderen Ländern sind 60 SoldatInnen im KSA (vgl. Interview 5) eine sehr geringe Anzahl. Insofern kann davon ausgegangen werden, dass die Fähigkeiten der Bundeswehr in der Cyberverteidigung nicht ausreichend sind. Die Bundesministerin der Verteidigung plant hierzu bereits einen weiteren Ausbau (vgl. Bundesministerium der Verteidigung 2015b).

Die mangelnde Verfügbarkeit der hoch qualifizierten Fachkräfte auf dem Arbeitsmarkt und die schlechtere Bezahlung in der Bundesverwaltung im Vergleich zur Wirtschaft (vgl. Interview 5; 6; 7; 8) wirft die Frage auf, wie der vorgesehene Stellenausbau im Rahmen des IT-Sicherheitsgesetztes umgesetzt werden soll. Der Staat steht insofern vor der Herausforderung, Cyber Security in Deutschland zu stärken, jedoch fehlen hierzu die nötigen Fachkräfte auf dem Arbeitsmarkt.

Neben dem personellen Ressourcenmangel konnte auch ein technischer Ressourcenmangel festgestellt werden. Die technische Ausstattung ist insbesondere zur Bekämpfung von Cyber-Angriffen erforderlich, weist aber unter anderem im BND als auch im BKA erhebliche Mängel auf, die nachfolgend zusammengefasst werden (vgl. hierzu Interview 7; Neumann 2014, S. 12).

Technischer Ressourcenmangel

Der Ressourcenmangel hat sowohl einen personellen als auch einen technischen Aspekt. Dies wird von der Bundesregierung in der Digitalen Agenda bereits er-

kannt (vgl. Die Bundesregierung 14, S. 33) und wird an der Ausstattung des BNDs (vgl. Neumann 2014, S. 12), sowie des BKAs (vgl. Interview 7) deutlich. So ist davon auszugehen, dass die schlechte personelle und technische Ausstattung des BNDs bei der Ausgestaltung der Zusammenarbeit mit der NSA eine Rolle spielte. Denn durch die Zusammenarbeit konnten finanzielle Ausgaben gespart werden. In der Folge jedoch hat sich der BND in Abhängigkeit von einem anderen Staat begeben und der NSA dabei geholfen, europäische Unternehmen auszuspähen (vgl. Neumann 2014, S. 12). Aufgrund dessen stellt sich die Frage, ob die Budgeteinsparung im Bereich des BNDs sinnvoll ist. Das Bundeskanzleramt hat bereits einige Defizite in diesem Bereich zugestanden (vgl. Zeit Online 2015b).

Die erheblichen personellen Ressourcenmängel im BKA konnten in Kapitel 4.4.1 aufgezeigt werden. Bei den benötigten Kompetenzen (Know-how) der MitarbeiterInnen konnte ebenfalls ein Verbesserungsbedarf festgestellt werden. So wurde von Interviewpartner 7 (BKA) angegeben, dass nur acht InformatikerInnen mit Bachelorabschluss beschäftigt werden (vgl. Interview 7). In Anbetracht der hohen und weiterhin zunehmenden Cyberkriminalität scheinen weder die Anzahl des Personals noch seine Kompetenzen ausreichend. Die Beauftragung von externen Dienstleistern durch Bundesministerien und Bundesämter sowie der Bundeswehr kann als Folge des personellen und technischen Ressourcenmangels gesehen werden. Hierauf wird nun näher eingegangen.

Externe Dienstleister

Bundesministerien und Bundesämter beauftragen bereits externe Dienstleister, wofür der personelle und technische Ressourcenmangel unter anderem als Grund zu nennen ist. Als Beispiel kann die Kooperation zwischen der BWI Informationstechnik und der Bundeswehr angeführt werden. Es kann davon ausgegangen werden, dass die BWI Informationstechnik als Leistungsverbund der Bundeswehr, IBM und Siemens ein attraktiverer Arbeitgeber als die Deutsche Bundeswehr ist und dass die

BWI Informationstechnik aus diesem Grund, über bessere personelle Ressourcen verfügt (vgl. BWI Informationstechnik GmbH 2015b).

Die Bundeswehr hat in der Rekrutierung unter anderem das Problem, dass *Hacker* oftmals einem gewissen Klischee entsprechen und in die Strukturen und Organisation der Bundeswehr nicht hineinpassen, so Interviewpartner 5 (BMVg). Die Deutsche Bundeswehr gibt damit allerdings auch die gesamte Verantwortung für die Infrastruktur bis auf die Waffen-IT an einen Dienstleiser ab (vgl. Interview 5). Doch nicht nur die Deutsche Bundeswehr beauftragt externe Dienstleister, auch das AA beauftragt ExpertInnen als Fach- und Zeitkräfte (vgl. Interview 6). Derzeit wird z. B. auch ein Projekt der Stiftung Wissenschaft und Politik von dem AA unterstützt (vgl. Stiftung Wissenschaft und Politik 2015).

Das Vorgehen kann als kritisch betrachtet werden, da somit die direkte Kontrolle über die abgegebenen Aufgaben nicht mehr bei den Bundesministerien und Bundesämtern selbst liegt. Informationen können unerwünscht weitergereicht werden, die in der hier behandelten Thematik im Bereich der Sicherheitspolitik von besonders hoher Bedeutung für Staat, Wirtschaft und Gesellschaft sind. Andererseits ist das IT-System der Bundeswehr durch die BWI Informationstechnik sehr sicher geworden und dient nun als Vorbild für andere europäische Länder (vgl. Interview 9). Die Tatsache, dass neben der Deutschen Bundeswehr auch das BKA externe Dienstleister beauftragt, wirft jedoch auch die Frage auf, ob die Problematik nur im technischen und personellen Ressourcenmangel liegt, oder möglicherweise auch die bereits vorhandenen Kompetenzen der MitarbeiterInnen nicht ausreichend sind (vgl. BWI Informationstechnik GmbH 2015b; Neue Osnabrücker Zeitung 2014). Ein genereller Handlungsbedarf wird auch dadurch offensichtlich, dass sich das BBK zwar mit den möglichen Auswirkungen von Cyber-Angriffen auch hinsichtlich der Erhaltung der Arbeitsfähigkeit des Bundestages im Vorfeld beschäftigt hatte (vgl. Interview 8); nach dem tatsächlichen Eintritt eines solchen Falles, hatte dieser allerdings Probleme, seine Arbeit fortzuführen (vgl. Meiritz und Medick 2015). Aus dem aufgezeigten Ressourcenmangel geht hervor, dass Investitionen erforderlich

sind, wie auch von Interviewpartner 4 (BMVi) bestätigt wird (vgl. Interview 4). Neben den personellen und technischen Ressourcenmängeln ist eine weitere Schwäche die fragmentierte Organisation von Cyber Security der Bundesministerien und Bundesämter wodurch letztlich ein Informationsverlust entsteht. Nachfolgend soll hierauf eingegangen werden.

Fragmentierung und Informationsverlust

In der Fragmentierung von Cyber Security in Deutschland sehen die befragten VertreterInnen der Bundesbehörden Vor- und Nachteile (vgl. Interview 3; 6). So sind dezentrale Netzwerke stabiler, da der Totalausfall eines bestimmten Elementes nicht zum Systemzusammenbruch führt. Allerdings fehlt es an einer koordinierenden Instanz, die letztlich auch Entscheidungen fällt, so Interviewpartner 6 (AA) (vgl. Interview 6). Dies wird bekräftigt durch einen Vertreter aus dem BBK: Demnach wäre eine Institution wünschenswert, die alle Beteiligten aus der Politik und Wirtschaft koordiniert und einen Austausch ermöglicht, der im Cyber-AZ oder beim KRITIS-Rat nur zum Teil festzustellen ist (vgl. Interview 7).

Da die Organisation des Austausches aller Beteiligten einige Mängel aufweist, entsteht hier ein Informationsverlust zwischen den Bundesministerien und Bundesämtern. Dessen Ursache ist in der fragmentierten Organisation der Cyber Security in Deutschland festzustellen (vgl. Interview 3; 7; 8). Denn die Vielzahl der beteiligten und verantwortlichen Organisationseinheiten führt dazu, dass sich teilweise Zuständigkeiten überschneiden, wie dies etwa beim BMWi und dem BMVi festzustellen ist. So befand sich die Zuständigkeit für das Telekommunikationsgesetz beim BMWi in der Zusammenarbeit mit der Bundesnetzagentur und wurde mit Umbenennung des BMVi an dieses übertragen. Das BMWi betrachtet sich aber noch immer als zuständig (vgl. Interview 3), was auch daran liegen kann, dass die Bundesnetzagentur zu dem Geschäftsbereich des BMWi gehört (vgl. Bundesnetzagentur 2015). Dies kann aber auch den Kampf der Bundesbehörden um Ressourcen wiederspiegeln, der auch von Interviewpartner 7 (BKA) bestätigt wird (vgl. Interview 7). Interviewpartner 8 (BBK) ist der Auffassung, dass es keine klare Aufgabentei-

lung gebe, sodass verschiedene Institutionen sich die Aufgaben gegenseitig zuschieben (vgl. Interview 8). Hierdurch kann es zu Doppelarbeit kommen oder auch dazu, dass Aufgaben gar nicht wahrgenommen werden, wenn eine Bundesbehörde davon ausgeht, dass eine andere Bundesbehörde die Aufgabe bereits wahrnimmt. Hierdurch zeigen sich neben organisatorischen Mängeln auch administrative und strategische Schwächen als mögliche Ursache des Informationsverlustes, da keine klaren Vorgaben gemacht werden.

Der Informationsverlust wird aber nicht von allen Bundesministerien und Bundesämtern bestätigt, so sieht gerade Interviewpartner 1 (BMI) diesen nicht, da eine enge Verzahnung der Bundesministerien, Bundesämter und Unternehmen durch das Cyber-AZ bestehen würde. Doch gerade das BMI, zu dessen Geschäftsbereich viele Sicherheitsbehörden gehören – wie auch das BSI und dem dazugehörigen Cyber-AZ – erkennt hier nicht, dass einige VertreterInnen der Bundesbehörden einen Informationsverlust bestätigen (vgl. Interview 3; 7; 8). Diese äußern zum Teil auch den Wunsch nach einer Verbesserung in der Zusammenarbeit mit dem nationalen Cyber-AZ (vgl. Interview 3; 4). Interviewpartner 5 (BMVg) äußert erhebliche Kritik darüber, dass die Anzahl von 15 festen MitarbeiterInnen zu gering sei, um einen Mehrwehrt für Cyber Security leisten zu können (vgl. Interview 5).

Um den hier festgestellten Informationsverlust zu beheben, wird wiederum auch eine Änderung der föderalen Strukturen als Lösung erwähnt (vgl. Interview 4). Insgesamt sind somit die Entscheidungsprozesse und die Koordination effizienter zu gestalten. Weiterhin konnte aufgezeigt werden, dass ein personeller und technischer Ressourcenmangel in den Bundesministerien und Bundesämtern besteht und hier ein Handlungsbedarf festgestellt wird. Letztlich lässt sich aber feststellen, dass zukünftig alle Bundesministerien und Bundesämter sich verstärkt für ihre Aufgaben im Bereich Cyber Security einsetzen wollen.

5 Cyber Security in der Wirtschaft

Jedes deutsche Unternehmen ist einer potenziellen Bedrohung durch Cyber-Angriffe ausgesetzt (vgl. Bundesamt für Sicherheit in der Informationstechnik 2012, S. 5). Viele Unternehmen sind jedoch auf diese neuen Bedrohungen nicht vorbereitet und haben in Zusammenhang mit ihrem IT- und Informationsmanagement erheblichen Nachholbedarf (vgl. Deutscher/ Bohmayr/ Yin und Russo 2014, S. 3). So hat die deutsche Wirtschaft jährlich durch Cyberspionage Schäden in Milliardenhöhe zu verzeichnen (vgl. KPMG 2013, S. 8-9). Eine Studie von Corporate Trust Business Risk & Crisis Management zeigte 2012, dass die Schäden nicht nur durch Hackerangriffe von außen, sondern oftmals intern durch eigene MitarbeiterInnen oder GeschäftspartnerInnen verursacht werden (vgl. Corporate Trust Business Risk & Crisis Management GmbH 2012, S. 8). Mittlerweile ist jedoch die Spionage durch ausländische Nachrichtendienste zu einer der größten Cyberbedrohungen in der Wirtschaft geworden (vgl. Corporate Trust Business Risk & Crisis Management GmbH 2014). Dies äußert sich unter anderem durch die Tatsache, dass seit der NSA-Affäre jedes dritte Unternehmen seine IT-Sicherheit überprüft hat (vgl. Spiegel Online 2013a).

Insofern hat sich die Wirtschaft durch die Digitalisierung erheblich verändert, indem z. B. Produktionsprozesse vernetzt werden. Hieraus ergeben sich dann neue Möglichkeiten, durch Cyberspionage Informationen über Entwicklungen und Innovationen zu erhalten, oder durch Cybersabotage die Produktion zu stören oder zerstören. Dadurch können andere Staaten sich Wettbewerbsvorteile verschaffen, indem sie z. B. ihre Nachrichtendienste mit Industriespionage beauftragen. Dieser Gefahr sind deutsche Unternehmen täglich ausgesetzt. Darüber hinaus spielt die Verwendung von den gesammelten und verknüpften Daten der Unternehmen eine zunehmend vordergründige Rolle. Für die große Datenmenge, die immer leichter anzusammeln ist, ist der Begriff *Big Data* entstanden. Die Herausforderung von Big

Data besteht darin, aus den Daten nutzbares Wissen zu generieren. Für das Sammeln und die Auswertung von Daten werden wiederum neue Dienstleistungen und Produkte benötigt (vgl. Die Bundesregierung 2015a).

Für die Branchen der Maschinen- und Anlagenbau, Elektrotechnik, Automobilbau, chemische Industrie, Informations- und Kommunikationstechnologien und Landwirtschaft entstehen neue Wertschöpfungsketten. Durch die Vernetzung der Produktion und der Produkte wird für 2025 ein Wertschöpfungspotenzial von 78 Millionen für Deutschland erwartet (vgl. BITKOM und Fraunhofer IAO 2014, S. 5). Mittlerweile spricht man von einer vierten industriellen Revolution, der Industrie 4.0 (vgl. Zypries 2014). Neben dem erforderlichen Breitbandausbau werden dabei Standards auf der Technologie- und Anwendungsseite sowie der Datenschutz weiterhin an Bedeutung gewinnen (vgl. BITKOM und Fraunhofer IAO 2014, S. 5). Dieses Ergebnis wurde auch auf dem World Economic Forum 2014 präsentiert, bei dem Datenschutz eine wichtige Rolle einnahm. Die Länder wurden dazu aufgefordert, mehr für den Datenschutz zu tun. Neben dem Datenschutz ist aber auch die Sicherheit der IKT-Systeme im Hinblick auf die Förderung von Industrie 4.0 noch eine große Herausforderung für die Unternehmen.

„Die Sicherheit der Informations- und Kommunikationssysteme der Industrie 4.0-Technologien stellt – gerade im Kontext aktueller Diskussionen über Industriespionage – den relevanten Faktor bei der Ausgestaltung von Systemen dar." (BITKOM und Fraunhofer IAO 2014, S. 7). Cyber Security ist also eine der Voraussetzungen für die Umsetzung von Industrie 4.0 (vgl. BITKOM und Fraunhofer IAO 2014, S. 37). Dabei liegt die Herausforderung in dem Schutz der neuen Produktionssysteme und auch der Notwendigkeit, innerhalb der Wertschöpfungskette Cyber Security herzustellen. Für Unternehmen ist Cyber Security also durch den hohen Vernetzungsgrad auch bei ihren Dienstleistern von erheblicher Bedeutung (vgl. Wissenschaft und acatech – Deutsche Akademie der Technikwissenschaften e.V. 2013, S. 50). Diese Bedeutung wird weiterhin zunehmen, um Industrie 4.0 zu fördern, aber auch um das „Digitale Wachstumsland Nr. 1" in Europa zu werden. Um

dieses Ziel zu erreichen bestehen noch Herausforderungen in der Entwicklung von sicheren IT-Systemen.

Wie erwähnt, formuliert die Bundesregierung in ihrer Digitalen Agenda das Ziel, zum digitalen Wachstumsland Nr. 1 in Europa aufzusteigen (vgl. Die Bundesregierung 2015a). Es sei notwendig, dass die internationalen deutschen Unternehmen „[...] marktfähige und sichere Technologien entwickeln und Standards bei wichtigen digitalen Anwendungen setzen, um Deutschland gleichzeitig zum Leitanbieter für intelligente Produktion und Logistik und Leitmarkt für intelligente Produkte zu machen und wettbewerbsfähig zu bleiben“ (Die Bundesregierung 2015a). Die mittelständischen und kleinen Unternehmen sollen hierbei eine besondere Unterstützung erhalten, damit auch sie ihre Innovationsfähigkeit in der Anwendung und Entwicklung neuer Technologien ausbauen können. Dies bedarf einer Unterstützung für alle Unternehmen durch Dialoge und unter anderem durch Förderung von Forschungstätigkeiten der Unternehmen (vgl. Die Bundesregierung 2015a). Seitens der Regierung wird durch das Bundesministerium für Bildung und Forschung unter anderem Forschungsarbeit im Bereich IT-Sicherheit in der Wirtschaft betrieben (vgl. Bundesministerium für Bildung und Forschung 2015). Die Förderung von Forschungstätigkeiten durch die Politik benötigt eine gute Zusammenarbeit von Politik und Wirtschaft.

Für die Zusammenarbeit von Politik und Wirtschaft gibt es, wie bereits dargelegt, unter anderem die Allianz für Cyber-Sicherheit (vgl. Bundesamt für Sicherheit in der Informationstechnik 2015b), den UP KRITIS-Rat (vgl. Bundesamt für Sicherheit in der Informationstechnik und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2011-2013b), den vom BKA initiierten Public Private Partnership German Competence Center Against Cyber Crime (vgl. German Competence Center against Cyber Crime e. V. 2015) und die Initiative des Bundesministeriums für Wirtschaft und Energie namens IT-Sicherheit in der Wirtschaft (vgl. Bundesministerium für Wirtschaft und Energie 2015a).

Im weiteren Verlauf sollen exemplarisch ausgewählte Unternehmen dargestellt werden. Es sollen unter anderem ihr Umgang mit Cyber Security, ihre Einschätzungen zu Cyber Security in Deutschland und ihre Bewertung der Zusammenarbeit mit der Politik im Bereich Cyber Security erläutert werden. Dazu wurde die Deutsche Telekom AG als eines der führenden Telekommunikationsunternehmen in Deutschland ausgewählt, die als Betreiber Kritischer Infrastrukturen für das hier behandelte Thema von besonderer Bedeutung ist. Die Open Grid Europe wurde als ein Betreiber Kritischer Infrastrukturen im Bereich der Energieversorgung ausgewählt und als exemplarischer Vertreter eines der Schlüsselindustrien in Deutschland wurde die Daimler AG ausgewählt.

5.1 Deutsche Telekom AG

Die Deutsche Telekom AG ist in mehr als 50 Ländern mit insgesamt 228.000 MitarbeiterInnen vertreten und mit 151 Millionen Mobilfunk-KundInnen, 30 Millionen Festnetz- und mehr als 17 Millionen Breitbandanschlüssen der führende Telekommunikationsanbieter in Europa und weltweit eines der führenden integrierten Telekommunikationsunternehmen (vgl. Deutsche Telekom AG 2015). Damit gilt die Deutsche Telekom AG als Betreiber von Kritischen Infrastrukturen in Deutschland (vgl. Bundesministerium des Innern 2009, S 5). Deutschlandweit gibt es 1.500 MitarbeiterInnen, die für die Sicherheit verantwortlich sind. Davon sind 400 MitarbeiterInnen im grundlegenden Sicherheitsbereich (inklusive PersonenschützerInnen) und von diesen wiederum 200 im Bereich Cyber Security tätig. Die MitarbeiterInnen werden von der Deutschen Telekom AG überwiegend selbst ausgebildet, da es auf dem Arbeitsmarkt schwierig ist, entsprechende Kompetenzen zu erhalten. Interviewpartner 10 (Deutsche Telekom AG) zufolge, gebe es auf dem Arbeitsmarkt zwar InformatikerInnen, BetriebswirtschaftswissenschaftlerInnen und IngenieurInnen, diese hätten jedoch nicht das nötige Know-how für Cyber Security (vgl. Interview 10).

Die Bedrohungen für Unternehmen durch Cyber-Angriffe wird von Interviewpartner 10 (Deutsche Telekom AG) weltweit als kontinuierlich steigend eingeschätzt – davon sei auch die Deutsche Telekom AG betroffen. Dies wird mit dem allgemein zunehmenden Vernetzungsgrad begründet (vgl. Interview 10). Eine große Krise hatte die Deutsche Telekom AG 2008 erlitten, als Datendiebstähle bekannt wurden. Insofern steht auch die Deutsche Telekom AG vor der Herausforderung, sich vor Cyber-Angriffen zu schützen (vgl. Interview 10).

Die Datendiebstähle lösten daraufhin in der Deutschen Telekom AG ein neues Sicherheitsbewusstsein aus und Cyber Security wurde in der Deutschen Telekom in drei Säulen aufgebaut: 1) der Eigenschutz des Unternehmens, 2) Sicherheit der Produkte und der Marke und 3) mit Sicherheit als kommerzielles Angebot. Für die Deutsche Telekom AG bedeutet dies aber auch, Sicherheit und Datenschutz anzubieten. Um dies umzusetzen, ist es laut Interviewpartner 10 (Deutsche Telekom AG) unter anderem wichtig, bei der Entstehung von neuen Produkten, die Sicherheit von Anfang an zu integrieren. Letztlich muss jedes Produkt weiterhin nach Schwachstellen getestet werden. Die Deutsche Telekom AG bezahlt eine Prämie (Bug Bonty Programm), wenn Sicherheitslücken entdeckt und gemeldet werden. Es werden außerdem für die Software auch immer wieder Updates erstellt. Darüber hinaus müssen bei der Außerbetriebnahme eines IT-Systems die Daten vernichtet werden. Der Ansatz *never touch a running system* wird hier als die falsche Vorgehensweise bewertet (vgl. Interview 10).

Aufgrund des Telekommunikationsgesetztes ist die Deutsche Telekom AG bereits verpflichtet, Cyber-Angriffe zu melden. Aus Sicht von Interviewpartner 10 (Deutsche Telekom AG) haben Angriffe nur Erfolg durch schlecht konfigurierte Systeme und Systeme mit fehlenden Updates. An dieser Stelle übt der Interviewte Kritik am IT-Sicherheitsgesetz. Die Hersteller der IT-Systeme müssten ebenfalls zur Verantwortung gezogen werden, regelmäßige Updates zur Verfügung zu stellen. Ohne dass die Hersteller diese zur Verfügung stellen, können Anwender Sicherheitslücken in ihren IT-Systemen nicht beheben. Insofern werden Benutzer und Be-

treiber vernachlässigt, sodass diesbezüglich Rahmenbedingungen von der Politik zu setzen wären (vgl. Interview 10).

