LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Studienabschlussarbeiten
Sozialwissenschaftliche Fakultät

Frystatzki, Gerd:

Cyber-Governance-Struktur im Vergleich

Bachelorarbeit, Sommersemester 2022

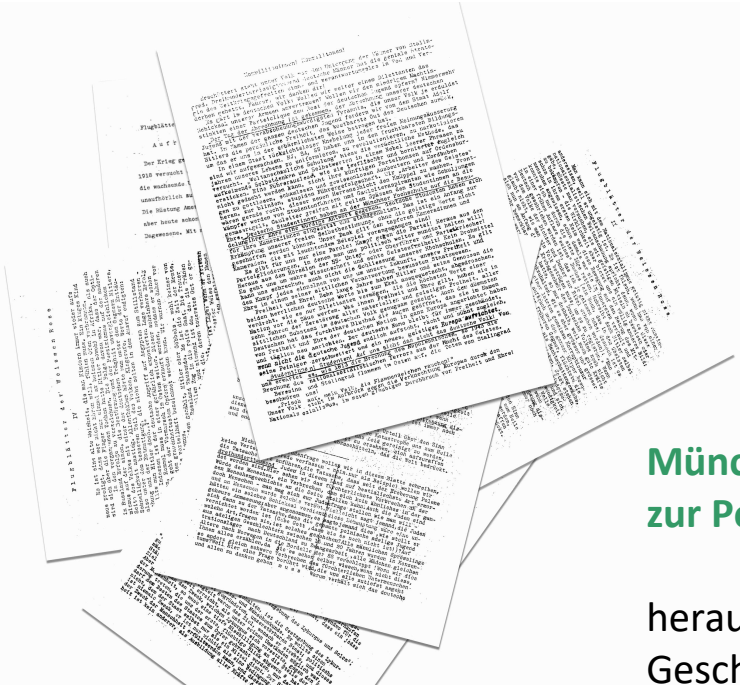
Sozialwissenschaftliche Fakultät

Ludwig-Maximilians-Universität München

https://doi.org/10.5282/ubm/epub.93939

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

GESCHWISTER-SCHOLL-INSTITUT
FÜR POLITIKWISSENSCHAFT



Münchener Beiträge zur Politikwissenschaft

herausgegeben vom
Geschwister-Scholl-Institut
für Politikwissenschaft

2022

Gerd Martin Frystatzki

Cyber-Governance-Struktur im Vergleich

Bachelorarbeit bei
Dr. Lars C. Colschen
2022

Abkürzungsverzeichnis

ANSSI	Agence nationale de la sécurité des systèmes d ' information
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BfV	Bundesamt für Verfassungsschutz
BKA	Bundeskriminalamt
BMI	Bundesministeriums des Innern
BND	Bundesnachrichtendienst
BPol	Bundespolizei
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVG	Bundesverfassungsgericht
CALID	Le Centre d’analyse de lutte informatique défensiv
CERTs	Computer Emergency Response Teams
COMCYBER	Le commandement de la cyberdéfense
COSSI	Centre opérationnel de la sécurité des systèmes d'information
CSIRTs	Computer Security Incident Response Teams
IT-KRZ	IT-Krisenreaktionszentrum
NCAZ	Nationales Cyber-Abwehrzentrum
NCS	Nationale Cybersicherheitsrat
NPSI	Nationalen Plan zum Schutz von Informationsstrukturen
SGDSN	Secrétariat général de la défense et de la sécurité nationale
ZKA	Zollkriminalamt

Inhaltsverzeichnis:

1. Einleitung

In vielen Ländern der Welt schreitet die Digitalisierung voran. Sowohl im öffentlichen als auch im privaten Leben ist sie nicht mehr aufzuhalten. Speziell in der Corona-Pandemie, wo persönliche Kontakte reduziert oder komplett eingestellt werden mussten, verlagerte sich der Alltag nach und nach ins Digitale. Daher ließen viele Arbeitgeber ihre Mitarbeiter im Home-Office arbeiten. Zoom-Meetings, kontaktloses Bezahlen oder auch Online-Shopping wurden in der Pandemie wichtiger denn je. Gleichzeitig bedeutete die Pandemie ein Stresstest für die kritische Infrastruktur. Die Sektoren Energie, Gesundheit, Finanzwesen, Staat und Verwaltung sowie die Informations- und Kommunikationstechnik mussten eine reibungslose Funktionalität gewährleisten, um das öffentliche Leben weiterhin aufrechtzuerhalten. Die Verlagerung des Alltags vom Analogen ins Digitale und die vergegenwärtigte Bedeutsamkeit der kritischen Infrastruktur erhöht die Gefahr der Cyberangriffe. Das Bundeskriminalamt vermeldete in seinem Bericht für 2020 einen Anstieg der Cyberkriminalität in Deutschland um +7,9% im Vergleich zum Jahr 2019 (vgl. Bundeskriminalamt 2021, S. 9 ff.). Neben Unternehmen waren dabei oftmals auch öffentliche Einrichtungen Ziel dieser Cyberangriffe. Besonders besorgniserregend – auch vor dem Hintergrund der Pandemie – war die gestiegene Anzahl an Angriffen auf die kritische Infrastruktur (ebd S. 4 ff.). Die Cyberkriminalität richtete sich verstärkt auf das Gesundheitswesen. Die Düsseldorfer Uniklinik musste im September 2020 nach einem Angriff ihre Notfallversorgung einstellen (vgl. tagesschau 2021). In Frankreich wurden nach einem Cyberangriff Patientendaten von fast 500.000 Bürgern entwendet und veröffentlicht (vgl. DER STANDARD 2021).

Die Bedrohung durch Cyberangriffe existiert nicht erst seit Beginn der Pandemie. Die Pandemie hat jedoch vergegenwärtigt, dass sowohl das Internet als auch die kritische Infrastruktur essenziell für die Aufrechterhaltung des täglichen Lebens sind. Deshalb ist der Schutz dieser Sektoren von größter Bedeutung. Staaten brauchen demnach ein gut funktionierendes Cyber-Krisen-Management, um Bedrohungen frühzeitig zu erkennen, abzuwehren oder die Schäden so gering wie möglich zu halten. Die

Zuständigkeitsbereiche und Verfahrensweisen des Cyber-Krisen-Managements können dabei weltweit variieren. Diese Tatsache resultiert aus unterschiedlichen Kapazitäten im Cyberbereich, verschiedenster Institutionen und Rechtsrahmen sowie spezifischer Cyber-Policies (vgl. Boeke 2016).

Zudem sind die Sektoren der kritischen Infrastrukturen nicht allein in staatlicher Hand. So teilt sich der Energiesektor in Deutschland beispielsweise auf mehrere private Unternehmen auf. Da private Unternehmen selbstständig nicht die Cybersicherheit gewährleisten können, insbesondere, wenn Cyberangriffe von anderen Staaten ausgeübt werden, kann sich ein Staat seiner Verantwortung nicht entziehen, wenn er die Sicherstellung der Funktionalität von kritischen Infrastrukturen erhalten möchte (vgl. Boeke 2016, S. 1 f.) Daher müssen Staaten mit privaten Akteuren kooperieren, um den Zustand von Cybersicherheit zu erreichen (vgl. Boeke 2016, S. 3 f.).

Hierbei unterscheiden sich Länder bei der Verfahrensweise mit den privaten Akteuren was unterschiedliche Cyber-Governance-Strukturen hervorbringt. Einige Staaten nehmen eine führende Rolle ein und delegieren Maßnahmen und Strategien von oben nach unten (vgl. Boeke 2018). Andere wiederum führen eine Kultur des Konsenses (vgl. ebd)

Die Art und Weise der Zusammenarbeit kann sich in unterschiedlichen Verfahrensweisen zeigen, wie beispielsweise im Cyber-Krisen-Management.

Dr. Sergei Boeke von der Universität Leiden hat sich in seiner Arbeit „National cyber crisis management: Different European approaches“ der Cyber-Governance-Struktur von Staaten gewidmet und eine Taxonomie erstellt, mit welcher sich diese kategorisieren und untersuchen lässt (vgl. Boeke 2018, S. 452).