Als Telekommunikationsanbieter ist die Deutsche Telekom AG dem Telekommunikationsgesetz (§§ 110 ff. TKG) unterstellt. Das bedeutet unter anderem, dass sie Sicherheitsbehörden Auskünfte erteilen oder Überwachungsmaßnahmen ermöglichen müssen. Hierfür sind insgesamt 40 MitarbeiterInnen an den Standorten Berlin, Hannover, Frankfurt am Main und Münster zuständig. Hierunter fällt auch die Zusammenarbeit mit dem BND. Diesem muss sie unter anderem den Zugang zu den Räumlichkeiten der Deutschen Telekom AG ermöglichen. Dieses geschieht laut der Deutschen Telekom AG nur, wenn die rechtlichen Voraussetzungen erfüllt sind (vgl. Deutsche Telekom AG 2015b).

Eine Zusammenarbeit mit weiteren Sicherheitsbehörden und Unternehmen findet im UP KRITIS statt, der als positiv bewertet wird, da die Betreiber Kritischer Infrastrukturen sich daran aktiv beteiligen, so Interviewpartner 10 (Deutsche Telekom AG). Von der Politik wird allerdings in diesem Rahmen gefordert, dass sie mehr Bewusstsein für die Thematik schafft. Dies werde zwar mit der Allianz für Cybersicherheit versucht, allerdings sei noch keine Breitenwirkung festzustellen und Bemühungen würden wirkungslos bleiben (vgl. Interview 10).

Eine weitere Zusammenarbeit gibt es mit dem BSI. Die Deutsche Telekom AG hat ein CERT und ein Lagezentrum, wie auch das BSI; von der Größe und Kompetenz sei jenes der Deutschen Telekom AG ähnlich gut aufgestellt, weshalb es hierüber schneller Informationen beziehen kann als vom BSI, wie Interviewpartner 10 (Deutsche Telekom AG) berichtet. Das CERT der Deutschen Telekom AG bearbeitet im Monat rund 400 neue Schwachstellenmeldungen zu Standard Softwareprodukten. Sich vor der Wirtschaftsspionage von ausländischen Nachrichtendiensten zu schützen, ist auch der Deutschen Telekom AG nicht möglich. Dies ist darauf zurückzuführen, dass Nachrichtendienste über umfangreiche Möglichkeiten und Fähigkeiten verfügen sowohl national als auch international. Vor diesem Hinter-

grund wäre laut Interviewpartner 10 (Deutschen Telekom AG) eine „Digital Border Control“ auf europäischer Ebene erstrebenswert (vgl. Interview 10).

Das BSI hat laut Interviewpartner 10 (Deutsche Telekom AG) nicht die nötigen Ressourcen, um Unternehmen beim Schutz gegen Angriffe aus dem Cyberraum ausreichend beraten zu können. Hingegen wird die Leistung des BSI auf Ebene der Bundesverwaltung als handlungsfähig eingeschätzt, obgleich für die Beratung der Wirtschaft die Ressourcen ausgebaut werden müssten. An dem Cyber-AZ wird kritisiert, dass keine Verbindung mit WirtschaftsvertreterInnen oder Infrastrukturbetreibern besteht. Insgesamt wird die Zusammenarbeit der Deutschen Telekom AG mit dem BSI aber als gut bewertet. Dies gilt auch für die Zusammenarbeit mit dem BKA und den Landeskriminalämtern, welche über sehr kompetente ExpertInnen verfügen würden. Mit dem BMI gebe es ebenfalls eine gute Zusammenarbeit (vgl. Interview 10).

Interviewpartner 10 (Deutschen Telekom AG) ist der Auffassung, dass nicht die Politik, sondern die Hersteller von Software-Produkten die Verantwortung für Cyber Security tragen. Hierfür werden von der Politik Rahmenbedingungen gefordert, in Form von Haftungsbedingungen für Softwarehersteller. Es wäre wünschenswert gewesen, die Haftungsbedingungen in das IT-Sicherheitsgesetz aufzunehmen (vgl. Interview 10).

Der Breitbandausbau in Deutschland von 50Mbit/s ist bis 2018 geplant. Der Ausbau von 50/Mbit/s wird von Interviewpartner 10 (Deutsche Telekom AG) als ausreichend eingeschätzt (vgl. Interview 10). Da der Ausbau kein staatliches Monopol mehr ist, investiert die Deutsche Telekom AG seit Jahren in den Ausbau, besonders in ländlichen Gebieten, die noch über keine flächendeckende Versorgung verfügen (vgl. Deutsche Telekom AG 2014b).

Die Deutsche Telekom AG setzt sich für Cyber Security ein und richtet zusammen mit der Münchner Sicherheitskonferenz jährlich den Cyber Security Summit aus. Im Jahr 2014 fand die dritte Konferenz mit VertreterInnen aus Politik und Wirtschaft statt. Auf den Konferenzen sollen in Diskussionen und Arbeitsgruppen

Strategien für einen sicheren Cyberraum entwickelt werden (vgl. Cyber Security Summit – telekom.com 2014). Die Themenschwerpunkte lagen 2012 bei der Cyberkriminalität und 2013 auf Wirtschaftsspionage (vgl. Deutsche Telekom AG 2014a). Diese Thematik wurde auch 2014 wieder aufgenommen und die Konferenz beschäftigte sich mit der NSA-Affäre. Anlassbezogen wurde auch die Ukraine-Krise thematisiert, in der die Verbreitung von Propaganda über das Internet eine große Rolle spielt. Allgemein ist zu beobachten, dass der Terrorismus von der Entwicklung des Internets profitiert hat, beispielsweise rekrutiert der Islamische Staat (IS) neue Anhänger über das Internet (vgl. Diersch 2015, S. 133-134).

Für die Zukunft hat die Deutsche Telekom AG ein Zehn-Punkte-Programm zum Schutz vor Cyber-Angriffen aufgestellt. Dabei setzt sie mehr auf die Zusammenarbeit mit Unternehmen, der Politik und den europäischen Ländern. Überdies wurden Hunderte MitarbeiterInnen zu IT-SicherheitsexpertInnen qualifiziert. Die zukünftige digitale Entwicklung sei aber durch Cyberüberwachung und Cyberkriminalität bedroht (vgl. Telekom 2015).

5.2 Open Grid Europe

Der Erdgastransporteur Open Grid Europe wurde 2004 als Tochter von E.ON unter dem Namen E.ON Gastransport gegründet. Erst 2010 wurde das Unternehmen als Open Grid Europe eine unabhängige Netzbetreibergesellschaft. Mit 1650 MitarbeiterInnen, 450 internationalen und nationalen Kunden sowie einem 12.000 Kilometer langen Ferngasleitungsnetz ist es zu Deutschlands führendem Erdgastransporteur aufgestiegen (vgl. Open Grid Europe 2015b). Die Netze gehören zum Teil Leitungsgesellschaften, an denen Open Grid Europe mit weiteren Partnerunternehmen Anteile besitzt. Des Weiteren hat Open Grid Europe Anteile an Dienstleistungsunternehmen für den Erdgastransport (vgl. Open Grid Europe 2015a).

Open Grid Europe ist als Erdgastransporteur in Deutschland Energieversorger und somit ein Betreiber Kritischer Infrastrukturen (vgl. Bundesministerium des Innern 2009, S. 5). Open Grid Europe beschäftigt einen Teamleiter und zwei Mitar-

beiterInnen für Cyber Security, da der gesamte Bereich an den externen Dienstleister Hewlett-Packard (HP) abgegeben wurde. Der gesamte Infrastrukturbetrieb ist bei HP, mit der ein vertraglicher Basisschutz gegen klassische Cyber-Angriffe besteht (vgl. Interview 11).

Die MitarbeiterInnen und die Technik von Open Grid Europe könnten die IT-Sicherheit mangels Ressourcen nicht übernehmen, wie ein interviewter Vertreter von Open Grid Europe (Interviewpartner 11 (Open Grid Europe)) angibt. Zum einen sei es schwierig, MitarbeiterInnen zu finden, da diese von den großen Unternehmen angeworben werden, und zum anderen könnte Open Grid Europe kein Monitoring betreiben, wie es von HP durchgeführt wird. HP verfügt darüber hinaus über eine weltweite Server-Infrastruktur.

Die Zusammenarbeit mit HP sei in den Zeiten als Open Grid Europe noch zu E.ON gehörte nicht sehr gut gewesen. Seit der Unabhängigkeit sei diese besser geworden und es gibt beispielsweise einen wöchentlichen Jour fixe (vgl. Interview 11). Dennoch würde Open Grid Europe für die Zukunft gerne intern selbständiger der Thematik Cyber Security nachgehen können und nicht nur abhängig vom Dienstleister HP sein, sondern die Lage selbst beurteilen können. Bisher ist das Unternehmen für die Umsetzung zu klein und hat dadurch zu wenige Ressourcen. In der Open Grid Europe werden aber die neuesten Entwicklungen im Markt aufmerksam verfolgt (vgl. Interview 11).

Laut Interviewpartner 11 (Open Grid Europe) haben sich die Angriffe auf Kritische Infrastrukturen in den letzten Jahren verändert. Das würde auch im UP KRITIS-Rat berichtet, an dem Open Grid Europe teilnimmt. Das Unternehmen selbst hatte allerdings keine diesbezüglichen Erfahrungen zu verzeichnen. Generell seien die Cyber-Angriffe sehr professionell geworden. Für Open Grid Europe bestehe ständig die Gefahr, dass das Gasnetz angegriffen werde. Daher sei es wichtig, das IT-System ständig nach Sicherheitslücken zu untersuchen. Dabei sei die Täterermittlung sehr schwer und oftmals werde ein Angreifer im IT-System erst spät entdeckt: Die Angreifer sehen sich meist erst das IT-System der Firma an, indem sie

sich verdeckt verhalten; oftmals bleiben Angriffe auch unbemerkt. Als Schutzmechanismus setze Open Grid Europe unter anderem ganz normale Firewalls ein. Das Netz sei relativ stabil nach außen, das Problem überwiege bei Cyber-Angriffen von innen. Open Grid Europe sei bereits gesetzlich dazu verpflichtet, Cyber-Angriffe zu melden (vgl. Interview 11). Intern gibt es ein Informationssicherheitsgremium, an dem viele Fachbereiche teilnehmen. Auf Führungsebene sei jedoch noch ein zu unsensibler Umgang mit der Thematik Cyber Security festzustellen, der verbessert werden müsse, so Interviewpartner 11 (Open Grid Europe).

Cyber Security ist für Open Grid Europe von hoher Bedeutung, weshalb auch Handlungsempfehlungen von Bundesbehörden umgesetzt werden würden. Interviewpartner 11 (Open Grid Europe) kritisiert daran aber, dass es keinen operativen Austausch mit der Politik gebe. So gebe es mit dem BSI keine direkte Zusammenarbeit, was für Open Grid Europe jedoch wünschenswert wäre. Über den UP KRITIS-Rat gibt es zwar eine Zusammenarbeit, jedoch wäre ein direkter Ansprechpartner erstrebenswert, mit dem ein bis zwei Treffen im Jahr stattfinden würden. Denn jede Branche habe spezielle Anliegen, die mit einem direkten Ansprechpartner vom BSI besser ausgetauscht werden könnten. Ferner würden Informationen über Cyber-Angriffe vom BSI nicht zeitnah gemeldet werden und entsprechende Meldeketten seien noch nicht ausreichend umgesetzt worden. Insgesamt wünsche sich Open Grid Europe von dem BSI eine aktivere Rolle. Mit dem BBK gebe es in Branchenarbeitskreisen eine gute Zusammenarbeit, ebenso mit der Bundesnetzagentur. In Gremien werde auch mit dem BMWi zusammengearbeitet, die direkte Zusammenarbeit erfolge dann aber mit der Bundesnetzagentur (vgl. Interview 11).

Der UP KRITIS-Rat wird von Interviewpartner 11 (Open Grid Europe) scharf kritisiert, da die Bundesbehördenvertretungen unter anderem unvorbereitet in den Sitzungen erscheinen würden. Es gebe viele Gespräche innerhalb des UP KRITIS-Rat wie eine Zusammenarbeit mit den Betreibern und den VertreterInnen aus der Politik funktionieren könnte. Die Bereitschaft der VertreterInnen der Politik sei allerdings nicht sehr groß. Diese würden die Diskussionen und Vorschläge der Be-

treiber lediglich anhören, aber letztlich nicht ausreichend darauf eingehen und diese umsetzen. Die Politik, so fordert Interviewpartner 11 (Open Grid Europe), müsse mit den Unternehmen sensibler umgehen. So ließe beispielsweise das IT-Sicherheitsgesetz offen, inwiefern eine Meldung von Cyber-Angriffen anonymisiert von den Bundesbehörden behandelt wird. Der UP KRITIS-Rat sei sehr wichtig, die Umsetzung sei aber zögerlich. Dies sei darauf zurückzuführen, dass im UP KRITIS-Rat und auch generell in der Cybersicherheitspolitik ein Leitbild fehle (vgl. Interview 11).

Weitere Kritik an der Politik wird von Interviewpartner 11 (Open Grid Europe) an dem Breitbandausbau in Deutschland geäußert. Hier würde Deutschland weit zurück liegen, obwohl dieser dringend erforderlich ist. Auf europäischer Ebene wird kritisiert, dass bisher zu wenige Vorgaben für die Mitgliedsländer bestehen würden. Es seien internationale Rahmenbedingungen notwendig, wie z. B. die NIS-Richtlinie, welche auf europäischer Ebene schon umgesetzt werden konnte (vgl. Interview 11).

5.3 Daimler AG

Daimler AG ist einer der weltweit größten Automobilkonzerne. Mit den Geschäftsfeldern Mercedes-Benz Cars, Daimler Trucks, Mercedes-Benz Vans, Daimler Buses und Daimler Financial Services ist die Daimler AG der größte Premium-PKW-Anbieter und weltweit der größte Nutzfahrzeuganbieter. Die Fahrzeuge und Dienstleistungen werden fast weltweit vertrieben. Die Produktion findet in Europa, Südamerika, Asien und Afrika statt. Der Konzern beschäftigt insgesamt 279.972 MitarbeiterInnen (vgl. Daimler AG 2015). Aufgrund dieser Bedeutung in der Automotive-Branche und da diese Branche zu den deutschen Schlüsselindustrien zählt (vgl. Manager Magazin 2010) soll nachfolgend die Cyber Security in der Daimler AG betrachtet werden.

Cyber Security ist bei der Daimler AG dem Bereich der Unternehmenssicherheit zugeordnet. Mit dem Thema beschäftigen sich unterschiedliche Bereiche

und MitarbeiterInnen, da es aus Sicht der Daimler AG nicht richtig ist, wenn die Verantwortung nur bei einer Abteilung liegt. Zu den Abteilungen und Bereichen gehören Governance, Prävention, IT, Entwicklung, Corporate Security und Datenschutz, wobei die Sicherheit der Kundendaten im Interview betont wird (vgl. Interview 12).

MitarbeiterInnen stellen ein Sicherheitsrisiko dar, weshalb besonders im Entwicklungs- und Vorstandsbereich nur bestimmte Personen Zugang zu sensiblen Informationen erhalten. Die Bereiche, die eine hohe Priorität für die Daimler AG haben, werden vor Cyber-Angriffen besonders geschützt: Personendaten (aus den Fahrzeugen der KundInnen), Fahrzeugdaten, Forschung und Entwicklung, Finanzdaten, Vertrieb und Produktionsplanung. Datenschutz ist hierbei eine der Herausforderungen, die von den schwer zu kontrollierenden IT-Systemen ausgehen. Cyber-Angriffe erfolgen meist in Form von Manipulation durch das Eindringen in die Systeme, um dort eine Veränderung vorzunehmen. Davon sind insbesondere Computer der Produktion betroffen. Die Cyber-Angriffe werden von der Daimler AG an staatliche Behörden nicht gemeldet. Dies würde sich durch das IT-Sicherheitsgesetz aber ändern, wie Interviewpartner 12 (Daimler AG) bestätigt, da die Daimler AG auch ein Telefonanbieter sei (vgl. Interview 12). Denn die Fahrzeuge sind zum Teil mit einem Telekommunikationssystem ausgestattet.

Die Daimler AG setzt zur Erkennung von Cyber-Angriffen Virenscanner ein und nutzt die klassische Firewall. Die MitarbeiterInnen stellen aber, wie bereits erwähnt, eines der größten Sicherheitsrisiken im Rahmen der Cyber Security dar. Um dagegen vorzugehen, müsste bei den MitarbeiterInnen mehr *awareness* geschaffen werden, durch die Klassifizierung von Informationen, Schulungen, vertragliche Verpflichtung, Sensibilisierung und die Möglichkeit der Strafbarkeit, wie Interviewpartner 12 (Daimler AG) fordert. *Awareness* bei den MitarbeiterInnen zu schaffen, sei oftmals schwierig zu vereinbaren mit der *user convenience*. Dies zeige sich in der Nutzung von iPhones, die verwendet werden, obwohl sie keine Kryptotechnologie zulassen.

Aber nicht nur bei den MitarbeiterInnen sei eine Verankerung des Bewusstseins für Cyber Security notwendig, sondern im gesamten Prozess von der Produktion bis zum Kunden. Eine weitere Herausforderung ginge von Zulieferern aus. So könne es passieren, dass bei den Zulieferern Viren eingebaut werden, die dann bis zum Kunden gelangen können (vgl. Interview 12).

Auf politischer Ebene gebe es eine immer bessere Zusammenarbeit mit dem BKA, den Landeskriminalämtern und dem BSI. Dennoch komme das BSI seinen Aufgaben nicht nach, da es zu wenig koordiniert und zentralisiert sei. Das BSI müsste sich vielmehr zu einer operativen Einheit entwickeln. So würden Informationen z. B. zu Cyber-Angriffen teilweise erst zwei Wochen später weitergeleitet. Deshalb sei im Informationsaustausch eine dringende Verbesserung notwendig. Insgesamt müsse das Handeln der Politik in dieser Thematik deutlich agiler werden (vgl. Interview 12). In der Zusammenarbeit mit Cybervereinen, -verbänden und -organisationen sei die Daimler AG eher zurückhaltend. Ein Austausch bestehe allerdings mit dem ASW-Bundesverband, der BITKOM und dem Verband der deutschen Autoindustrie (vgl. Interview 12).

Für die Standorte im Ausland hat Daimler AG spezielle regionale MitarbeiterInnen, da diese vor Ort besser vernetzt seien. Aus der Sicht von Interviewpartner 12 (Daimler AG) ist die Sicherheitslage im Bereich Cyber Security im Ausland nicht besser als in Deutschland. In den USA stelle sich allerdings die Frage, ob der Staatsschutz von der Industrie getrennt wird. Die Daimler AG habe keine Chance, sich gegen die Cyberspionage amerikanischer Geheimdienste zu schützen (vgl. Interview 12).

Zurzeit würde Cyber Security von den Unternehmen vorangetrieben werden, so Interviewpartner 12 (Daimler AG). Die Politik müsse allerdings die Gewährleistung von Cyber Security übernehmen, indem sie Rahmenbedingungen schafft und somit einen stärkeren Wirtschaftsschutz erzielt. Außerdem sollte die Politik die Forschung im Bereich Cyber Security mehr unterstützen. Zunächst müsse hierzu überhaupt ein Feld geschaffen werden, indem Forschung ermöglicht werden kann.

Insbesondere sollen innovative Unternehmen in dem Bereich unterstützt werden und Hochschulen sollten mehr Fördergelder erhalten und aktiver in dem Bereich werden. Unternehmen und gerade große Konzerne sind bereits sehr aktiv in diesem Bereich, weshalb dies auch von der Politik zu wünschen sei. Auch bei der Aufklärung der BürgerInnen durch die Politik bestünde ein großer Bedarf (vgl. Interview 12).

Für die Zukunft plant Daimler AG, das Thema in Teilbereiche zu gliedern und damit eine Kulturveränderung im Unternehmen einzuleiten. Nicht nur InformatikerInnen sollen für die IT-Sicherheit verantwortlich sein, sondern die unterschiedlichen Kompetenzen der MitarbeiterInnen sollen einbezogen werden. Dabei soll der Fokus auf Analysen gelegt werden, um die Cyber-Angriffe und ihre Herkunft besser bestimmen zu können. Daneben soll die Zusammenarbeit mit der Politik weiter fortgesetzt werden, welche davon jedoch den größeren Mehrwert habe, denn dadurch erfahre die Politik, was die Industrie benötigt. Generell sollte eine Balance zwischen Politik und der Wirtschaft angestrebt werden und Unternehmen sollten nicht mit administrativen und gesetzlichen Vorgaben behindert werden. Ein sensibleres Vorgehen der Politik sei nützlich für die Zusammenarbeit (vgl. Interview 12).

5.4 Diskussion der Cyber Security in der Wirtschaft

Die hier analysierten Unternehmen sind sowohl der ständigen Bedrohung von, als auch realen Cyber-Angriffen ausgesetzt (vgl. Interview 10; 11; 12). Sie schützen sich zwar vor Cyber-Angriffen, jedoch sind Verbesserungen notwendig. Zu den erforderlichen Verbesserungen zählen beispielsweise die Reduzierung der Anzahl der unbemerkten Angriffe (vgl. Interview 11) oder die Schaffung von mehr Bewusstsein und Aufmerksamkeit (awareness) bei den MitarbeiterInnen im Umgang mit IT-Systemen und Daten (vgl. Interview 12).

Auch in der Zusammenarbeit mit der Politik sehen alle drei Unternehmen Verbesserungsmöglichkeiten. Kritik erhält vor allem das BSI: Es könne seinen Auf-

gaben nicht ausreichend nachkommen (vgl. Interview 12) und verfüge über zu wenig Personal, um die Unternehmen entsprechend zu beraten (vgl. Interview 10). Zudem werden Cyber-Angriffe teilweise erst zwei Wochen später an Unternehmen weitergeleitet, die von diesen Angriffen betroffen sein könnten (vgl. Interview 10; 11; 12). Große Unternehmen haben somit ihre eigenen CERT-Lagezentren, die in der Lage sind, Cyberbedrohungen schneller zu bemerken als sie ihnen übermittelt werden (vgl. Interview 10; 12), während kleinere Unternehmen nicht über diese Mittel verfügen und sich auch eine intensivere operative Zusammenarbeit mit dem BSI wünschen würden (vgl. Interview 11). So besteht z. B. keine direkte Zusammenarbeit zwischen dem größten Erdgastransporteur in Deutschland und dem BSI (vgl. Interview 11). Da dem Schutz Kritischer Infrastrukturen eine besondere Bedeutung zukommt, wäre eine intensivere Zusammenarbeit mit dem BSI förderlich, die den spezifischen Bedürfnissen einzelner Branchen nachkommt (vgl. Interview 11). Open Grid Europe ist ein Beispiel dafür, dass die Zusammenarbeit mit Unternehmen noch weiter ausgebaut werden müsste, das BSI aber nicht über die hierzu notwendigen Ressourcen verfügt, wie in Kapitel 4.1.2 ausgeführt.

Die Zusammenarbeit im UP KRITIS-Rat wird von den Betreibern Kritischer Infrastrukturen zum Teil positiv bewertet (vgl. Interview 10), auf der anderen Seite auch kritisiert, da BehördenvertreterInnen nicht regelmäßig erscheinen würden und Entscheidungsprozesse aufgrund eines fehlenden Leitbildes langwierig sein können (vgl. Interview 11).

Ferner wünschen sich die Unternehmen von der Politik auch einen sensibleren Umgang sowie weniger administrative Auflagen (vgl. Interview 11; 12). Folglich wäre insgesamt eine Verbesserung der Zusammenarbeit des BSIs mit den Betreibern Kritischer Infrastrukturen anzustreben. Mit der Meldepflicht aus dem IT-Sicherheitsgesetz werden die Unternehmen gesetzlich zu einer Zusammenarbeit verpflichtet (vgl. Interview 1), was aber den von den befragten VertreterInnen aus der Wirtschaft geäußerten Wünschen nach einer sensibleren und weniger administrativen Zusammenarbeit widerspricht (vgl. Interview 11; 12).

Von VertreterInnen aus der Wirtschaft wird ein agileres Handeln der Politik gefordert (vgl. Interview 12), was sich auch auf die Definition von Rahmenbedingungen bezieht (vgl. Interview 10; 12). Über die Frage, wer die Hauptverantwortung für Cyber Security übernehmen sollte, besteht Meinungsverschiedenheit unter den Unternehmen. Interviewpartner 10 (Deutsche Telekom) sieht die Softwarehersteller in der Pflicht und hätte sich Bestimmungen zur Haftungsverpflichtung bei Software-Produkten im IT-Sicherheitsgesetz gewünscht (vgl. Interview 10). Hingegen sieht Interviewpartner 12 (Daimler AG) die Politik als Hauptverantwortlichen für die Cyber Security, da diese die Rahmenbedingungen definiere (vgl. Interview 12). Die Daimler AG und die Deutsche Telekom AG gehören zu den größten Unternehmen in Deutschland und geben an, dass sie sich vor Cyberspionage der ausländischen Nachrichtendienste nicht schützen können. Während beispielsweise die NSA über ein Milliardenbudget verfüge, hätte ein Unternehmen nicht die entsprechenden Mittel, die eventuellen Gegenmaßnahmen möglicherweise ermöglichen würden (vgl. Interview 10; 12). Insofern schließt Cyber Security den Schutz vor Cyberspionage durch ausländische Nachrichtendienste aus, insbesondere durch die NSA und GCHQ. Es ist aber davon auszugehen, dass nicht alle ausländischen Nachrichtendienste die Stärke der US-amerikanischen und britischen Nachrichtendienste aufweisen und somit Unternehmen sich gegen schlechter ausgestattete Dienste schützen können, auch wenn Interviewpartner 10 (Deutsche Telekom AG) allgemein die ausländischen Nachrichtendienste nennt, gegen deren Cyberspionage keine Cyber Security möglich sei (vgl. Interview 10). Somit ist festzuhalten, dass deutsche Unternehmen gegen die größeren Nachrichtendienste, wie den US-amerikanischen, britischen, chinesischen oder russischen, nicht geschützt sind.

„Unternehmenssicherheit und Know-how-Schutz der Eigenverantwortlichkeit der Wirtschaft“ (Bundesamt für Verfassungsschutz 2015f) zuzuschreiben, ist kritisch zu betrachten. Es ist zwar möglich, die Verantwortung auf die Unternehmen zu übertragen, allerdings stellt sich die Frage, inwieweit diese eine solche Verantwortung überhaupt tragen können, insbesondere bei dem zuvor erwähnten

Schutz vor Cyberspionage ausländischer Geheimdienste. Große Konzerne sind aufgrund ihrer gut ausgestatteten CERT-Lagezentren prinzipiell in der Lage, bestimmte Cyberbedrohungen abzuwehren. Unter anderem können ein Lagezentrum oder Frühwarnsysteme zu einem guten Grundschutz vor Cyberbedrohungen beitragen. Auch die Sensibilisierung der MitarbeiterInnen ist beim Schutz vor Cyber-Angriffen von großer Bedeutung. Keine Kryptotechnologie einzusetzen, beispielsweise damit die MitarbeiterInnen Apple-Produkte benutzen können (vgl. Interview 12), deutet auf Fahrlässigkeit der Unternehmen hin, da durch Kryptotechnologie die Unternehmenskommunikation gesichert wird. Die geforderte Eigenverantwortlichkeit der Unternehmen für Cyber Security kann aber aufgrund mangelnder Ressourcen von kleinen und mittelständischen Unternehmen nicht geleistet werden. Dies wird sogar beim größten deutschen Erdgastransporteur deutlich, der nicht in der Lage ist, sich selbst zu schützen, sondern einen externen Dienstleister damit beauftragt hat (vgl. Interview 11). Die kleinen und mittelständischen Unternehmen haben jedoch für die deutsche Wirtschaft eine große Bedeutung, um als führendes Industrieland bestehen zu können und die Wettbewerbsfähigkeit und somit den Wohlstand zu sichern. Wirtschaftsspionage richtet sich aber gerade gegen „technologieorientierte und innovative mittelständische“ Unternehmen in Deutschland (vgl. Corporate Trust Business Risk & Crisis Management GmbH 2014, S. 4-5). Auch die größten deutschen Konzerne können sich vor ausländischen Nachrichtendiensten nicht schützen. Sie erhalten keinen Schutz der Bundesregierung, die nicht in der Lage ist, sich selbst zu schützen, wie der Cyber-Angriff auf den Bundestag zeigt. Darüber hinaus hat die NSA-Affäre gezeigt, dass der BND sogar ausländische Geheimdienste unterstützt statt die Unternehmen vor ihnen zu schützen. Ohne die Unterstützung des Staates ist jedoch kein effektiver Schutz vor Wirtschaftsspionage möglich.

Das Interview mit der Daimler AG zeigt auch, dass sich Cyber Security nicht auf das eigene Unternehmen beschränkt, da beispielsweise von den Zulieferbetrieben und ihren Produkten Gefahren ausgehen können (vgl. Interview 12). Cybersi-

cherheitsstandards auch bei mittelständischen Zulieferbetrieben würden hier die Sicherheit erhöhen.

Der Breitbandausbau wird von Interviewpartner 11 (Open Grid Europe) als wichtig erachtet (vgl. Interview 11). Interviewpartner 10 der Deutschen Telekom, der diese Aufgabe zukommt, betrachtet den Ausbau auf 50 Mbit/s bis 2018 als ausreichend (vgl. Interview 10). Dieser Punkt lässt sich kritisch hinterfragen, da mit der rasanten digitalen Entwicklung der Bedarf an einem Breitbandausbau diese Grenze überschreiten dürfte. Für ländliche Gebiete ist er dennoch ein Fortschritt und verbessert die Versorgung. Dagegen nehmen mit einem Breitbandausbau aber die Möglichkeiten der Nutzung des Internets weiter zu, indem durch ein schnelleres Internet auch private Bereiche stärker vernetzt werden und zukünftig Entwicklungen, wie z. B. *smart home*, zunehmen werden. Durch die Vernetzung entstehen auch hier wiederum mehr Angriffsmöglichkeiten.

Wie die Bundesbehörden werben auch Unternehmen um geeignete MitarbeiterInnen mit entsprechenden Kompetenzen im Bereich Cyber Security auf dem Arbeitsmarkt (vgl. Interview 10). Daraus kann geschlossen werden, dass wenn große Unternehmen wie die Deutsche Telekom AG von derartigen Schwierigkeiten berichten, tatsächlich ein Fachkräftemangel existiert, der auch für viele andere Unternehmen eine Herausforderung darstellt. Die Ausbildung der MitarbeiterInnen im eigenen Unternehmen scheint hier eine Lösung zu sein. Somit ist davon auszugehen, dass nicht nur die Deutsche Telekom AG (vgl. Interview 10), sondern auch weiter Unternehmen im eigenen Unternehmen ausbilden. Dieses Vorgehen könnte auch für die Politik eine Lösung darstellen, indem sie in den Bundesministerien und Bundesbehörden im Bereich Cyber Security ausbilden würde.

Für die Zukunft planen alle genannten Unternehmen, den Bereich Cyber Security unternehmensintern weiter zu stärken, wie beispielsweise durch eine Umstrukturierung bei der Daimler AG, oder die verstärkte Zusammenarbeit mit anderen Unternehmen sowie mit der Politik auf nationaler und europäischer Ebene bei der Deutschen Telekom AG. Auch Open Grid Europe möchte zukünftig vom exter-

nen Dienstleister HP unabhängiger werden (vgl. Interview 10; 11; 12). Dies deutet darauf hin, dass Outsourcing im Bereich Cyber Security für Kritische Infrastrukturen keine Lösung sein kann, da es notwendig ist, selbst die Übersicht über die Bedrohungen und Gefahren zu behalten. Die Planung der Deutschen Telekom AG ihre Zusammenarbeit mit den erwähnten Akteuren zu verstärken, verdeutlicht zudem die Notwendigkeit, Cyber Security auch international zu bekämpfen.

6 Analyse

Ausgehend von den erhobenen Informationen (Kapitel 2-5) und der in Kapitel 1.3 beschriebenen Methodik folgend, sollen nun die Handlungsfelder der Politik zusammengefasst und anhand ihrer Bedeutung für die strategische Organisation der Cyber Security in Deutschland gewichtet werden. Dies erfolgt mittels einer SWOT-Analyse, bei der zunächst die internen Faktoren (Stärken und Schwächen, Kapitel 6.1) und die externen Faktoren (Chancen und Risiken, Kapitel 6.2) zusammengetragen und anschließend (Kapitel 6.3) zueinander in Beziehung gesetzt werden.

6.1 Interne Analyse

Nachfolgend sollen die Stärken und Schwächen in einer internen Analyse betrachtet und anschließend übersichtlich zusammengefasst werden.

Stärken

Es wurde als Stärke festgestellt, dass die MitarbeiterInnen in den untersuchten Bundesministerien und Bundesämtern Cyberbedrohungen und die daraus resultierende Notwendigkeit von Cyber Security auf nationaler und internationaler Ebene erkennen (vgl. Kapitel 4). Dies zeigt sich auch in der Organisation der zahlreichen Ressorts, die sich in ihrem Fachgebiet mit Cyber Security beschäftigen (vgl. Kapitel 4), sowie den bereits vorhandenen Dokumenten wie die Cyber-Sicherheitsstrategie (vgl. Kapitel 3). Hierbei wird ein Schwerpunkt auf die Sicherheit der Kritischen Inf-

rastrukturen gelegt (vgl. Kapitel 3). Außerdem wurden mit der Digitalen Agenda und der Cyber-Sicherheitsstrategie bereits einige Rahmenbedingungen geschaffen. Aus der Cyber-Sicherheitsstrategie konnten einige Punkte bereits umgesetzt werden, hierzu gehören die Errichtung des Cyber-AZs (vgl. Kapitel 4.3.1) und des Cyber-SRs (vgl. Kapitel 4.3.2).

Eine Stärke, die aus den bereits geschaffenen Rahmenbedingungen besonders hervortritt, ist der beschlossene Entwurf des IT-Sicherheitsgesetzes. Durch die Meldepflicht für Betreiber Kritischer Infrastrukturen wird das BSI besser informiert, kann dadurch schneller mehr Gefahren erkennen, diese besser analysieren und schließlich schneller bessere Handlungsempfehlungen geben. Darüber hinaus können gesicherte Daten zu Cyber-Angriffen an das BKA zur Strafverfolgung weitergeleitet werden, was eine bessere Bekämpfung der Cyberkriminalität ermöglicht; zudem ist davon auszugehen, dass hierdurch die Dunkelziffer der Cyber-Angriffe sinken wird. Dadurch kann eine noch konkretere Lagebeurteilung der Cyber-Angriffe in Deutschland erfolgen. Mit dieser Grundlage können dann weitere Maßnahmen und Handlungsempfehlungen der Politik folgen (vgl. Kapitel 3.5). Betreiber Kritischer Infrastrukturen müssen nun auch Standards in der IT-Sicherheit einhalten, wodurch die Cyber Security in der Wirtschaft gestärkt wird (vgl. Kapitel 3.5). Das IT-Sicherheitsgesetz stärkt ferner einige Bundesministerien und Bundesämter in ihren Aufgaben im Bereich Cyber Security mit einem personellen und finanziellen Ressourcenausbau (vgl. Interview 1).

Die Zusammenarbeit des BSI konnte mit einigen Bundesministerien und Bundesämtern verbessert werden (vgl. Interview 3; 4; 7; 8). Eine weitere interne Verbesserung plant das BMVg, zum Ausbau der Verteidigung von Cyberterrorismus (vgl. Interview 5). Eine weitere Stärke ist die internationale Zusammenarbeit durch die weltweite Vernetzung des BKAs zur Strafverfolgung im Cyber-Raum (vgl. Interview 7) und die internationale Zusammenarbeit des AAs auf EU- und NATO-Ebene (vgl. Interview 6) in Bezug auf Cyber-Security. Hervorzuheben ist die

gute Zusammenarbeit mit den europäischen Staaten Großbritannien, Frankreich, Niederlande, Ukraine und Estland (vgl. Interview 2; 6; 7).

Die Bundesregierung verfolgt das Ziel, digitales Wachstumsland Nr. 1 in Europa zu werden (vgl. Die Bundesregierung 2015a; Die Bundesregierung 2015b). In diesem Zusammenhang unterstützt sie auch die Fortentwicklung von Industrie 4.0 in ihrer Digitalen Agenda (vgl. Die Bundesregierung 2014b, S. 4). Digitale Innovationen und Wettbewerbsfähigkeit können jedoch nur mit einer guten Cyber Security erreicht werden.

Schwächen

Die Ausarbeitung in Kapitel 4 führt zu der Erkenntnis, dass es keine zentral koordinierende Institution in Deutschland gibt, welche die gesamthafte Verantwortung für Cyber Security übernimmt (vgl. Interview 4; 6; 8). Dadurch fehlt eine Institution, die eine umfassende strategische Richtung vorgibt. Insofern ist die Fragmentierung in der politischen und institutionellen Organisation eine Schwäche, da zahlreiche Bundesministerien und Bundesämter Aufgaben im Bereich Cyber Security wahrnehmen und dadurch ein Informationsverlust entsteht (vgl. Interview 3; 7; 8). Zudem ergeben sich teilweise lang andauernde Entscheidungsprozesse (vgl. Interview 6).

Hieraus resultierende Probleme äußeren sich auch in der internationalen Zusammenarbeit mit der NATO. Die Zusammenarbeit bedeutet zum Teil lange Wege, erst über das Cyber-AZ, dann über das BSI bis hin zum BMI. Zustimmungs-, Meinungs- und Entscheidungsprozesse werden dadurch verzögert (vgl. Varwick und Schmid 2012). Auch aus der Aussage von Interviewpartner 6 (AA) lässt sich schließen, dass die formelle Zusammenarbeit bzw. die Organisation der Zusammenarbeit Defizite aufweist, wobei die informelle Zusammenarbeit als gut bewertet wird (vgl. Interview 6).

Ebenfalls wurde aufgezeigt (vgl. Kapitel 4.6), dass es stellenweise keine klare Aufgabenverteilung zwischen den Bundesbehörden gibt. Dies ist eine Schwäche, da durch Doppelarbeit unnötig mehr Ressourcen benötigt werden oder dies könnte

dazu führen, dass Aufgaben gar nicht bearbeitet werden, wenn nicht klar ist, bei wem die jeweilige Zuständigkeit liegt. Auch dies kann wiederum zu einem Informationsverlust führen.

Interviewpartner 1 des Bundesministeriums des Innern, in dessen Geschäftsbereich sich die meisten Bundesämter mit Aufgaben im Bereich Cyber Security befinden, erkennt die Problematik in der formellen Zusammenarbeit der Bundesämter und Bundesministerien und den Informationsverlust nicht (vgl. Interview 1). Laut Interviewpartner 1 (BMI) ist die Ursache nicht in der Organisation zu finden, sondern der Faktor Mensch ist dafür verantwortlich. Diese Aussage widerspricht jener einiger anderer VertreterInnen aus Bundesämtern und auch Bundesministerien (vgl. Interview 4; 6; 7; 8). Hierin besteht unter anderem die Schwäche des BMIs, da ihm Bundesämter unterstellt sind, deren Zusammenarbeit untereinander und mit anderen Bundesbehörden sowie mit Unternehmen Defizite aufweisen (vgl. Interview 3; 4; 5; 7; 8; 11; 12). Für diese Defizite allein den Faktor Mensch verantwortlich zu sehen, erscheint hier nicht ausreichend und kann zumindest infrage gestellt werden. Die Beseitigung von Defiziten und Problemen setzt aber ihre Erkennung voraus.

Die zum Teil schlechte Zusammenarbeit der Bundesbehörden untereinander äußert sich auch beim Cyber-AZ, welches insbesondere für die Kooperation der Bundesministerien und Bundesämter sowie mit den Unternehmen zuständig ist, dieser Aufgabe aber teilweise nicht nachkommt (vgl. Interview 3; 4; 5).

Eine weitere Schwäche der Zusammenarbeit besteht in der zum Teil schlechten Zusammenarbeit der Bundesministerien, Bundesämter und Unternehmen im UP KRITIS-Rat, so seien beispielsweise die VertreterInnen aus der Politik oft nicht anwesend (vgl. Interview 11).

Darüber hinaus führt dies zu einer weiteren Schwäche, die sich aus der Vielzahl von bestehenden Vereinen und Arbeitsgruppen ergibt (vgl. Interview 2; 3; 7). Es kann davon ausgegangen werden, dass die Vielzahl von Vereinen und Arbeitsgruppen durch eine unzureichend präzise Aufgabenverteilung und damit einher-

gehend einer schlechten Abstimmung mit den Bundesministerien und Bundesämtern zu Unsicherheit bei den Unternehmen führt, an welche Institution sie sich im Bereich Cyber Security wenden sollen (vgl. Interview 7).

Andererseits bietet das BSI nicht für alle Unternehmen eine individuelle Zusammenarbeit an. Die Branchen in der Wirtschaft und die Unternehmen sind jedoch sehr unterschiedlich, woraus sich spezielle Probleme ergeben (vgl. Interview 11). Es gibt zwar eine Vielzahl an Arbeitsgruppen und Vereinen, jedoch können diese das Problem der individuellen Beratung nicht ersetzen. Der UP KRITIS-Rat ist zwar an Betreiber Kritischer Infrastrukturen gerichtet, aber auch diese unterteilen sich nochmals in einzelne Branchen (vgl. Interview 11). Dies ist eine Schwäche, da besonders mittelständische Unternehmen noch eine bessere individuelle Beratung ihrer Cyber Security benötigen würden (vgl. Interview 3; Die Bundesregierung 2015a).

Damit die Unternehmen gut geschützt sind, hat das BSI die Aufgabe, festgestellte Cyber-Angriffe bzw. akute Cyberbedrohungen aus seinem CERT an Unternehmen weiterzuleiten, damit diese rechtzeitig reagieren können. Die Schwäche ist hieran, dass diese Meldungen teilweise mit erheblicher Verspätung erfolgen (vgl. Interview 10; 11) und Unternehmen bis dahin schon von einem Cyber-Angriff hätten betroffen sein können, da sie nicht gewarnt wurden und Abwehrmaßnahmen nicht schnell genug ergreifen konnten.

Eine weitere Schwäche ist der personelle und technische Ressourcenmangel in den Bundesministerien und Bundesämtern (vgl. Kapitel 4). Dadurch können Aufgaben im Bereich Cyber Security nicht ausreichend wahrgenommen werden (vgl. Interview 7; Neumann 2014, S. 12). Außerdem gibt es laut Interviewpartner 8 (BBK) Ressorts, die Cyber Security in ihrem Fachgebiet noch nicht ausreichend berücksichtigen (vgl. Interview 8). Es ist zu vermuten, dass auch dies mit einem personellen und technischen Ressourcenmangel zusammenhängt. Darüber hinaus ist aber auch eine Sensibilisierung der MitarbeiterInnen nicht nur in den Unternehmen,

sondern auch in den Bundesministerien und Bundesbehörden notwendig (vgl. Interview 1).

So besteht Handlungsbedarf im Ausbau der personellen und technischen Ressourcen, aber auch der Bundeswehrkompetenzen im Bereich Cyberverteidigung. In der Verteidigung von Cyberterrorismus muss intern eine Verbesserung stattfinden. Da Cyberterrorismus eine Bedrohung für Deutschland darstellt, kann beispielsweise davon ausgegangen werden, dass die derzeitige Cyberverteidigung von 60 SoldatInnen im KSA im Vergleich mit anderen Ländern nicht ausreichend ist (vgl. Kapitel 4.2.3).

Der Personalmangel und der Mangel an nötiger Expertise zur Sicherung der IT-Systeme hat bei der Bundeswehr dazu geführt, dass diese mit der BWI Informationstechnik einen externen Dienstleister damit beauftragt hat, die Modernisierung und Cyber Security für die digitale Infrastruktur der Bundeswehr zu übernehmen. Auch wenn die Hälfte der MitarbeiterInnen freigestellte SoldatInnen sind, ist die Bundeswehr auf externe MitarbeiterInnen angewiesen und kann diese nicht selbst stellen (vgl. Kapitel 4.4.5). Diese Abhängigkeit ist als militärische Schwäche zu benennen.

Eine weitere Schwäche ist die Abhängigkeit der Bundesverwaltung bzw. des Bundestags von der digitalen Vernetzung (Inter-/Intranet) ohne ausreichende Cyber Security, wie zuletzt der Cyber-Angriff auf den Bundestag gezeigt hat (vgl. Meiritz und Medick 2015). Hier stellt sich die Frage, ob neben dem Bundestag die Cyber Security der Bundesverwaltung ebenso große Sicherheitslücken aufweist. Laut Interviewpartner 4 (BMVi) sind Bundesministerien gut ausgestattet, die Bundesämter allerdings nicht (vgl. Interview 4).

Letztlich wurden bisher von der Politik zu wenige Rahmenbedingungen geschaffen (vgl. Interview 10; 12). Von Interviewpartner 10 (Deutsche Telekom AG) wird beispielsweise gefordert, dass für Sicherheitslücken in der Software die Haftungspflicht der Hersteller angepasst werden sollte. Dies hätte im Rahmen des IT-Sicherheitsgesetzt umgesetzt werden können und würde dazu führen, dass die

Softwarehersteller zur Verantwortung gezogen werden und letztlich ihre Produkte im Bereich Cyber Security sicherer gestalten würden (vgl. Interview 10).

Im Entwurf des IT-Sicherheitsgesetzes fehlen klar voneinander abgegrenzte Definitionen für Kritische Infrastrukturen. Somit besteht Unklarheit darüber, welche Branchen bzw. Branchenbereiche zu den Kritischen Infrastrukturen zählen, welche also von dem Gesetz betroffen sind (vgl. Plöger 2015). Eine weitere Schwäche ist, dass das IT-Sicherheitsgesetz nur Kritische Infrastrukturen betrifft (vgl. Schiller 2015). Ebenso wichtig wären z. B. zur Bekämpfung der Wirtschaftsspionage alle anderen Sektoren der Wirtschaft. Ein Fokus sollte dabei auf die deutschen Schlüsselindustrien gelegt werden, um die Wettbewerbsfähigkeit der deutschen Unternehmen erhalten zu können, die letztlich den Wohlstand in Deutschland sichert.

Des Weiteren ergeben sich aus den fehlenden Rahmenbedingungen Unklarheiten in Politik und Wirtschaft darüber, wer die Verantwortung für Cyber Security trägt: Interviewpartner 6 (AA) sieht die Verantwortung in der Wirtschaft (vgl. Interview 6), während von Interviewpartner 12 (Daimler AG) Cyber Security vorrangig als Aufgabe der Politik betrachtet wird, da diese die Rahmenbedingungen definiert (vgl. Interview 12). Aus den Dokumenten zur deutschen Cybersicherheitspolitik geht hervor, dass die Politik die Verantwortung bei „Staat, Wirtschaft und Gesellschaft“ sieht (vgl. Kapitel 3.7).

Darüber hinaus wurde von VertreterInnen aus den Bundesämtern auf das Problem hingewiesen, dass die Bezahlung in der Bundesverwaltung im IT-Bereich weitaus schlechter ist als in der Wirtschaft und es daher schwierig ist, MitarbeiterInnen zu gewinnen (vgl. Interview 7; 8).

Ferner ist als Schwäche zu werten, dass die Politik zu wenig in Forschung und Entwicklung im Bereich Cyber Security investiert (vgl. Interview 12), worauf aber sowohl die Politik als auch die Unternehmen angewiesen sind, um Cybersicherheit zu schaffen (vgl. Interview 2; 12).

Die derzeit schlechten diplomatischen Beziehungen zu Russland stellen eine weitere Schwäche dar. Dadurch ist die gemeinsame Bekämpfung von Cyber-

Angriffen und deren Strafverfolgung vollständig zum Erliegen gekommen (vgl. Interview 7). Zur Aufklärung und Verfolgung des Cyber-Angriffes auf den Deutschen Bundestag wäre eine Zusammenarbeit mit Russland hilfreich gewesen, da vermutet wurde, dass der Angriff aus Russland stammt (vgl. Baumgärtner et al. 2015). Die erarbeiteten Stärken (Tab. 2) und Schwächen (Tab. 3) sollen nachfolgend übersichtlich zusammengefasst und für die SWOT-Matrix in Kapitel 6.3 aufbereitet werden.

Tab. 2: Stärken der Organisation der Cyber Security in Deutschland **(**Quelle: Eigene Darstellung.)

Stärken (S)
S1: Cyberbedrohungen werden von der Politik wahrgenommen, zahlreiche Ressorts beschäftigen sich in ihrem Fachbereich mit Cyber Security. **S 2:** Politik legt einen Schwerpunkt auf den KRITIS-Schutz. **S 3:** Einige Rahmenbedingungen wurden umgesetzt (IT-Sicherheitsgesetz, Cyber-AZ, Cyber-SR). **S 4:** Die Zusammenarbeit des BSIs konnte mit einigen Bundesministerien und Bundesämtern verbessert werden. **S 5:** Das BMVg plant den Ausbau der Cyberverteidigung in der Deutschen Bundeswehr. **S 6:** Das BKA verfügt über eine weltweite Vernetzung zur Strafverfolgung von Cyberkriminalität. **S 7:** Cyber-Außenpolitik: internationale Zusammenarbeit durch die Teilnahme in Gremien und Arbeitsgruppen auf EU- und NATO-Ebene **S 8:** Es gibt eine gute Zusammenarbeit mit europäischen Ländern (Großbritannien, Frankreich, Niederlande, Ukraine, Estland). **S 9:** Ziel der Bundesregierung, das digitale Wachstumsland Nr.1 in Europa zu werden: Industrie 4.0 wird unterstützt und somit Cyber Security gefördert.

Tab. 3: Schwächen der Organisation der Cyber Security in Deutschland **(**Quelle: Eigene Darstellung.)

Schwächen (W)
W 1: Keine zentral koordinierende Institution auf Ebene der Bundesverwaltung, welche die gesamthafte Verantwortung für Cyber Security übernimmt ***W 2:*** *Durch die Fragmentierung von Cyber Security in der politischen und institutionellen Organisation entsteht ein Informationsverlust sowie eine erschwerte Zusammenarbeit mit der NATO* **W 3:** Stellenweise keine klare bzw. überschneidende Aufgabenteilung zwischen den Bundesministerien und Bundesämter **W 4:** BMI erkennt nicht die bestehende Problematik in der organisatorischen Zusammenarbeit der Bundesministerien und Bundesämter. **W 5:** Das Cyber-AZ kommt seinen Aufgaben nur bedingt nach. **W 6:** Es bestehet ein Bedarf der verbesserten Zusammenarbeit im UP KRITIS-Rat zwischen Bundesbehörden und Unternehmen.

W 7: Keine Abstimmung innerhalb der Bundesministerien und Bundesämter, daher zu viele Initiativen von Vereinen und Arbeitsgruppen. Unternehmen wissen nicht mehr, an wen sie sich im Bereich Cyber Security wenden sollen.
W 8: Mangelnde individuelle Angebote der Zusammenarbeit des BSIs mit einzelnen Unternehmen
W 9: Das BSI meldet Cyber-Angriffe/Sicherheitslücken zu spät an die Unternehmen.
W 10: Technischer und personeller Ressourcenmangel in den Bundesministerien und Bundesämtern
W 11: Einige Ressorts berücksichtigen für ihr Fachgebiet Cyber Security noch nicht ausreichend.
W 12: Die Kompetenzen/Fähigkeiten im Ressort für Cyberterrorismus des BMVgs und bei der Bundeswehr sind unzureichend.
W 13: Personalmangel in der Bundeswehr, daher externer Dienstleister für IT-Systeme beauftragt
W 14: Abhängigkeit der Bundesverwaltung bzw. des Bundestags von digitaler Vernetzung (Inter-/Intranet) ohne ausreichende Cyber Security
W 15: Mangelnde politische Rahmenbedingungen
W 16: Unzureichende Definitionsklarheit von Kritischen Infrastrukturen (besonders auch im IT-Sicherheitsgesetz)
W 17: Im IT-Bereich gibt es eine geringere Bezahlung in der Bundesverwaltung als in der Wirtschaft.
W 18: Zu wenig Forschung und Investition in Cyber Security
W19: Keine Zusammenarbeit mit Russland, dadurch keine Strafverfolgung einer großen Täterschaft

6.2 Externe Analyse

Nachfolgend sollen die externen Chancen und Bedrohungen dargestellt werden, die im Anschluss im Zusammenhang mit den dargelegten internen Faktoren (Kapitel 6.1) zu bewerten sind.

Chancen

Durch die NSA-Affäre (vgl. Spiegel Online 2013a) und den Cyber-Angriff auf den Bundestag (vgl. Wendt 2015) sowie der umfangreichen Berichterstattung in den Medien erhält Cyber Security einen höheren Stellenwert in der Politik und Wirtschaft. Jedes dritte Unternehmen hat, diesen Entwicklungen folgend, seine IT-Sicherheit überprüft (vgl. Spiegel Online 2013a) und die Bundesregierung hat nach dem Cyber-Angriff auf den Bundestag zügig den Entwurf des IT-Sicherheitsgesetzes beschlossen (vgl. Bundestag 2015).

Eine weitere Chance ist, dass Unternehmen sich auch in Zukunft für Cyber Security einsetzen wollen (vgl. Interview 10; 11; 12). Zudem bilden sie MitarbeiterInnen im Bereich Cyber Security selber aus, wie an der Deutschen Telekom zu erkennen ist (vgl. Interview 10). Indem die Unternehmen sich auch in Zukunft für Cyber Security einsetzen (vgl. Interview 10; 11; 12), ergibt sich wiederum ein erhöhter Bedarf und Nachfrage nach Cyber Security.

Als einer der größten Betreiber Kritischer Infrastrukturen in Deutschland setzt sich die Telekom AG verstärkt für Cyber Security ein. Daraus entsteht z. B. eine weitere Chance durch die jährlich ausgerichtete Konferenz Cyber Security Summit mit der Münchner Sicherheitskonferenz, die VertreterInnen aus Wirtschaft und Politik zusammenbringt und bei der aktuelle Sicherheitsthemen auf die Agenda gesetzt werden, wie Cyberterrorismus oder die NSA-Affäre (vgl. Kapitel 5.1).

Eine weitere Chance sind die gut ausgestatteten CERT-Lagezentren der großen Konzerne. Diese können dadurch Cyber-Angriffe frühzeitig erkennen und abwehren (vgl. Interview 10), nur bei Angriffen ausländischer Geheimdienste sehen sie sich dazu nicht in der Lage (vgl. Interview 10; 12). Trotzdem erhöht sich dadurch letztlich die Cyber Security der Unternehmen, aber auch durch die Umsetzung der Handlungsempfehlungen des BSIs (vgl. Interview 11).

Industrie 4.0 ist eine Chance, indem durch neue digitale Entwicklungen und vernetzten Produktionssystemen (vgl. BITKOM und Fraunhofer IAO 2014, S. 7) davon ausgegangen werden kann, dass auch die Nachfrage nach deutschen Softwareprodukten steigen wird. Damit würde sich z. B. die Wahrscheinlichkeit von Manipulationen der Software zwecks Spionage aus dem Ausland reduzieren.

Bedrohungen

Durch die rasante digitale Entwicklung nehmen potenzielle Sicherheitslücken zu, die von den TäterInnen für Cyber-Angriffe ausgenutzt werden können (vgl. Bundesamt für Sicherheit in der Informationstechnik 2014, S. 4, 11). Hierbei ist die Gefährdungslage aufgrund der Angriffsmöglichkeiten und der Cyberbedrohungen für IT-Systeme in Deutschland als kritisch einzustufen (vgl. Bundesamt für

Sicherheit in der Informationstechnik 2014, S. 4). In der Ausarbeitung in Kapitel 2 wurde deutlich, dass Staat, Wirtschaft und Gesellschaft durch einen Cyber-Angriff auf Kritische Infrastrukturen oder Unternehmen besonders bedroht sind – in Form von Cyberspionage (ausländischer Nachrichtendienste), Cyberkriminalität und Cyberterrorismus.

Eine Cyberbedrohung für Unternehmen äußert sich insbesondere in der Wirtschaftsspionage durch ausländische Nachrichtendienste. UnternehmensvertreterInnen berichten, dass sie keine Chance haben, sich vor derartiger Spionage zu schützen (vgl. Interview 10; 12).

Ferner werden laut Interviewpartner 11 (Open Grid Europe) Cyber-Angriffe im IT-System des Unternehmens nicht immer entdeckt (vgl. Interview 11). Zudem ist der größte Erdgastransporteuer in Deutschland nicht in der Lage, Cyber Security im eigenen Unternehmen durchzuführen, sondern hat einen externen Dienstleister damit beauftragt (vgl. Interview 11). Insofern könnte die Abhängigkeit von externen Unternehmen ein weiteres Sicherheitsrisiko darstellen. Die Unternehmen verlassen sich auf die externen Dienstleister, deren Arbeit sie nur eingeschränkt kontrollieren können. Da es hier um die Sicherheit der IT-Systeme einer Kritischen Infrastruktur handelt, ist dies ein sensibler Bereich, da deren einwandfreie Funktion für die Wirtschaft und die Gesellschaft essenziell ist. Es stellt sich die Frage, wer letztlich die Verantwortung übernimmt, wenn es zu Cyber-Angriffen kommt, die nicht zu den klassischen Angriffen gehören bzw. wie diese definiert werden – bei generellen Unklarheiten der Definitionen zu Cyberbedrohungen (Kapitel 2.2).

Eine Bedrohung durch unzureichende Cyber Security besteht für Unternehmen auch durch andere Unternehmen in der Lieferkette. Haben beispielsweise Zulieferer eines Unternehmens keine gute Cyber Security, können Viren über Produkte der Zulieferer bis zum Kunden gelangen (vgl. Interview 12).

Eine weitere Bedrohung sind die mangelnden Kompetenzen im Bereich Cyber Security auf dem Arbeitsmarkt. Dadurch haben die Unternehmen und Bundesministerien sowie Bundesämter Probleme, Stellen im Bereich Cyber Security mit

geeignetem Personal zu besetzen (vgl. Interview 5; 6; 7; 8; 10). Somit kann auch davon ausgegangen werden, dass der angestrebte Stellenausbau im Rahmen des IT-Sicherheitsgesetztes davon beeinträchtigt sein wird.

Von dem BMI und dem BSI wird die mangelnde Bereitschaft zur Zusammenarbeit bei den Unternehmen kritisiert (vgl. Interview 1; 2). In der Zusammenarbeit mit dem BSI stellt dies eine Bedrohung dar, sofern beispielsweise Cyber-Angriffe der Unternehmen nicht gemeldet werden und das Bundesamt die Cyberbedrohungen nicht an andere Unternehmen weiterleiten kann bzw. keine angemessenen Handlungsempfehlungen aussprechen kann.

Insgesamt gibt es zu wenige Innovationen und Entwicklungen von deutschen Unternehmen aus dem Bereich der IT zu relevanter Software für Cyber Security. Die Deutsche Telekom AG kann beispielsweise kaum deutsche Software beziehen und muss diese aus den USA oder Asien einkaufen (vgl. Interview 10). Die Bedrohung liegt schließlich in der Abhängigkeit von importierter Software, die bewusste Sicherheitslücken aufweisen könnte, die Cyber-Angriffe durch ausländische Geheimdienste erlauben.

Generell verschiebt sich Kriminalität immer mehr in den Cyberraum. Für die Polizei ergibt sich daraus eine Herausforderung, da es in der polizeilichen Ausbildung an Fähigkeiten zur Strafverfolgung von Cyberkriminalität mangelt (vgl. Interview 7). Die Möglichkeiten für Cyber-Angriffe nehmen nicht nur durch technologische Weiterentwicklung zu, sondern auch durch die Digitalisierung und Vernetzung in Bereichen von Staat, Wirtschaft und Gesellschaft (vgl. Bundesamt für Sicherheit in der Informationstechnik 2014, S. 11). Mit der Industrie 4.0 wird es im Zuge der rasanten Digitalisierung und vernetzten Produktionssystemen auch mehr Angriffsmöglichkeiten geben, z. B. Produktionssysteme zu stören oder zu zerstören (vgl. BITKOM und Fraunhofer IAO 2014, S. 7). Somit können die erarbeiteten Chancen und Bedrohungen in den Tabellen 4 und 5 zusammenfassend aufgelistet werden.

Tab. 4: Chancen der Organisation der Cyber Security in Deutschland (Quelle: Eigene Darstellung.)

Chancen (O)
O1: Aktuelle Vorkommnisse (NSA-Affäre, Cyber-Angriff auf den Bundestag) erhöhen das Interesse in den Medien. **O 2:** Unternehmen planen auch für die Zukunft, sich für Cyber Security verstärkt einzusetzen, auch auf internationaler Ebene. **O 3**: Unternehmen bilden selbst MitarbeiterInnen mit Kompetenzen im Bereich Cyber Security aus. **O4:** Der Cyber Security Summit der Deutschen Telekom AG und Münchner Sicherheitskonferenz fördert die Zusammenarbeit zwischen Wirtschaft und Politik. **O 5:** Durch die eigene CERT-Lagezentren der Unternehmen können Cyber-Angriffe frühzeitig erkannt oder verhindert werden. **O 6:** Die Unternehmen setzen die Handlungsempfehlungen des BSI um, dadurch können Cyberbedrohungen besser und schneller erkannt werden und Maßnahmen eingeleitet werden. **O 7:** Industrie 4.0 führt zu neuen Entwicklungen, kann nur mit Cyber Security fortentwickelt werden, daher steigt das Interesse an sicheren IT-Systemen/Softwareprodukten.

Tab. 5: Bedrohungen der Organisation der Cyber Security in Deutschland **(**Quelle: Eigene Darstellung.)

Bedrohungen (T)
T 1: Cyber-Angriffe nehmen durch die rasante digitale Entwicklung zu und somit die Möglichkeiten und Sicherheitslücken, die TäterInnen ausnutzen. **T 2:** Gefährdungslage ist kritisch für IT-Systeme in Deutschland durch die Angriffsmöglichkeiten **T 3:** Staat, Wirtschaft und Gesellschaft sind besonders den drei Cyberbedrohungen Cyberspionage (ausländischer Nachrichtendienste), Cyberkriminalität und Cyberterrorismus ausgesetzt. **T 4:** Cyberbedrohungen bestehen besonders für Kritische Infrastrukturen und Unternehmen. **T 5:** Unternehmen können sich gegen Wirtschaftsspionage ausländischer Nachrichtendienste nicht schützen. **T 6:** Oft werden Cyber-Angriffe und daraus resultierende Schäden im IT-System der Unternehmen nicht entdeckt, wodurch keine Abwehrmaßnahmen getroffen werden können **T 7:** Betreiber kritischer Infrastrukturen müssen externe Dienstleister zum Schutz vor Cyber-Angriffen beauftragen, können aber deren Arbeit nicht überwachen. **T 8:** Cyber Security bei Zulieferern kann die Sicherheit des Produktes gefährden. **T 9:** Keine ausreichenden Kompetenzen für Cyber Security auf dem Arbeitsmarkt für Unternehmen und Bundesverwaltung, geplanter Stellenausbau des IT-Sicherheitsgesetztes kann dadurch gefährdet sein. **T 10:** Mangelnde Bereitschaft der Unternehmen zur Zusammenarbeit mit dem BSI **T 11:** Zu wenige Innovationen/Entwicklungen deutscher Unternehmen im Bereich der IT **T 12:** Wenige Softwarehersteller für sichere IT-Systeme und Cyber-Sicherheitsprodukte in Deutschland und somit eine schwache digitale Industrie **T 13:** Kriminalität verschiebt sich in den Cyberraum.

T 14: Industrie 4.0: mehr Angriffsmöglichkeiten durch Digitalisierung und vernetzte Produktionssysteme

6.3 Strategische Gewichtung

Die identifizierten internen und externen Faktoren (Kapitel 6.1 und 6.2) bilden Handlungsfelder, die dem unmittelbaren (interne Faktoren) oder mittelbaren (externe Faktoren) Einfluss des politischen Akteurs unterliegen. Einige der aufgezeigten Faktoren können in einer SWOT-Matrix (Tab. 6) einander gegenüber gestellt werden, um eine strategische Gewichtung vornehmen zu können. Im Anschluss hieran wären konkrete Strategien zu erarbeiten und basierend hierauf Maßnahmen festzulegen, die insgesamt zu einer Erhöhung der Cyber Security in Deutschland beitragen könnten, was allerdings den Rahmen dieser Arbeit überschreitet. Nachfolgend sollen lediglich zusammenhängende Handlungsoptionen aufgezeigt werden. Folgende Stärken und Schwächen stellen Handlungsfelder dar, konnten aber der SWOT-Matrix nicht zugeordnet werden: S3, W1, W2, W3, W4, W7, W11, W16, W17 (vgl. Tabellen 2 und 3).

Tab. 6: SWOT-Matrix **(**Quelle: eigene Darstellung.)

SWOT-Matrix		**Interne Faktoren**	
		Stärken (S)	**Schwächen (W)**
Externe Fak	**Chancen (O)**	**S1-O1:** Die Wahrnehmung für Cyber Security in der Politik und Wirtschaft wird durch die Berichterstattung über Cyber Angriffe noch weiter gestärkt. **S3-O2:** Dadurch, dass die Politik bspw. mit dem IT-Sicherheitsgesetz die eigenen personellen und technischen Ressourcen für Cyber Security ausbaut, wird die Chance erhöht, dass auch die Unternehmen sich für Cyber Security verstärkt einsetzen. **S3-O6:** Durch die Stärkung (IT-Sicherheitsgesetz) des BSIs können bessere Handlungsempfehlungen an Unternehmen gegeben werden, dadurch könnten auch mehr Maß-	**O5-W9:** Die CERT-Lagezentren der Konzerne wirken der Problematik entgegen, dass Cyber-Angriffe vom BSI zu spät gemeldet werden. **O4-W6, W5:** Der Cyber Security Summit ist trotz der teilweise schlechten Zusammenarbeit zwischen Politik und Wirtschaft ein Angebot eines Unternehmens an die Politik zur Zusammenarbeit und fördert auch die Zusammenarbeit zwischen den Unternehmen, was durch das Cyber-AZ oder den KRITIS-Rat nicht ausreichend ermöglicht wird. **O2, O7-W14:** Indem Unternehmen sich auch in Zukunft für Cyber Security einsetzen und Industrie 4.0 voran bringen, das nur mit einer

toren		nahmen zur Erhöhung der Cyber Security von den Unternehmen umgesetzt werden. **S7, S8-O2:** Die Bekämpfung von Cyber Security auf internationaler Ebene wird sowohl von der Politik als auch von den Unternehmen umgesetzt. Die guten außenpolitischen Beziehungen auf europäischer Ebene bestärken das internationale Engagement der Unternehmen für Cyber Security. **S9-O7:** Die Politik hat selbst das Ziel für Deutschland gesetzt „Digitales Wachstumsland Nr. 1 in Europa" zu werden und unterstützt Industrie 4.0. Damit steigt die Chance, dass mehr deutsche Softwareprodukte entwickelt werden bzw. Cyber Security verstärkt umgesetzt wird. **S2-O2:** Da Unternehmen inkl. Betreiber Kritischer Infrastrukturen sich auch zukünftig für Cyber Security einsetzen, wird auch der KRITIS-Schutz erhöht. **O3-S3:** Indem Unternehmen im Bereich Cyber Security ausbilden, könnte auch die Politik durch ein höheres Angebot an Arbeitskräften profitieren, insbesondere beim geplanten Stellenausbau im Rahmen des IT-Sicherheitsgesetzes.	guten Cyber Security möglich ist wird die Nachfrage nach deutschen sicheren Softwareprodukten und Cyber-Sicherheitsprodukten steigen, mit denen dann auch die IT-Systeme der Bundesverwaltung sicherer gemacht werden könnten. **O6-W15:** Keine ausreichenden Rahmenbedingungen der Politik, die Handlungsempfehlungen des BSIs werden aber zumindest umgesetzt. **O7-W18:** Mit Industrie 4.0 kann davon ausgegangen werden, dass Unternehmen mehr Forschung und Investitionen im Bereich Cyber Security fördern werden, da sie darauf angewiesen sind, wenn dies von der Politik nicht ausreichend getan wird.
	Bedrohungen (T)	**S1-T2:** Die Politik hat die kritische Gefährdungslage für Deutschland erkannt, viele Ressorts beschäftigen sich mit der Thematik, dadurch wird der kritischen Gefährdungslage entgegengewirkt. **S3-T1:** Die Politik hat auf die zunehmenden Cyberbedrohungen reagiert und einige Rahmenbedingungen geschaffen. **S3-T9:** Der im IT-Sicherheitsgesetz geplante Stellenausbau ist durch den Fachkräftemangel gefährdet. **S2-T2:** Die Politik setzt sich	**W15-T3:** Ohne geeignete politische Rahmenbedingungen können Cyberbedrohungen nur unzureichend bekämpft werden. **W6-T2:** Cyberbedrohungen bestehen insbesondere für Kritische Infrastrukturen, durch die schlechte Zusammenarbeit im UP KRITIS-Rat wird dem nicht ausreichend entgegengewirkt. **W19-T3/T5:** Die schlechten diplomatischen Beziehungen zu Russland könnten Cyber-Angriffe/Wirtschaftsspionage aus

		schwerpunktmäßig für den KRITIS-Schutz ein, damit wird der Bedrohung von Cyber Angriffen auf Kritische Infrastrukturen entgegengewirkt. **S3-T1/T2:** Mit dem IT-Sicherheitsgesetz wird ein Mindestmaß an IT-Standards für Betreiber Kritischer Infrastrukturen gefordert und somit der kritischen Gefährdungslage für IT-Systeme und den zunehmenden Möglichkeiten für Cyber-Angriffe zum Teil entgegengewirkt. **S4-T10:** Da die Zusammenarbeit des BSIs mit einigen Bundesbehörden verbessert werden konnte, ist davon auszugehen dass dies auch mit Unternehmen umgesetzt werden könnte. **S7-T5:** Die weltweite Vernetzung und die int. Zusammenarbeit der Politik kann für die Unternehmen unterstützend wirken im Kampf gegen Cyberspionage von ausl. Nachrichtendiensten. **S6-T3:** Mit der weltweiten Vernetzung des BKAs kann Cyberkriminalität erfolgreicher begegnet werden. **S5-T3/T9:** Der Bedrohung durch Cyberterrorismus wird mit Ausbau der Bundeswehr in der Cyberverteidigung und der Verbesserung im Ressort des BMVgs besser begegnet werden können. Das Vorhaben kann allerdings wiederum durch mangelnde Kompetenzen auf dem Arbeitsmarkt bedroht sein. **S9-T1:** Den zunehmenden Cyberbedrohungen durch die Digitalisierung wird mit der Unterstützung der Industrie 4.0 entgegengewirkt. Indem Industrie 4.0 gefördert wird, entsteht mehr Cyber Security in den Unternehmen, da ansonsten Industrie 4.0 nicht umzusetzen wäre. Zudem wird die Nachfrage	Russland verstärken, zumal Unternehmen sich vor ausl. Nachrichtendiensten kaum schützen können. **W8-T10:** Die unzureichenden individuellen Angebote des BSIs für Unternehmen verstärken das Problem der mangelnden Bereitschaft der Unternehmen zur Zusammenarbeit. **W15-T1:** Ohne ausreichende Haftungspflicht für Softwarehersteller werden Sicherheitslücken in der Software unzureichend bekämpft **W18-T1/T6/T11/T15:** Durch unzureichende Unterstützung der Forschung und Investitionen der Politik wird die Herstellung sicherer inländischer Software nicht unterstützt, um der rasanten Digitalisierung und zunehmenden Möglichkeiten für Cyber-Angriffe standzuhalten und um Cyber-Angriffe schneller in IT-Systemen zu erkennen. Auch für Industrie 4.0 müsste es mehr Entwicklungen für sichere vernetzte Produktionssysteme geben. **W6-T7:** Durch die schlechte Zusammenarbeit im UP KRITIS-Rat lässt sich die Politik die Möglichkeit entgehen, Unternehmen bspw. zu unterstützen, Kompetenzen intern aufzubauen und keine externen Dienstleister beauftragen zu müssen. **W10/W18-T9:** Der technische und personelle Ressourcenmangel in den Bundesministerien und Bundesämtern könnte noch weiter verschärft werden, wenn keine hoch qualifizierten Fachkräfte auf dem Arbeitsmarkt zur Verfügung stehen und zugleich nicht in technische Entwicklungen investiert wird. **W12/W13-T3:** Cyberterrorismus ist eine der größten Bedrohungen. Durch den bestehenden Handlungsbedarf in den Ressorts für Cyberterrorismus des BMVgs und in der Bundeswehr kann der Bedrohung nicht ausreichend entgegengewirkt

		nach deutschen Softwareprodukten und Cyber-Sicherheitsprodukten steigen.	werden. **W15-T8:** Durch mangelnde Rahmenbedingungen sind Unternehmen vor unsicheren IT-Systemen der Zulieferer nicht geschützt, wodurch mit Schad-Software infizierte Produkte an Endkunden weitergegeben werden könnten.

Schwächen und Bedrohungen

Die Handlungsfelder, welche sich aus der Gegenüberstellung von Schwächen und Bedrohungen ableiten lassen, können als dringendste Handlungsfelder betrachtet werden (Tab. 4). Durch die externen Bedrohungen ist Cyber Security in Deutschland unmittelbar gefährdet. Zusammen mit internen Schwächen stellen sie eine hohe Gefährdung dar. Demzufolge sollten diese Schwächen beseitigt werden, um die akuten Cyberbedrohungen zu minimieren. Unter den identifizierten Handlungsfeldern fällt auf, dass sich einige aufgrund der schlechten Zusammenarbeit von Politik und Wirtschaft ergeben (W6-T2, W8-T10, W6-T7). Weitere Handlungsfelder ergeben sich aus unzureichenden Rahmenbedingungen von der Politik (W15-T3, W15-T1, W15/T8). Darüber hinaus bestehen Handlungsfelder in den internationalen Beziehungen zur Bekämpfung von Wirtschaftsspionage insbesondere durch ausländische Nachrichtendienste (W19-T3/T5). Zur Bekämpfung von Cyberterrorismus besteht ein dringender Handlungsbedarf im personellen und technischen Ausbau sowie den Kompetenzen des BMVgs und der Bundeswehr (W12, W13-T3). Ein weiteres Handlungsfeld ist der personelle und technische Ressourcenmangel in den Bundesministerien und Bundesämtern sowie die mangelnden Kompetenzen auf dem Arbeitsmarkt, denen entgegengewirkt werden sollte, um das IT-Sicherheitsgesetz umsetzen zu können, da ansonsten die Maßnahmen zur Sicherung Kritischer Infrastrukturen nicht umgesetzt werden können (W10, W18-T9). Ein weiterer finanzieller Faktor sind Mängel bei Investitionen in die Forschung durch die Politik sowie bei Entwicklungen sicherer Softwareprodukte in der Wirtschaft (W18-T1/T6/T11/T15).

Schwächen und Chancen

Durch die Gegenüberstellung von den internen Schwächen und den externen Chancen lassen sich Handlungsfelder identifizieren, bei denen die Chancen genutzt werden sollten, um den Schwächen entgegenzuwirken (Tab. 4). Die Chance, dass im Rahmen von Industrie 4.0 auch mehr Forschung und Investition zu erwarten ist, sollte z. B. insbesondere genutzt werden und von der Politik unterstützt werden, um die entsprechenden Mängel in diesem Bereich zu beseitigen (O7-W18). Zu den mangelnden Rahmenbedingungen kann hier festgestellt werden, dass die bestehenden Handlungsempfehlungen vom BSI zumindest von Unternehmen umgesetzt werden. Demnach sollten die Handlungsempfehlungen weiterhin gestärkt werden. Industrie 4.0 wird hier als Chance identifiziert und als Handlungsfeld der Förderung von Forschung und Entwicklung, um somit auch die Nachfrage nach sicheren Softwareprodukten und Cyber-Sicherheitsprodukten zu steigern und somit sicherere IT-Systeme zu generieren (O2/ O7-W14). Die CERT-Lagenzentren wirken den Schwächen des BSIs entgegen, allerdings ist davon auszugehen, dass diese nur in Konzernen bestehen und kleine sowie mittelständische Unternehmen sich CERT-Lagezentren nicht leisten können und dies somit einen der Gründe für ihren unzureichenden Schutz vor Cyber-Angriffen darstellt (O5-W9). In der Ausrichtung des Cyber Security Summits durch die Deutsche Telekom AG mit der Münchner Sicherheitskonferenz besteht das Handlungsfeld auf der Seite der Politik, diese Chance zu nutzen und zu unterstützen, um die Zusammenarbeit mit den Unternehmen zu verbessern und letztlich davon zu profitieren (O4-W6/W5).

Stärken und Bedrohungen

Die internen Stärken der Politik sollten ausgebaut werden, um den Bedrohungen entgegenzuwirken (Tab. 4). Dringender Handlungsbedarf besteht bei der Umsetzung des IT-Sicherheitsgesetzes, indem der Bedrohung des Mangels an hochqualifizierten Fachkräften entgegengewirkt wird. Die Dringlichkeit resultiert daraus, da das IT-Sicherheitsgesetz bereits beschlossen wurde und in naher Zukunft in Kraft

treten wird (S3-T9, S3-T1). Einigen Cyberbedrohungen können zudem mit der Stärke einer guten nationalen und internationalen Zusammenarbeit sowie der weltweiten Vernetzung entgegengewirkt werden (S4-T10, S7-T5, S6-T3). Da von Cyberterrorismus eine große Bedrohung ausgeht und der personelle Ausbau im BMVg und der Bundeswehr nicht gefährdet sein sollte, besteht auch hier ein dringender Handlungsbedarf in dem Ausbau der Kompetenzen auf dem Arbeitsmarkt (S5-T3/T9). Mit dem IT-Sicherheitsgesetz und dem UP KRITIS-Rat hat die Politik erste Schritte unternommen, um einen Schwerpunkt auf den Schutz der Kritischen Infrastrukturen zu legen (S3-T1). Den zunehmenden Cyberbedrohungen kann die Politik aber auch durch die Unterstützung von Industrie 4.0 entgegenwirken. Die Unterstützung seitens der Politik sollte sich fortsetzen, um die technische Fortentwicklung von Cyber Security zu stärken (S9-T1).

Stärken und Chancen

Jene Handlungsfelder, bei denen Stärken auf Chancen treffen, stellen den Idealfall dar (Tab. 4). Dennoch kann man diese Felder in der weiteren Betrachtung nicht außer Acht lassen. Gerade bei Chancen, wie dem Ziel der Politik das Digitale Wachstumsland Nr.1 in Europa zu werden und die Unterstützung der Entwicklung von Industrie 4.0, kann davon ausgegangen werden, dass Cyber Security gefördert wird und sichere deutsche Softwareprodukte entstehen, was aber so nicht eintreffen muss (S9-O7). Auch muss darauf geachtet werden, dass die bestehenden Chancen zur weiteren Stärkung tatsächlich genutzt werden (S7/S8-O2; S2-O2; O3-S3; S3-O6; S3-O2).

6.4 Auswertung

Mit der Analyse konnten zur Beantwortung der Fragestellung einige Handlungsfelder für die Politik identifiziert werden. Es hat sich unter anderem herausgestellt, dass insgesamt eine Reduktion der kritischen Gefährdungslage durch Cyberbedrohungen für Staat, Wirtschaft und Gesellschaft (Wirtschaftsspionage, Cyberkrimina-

lität, Cyberterrorismus) notwendig ist (T2; T3), die durch die digitale Entwicklung (T1) weiter zunehmen werden. Insofern besteht ein dringender Handlungsbedarf in jenen Handlungsfeldern, bei denen Schwächen auf Bedrohungen treffen (W15-T3; W6-T2; W19-T3, T5; W12, W13-T3). Die Analyse zeigt aber auch einige Schwächen, denen nicht durch Stärken oder Chancen entgegengewirkt werden können und daher ebenfalls dringlich zu beseitigen oder zu minimieren sind (W1; W2; W3; W4; W7; W11; W16; W17). Diese ergeben sich größtenteils aus einer zum Teil schlechten Zusammenarbeit der Bundesministerien und Bundesämter untereinander, die zum Informationsverlust führt, sowie aus mangelnder Abstimmung innerhalb der Bundesministerien und Bundesämter und einer stellenweise überschneidenden Aufgabenteilung (W1; W2; W3; W7). Ferner ist davon auszugehen, dass diese Faktoren unter anderem mit dem Fehlen einer zentralen koordinierenden Institution auf Ebene der Bundesverwaltung zusammenhängen, welche die gesamthafte Verantwortung für Cyber Security übernimmt (W1). Da bereits das Problem besteht, dass es nicht genügend hochqualifizierte Fachkräfte auf dem Arbeitsmarkt gibt, könnte sich diese Schwäche zukünftig noch stärker auswirken, gerade im Hinblick auf den Stellenausbau. Hiervon und von der unzureichenden Definitionsklarheit Kritischer Infrastrukturen (W16) wird das IT-Sicherheitsgesetz in seiner Umsetzung stark betroffen sein, davon ist zumindest auszugehen wenn diese Schwächen nicht beseitigt oder reduziert werden. Das Ziel der Politik, mit dem IT-Sicherheitsgesetz sicherere Kritische Infrastrukturen zu schaffen, würde somit nicht erreicht werden, und die kritische Gefährdungslage würde sich gleichzeitig mit den zunehmenden Angriffsmöglichkeiten zuspitzen. Das IT-Sicherheitsgesetz zeigt aber dennoch eine Aktion der Politik, Cyberbedrohungen entgegenzuwirken.

Zusammenfassend ist festzustellen, dass die Politik die von Cyber-Angriffen ausgehende Bedrohung erkennt und erste Schritte zum Schutz und Abwehr unternommen hat; so wurden neben dem IT-Sicherheitsgesetz einige weitere politische Rahmenbedingungen geschaffen und viele Ressorts nehmen Aufgaben im Bereich Cyber Security wahr (S3). Dennoch besteht gerade hinsichtlich der institutionellen

Organisation noch Handlungsbedarf, da die Zusammenarbeit der einzelnen Ressorts untereinander, aber auch mit den Bundesämtern und der Wirtschaft mehr oder weniger stark verbesserungswürdig ist. Dieser Aspekt kann als Nachteil der Organisationsstruktur betrachtet werden, da der Handlungsbedarf bei der Zusammenarbeit innerhalb der Politik und mit der Wirtschaft aus der fehlenden gesamthaften Verantwortung für Cyber Security in Deutschland resultiert (W2; W3; W4; W7; W6-T2; W8-T10; W6-T7). Dieses Problem setzt sich auf europäischer und internationaler Ebene fort, insbesondere bei der formellen Zusammenarbeit (vgl. Interview 6). Insofern könnte einigen Bedrohungen und Schwächen entgegengewirkt werden, indem die Zusammenarbeit verbessert wird, was zum Teil allerdings bereits gelungen ist (S4). Hier könnte angesetzt und untersucht werden, wie die Zusammenarbeit bereits verbessert werden konnte und dieses Vorgehen eventuell weiter genutzt werden, um die Zusammenarbeit innerhalb der Politik und auch mit der Wirtschaft weiter zu verbessern (S4-T10).

Weiterhin hat die Analyse ergeben, dass politischer Handlungsbedarf bei der Festlegung der Rahmenbedingungen besteht. Die Rahmenbedingungen, welche bereits umgesetzt werden konnten, wie das Cyber-AZ, oder der Cyber-SR oder jüngst das IT-Sicherheitsgesetz, sollten somit insbesondere weiterhin gestärkt werden (W15-T3; W15-T1; W15; T8). Wie erwähnt, wirkt hier die Umsetzung des IT-Sicherheitsgesetzes als besonders gefährdet (S3-T9), weshalb strategische Maßnahmen der Politik erforderlich wären, die auf dem Arbeitsmarkt hochqualifizierte Fachkräfte im Bereich Cyber Security fördern. Denn anderenfalls ist davon auszugehen, dass nicht nur die geplanten neuen Stellen in staatlichen Institutionen nicht besetzt werden können, sondern auch die vorhandenen und entstehenden Arbeitsplätze in der Wirtschaft nicht mit hochqualifizierten Fachkräften (InformatikerInnen mit Spezialisierung in Cyber Security) besetzt werden können. Einige Unternehmen begegnen diesem Mangel bereits, indem sie selbst ausbilden. Folglich kann zukünftig davon ausgegangen werden, dass Unternehmen von der Politik fordern werden, sich für die Ausbildung insbesondere von InformatikerInnenn im Bereich Cybersi-

cherheit stärker einzusetzen. Auch bei der Bundesverwaltung könnte die Ausbildung von Fachkräften eine Lösung darstellen, um dem Mangel an geeignetem Fachpersonal entgegenzuwirken. Eine grundsätzliche Beseitigung des Mangels kann jedoch dadurch mutmaßlich nicht erreicht werden. Das wird deutlich durch die großen Unternehmen, die selbst ausbilden, aber dennoch über einen Mangel an kompetenten MitarbeiterInnen klagen, aber auch durch die naheliegende Annahme, dass die Mehrheit der von der Problematik betroffenen Unternehmen eine derartige Ausbildung nicht anbieten können. Hierunter fallen insbesondere kleine und mittelständische Unternehmen, denen die Ressourcen dazu fehlen, vor allem die erforderliche Expertise. Dies wird deutlich anhand des größten deutschen Erdgastransporteurs, der nicht imstande ist, sich selbst zu schützen und seine Cyber Security deshalb ausgelagert hat, dies aber selbst als Schwäche erkennt (vgl. Interview 11), wodurch die Aussage gerechtfertigt wird, dass eine entsprechende Ausbildung im Unternehmen nicht als Lösung betrachtet wurde. Hieran schließt sich das Handlungsfeld an, dass insgesamt zu wenig in Forschung und Entwicklung investiert wird, sei es von der Politik oder von den Unternehmen (T11; T12; W18). Die Aufgabe der Politik, zumindest ein Feld zu schaffen, in dem Forschung möglich ist (vgl. Interview 12) ist insofern stärker zu betonen als die der Unternehmen. Die wenigen vorhandenen und dringend benötigten Fachkräfte werden nicht vorrangig in Forschung und Entwicklung eingesetzt werden. Der Mangel an hochqualifizierten Fachkräften weist demnach auf Mängel in der Ausbildung, unzureichende Forschung und Lehre im Hochschulbereich und auf ein im Vergleich zur freien Wirtschaft zu niedriges Lohnniveau an öffentlichen Einrichtungen hin (W17). Doch aus mangelnder Investition der Politik in Forschung und Entwicklung entsteht eine Schwäche, da hierdurch neuen Cyberbedrohungen zukünftig nicht angemessen begegnet werden kann. Neben fehlenden Kompetenzen und dem Fachwissen ist in diesem Zusammenhang der Mangel an technischen Ressourcen zu erwähnen (W10; W18-T9). Die Vernachlässigung dieser Handlungsfelder kann nachteilige Auswirkungen auf den Schutz der Kritischen Infrastrukturen und der Wirtschaft sowie auf

die Cyberverteidigung (W12) haben. Hiermit wird deutlich, dass die ermittelten Handlungsfelder Zusammenhänge aufweisen, auf die jedoch im Rahmen dieser Arbeit nicht tiefergehend eingegangen werden kann. Es bleibt jedoch festzuhalten, dass die gemeinsame Berücksichtigung der zusammenhängenden Handlungsfelder eine erfolgreichere Verbesserung der Cyber Security in Deutschland bedingen kann als eine Einzelbetrachtung.

7 Fazit

In der vorliegenden Ausarbeitung wurde den Fragestellungen nachgegangen, wie Cyber Security politisch und institutionell in Deutschland organisiert ist und welche strategischen Planungen es hierzu gibt. Zur Beantwortung dieser Fragen wurden zunächst die Cyberbedrohungen analysiert (Kapitel 2). Dabei wurde deutlich, dass die Cybersicherheit vielfältigen Bedrohungen entgegenwirken soll, die sowohl eine große Vielfalt als auch Querverbindungen aufweisen, was wiederum zu Definitionsproblemen bei der Abgrenzung führen kann.

Aufbauend hierauf wurden die Verträge, Pläne und Strategien zur Cyber Security betrachtet (Kapitel 3). Hieraus ging hervor, dass Cyber-Angriffe eine hohe Gefährdung für Kritische Infrastrukturen und Unternehmen darstellen, generell jedoch *Staat, Wirtschaft und Gesellschaft* bedrohen. Die Politik legt bereits seit 2005 einen Schwerpunkt auf den Schutz der Kritischen Infrastrukturen, wobei dieser ausgehend von Kommunikationsinfrastrukturen nach und nach auch auf technische Basisinfrastrukturen und sozioökonomische Infrastrukturen ausgeweitet wurde. Zugleich wird jedoch die Verantwortung für den Schutz vor Cyber-Angriffen in erster Linie bei den Unternehmen selbst gesehen.

Die politische und institutionelle Organisation der Cyber Security in Deutschland wurde eingehender untersucht, indem die jeweiligen Aufgaben der Bundesministerien und Bundesämter analysiert wurden (Kapitel 4). Hierzu wurden qualitative Interviews mit VertreterInnen aus der Politik und der Wirtschaft durch-

geführt und ausgewertet. Die Analyse hat gezeigt, dass die Aufgaben im Bereich Cyber Security fragmentiert organisiert sind und dadurch ein Informationsverlust zwischen den Bundesministerien und Bundesämtern entsteht. Der Grund hierfür ist unter anderem eine unzureichende Zusammenarbeit zwischen den Bundesministerien und Bundesämtern, die sich letztlich bis auf die NATO-Ebene auswirkt.

Da die Wirtschaft besonders von Cyber-Angriffen bedroht ist, wurde sie ebenfalls analysiert (Kapitel 5). Dabei wurden exemplarisch drei Unternehmen betrachtet, da die Wirtschaft nicht den Schwerpunkt dieser Arbeit bildet. Aufgrund ihrer Bedrohungslage wurden zwei Betreiber Kritischer Infrastrukturen analysiert. Das dritte Unternehmen wurde stellvertretend für eine Schlüsselindustrie in Deutschland ausgewählt. Aus der Analyse der betrachteten Unternehmen ist zu schließen, dass diese stark von Wirtschaftsspionage betroffen sind. Eine Bedrohung für Unternehmen in Deutschland geht insbesondere von der Cyberspionage durch ausländische Nachrichtendienste aus. Unternehmen sind jedoch nicht in der Lage, sich davor zu schützen. Die Analyse hat außerdem gezeigt, dass bei der Zusammenarbeit mit der Politik eine Verbesserung notwendig wäre, insbesondere bei jener im UP KRITIS-Rat sowie bei der Zusammenarbeit mit dem BSI und dem Cyber-AZ.

Die Frage zur strategischen Planung von Cyber Security konnte mithilfe der Analyse der Bundesministerien, Bundesämter und Unternehmen, aber auch anhand der durchgeführten Experteninterviews mit VertreterInnen aus Politik und Wirtschaft beantwortet werden. Dabei zeigte sich, dass die untersuchten Strategien, Pläne und Verträge der Politik, wie auch die Interviewpartner bestätigen, zwar strategische Planungen zu Cyber Security im Ansatz erkennen lassen, eine übergeordnete Gesamtstrategie war jedoch kaum festzustellen, und auch die strategischen Maßnahmen bedürfen einer Kritik: Bei den einzelnen Bundesministerien und Bundesämtern zeigen sich zwar einzelne Ansätze strategischer Planung, allerdings war keine konkrete und keine übergeordnete Strategie aller Bundesministerien und Bundesämter zu ermitteln. Diese folgen zwar der Cyber-Sicherheitsstrategie der

Bundesregierung, aus denen strategische Planungen hervorgehen, jedoch konnten keine derartigen neu geplanten Strategien aufgezeigt werden. Das BSI plant zwar, z. B. den IT-Grundschutz zu erneuern, aber konkrete Umsetzungsmaßnahmen wurden hierzu noch nicht erwogen. Auch das BMVg braucht dringend einen Ausbau der Kompetenzen zum Cyberterrorismus, doch auch hierzu ist scheinbar keine strategische Planung vorhanden. Einen Mangel an strategischer Planung und konkreten Umsetzungsmaßnahmen offenbarte auch die Untersuchung der Bundeswehr bei der Cyberverteidigung und des BBKs beim Bevölkerungsschutz im Falle einer Katastrophe durch einen Cyber-Angriff. Zwar wird von der Politik eine Strategie verfolgt, die Kritischen Infrastrukturen sicherer zu machen, das IT-Sicherheitsgesetz selbst kann letztlich aber nur als eine Maßnahme hierzu betrachtet werden. Dennoch legen die Experteninterviews nahe, dass die untersuchten Bundesministerien und Bundesämter die kritische Bedrohungslage durch Cyber-Angriffe wahrnehmen und eine Stärkung der Cyber Security anstreben.

Abschließend wurde zur weiteren Beantwortung der Forschungsfrage zur Wirksamkeit von Cyber Security in Deutschland und zu den Handlungsfeldern der Politik eine SWOT-Analyse durchgeführt (Kapitel 6). Anhand der vorangegangenen Analyse der Politik und der Wirtschaft konnten Stärken und Schwächen der Cybersicherheitspolitik herausgearbeitet werden. Die Chancen und Bedrohungen wurden ebenfalls identifiziert, wobei die Wirtschaft als wesentlicher Teil der politischen Umwelt einbezogen wurde. Im nächsten Schritt wurden in der SWOT-Matrix die Stärken und Schwächen den Chancen und Bedrohungen zugeordnet und gegenübergestellt, um eine strategische Gewichtung des Handlungsbedarfes vorzunehmen. So besteht insbesondere Verbesserungsbedarf bei der Zusammenarbeit der Bundesministerien und Bundesämter untereinander sowie mit den Unternehmen – letzterer beidseitig. Ein weiteres Handlungsfeld bildet die personelle und technische Ressourcenausstattung der Bundesministerien und Bundesämter.

Das IT-Sicherheitsgesetz kann als erster Schritt zur Verbesserung der Cyber Security in Deutschland betrachtet werden. Es gilt jedoch nur für die Betreiber Kriti-

scher Infrastrukturen. Auch sind nicht nur die Betreiber Kritischer Infrastrukturen von Cyber-Angriffen bedroht, sondern grundsätzlich alle Unternehmen. Darüber hinaus weist das IT-Sicherheitsgesetz einige weitere Schwächen auf. So sind bislang die betroffenen Kritischen Infrastrukturen noch nicht klar definiert worden. Somit bleibt offen, welche Unternehmen mit dem Inkrafttreten der Rechtsverordnung betroffen sein werden. Darüber hinaus ist es fraglich, ob mit dem vorgeschriebenen Mindestmaß an IT-Sicherheit überhaupt ausreichende Cyber Security bewirkt werden kann. Denn es gibt zu wenige Innovationen und Entwicklungen der deutschen IT-Industrie, die jedoch für sichere deutsche Softwareprodukte notwendig wären. Allerdings fordern die Unternehmen von der Politik mehr Investitionen in Forschung und Entwicklung für Cyber Security. Letztlich besteht eine große Gefahr besonders für die Umsetzung des IT-Sicherheitsgesetzes in dem Mangel hochqualifizierter Fachkräfte auf dem Arbeitsmarkt, aber auch beschäftigter Arbeitnehmer im Bereich Cyber Security. Hiervon ist sowohl die Wirtschaft als auch die Politik betroffen. Zusammenfassend ergibt sich ein Handlungsbedarf in folgenden Bereichen:

- Dadurch dass es keine gesamthafte Verantwortung für Cyber Security in Deutschland gibt, ergibt sich Handlungsbedarf bei der Zusammenarbeit innerhalb der Politik und mit der Wirtschaft sowie der strategischen Koordination.
- Die kritische Gefährdung durch Cyberbedrohungen (Wirtschaftsspionage, Cyberkriminalität, Cyberterrorismus) für Staat, Wirtschaft und Gesellschaft muss reduziert werden.
- Die Politik muss weitere Rahmenbedingungen schaffen.
- Die Kompetenzen der Arbeitnehmer sind auszubauen.
- Die personelle und technische Ausstattung der Bundesministerien und Bundesämter bedarf einer Verbesserung.
- Die Bundeswehr muss mit den für die Cyberverteidigung notwendigen Ressourcen ausgestattet werden.
- Durch Förderung von Forschung und Entwicklung sollten sichere IT-Systeme und Softwareprodukte entworfen werden.

- Auf europäischer Ebene ist eine Verbesserung der formellen Zusammenarbeit erforderlich.
- Auf internationaler Ebene muss die bestehende formelle Zusammenarbeit weiter ausgebaut und verbessert werden. Aufgrund der politischen Ereignisse findet gegenwärtig bei der Strafverfolgung von Cyberkriminalität keine Zusammenarbeit mit Russland statt. Mit China ist die Zusammenarbeit bei der Strafverfolgung von Cyberkriminalität aufgrund möglicher Todesurteile für StraftäterInnen erschwert.

Weitergehend kann eine Gewichtung vorgenommen werden, die sich aus der Feststellung ergibt, dass einige der identifizierten Handlungsfelder zusammenhängen und dass es zentrale Handlungsfelder gibt, die sich stark auf andere auswirken. Ausgehend von der Analyse lässt sich somit das Ergebnis der vorliegenden Arbeit wie folgt zusammenfassen: Die politisch-institutionelle Organisation von Cyber Security in der Bundesrepublik Deutschland ist durch eine Vielfalt an Ressorts und die Vielschichtigkeit der Aufgabenteilung und Kooperationen unter besonderer Berücksichtigung Kritischer Infrastrukturen gekennzeichnet. Sie steht gegenwärtig allerdings vor den Herausforderungen, a) eine übergeordnete Strategie zu erarbeiten, diese begrifflich präzise zu definieren und hieraus konkrete Maßnahmen abzuleiten, b) kompetentes Fachpersonal zu akquirieren und die Kompetenz des vorhandenen Personals zu steigern und c) die Koordination und Zusammenarbeit der Akteure zu optimieren, möglicherweise durch die Schaffung einer zentralen Institution.

Die Forschungsfrage konnte somit beantwortet werden, wenn auch aufgrund der Umfangsbeschränkung auf einige Stärken, Schwächen, Chancen und Bedrohungen nicht intensiver eingegangen werden konnte. Methodisch sind die Interviews kritikwürdig, da lediglich nur ein Vertreter pro politischer Institution oder Unternehmen interviewt wurde und damit nur eine subjektive Wahrnehmung wiedergegeben werden konnte. Folglich sind die Ergebnisse nicht repräsentativ.

Dennoch konnten Tendenzen von Stärken, Schwächen, Chancen und Bedrohungen, sowie Handlungsfelder für die Politik aufgezeigt werden.

In dieser Arbeit wurde die SWOT-Analyse adaptiert, um zunächst nur Handlungsfelder für die Politik strategisch zu gewichten. In den Sozialwissenschaften wird die SWOT-Analyse meist nur für die Analyse der internen und externen Faktoren verwendet und auf eine Ableitung von Strategien verzichtet. In dieser Arbeit wurde der Versuch unternommen, dennoch einen strategischen Handlungsbedarf abzuleiten, an denen künftige Arbeiten ansetzen können, um konkrete Handlungsempfehlungen in Form von Strategien und Maßnahmen zu erarbeiten. Hierzu könnte unter anderem eine repräsentative Studie angefertigt werden, die einzelne politische Institutionen und (größere) Unternehmen tiefgehender analysiert, mitunter anhand von standardisierten Fragebögen und weiteren Interviews. Hierbei müsste auch der Schutz der Bundesverwaltung vor Cyber-Angriffen untersucht werden.

Da insbesondere Handlungsbedarf beim Auf- und Ausbau der hochqualifizierten Fachkräfte auf dem Arbeitsmarkt besteht, könnte untersucht werden, ob eine Förderung der Hochschul-Ausbildung im Bereich Cyber Security sinnvoll wäre. Weiterhin wäre zu überprüfen, ob und inwiefern in politischen Institutionen auch Fachkräfte speziell im Bereich der Cyber Security ausgebildet werden können und auch die Höhe der Gehälter für hochqualifizierte InformatikerInnen aus diesem Bereich wäre zu überdenken.

In der vorliegenden Arbeit wird anhand der Analyse zwar die Annahme vertreten, dass sich eine zentral koordinierende Institution auf Ebene der Bundesverwaltung, welche die gesamthafte Verantwortung für Cyber Security übernimmt, positiv auf die politische und institutionelle Organisation von Cyber Security in Deutschland auswirken würde. Hierzu wäre jedoch eine genaue Untersuchung erforderlich, inwiefern durch eine zentrale Koordination eine bessere Zusammenarbeit innerhalb der Politik, aber auch mit der Wirtschaft geschaffen und dem Informationsverlust entgegengewirkt werden könnte. Wenn für diese Handlungsfelder

Strategien entwickelt werden würden, könnte bereits eine große Verbesserung der Cyber Security in Deutschland erzielt werden, da hier zusammenhängende Handlungsfelder bestehen.

Eine weitere Forschungsfrage wäre, inwieweit die Bundeswehr ihre Cyberverteidigung ausbauen müsste. Hier wäre auch eine intensivere Untersuchung der Bedrohungslage durch Cyber-Angriffe für Deutschland oder die EU erforderlich. Die Zusammenarbeit auf EU- und NATO-Ebene wurde in dieser Arbeit nur angeschnitten, sodass die politische und institutionelle Organisation auf europäischer und internationaler Ebene weiterführend analysiert werden sollte. Ein Vergleich Deutschlands mit anderen Staaten könnte Möglichkeiten zur Verbesserung der politischen und institutionellen Organisation von Cyber Security aufzeigen. Insgesamt ist die Thematik Cyber Security ein sehr junges Forschungsfeld und es gibt noch viele Forschungsansätze, die verfolgt werden könnten.

Es konnten bereits einige Maßnahmen zur Verbesserung der Cyber Security in Deutschland umgesetzt werden. Es besteht aber noch großer Handlungsbedarf insbesondere vor dem Hintergrund der fortschreitenden Digitalisierung. Diese Ausarbeitung hat Handlungsfelder der Politik im Bereich Cyber Security in Deutschland aufgezeigt, für die von der Politik, Wirtschaft und Wissenschaft ein Handlungsbedarf besteht. Denn mit der digitalen Entwicklung werden Cyberbedrohungen für Staat, Wirtschaft und Gesellschaft weiterhin zunehmen und letztlich wird das Gefährdungspotenzial für Kritische Infrastrukturen und für die Wettbewerbsfähigkeit der deutschen Industrie aber auch auf längere Sicht für den Wohlstand zunehmen.

8 Literatur- und Quellenverzeichnis

Amtsblatt der Europäischen Union (2004). Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10. März zur Erreichung der Europäischen Agentur für Netz- und Infomrationssicherheit. http://eur-

lex.europa.eu/legal-content/DE/TXT/HTML/?uri=URISERV:l24153&from=DE. Zugegriffen: 4. Juli 2015.

ASW Bundesverband (2015). Über den ASW Bundesverband. http://asw-bundesverband.de/ueber-uns/. Zugegriffen: 7. Juni 2015.

Auswärtiges Amt (2014). Cyber-Außenpolitik. http://www.auswaertiges-amt.de/sid_847A505CCFFAD7AEAD7081B3BBC234D7/DE/Aussenpolitik/GlobaleFragen/Cyber-Aussenpolitik/KS_Cyber-Aussenpolitik_node.html. Zugegriffen: 9. Februar 2015.

Auswärtiges Amt (2015a). Organisationsplan des Auswärtigen Amts. http://www.auswaertiges-amt.de/cae/servlet/contentblob/373560/publicationFile/205768/Organisationsplan.pdf. Zugegriffen: 7. Juni 2015.

Auswärtiges Amt (2015b). Sonderbeauftragter für Cyber-Außenpolitik. http://www.auswaertiges-amt.de/sid_F56FC42E55D8ABFCA26C99582A9279E5/DE/AAmt/Koordinatoren/Cyber-AP/Uebersicht_node.html. Zugegriffen: 7. Juni 2015.

Baumgärtner, M., Röbel, S. & Schindler, J. (2015, 2. Juni). Cyberattacke auf den Bundestag. Spur der Hacker führt nach Russland. In: Spiegel Online. http://www.spiegel.de/netzwelt/netzpolitik/cyberangriff-auf-bundestag-experten-vermuten-russische-taeter-a-1036823.html. Zugegriffen: 22. Juli 2015.

Bendiek, A. (2013). Kritische Infrastrukturen, Cybersicherheit, Datenschutz. Die EU schlägt Pflöcke für digitale Standortpolitik ein. *SWP-Aktuell 35*. Stiftung Wissenschaft und Politik (SWP).

Bendiek, A., Dickow, M. & Meyer, J. (2012). Europäische Außenpolitik und das Netz. Orientierungspunkte für eine Cyber-Außenpolitik der EU. *SWP-Aktuell 60*. Stiftung Wissenschaft und Politik (SWP). .

Bendiek, A., Ulmer, K. (2013). Cybersicherheit - eine facettenreiche politische Herausforderung. Aus internationale Zeitschriften 2012/2013. *SWP-Aktuell 3*. Stiftung Wissenschaft und Politik (SWP).

Berger, C. (2013). Zwischen Strafverfolgung und nachrichtendienstlicher Analyse. Konsequenzen aus der Europäisierung der Cybersicherheitspolitik für Deutschland. *Vierteljahreszeitschrift des Instituts für Europäische Politik in Zusammenarbeit mit dem Arbeitskreis Europäische Integration (4)*. S. 307-324.

Bewarder, M., Clauß, U. & Flade, F. (2015, 11. Juni). Verfassungsschutz verfolgt Spur nach Russland. Die Welt.http://www.welt.de/politik/deutschland/article142372328/Verfassungsschutz-verfolgt-Spur-nach-Russland.html. Zugegriffen: 14. Juli 2015.

Biermann, K. (2014, 7. Juni). Angriffe aus dem Internet. Deutsches Cyber-Abwehrzentrum kann nichts abwehren. Zeit Online. http://www.zeit.de/digital/internet/2014-06/cyber-abwehrzentrum-bundesrechnungshof. Zugegriffen: 8. Juni 2015.

Biermann, K. (2015, 21. Mai). Hacker. Bundestag kann Cyberangriff nicht stoppen. Zeit Online. http://www.zeit.de/digital/datenschutz/2015-05/hackerangriff-bundestag-sommerpause. Zugegriffen: 20. Juni 2015.

BITKOM (2015). Über uns. http://www.bitkom.org/Bitkom/%C3%9Cber-uns.html. Zugegriffen: 3. Juli 2015.

BITKOM und Fraunhofer IAO (2014). Industrie 4.0 – Volkswirtschaftliches Potenzial für Deutschland. Studie. https://Masterarbeit 09.08.docx. Zugegriffen: 5. Juli 2015.

Bötticher, A. (2015). Die Strukturlandschaft der Inneren Sicherheit der Bundesrepubik Deutschland. In Lange, H-J., Bötticher, A. (Hrsg.). *Cyber-Sicherheit*, *Studien zur Inneren Sicherheit*, Bd. 18. (S. 69-102). Wiesbaden: Springer VS.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2014). Organigramm. http://www.bbk.bund.de/DE/DasBBK/UeberdasBBK/Organigramm/Organigramm2.html. Zugegriffen: 11. Juni 2015.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2015a). Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. http://www.bbk.bund.de/DE/DasBBK/UeberdasBBK/ueberdasbbk_node.html. Zugegriffen: 11. Juni 2015.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2015b). Kritische Infrastrukturen. http://www.bbk.bund.de/DE/AufgabenundAusstattung/KritischeInfrastrukturen/kritischeinfrastrukturen_node.html. Zugegriffen: 11. Juni 2015.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und Bundesamt für Sicherheit in der Informationstechnik (2011-2013). NIS-Richtline (Netz- und Informationssicherheit).: http://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Internationales/NIS_Richtlinie/NIS-Richtlinie_node.html. Zugegriffen: 4. Juli 2015.

Bundesamt für Sicherheit in der Informationstechnik (2012). Sicherheit und Verantwortung im Cyber-Raum. http://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/Sicherheit_Verantwortung_im_Cyber_Raum.pdf;jsessionid=60FEBB0C5392AAE255BA4711A178E9E4.2_cid368?__blob=publicationFile. Zugegriffen: 12. Feb. 2015.

Bundesamt für Sicherheit in der Informationstechnik (2014). Die Lage der IT-Sicherheit in Deutschland 2014. http://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile. Zugegriffen: 16. Jan. 2015.

Bundesamt für Sicherheit in der Informationstechnik (2015a). Allianz für Cyber-Sicherheit. Teilnehmer. http://www.allianz-fuer-cybersicherheit.de/ACS/DE/Ueber_uns/Akteure/Teilnehmer/teilnehmer.html. Zugegriffen: 3. Juli 2015.

Bundesamt für Sicherheit in der Informationstechnik (2015b). Allianz für Cyber-Sicherheit. Über uns. http://www.allianz-fuer-cybersicherheit.de/ACS/DE/Ueber_uns/ueber_uns.html. Zugegriffen: 3. Juli 2015.

Bundesamt für Sicherheit in der Informationstechnik (2015c). Fragen und Antworten zum Inkrafttreten des IT-Sicherheitsgesetzes. http://www.bsi.bund.de/SharedDocs/FAQs/DE/BSI/IT-SiGesetz/faq_node.html. Zugegriffen: 6. Aug. 2015.

Bundesamt für Sicherheit in der Informationstechnik (2015d). IT-Grundschutz. http://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html. Zugegriffen: 4. Juni 2015.

Bundesministerium für Sicherheit in der Informationstechnik (2015e). Nationale und internationale Zusammenarbeit. http://www.bsi.bund.de/DE/Themen/IT-Krisenmanagement/CERTBund/Zusammenarbeit/zusammenarbeit_node.html. Zugegriffen: 4. Juli 2015.

Bundesamt für Sicherheit in der Informationstechnik (2015f). Organisationsübersicht des BSI. Aufgaben. http://www.bsi.bund.de/DE/DasBSI/Aufgaben/aufgaben_node.html. Zugegriffen: 19. Jan. 2015.

Bundesamt für Sicherheit in der Informationstechnik und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2011-2013a). Internationale Aktivitäten zum Schutz Kritischer Infrastrukturen. http://www.bbk.bund.de/SubSites/Kritis/DE/Aktivitaeten/Internationales/internationales_node.html. Zugegriffen: 4. Juli 2015.

Bundesamt für Sicherheit in der Informationstechnik und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2011-2013b). Zusammenarbeit im Rahmen des UP KRITIS. http://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/upk_node.html. Zugegriffen: 25. Feb. 2015.

Bundesamt für Verfassungsschutz (2015a). Die Organisation des Amtes ist kein Geheimnis. http://www.verfassungsschutz.de/de/das-bfv/aufgaben/die-organisation-des-amtes-ist-kein-geheimnis. Zugegriffen: 16. Juni 2015.

Bundesamt für Verfassungsschutz (2015b). Elektronische Angriffe. http://www.verfassungsschutz.de/de/arbeitsfelder/af-elektronische-angriffe. Zugegriffen: 9. Feb. 2015.

Bundesamt für Verfassungsschutz (2015c). Sabotageschutz. http://www.verfassungsschutz.de/de/arbeitsfelder/af-geheim-und-sabotageschutz/sabotageschutz. Zugegriffen: 16. Juni 2015.

Bundesamt für Verfassungsschutz (2015d). Was genau macht der Verfassungsschutz?. http://www.verfassungsschutz.de/de/das-

bfv/aufgaben/was-genau-macht-der-verfassungsschutz. Zugegriffen: 16. Juni 2015.

Bundesamt für Verfassungsschutz (2015e). Was tut das BfV? http://www.verfassungsschutz.de/de/arbeitsfelder/af-spionage-und-proliferationsabwehr/was-tut-das-bfv. Zugegriffen: 16. Juni 2015.

Bundesamt für Verfassungsschutz (2015f). Wirtschaftsschutz. http://www.verfassungsschutz.de/de/arbeitsfelder/af-wirtschaftsschutz. Zugegriffen: 16. Juni 2015.

Bundesamtes für Ausrüstung Informationstechnik und Nutzung der Bundeswehr (BAAINBw) (2014, 27. Nov.). Portrait des IT-ZentrumBw. http://www.baainbw.de/portal/a/baain/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK9pMTEzDy9lMzUvOKSYr3MkiqgWEF-UUlRYmaJfkG2oyIAPt3icg!!/. Zugegriffen: 17. Juli 2015.

Bundeskriminalamt (2013). Cybercrime. Bundeslagebild 2013. http://www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true. Zugegriffen: 17. Juli 2015.

Bundeskriminalamt (2015a). Der gesetzliche Auftrag. http://www.bka.de/nn_206342/DE/DasBKA/Auftrag/auftrag__node.html?__nnn=true. Zugegriffen: 10. Juni 2015.

Bundeskriminalamt (2015b). Internetkriminalität/ Cybercrime. http://www.bka.de/nn_238144/DE/ThemenABisZ/Deliktsbereiche/InternetKriminalitaet/internetKriminalitaet__node.html?__nnn=true. Zugegriffen: 10. Juni 2015.

Bundeskriminalamt (2015c). Organisation/ Aufbau des Bundeskriminalamtes. http://www.bka.de/nn_205958/DE/DasBKA/Organisation/organisation__node.html?__nnn=true. Zugegriffen: 10. Juni 2015.

Bundeskriminalamt (2015d). Organisationsübersicht. http://www.bka.de/DE/DasBKA/Organisation/Organigramm/organigramm__node.html?__nnn=true. Zugegriffen: 9. Juni 2015.

Bundesministerium der Verteidigung (2006). Weißbuch 2006 zur Sicherheitspolitik Deutschlands und zur Zukunft der Bundeswehr. Berlin: Bundesministerium der Verteidigung.

Bundesministerium der Verteidigung (2015a). Das Bundesministerium der Verteidigung.http://www.bmvg.de/portal/a/bmvg/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK9pNyydL3czLzM4pLUoszSXP2CbEdFAIh6LHQ!/. Zugegriffen: 2. Juli 2015.

Bundesministerium der Verteidigung (2015b). Ministerin trifft Cyber-Experten der Bundeswehr. http://www.bmvg.de/portal/a/bmvg/!ut/p/c4/NYuxDsIwDET_yE4WEGxUGYCRpYQtbaPIqEkq12mXfjzJwJ30hns6_GBtchsFJ5STm_GNdqTrsMMQtwDfXLiuECnRKp6pROzbZ_Iw5uSlUXwSqgzsJDMsmWVupjBXAzShVdp0Sqt_9HGx5v7s9flkHt0LlxhvP23z4Qg!/. Zugegriffen: 17. Juli 2015.

Bundesministerium der Verteidigung (2015c). Sicherheitspolitik. http://www.bmvg.de/portal/a/bmvg/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK9pNyydL3izOSM1KKM1MyS4oL8nMySzGz9gmxHRQDTl3MX/. Zugegriffen: 4. Juli 2015.

Bundesministerium der Verteidigung (2015d). Überblick: Cyber-Abwehr der Bundeswehr. http://www.bmvg.de/portal/a/bmvg/!ut/p/c4/NYu7DsIwEAT_yGdLNKEjCiBaioTQOY7lHPilyyU0fDx2wa40xY4WnlAa9Y5OM6aoPTxgNHicPmIKuxOvtFFZxYpmsbRY5DUnj4xvGOp1tsKkaLmSbWQsdKQ5kciJ2FezERUjcIZRqq6VSv6jvs1wvlz7QyO7W3uHHMLpB0N2Un0!/. Zugegriffen: 2. Juli 2015.

Bundesministerium des Innern (2005). Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI). http://www.bmi.bund.de/cae/servlet/contentblob/121734/publicationFile/13577/Nationaler_Plan_Schutz_Informationsinfrastrukturen.pdf. Zugegriffen: 27. Feb. 2015.

Bundesministerium des Innern (2007). Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2007/Kritis.pdf?__blob=publicationFile. Zugegriffen: 9. Feb. 2015.

Bundesministerium des Innern (2009, 17. Juni). Nationale Stra-te-gie zum Schutz Kri-ti-scher Infrastrukturen (KRI-TIS-Stra-te-gie). http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.pdf;jsessionid=718B22455996289CD1F50ECE749ADBF1.2_cid373?__blob=publicationFile. Zugegriffen: 5. Feb. 2015.

Bundesministerium des Innern (2011). Cyber-Sicherheitsstrategie für Deutschland. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile. Zugegriffen: 5. Feb. 2015.

Bundesministerium des Innern (2014a, 17. Dez.). Bundesregierung beschliesst IT-Sicherheitsgesetz. http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2014/12/bundeskabinett-beschlie%C3%9Ft-it-sicherheitsgesetz.html. Zugegriffen: 5. Feb. 2015.

Bundesministerium des Innern (2014b). Digitale Agenda im Fokus. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2014/digitale-agenda-im-fokus.pdf?__blob=publicationFile. Zugegriffen: 5. Feb. 2015.

Bundesministerium des Innern (2014c, 8. Dez.). Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). http://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Kurzmeldungen/entwurf-it-sicherheitsgesetz.pdf?__blob=publicationFile. Zugegriffen: 5. Feb. 2015.

Bundesministerium des Innern (2015a). CyberSicherheitsrat. http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/Cybersicherheitsrat/cybersicherheitsrat_node.html. Zugegriffen: 5. Feb. 2015.

Bundesministerium des Innern (2015b). CyberSicherheitsstrategie für Deutschland. http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/cybersicherheitsstrategie_node.html. Zugegriffen: 11. März 2015.

Bundesministerium des Innern (2015c). Das BMI stellt sich vor. http://www.bmi.bund.de/DE/Ministerium/BMI-Vorstellung/bmi-vorstellung_node.html;jsessionid=DCFB3F173DDB35D5C8202A53BAD17A67.2_cid373. Zugegriffen: 25. Feb. 2015.

Bundesministerium des Innern (2015d, 23. Jan.). "Innenpolitik ist schon längst keine rein nationale Angelegenheit mehr". http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2015/01/bundesinnenminister-beim-weltwirtschaftsforum-in-davos.html?nn=3314802. Zugegriffen: 5. Feb. 2015.

Bundesministerium des Innern (2015e). Ministerium. Behörden und Einrichtungen. http://www.bmi.bund.de/DE/Ministerium/BehoerdenEinrichtungen/behoerdeneinrichtungen_node.html. Zugegriffen: 25. Feb. 2015.

Bundesministerium des Innern (2015f). Nationales Cyber-Abwehrzentrum. http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/Cyberabwehrzentrum/cyberabwehrzentrum_node.html. Zugegriffen: 5. Feb. 2015.

Bundesministerium des Innern (2015g, 2. Feb.). Organisationsplan. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Ministerium/PDF_Organigramm_BMI.pdf?__blob=publicationFile. Zugegriffen: 25. Feb. 2015.

Bundesministerium des Innern (2015h, 5. Juli). Sondersitzung des Nationalen CyberSicherheitsrates. http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2013/07/cybersicherheitsrat.html. Zugegriffen: 8. Juni 2015.

Bundesministerium für Bildung und Forschung (2015). Sicher in der digitalen Welt. http://www.bmbf.de/de/73.php. Zugegriffen: 20. Juli 2015.

Bundesministerium für Verkehr und digitale Infrastruktur (2014). Sicherheitsstrategie für die Güter- verkehrs- und Logistikwirtschaft. Schutz kritischer Infrastrukturen und verkehrsträgerübergreifende Gefahrenabwehr. http://www.bmvi.de/SharedDocs/DE/Anlage/Presse/baer_sicherheitsstrategie_15-01-2015.pdf?__blob=publicationFile. Zugegriffen: 5. Juni 2015.

Bundesministerium für Verkehr und digitale Infrastruktur (2015a). BBB News. Organisationserlass der Bundeskanzlerin. http://www.breitbandbuero.de/index.php?id=191&tx_ttnews%5Btt_news%5D=165&cHash=ca4272fab8c2ae3e97137bf8a4bbe13b&PHPSESSID=0a1aaa4359b1ced7b5c9d615dfc42cc0. Zugegriffen: 4. Juni 2015.

Bundesministerium für Verkehr und digitale Infrastruktur (2015b). Das Ministerium stellt sich vor. http://www.bmvi.de/DE/DasMinisterium/das-ministerium_node.html. Zugegriffen: 4. Juni 2015.

Bundesministerium für Verkehr und digitale Infrastruktur (2015c). Digitale Infrastruktur: Was wir wollen, was wir tun. http://www.bmvi.de/SharedDocs/DE/Artikel/DG/digitale-infrastruktur.html. Zugegriffen: 4. Juli 2015.

Bundesministerium für Verkehr und digitale Infrastruktur (2015d). Digitale Infrastruktur. Breitbandstrategie. http://www.bmvi.de/SharedDocs/DE/Artikel/DG/breitbandstrategie.html. Zugegriffen: 5. Juni 2015.

Bundesministerium für Wirtschaft und Energie (2015a). IT-Sicherheit in der Wirtschaft. Steuerkreis. http://www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Navigation/Task-Force/steuerkreis.html. Zugegriffen: 4. Juni 2015.

Bundesministerium für Wirtschaft und Energie (2015b, 29. Mai). Organisationsplan. http://www.bmwi.de/BMWi/Redaktion/PDF/M-O/organisationsplan-bmwi,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf. Zugegriffen: 4. Juni 2015.

Bundesnachrichtendienst (2015a). Abteilung TA. http://www.bnd.bund.de/DE/Einblicke/Aufbauorganisation/TA/ta_node.html. Zugegriffen: 11. Juni 2015.

Bundesnachrichtendienst (2015b). Arbeitsfelder. http://www.bnd.bund.de/DE/Arbeitsfelder/arbeitsfelder_node.html. Zugegriffen: 11. Juni 2015.

Bundesnachrichtendienst (2015c). Aufgaben. http://www.bnd.bund.de/DE/Arbeitsfelder/Aufgaben/aufgaben_node.html;jsessionid=B97478B34F0F188659BA463FFA88FA8B.2_cid377. Zugegriffen: 11. Juni 2015.

Bundesnachrichtendienst (2015d). Cyber-Sicherheit – Sicherung der nationalen Informationstechnik in Zeiten globaler Vernetzung. http://www.bnd.bund.de/DE/Themen/Lagebeitraege/Cyber-Sicherheit/Cyber-Sicherheit_node.html. Zugegriffen: 11. Juni 2015.

Bundesnachrichtendienst (2015e). Herausforderungen für den Bundesnachrichtendienst. http://www.bnd.bund.de/DE/Arbeitsfelder/Herausforderungen/herausforderungen_node.html. Zugegriffen: 11. Juni 2015.

Bundesnachrichtendienst (2015f). Kooperationen. http://www.bnd.bund.de/DE/Arbeitsfelder/Kooperationen/Kooperationen_node.html. Zugegriffen: 11. Juni 2015.

Bundesnetzagentur (2015). Über die Agentur. http://www.bundesnetzagentur.de/cln_1431/DE/Allgemeines/DieBundesnetzagentur/UeberdieAgentur/ueberdieagentur-node.html. Zugegriffen: 22. Juli 2015.

Deutscher Bundestag (2015, 18. März). Bundesregierung legt IT-Sicherheitsgesetz vor. http://www.bundestag.de/dokumente/textarchiv/2015/kw12_ak_it_sicherheitsgesetz/364984. Zugegriffen: 10. Juni 2015.

Bundesverband der Deutschen Industrie e. V. (2015). IT- und Cybersicherheit. http://www.bdi.eu/IT-und-Cybersicherheit.htm. Zugegriffen: 3. Juli 2015.

Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2970) (1990). Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), das zuletzt durch Artikel 1 des Gesetzes vom 7. Dezember 2011 (BGBl. I S. 2576) geändert worden ist.

http://www.bmi.bund.de/SharedDocs/Downloads/DE/Kurzmeldungen/statement_gesetz.pdf?__blob=publicationFile. Zugegriffen: 16. Juni 2015.

BWI Informationstechnik GmbH (2015a). Bundeswehr und BWI für erfolgreichen IT-Betrieb ausgezeichnet. http://www.bwi-it.de/index.php?id=613. Zugegriffen: 17. Juli 2015.

BWI Informationstechnik (2015b). Das IT-Projekt HERKULES. http://www.herkules-fakten.de. Zugegriffen: 2. Juli 2015.

Chaos Computer Club (2015). Chaos Computer Club. Home. http://www.ccc.de. Zugegriffen: 3. Juli 2015.

Clauß, U. (2015, 12. Juni). Die Welt kompakt. Ist dieser Angriff ein Fall für die Nato?. http://www.welt.de/print/welt_kompakt/article142373166/Ist-dieser-Angriff-ein-Fall-fuer-die-Nato.html. Zugegriffen: 5. Juli 2015.

Corporate Trust Business Risk & Crisis Management GmbH (2012). Studie: Industriespionage 2012. http://www.corporate-trust.de/pdf/CT-Studie-2014_DE.pdf. Zugegriffen: 5. Juli 2015.

Corporate Trust Business Risk & Crisis Management GmbH (2014). Studie: Industriespionage 2014. http://www.corporate-trust.de/pdf/CT-Studie-2014_DE.pdf. Zugegriffen: 9. Feb. 2015.

Cyber Security Summit - telekom.com (2014). Kontinuität für mehr Cyber-Sicherheit. http://www.cybersecuritysummit.de/current. Zugegriffen: 7. Juli 2015.

Daimler AG (2015). Unternehmen. http://www.daimler.com/unternehmen. Zugegriffen: 7. Juli 2015.

Daun, A. (2011). Nachrichtendienste in der deutschen Außenpolitik. In T. Jäger, A. Höse & K. Oppermann (Hrsg.), *Deutsche Außenpolitik: Sicherheit, Wohlfahrt,*

Institutionen und Normen (S. 171-197). Wiesbaden: VS Verlag für Sozialwissenschaften.

Deutsche Bundeswehr (2013, 17. Sep.). Neues Forschungszentrum Cyber Defense forciert IT-Netzwerk. http://www.bundeswehr.de/portal/a/bwde/!ut/p/c4/NYu7DsIwEAT_yGcXKIIuVhqEaGggaZCTnMIJP6LjEjd8PHbBrjTN7MIApdHttDihFJ2HB_QTncasxjyjcm_Z0Hv8qIwkyPiUFwaMcK_HMphSRKkUjEKFCztJrNbE4qvZmItRNEOvTWdNo_8x36O92svQHHR3tjdYQ2h_cChIGw!!/. Zugegriffen: 2. Juli 2015.

Deutsche Bundeswehr (2015a). Auftrag und Aufgaben. http://www.bundeswehr.de/portal/a/bwde/!ut/p/c4/DcLBDYAwCADAWVwA_v7cQvujlhLSBg1Su77mDhP-jF4VCr2MOu54nLrmCXkWhiecNZoT12AQH1Y6CRvQqOEkeLdt-QDDPuoC/. Zugegriffen: 2. Juli 2015.

Deutsche Bundeswehr (2015b, 23. Juni). Das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw). http://www.baainbw.de/portal/a/baain/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK9pMTEzDy90tSk1KLSPL2UxGKwgH5BtqMiAO1YLUk!/. Zugegriffen: 2. Juli 2015.

Deutsche Bundeswehr (2015c, 28. Apr.): Die organisatorische Struktur des Bundesamtes für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr. http://www.baainbw.de/portal/a/baain/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK9pMTEzDy90tSk1KLSPL38ovTEvMxi_YJsR0UAqDnulg!!/. Zugegriffen: 2. Juli 2015.

Deutsche Telekom AG (2014a, 31. Jan.). 3. Cyber Security Summit am 3. November. http://www.telekom.com/medien/konzern/212994. Zugegriffen: 7. Juli 2015.

Deutsche Telekom AG (2014b, 9. Mai). Schnelles Internet nicht nur für die Metropolen auf dem Land. http://blog.telekom.com/2014/05/09/schnelles-internet-nicht-nur-fuer-die-metropolen-auf-dem-land/. Zugegriffen: 7. Juli 2015.

Deutsche Telekom AG (2015a). Führender Europäischer Telekommunikationsanbieter. http://www.telekom.com/konzern/konzernprofil/92462. Zugegriffen: 7. Juli 2015.

Deutsche Telekom AG (2015b, 21. Jan.). ReSA: Unterstützung für Sicherheitsbehörden. http://www.telekom.com/verantwortung/sicherheit/news/263304. Zugegriffen: 11. Juni 2015.

Deutscher Bundestag (2011, 9. Sep.). Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Agnes Malczak, Omid Nouripour, Tom Koenigs, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 17/6802 –. Cyber-Strategie und Cyber-Außenpolitik der Bundesregierung. Drucksache 17/6971. http://dipbt.bundestag.de/doc/btd/17/069/1706971.pdf. Zugegriffen: 14. Juli 2015.

Deutscher Bundestag (2015a, 10. Juni). Beschlussempfehlung und Bericht des Innenausschusses (4. Ausschuss), zu dem Gesetzentwurf der Bundesregierung – Drucksache 18/4096 – Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), Drucksache 18/5121. http://dip21.bundestag.de/dip21/btd/18/051/1805121.pdf. Zugegriffen: 18. Juli 2015.

Deutscher Bundestag (2015b, 12. Juni). Bundestag beschließt das IT-Sicherheitsgesetz. http://www.bundestag.de/dokumente/textarchiv/2015/kw24_de_it_sicherheit/377026. Zugegriffen: 18. Juli 2015.

Deutscher Bundestag (2015c, 25. Feb.). Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), Drucksache 18/4096. http://dip21.bundestag.de/dip21/btd/18/040/1804096.pdf. Zugegriffen: 10. Juni 2015.

Deutscher, S., Bohmayr, W., Yin, W., Russo, M. (2014). Cybersecurity Meets IT Risk Management. A Corporate Immune and Defense System, in: bcg.perspectives by The Boston Consulting Group (Hrsg.), Oktober 2014. http://www.bcgperspectives.com/content/articles/technology_strategy_technology_organization_cybersecurity_meets_it_risk_management/. Zugegriffen: 21. Jan. 2015.

Deutschland sicher im Netz e.V. (2015). Verein. http://www.sicher-im-netz.de/handlungsversprechen. Zugegriffen: 03. Juli 2015.

Die Bundesregierung (2014a). Beschluss im Bundeskabinet. Eine "Digitale Agenda" für Deutschland. http://www.bundesregierung.de/Content/DE/Artikel/2014/08/2014-08-20-kabinett-digitale-agenda.html. Zugegriffen: 11. März 2015.

Die Bundesregierung (2014b). Digitale Agenda 2014-2017,. http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/digitale-agenda-2014-2017,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf. Zugegriffen: 03. Feb. 2015.

Die Bundesregierung (2015a). Digitale Wirtschaft und digitales Arbeiten, URL: http://www.digitale-agenda.de/Webs/DA/DE/Handlungsfelder/2_DigitaleWirtschaft/digitale-wirtschaft_node.html;jsessionid=5DF5DCE2EDF0196D3C9BC507CE7D14A5.s2t2. Zugegriffen: 08. Feb. 2015.

Die Bundesregierung (2015b). Grundsätze unserer Digitalpolitik. http://www.digitale-agenda.de/Webs/DA/DE/Grundsaetze/Grundsaetze_Digitalpolitik/grundsaetze-digitalpolitik_node.html. Zugegriffen: 05. Feb. 2015.

Die Bundesregierung (2015c). IT-Sicherheitsgesetz. Schutz für die digitale Infrastruktur. http://www.bundesregierung.de/Content/DE/Artikel/2014/12/2014-12-17-kabinett-it-sicherheitsgesetz.html. Zugegriffen: 04. Juli 2015.

Diehl, J. (2015, 26. Juni). Vorratsdatenspeicherung: Selbst Ermittler halten Gesetzentwurf für untauglich. Spiegel Online. http://www.spiegel.de/netzwelt/netzpolitik/vorratsdatenspeicherung-ermittler-halten-gesetzentwurf-fuer-untauglich-a-1040779.html. Zugegriffen: 20.07.2015.

Diersch, V. (2015). Ein Bericht über den Cyber Security Summit 2014 der Münchner Sicherheitskonferenz und der Deutschen Telekom in Bonn. *Zeitschrift für Außen- und Sicherheitspolitik*, 8 (1), 133-137.

eco - Verband der deutschen Internetwirtschaft e.V. (2015). IT-Sicherheitsgesetz: Rechtsverordnung muss Schwerpunkt auf nicht regulierte Branchen setzen. http://www.eco.de/2015/pressemeldungen/it-sicherheitsgesetz-rechtsverordnung-muss-schwerpunkt-auf-nicht-regulierte-branchen-setzen.html Zugegriffen: 18. Juli 2015.

Verband der deutschen Internetwirtschaft e.V. (2015). Über eco. Wir gestalten das Internet. http://www.eco.de/about.html. Zugegriffen: 03. Juli 2015.

ENISA (2013, 18. Juni). Neue Verordnung für die EU-Agentur für Cybersicherheit ENISA, mit weiteren Aufgaben, Pressemitteilung. http://www.enisa.europa.eu/media/press-releases/prs-in-german/neue-verordnung-fur-die-eu-agentur-fur-cybersicherheit-enisa-mit-weiteren-aufgaben. Zugegriffen: 04. Juli 2015.

ENISA (2014, 30. Okt.). Bisher größte Übung zur Cyber-Sicherheit in Europa. Pressemitteilung. http://www.enisa.europa.eu/media/press-releases/prs-in-german/bisher-grosste-ubung-zur-cyber-sicherheit-in-europa. Zugegriffen: 04.07.2015.

Europäische Kommission (2010). Mitteilung der Kommission an das Europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Eine Digitale Agenda für Europa, Brüssel, den KOM(2010) 245. http://www.kowi.de/Portaldata/2/Resources/fp/2010-com-digital-agenda-de.pdf. Zugegriffen: 04. Juli 2015.

Europäische Kommission (2013a). Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Comittee of the Regions. Cybersecurity Strategy of the European Union: An open, Safe and Secure Cyberspace. http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667 Zugegriffen: 03. Juli 2015.

Europäische Kommission (2013b). Pressemitteilung. Cybersicherheitsplan der EU für ein offenes, freies und chancenreiches Internet. http://europa.eu/rapid/press-release_IP-13-94_de.htm Zugegriffen: 05. Juli 2015.

Europäische Kommission (2014). Die Digitale Agenda für Europa, Letzte Aktualisierung: November 2014. http://europa.eu/pol/pdf/flipbook/de/digital_agenda_de.pdf. Zugegriffen: 05. Juli 2015.

EUROPOL (2015a). Combating cybercrime in a digitale age. http://www.europol.europa.eu/ec3 Zugegriffen: 04. Juli 2015.

EUROPOL (2015b). EU Policy Cycle - Empact. http://www.europol.europa.eu/content/eu-policy-cycle-empact Zugegriffen: 20. Juli 2015.

faz.net (2015, 24. Apr.). Nachrichtendienst half NSA. Generalbundesanwaltschaft dementiert neue Ermittlungen. faz.net. http://www.faz.net/aktuell/politik/inland/nsa-affaere-bundesanwaltschaft-dementiert-ermittlungen-13556400.html. Zugegriffen: 22. Juli 2015.

Flade, F. (2014, 15. Dez.). Polizei warnt vor den "tickenden Zeitbomben". Die Welt. http://www.welt.de/politik/deutschland/article135405837/Polizei-warnt-vor-den-tickenden-Zeitbomben.html. Zugegriffen: 19. Juni 2015.

Flade, F. (2014, 20. Sep.). Industriespioange. Deutschland wehrt sich gegen Chinas Hacker-Armee. Die Welt. http://www.welt.de/wirtschaft/article132440947/Deutschland-wehrt-sich-gegen-Chinas-Hacker-Armee.html. Zugegriffen: 16. Juli 2015.

Flade, F./ Meyer, S. (2013, 18. Feb.). Neuer MAD Präsident. Geheimdienst der Bundeswehr bricht das Schweigen. Die Welt. http://www.welt.de/politik/deutschland/article113695087/Geheimdienst-der-Bundeswehr-bricht-das-Schweigen.html. Zugegriffen: 02. Juli 2015.

Flade, F./ Nagel, L.-M. (2015, 14. Juni). Internet als Waffe. Warum Deutschland im Cyberkrieg nicht mithalten kann. Die Welt.

http://www.welt.de/politik/deutschland/article142439200/Warum-Deutschland-im-Cyberkrieg-nicht-mithalten-kann.html. Zugegriffen: 01. Juli 2015.

Fraunhofer (2014). Strategie und Positionspapier Cyber-Sicherheit 2020: Herausforderungen für die IT-Sicherheitsforschung. http://www.fraunhofer.de/content/dam/zv/de/ueber-fraunhofer/wissenschaftspolitik/Fraunhofer-Strategie- und Positionspapier Cyber-Sicherheit 2020.pdf. Zugegriffen: 05. Feb. 2015.

Fraunhofer INT (2014). Europäische Verteidigungsagentur (European Defence Agency, EDA). http://www.sicherheitsforschung-europa.de/servlet/is/2776/. Zugegriffen: 04. Juli 2015.

Gaycken, S. (2010, 26. Nov.). Stuxnet. Wer war's? Und wozu?. Zeit Online. http://www.zeit.de/2010/48/Computerwurm-Stuxnet. Zugegriffen: 22. Juli 2015.

Gaycken, S. (2012). *Cyberwar. Das Wettrüsten hat längst begonnen. Vom digitalen Angriff zum realen Ausnahmezustand.* München: Wilhelm Goldmann Verlag.

German Competence Center against Cyber Crime e. V. (2015). Mitglieder und Kooperationspartner. http://www.g4c-ev.org/mitglieder.html. Zugegriffen: 10. Juni 2015.

Gesetz über den Bundesnachrichtendienst (BND-Gesetz - BNDG). http://www.gesetze-im-internet.de/bndg/BJNR029790990.html. Zugegriffen: 16. Juni 2015.

Goetz, J./ Leyendecker, H. (2014, 07. Juni). Rechnungsprüfer halten Cyber-Abwehrzentrum für "nicht gerechtfertigt". Süddeutsche.de. http://www.sueddeutsche.de/digital/behoerde-in-bonn-rechnungspruefer-

halten-cyber-abwehrzentrum-fuer-nicht-gerechtfertigt-1.1989433. Zugegriffen: 01. März 2015.

Grunert, F. (2013). Ein Bericht über die Handelsblatt-Konferenz „Cybersecurity 2012“ in Berlin. *Zeitschrift für Außen- und Sicherheitspolitik*, 6 (1), 107-112.

Hange, M. (2015). Präsident des BSI, Michael Hange hier zit. nach Bundesamt für Sicherheit in der Informatiosntechnik: Chancen nutzen – Risiken vermeiden. http://www.bsi.bund.de/DE/DasBSI/dasbsi_node.html Zugegriffen: 02. Juni 2015.

Hansel, M. (2012). Stuxnet und die Sabotage des iranischen Atomprogramms: Ein neuer Kriegsschauplatz im Cyberspace?. In Jäger, Thomas/ Beckmann, Rasmus (Hrsg.), *Handbuch Kriegstheorien* (S. 564-576). Wiesbaden: VS Verlag für Sozialwissenschaften.

Hansel, M. (2013). Internationale Beziehungen im Cyberspace. Macht, Institutionen und Wahrnehmung. In Jäger, Thomas (Hrsg.): *Globale Gesellschaft und internationale Beziehungen*. Wiesbaden: Springer VS.

Heeg, T. (2015, 10. März). Cyberkriminalität. Deutsche Firmen erleiden Milliardenschaden. FAZ.net. http://www.faz.net/aktuell/wirtschaft/cebit/die-gefahren-der-cyberkriminalitaet-sind-gestiegen-13475164.html. Zugegriffen: 11.03.2015.

heise online (2013, 23. Jan.). US-Regierung: Aufruf zum Hacken für eine bessere Nation. heise online. http://www.heise.de/newsticker/meldung/US-Regierung-Aufruf-zum-Hacken-fuer-eine-bessere-Nation-1789660.html. Zugegriffen: 03. Juli 2015.

heise online (2015, 27. Mai). Deutschland und Indien gemeinsam gegen Cyber-Terrorismus. http://www.heise.de/newsticker/meldung/Deutschland-und-

Indien-gemeinsam-gegen-Cyber-Terrorismus-2668789.html. Zugegriffen: 14.07.2015.

Helfferich, C. (2014). Leitfaden- und Experteninterviews. In: Baur, Nina/ Blasius, Jörg (Hrsg.): *Handbuch Methoden der empirischen Sozialforschung* (S. 559-574). Wiesbaden: Springer Fachmedien.

Bundesamt für Sicherheit in der Informationstechnik (2015). Aufgaben und Ziele. CERT-Bund. http://www.bsi.bund.de/DE/Themen/IT-Krisenmanagement/CERTBund/certbund_node.html. Zugegriffen: 09. Feb. 2015.

IT-Planungsrat (2014a). Informationssicherheit. Verbesserung und Vereinheitlichung der Informationssicherheit. http://www.it-planungsrat.de/DE/Projekte/AbgeschlosseneProjekte/Informationssicherheit/informationssicherheit.html?nn=1335606. Zugegriffen: 21. März 2015.

IT-Planungsrat (2014b). IT-Planungsrat. Vernetzt in die digitale Zukunft. http://www.it-planungsrat.de/SharedDocs/Downloads/DE/ITPlanungsrat/Flyer_DE.pdf?__blob=publicationFile Zugegriffen: 21. März 2015.

IT-Planungsrat (2014c). Projekte und Anwendungen. http://www.it-planungsrat.de/DE/Projekte/projekte_node.html. Zugegriffen: 21.03.2015.

Kaspersky Lab (2013, 30. Okt.). Java under attack – the evolution of exploits in 2012-2013. securlist.com. http://securelist.com/analysis/57888/kaspersky-lab-report-java-under-attack/. Zugegriffen: 21.04.2015.

Koalitionsvertrag zwischen CDU, CSU und FDP (2009). Wachstum. Bildung. Zusammenhalt, 17. Legislaturperiode. https://http://www.bmi.bund.de/SharedDocs/Downloads/DE/Ministerium/koalitionsvertrag.pdf?__blob=publicationFile. Zugegriffen: 05.02.2015.

Koalitionsvertrag zwischen CDU, CSU und SPD (2013). Deutschlands Zukunft gestalten, 18. Legislaturperiode. http://www.bundestag.de/blob/194886/696f36f795961df200fb27fb6803d83e/koalitionsvertrag-data.pdf. Zugegriffen: 05.02.2015.

Kommando Streitkräftebasis (2013). Kommando Strategische Aufklärung. Über uns. http://www.kommando.streitkraeftebasis.de/portal/a/kdoskb/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK94uyk-OyUfL3s4kQwLk1NSi0qzSvWL8h2VAQAQvOGXA!!/. Zugegriffen: 02. Juli 2015.

Kommando Streitkräftebasis (2015). Amt über den Militärischen Abschirmdienst. Über uns. http://www.kommando.streitkraeftebasis.de/portal/a/kdoskb/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK94uyk-OyUfL3y1MySlOKS4hK93MQUvdLUpNSi0rxi_YJsR0UAUKJtgw!!/. Zugegriffen: 02. Juli 2015.

KPMG (2013). e-Crime. Computerkriminalität in der deutschen Wirtschaft mit Kennzahlen für Österreich und Schweiz. http://www.kpmg.com/CH/de/Library/Articles-Publications/Documents/Advisory/pub-20130327-e-crime-studie-de.pdf. Zugegriffen: 05. Feb. 2015.

KPMG (2014). IT-Sicherheit in Deutschland Handlungsempfehlungen für eine zielorientierte Umsetzung des IT-Sicherheitsgesetzes. http://www.bdi.eu/images_content/SicherheitUndVerteidigung/KPMG_IT-Sicherheit_in_Deutschland.pdf. Zugegriffen: 01. März 2015.

Kuehl, D. (2009). From Cyberspace to Cyberpower: Defining the Problem. In Kramer, Franklin D./ Starr, Stuart H./ Wentz, K., Larry (Hrsg.): *Cyberpower*

and National Security (S. 24-42). Washington DC: National Defence University Press.

Kullik, J. (2014). *Vernetzte (Un-)Sicherheit? Eine politisch-rechtliche Analyse der deutschen Cybersicherheitspolitik.* Hamburg: Kovač.

Lindstorm, G. (2012). Meeting the Cyber Security Challenge. In *Geneva Centre for Security Policy*, Genf. http://www.gcsp.ch/Emerging-Security-Challenges/Publications/GCSP-Publications/Geneva-Papers/Research-Series/Meeting-the-Cyber-Security-Challenge. Zugegriffen: 20. Feb. 2015.

Luiijf, E. (2014). New and emerging threats of cyber crime and terrorism. In Akhgar, Babak/ Staniforth, Andrew/ Bosco, Francesca (Hrsg.): *Cyber crime and cyber terrorism investigator's handbook* (S. 19-29). Waltham, MA: Syngress,.

Manager Magazin (2010, 27. Mai). Motoren, Märkte, Großfabriken. http://www.manager-magazin.de/unternehmen/autoindustrie/a-695484.html Zugegriffen: 09. Juli 2015.

Meiritz, A./ Medick, V. (2015, 20. Mai). Cyberattacke auf Bundestag: Abgeordnete fühlen sich nach Hackerangriff alleingelassen. Spiegel Online. http://www.spiegel.de/politik/deutschland/cyber-angriff-abgeordnete-kritisieren-bundestags-verwaltung-a-1034732.html. Zugegriffen: 20. Juli 2015.

Nationale Initiative für Informations- und Internet-Sicherheit (NIFIS e.V.) (2015). Über NIFIS. http://www.nifis.de/ueber-nifis/. Zugegriffen: 03. Juli 2015.

NATO (2011). Defending the networks. The NATO Policy on Cyber Defence. http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf. Zugegriffen: 04. Juli 2015.

NATO (2015, 08. Apr.). Cyber security. http://www.nato.int/cps/en/natohq/topics_78170.htm?. Zugegriffen: 04. Juli 2015.

NATO Cooperative Cyber Defence Centre of Excellence (2015). About Cyber Defence Centre. https://ccdcoe.org/about-us.html. Zugegriffen: 04. Juli 2015.

Neue Osnabrücker Zeitung (2014, 18. März). Dienstleister aus IT-Sektor. Kinderpornos: BKA heuert Firmen bei Ermittlungen an. Neue Osnabrücker Zeitung. http://www.noz.de/deutschland-welt/politik/artikel/459741/kinderpornos-bka-heuert-firmen-bei-ermittlungen-an. Zugegriffen: 09. Juni 2015.

Neumann, P. (2014). Algorithmen und Agenten. Wo es gerade in Deutschland bei der Geheimdienstarbeit hapert. *Internationale Politik*, 69 (6), 8-14.

Niederberger, M. (2015). Methoden der Experteneinbindung. In Niederberger, Marlen/ Wassermann, Sandra (Hrsg.): *Methoden der Experten- und Stakeholdereinbindung in der sozialwissenschaftliche*n *Forschung* (S. 33-47). Wiesbaden: Springer Fachmedien.

Niedermeier, A. (2012). Nicht(s) auf dem Radar: Cyberkrieg als komplexe Herausforderung für die hochgradig vernetzte Gesellschaft. *Zeitschrift für Politik*, 59(1), 39-63.

OECD (2012). Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy. OECD Digital Economy Papers, 211.

Open Grid Europe (2015a). Beteiligungen. http://www.open-grid-europe.com/cps/rde/xchg/open-grid-europe-internet/hs.xsl/2889.htm Zugegriffen: 07. Juli 2015.

Open Grid Europe (2015b). Unsere Historie. http://www.open-grid-europe.com/cps/rde/xchg/open-grid-europe-internet/hs.xsl/952.htm. Zugegriffen: 07. Juli 2015.

Pfister, R., Poitras, L., Rosenbach, M., Schindler, J., Stark, H. (2013, 22. Juli). Der fleißige Partner. Spiegel Online. http://www.spiegel.de/spiegel/print/d-104058608.html. Zugegriffen: 20.Juni 2015.

Plöger, I. (2015). BDI-Stellungnahme zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) (BT-Drs. 18/4096). Bundesverband der Deutschen Industrie. http://www.bundestag.de/blob/370300/8c907d1750439b380668c12f98a80d1b/18-4-284-e-data.pdf. Zugegriffen: 30.05.2015.

Schaar, P. (2015, 25. Mai). Reaktionen auf Vorratsdatenspeicherung: Von "Schnellschuss" bis "Dammbruch". Spiegel Online. http://www.spiegel.de/netzwelt/netzpolitik/vorratsdatenspeicherung-kritik-von-schaar-und-kuenast-a-1035714.html. Zugegriffen: 16. Juli 2015.

Schallbruch, M. (2014). Verantwortung zwischen Gesetzgebung und Wirtschaft, in: Bub, Udo/ Wolfenstetter, Klaus-Dieter (Hrsg.): *Beherrschbarkeit von Cyber Security, Big Data und Cloud Computing. Tagungsband zur dritten EIT ICT Labs-Konferenz zur IT-Sicherheit* (S. 1-8). Wiesbaden: Springer Fachmedien.

Schaller, C. (2014). Internationale Sicherheit und Völkerrecht im Cyberspace. Für klarere Regeln und mehr Verantwortung. In Stiftung Wissenschaft und Politik - SWP - Deutsches Institut für Internationale Sicherheit (Hrsg.): *SWP-Studie* (S. 18). http://www.swp-berlin.org/fileadmin/contents/products/studien/2014_S18_slr.pdf. Zugegriffen: 19. Feb. 2015.

Schiller, J.-H. (2015). Stellungnahme zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informations- technischer Systeme / Drucksache 18/4096 vom 25.02.2015. http://www.bundestag.de/blob/370160/b820bfd1949d230e5856d0c0774acbce/18-4-284-c-data.pdf. Zugegriffen: 30. Mai 2015.

Schnaas, D. (2014): Die Angst vor der Innovationsperipherie. Wirtschaftsspionage ganz neuer Qualität gefährdet den Vorsprung des Westens. *Internationale Politik*, 69(1), 8-15.

Schultz, T. (2015, 25. März). Das ändert sich für den Verfassungsschutz. sueddeutsche.de. http://www.sueddeutsche.de/politik/verfassungsschutz-vernetzung-der-spione-1.2408283. Zugegriffen: 19. Juli 2015.

Severin, T. (2015, 10. Apr.). Verfassungsschutz - Islamisten ändern Cyber-Kriegsführung. Reuters Deutschland. http://de.reuters.com/article/domesticNews/idDEKBN0N11HD20150410 Zugegriffen: 19. Juli 2015.

Sievers, U. (2013, 05. Aug.). BSI: "Der Cyberraum ist ein großes Haifischbecken". Ingenieur.de. http://www.ingenieur.de/Themen/IT-Sicherheit/BSI-Der-Cyberraum-grosses-Haifischbecken. Zugegriffen: 24.Feb.2015.

Singer, T. (2014). Cyberwarfare? Damoklesschwert für das Völkerrecht?. *Sicherheit & Frieden*, 32(1), 17-23. http://dx.doi.org/10.5771/0175-274x-2014-1-17. Zugegriffen: 09. Feb. 2015.

Spiegel Online (2013a, 07. Nov.). Angst vor Industriespionage. NSA-Affäre rüttelt deutsche Firmen auf. http://www.spiegel.de/wirtschaft/unternehmen/nsa-affaere-viele-deutsche-firmen-wollen-daten-verschluesseln-a-932337-druck.html. Zugegriffen: 23. Feb. 2015.

Spiegel Online (2013b, 22. Juli). Prism, XKeyscore und Co.: NSA-Überwachungsprogramme im Überblick. http://www.spiegel.de/netzwelt/netzpolitik/prism-tempora-xkeyscore-nsa-ueberwachung-im-ueberblick-a-912377.html. Zugegriffen: 08. Juli 2015.

Stiftung Wissenschaft und Politik (2015). Die Herausforderung der Digitalisierung für die deutsche Außen- und Sicherheitspolitik. http://www.swp-berlin.org/projekte/die-herausforderung-der-digitalisierung-fuer-die-deutsche-aussen-und-sicherheitspolitik.html. Zugegriffen: 11. Juli 2015.

sueddeutsche.de (2015, 12. Juni). Bundestag. De Maizière zu Cyber-Attacke: Verfassungsschutz kann Bundestag helfen. http://www.sueddeutsche.de/news/politik/bundestag-de-maizire-zu-cyber-attacke-verfassungsschutz-kann-bundestag-helfen-dpa.urn-newsml-dpa-com-20090101-150612-99-02655. Zugegriffen: 20. Juni 2015.

Deutsche Telekom (2015). Zehn-Punkte-Programm für mehr Sicherheit im Netz. http://www.telekom.com/medien/konzern/264246. Zugegriffen: 04. Feb. 2015.

Tessier-Stall, S. (2011). The future of cybersecurity. The Hague Centre for Strategic Studies and TNO: Paper, 4.

The Economist (2010, 01. Juli). Cyberwar. The thread from the Internet. economist.com. http://www.economist.com/node/16481504?story_id=16481504&source=features_box1. Zugegriffen: 26. Aug. 2015.

Tschersich, T. (2011). Zur Notwendigkeit eines Umdenkens beim Thema Cybersicherheit. *Datenschutz und Datensicherheit*, 6/2011, 408-411.

Tschersich, T. (2015, 27. März). Stellungnahme zum Referentenentwurf des Gesetzes zur „Erhöhung der Sicherheit informationstechnischer Systeme“ (ITSiG). Deutsche Telekom AG.

http://www.bundestag.de/blob/367988/5e1da4e4d1152266e8c409dcad15364a/18-4-284-a-data.pdf. Zugegriffen: 30. Mai 2015.

UP KRITIS Themenarbeitskreis Fortschreibung (2014). UP KRITIS. Offentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen. Geschäftsstelle des UP KRITIS (Hrsg.), http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/UP_KRITIS.pdf?__blob=publicationFile. Zugegriffen: 13. Feb. 2015.

Varwick, J., Schmid, M. (2012). Das neue Strategische Konzept der NATO-Allianz. *Reader Sicherheitspolitik*. Bundesministerium der Verteidigung (Hrsg.), 3. http://www.bmvg.de/portal/a/bmvg/!ut/p/c4/bU0xDoJAEHwRe1yCGu0kNIbORrExC6znBrgjywqNj_cojI0zk2lmMmNuJtLjzA6Vg8feXE3V8KFeoB5mBxM3T5InsU5j6Fm5A_SO6qAEQtiS3P9UbPLAToOQT0iWmJBEJb8mCE_ckTeX9b8laIInXV3JK0d3gnEAxiDar8lL4poCt6ZKbZGnNv3CvvfFtszKzS4rTvnZjMNw_AA1iCIs/. Zugegriffen: 04. Juli 2015.

Wassermann, S. (2015). Das qualitative Experteninterview. Niederberger, Marlen/ Wassermann, Sandra (Hrsg.): *Methoden der Experten- und Stakeholdereinbindung in der sozialwissenschaftlichen Forschung* (S. 51-67). Wiesbaden: Springer Fachmedien.

Wendelin, M., Löblich, M. (2013). Netzpolitik-Aktivismus in Deutschland. Deutungen, Erwartungen und Konstellationen zivilgesellschaftlicher Akteure in der Internetpolitik. *Medien & Kommunikationswissenschaft*, 61 (1), 58-75.

Wendt, J. (2015, 15. Mai). Cyber-Attacke. Warum der Bundestag verwundbar ist. Zeit Online. http://www.zeit.de/digital/internet/2015-05/deutscher-bundestag-hacker-angriff-bsi. Zugegriffen: 23. Juli 2015.

Promotorengruppe Kommunikation der Forschungsunion Wirtschaft - Wissenschaft, acatech - Deutsche Akademie der Technikwissenschaften e.V.

(2013). Deutschlands Zukunft als Produktionsstandort sichern. Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0. Abschlussbericht des Arbeitskreises Industrie 4.0. Gefördert vom Bundesministerium für Bildung und Forschung. http://www.bmbf.de/pubRD/Umsetzungsempfehlungen_Industrie4_0.pdf. Zugegriffen: 05. Feb. 2015.

Wollny, V., Paul, H. (2015). Die SWOT-Analyse: Herausforderungen der Nutzung in den Sozialwissenschaften. Niederberger, Marlen/ Wassermann, Sandra (Hrsg.): *Methoden der Experten- und Stakeholdereinbindung in der sozialwissenschaftlichen Forschung* (S. 189-213). Wiesbaden: Springer Fachmedien.

World Economic Forum (2014). Delivering Digital Infrastructure Advancing the Internet Economy. Industry Agenda. Prepared in Collaboration with The Boston Consulting Group. http://www3.weforum.org/docs/WEF_TC_DeliveringDigitalInfrastructure_InternetEconomy_Report_2014.pdf. Zugegriffen: 11. Feb. 2015.

Zeit Online (2008, 26. Mai). ÜberwachungsaffäreTelekom verspricht rasche Aufklärung. http://www.zeit.de/online/2008/22/telekom-spitzel-affaere. Zugegriffen: 07. Juli 2015.

Zeit Online (2015a, 12. Juni). BND-Affäre. Alles gewusst und doch nichts geändert. http://www.zeit.de/politik/deutschland/2015-06/bnd-ernst-uhrlau-nsa-ausschuss. Zugegriffen: 11. Juni 2015.

Zeit Online (2015b, 24. Apr.). Bundesnachrichtendienst. SPD wirft Kanzleramt Versagen vor. http://www.zeit.de/digital/datenschutz/2015-04/bundesnachrichtendienst-nsa-spionage-abhoerskandal. Zugegriffen: 11. Juni 2015.

Zeit Online (2015c, 26. Aug.). XKeyscore – das Dokument. http://www.zeit.de/digital/datenschutz/2015-08/xks-xkeyscore-vertrag. Zugegriffen: 27. Aug. 2015.

Zierke, J. (2013). Präsident des Bundeskriminalamtes, Begrüßung und Einführung in das Thema: Cybercrime –Bedrohung, Intervention, Abwehr. BKA-Herbsttagung vom 12. – 13. November 2013: Bundeskriminalamt, 1-8.

Zypries, B. (2014, 04. Nov.). Rede Brigitte Zypries, Parlamentarische Staatssekretärin. Chancen und Herausforderungen des digitalen Zeitalters. http://www.cybersecuritysummit.de/downloads/CSS_2014_Rede_Brigitte_Zypries.pdf. Zugegriffen: 12. Feb. 2015.

Quellenangabe Interviews

Interview 1	Bundesministerium des Innern
Interview 2	Bundesamt für Sicherheit in der Informationstechnik
Interview 3	Bundesministerium für Wirtschaft und Energie
Interview 4	Bundesministerium für Verkehr und digitale Infrastruktur
Interview 5	Bundesministerium der Verteidigung
Interview 6	Auswärtiges Amt
Interview 7	Bundeskriminalamt
Interview 8	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
Interview 9	BWI Informationstechnik GmbH
Interview 10	Deutsche Telekom AG
Interview 11	Open Grid Europe GmbH
Interview 12	Daimler AG