Die institutionellen Verantwortlichkeiten und Verfahrensweisen innerhalb des Cybersicherheitskomplexes eines Staates werden durch die Taxonomie abgebildet. Dabei sind die Beziehungen zwischen privaten und öffentlichen Akteuren bedeutsam, da sie während der Kategorisierung beachtetet werden müssen (vgl. Boeke 2018, S. 452). Boeke untersucht die Cyber-Governance-Struktur der Niederlande, Estlands, Dänemarks sowie der Tschechischen Republik und konnte mithilfe der Taxonomie Unterschiede und Gemeinsamkeiten aufzeigen.

In seiner Arbeit „First Responder or Last Resort? The role of the Ministry of Defence in national cyber crisis management in four European countries“ stellte Boeke die Frage wie Frankreich und Deutschland, als wichtige europäischen Sicherheitsmächte, ihre Strukturen für das Cyber-Krisenmanagement organisiert haben. Dies Impliziert eine

wissenschaftliche Lücke in Bezug auf die Cyber-Governance-Strukturen beider Länder (vgl. Boeke 2016, S. 47). An dieser Stelle soll die vorliegende Arbeit anschließen und Aufschluss geben.

Es soll untersucht werden, *wie Deutschland und Frankreich ihre Cyber-Governance-Struktur organisiert haben*.

Da beide Staaten wirtschaftlich wichtige Länder in der Europäischen Union sind, hat die Auseinandersetzung mit diesem Thema besondere Relevanz. Interessant ist zudem, wie zwei eher unterschiedlich strukturierte Staaten ihre Cyber-Governance-Struktur organisieren; zum einen Frankreich, welches einen eher zentralistischen Staatsapparat aufweist und auf der anderen Seite Deutschland, welches föderalistischer aufgebaut ist. Um diese Forschungsfrage zu beantworten, wird sich diese Arbeit an der Forschungsarbeit von Boeke orientieren und auf die von ihm erstellte Taxonomie zurückgreifen. Der Rückgriff auf die Taxonomie lässt sich mit der Komplexität von Cyber-Governance-Strukturen begründen, die aus den Interessen der verschiedenen Akteure, über die Verfahrensweisen von Staaten, bis hin zu den unterschiedlichen Auffassungen von Cybersicherheit resultieren.

In einem ersten Schritt soll daher der Begriff der Cyber-Governance erklärt und die Taxonomie der Cyber-Governance-Struktur erläutert werden.
Anschließend werden die Cyber-Governance-Strukturen beider Länder einzeln untersucht. Hierfür wird zuerst beschrieben, wie sich die nationale Cybersicherheitspolitik im zeitlichen Verlauf bis zum heutigen Stand entwickelte. Die Beschreibung soll zu dem Zeitpunkt beginnen, an dem die Länder entweder eine Behörde für Cybersicherheit gegründet haben, den Begriff „Cyber“ zum ersten Mal in einem Regierungsdokument erwähnten oder ein Cyberangriff auf das jeweilige Land stattfand. Konzentriert werden soll sich im weiteren Beschreibungsprozess auf staatliche Behörden, Gesetze, Richtlinien, Strategien und Maßnahmen auf nationaler Ebene im Bereich der Cybersicherheit. Dafür sollen Fachliteratur, Zeitungsartikel, Dokumente von Regierungsstellen und Behörden ausgewertet werden. Anschließend soll mithilfe der Beschreibung, die Einordnung, in die Taxonomie vorgenommen werden. Die daraus sichtbarwerdenden Cyber-Governance-Strukturen werden daraufhin gegenübergestellt und miteinander verglichen. Die aus dem

Beschreibungsprozess beider Länder gewonnen Erkenntnisse sollen hinzugezogen werden, um Aussagen über die Entwicklung der Cyber-Governance-Struktur zu machen.Anschließend wird diese Arbeit mit einem Fazit abgeschlossen.

2. Methodik: Taxonomie der Cyber-Governance-Strukturen

Die in der Einleitung erwähnte Komplexität von Cyber-Governance-Strukturen wird auch bei der Definition von Cyber-Governance deutlich. So lautet eine Definition von Savaş, S(..):

„Cyber governance can be defined as the operation of decision-making processes in a way that increases participation, transparency, and accountability in taking measures related to cyberspace, together with the mechanism of international agreements, strategies, laws, measures, regulations, and standards that interlock in the best way". (Savaş und Karataş 2022, S. 14)

Dieses Zitat ist ein gutes Beispiel dafür, wie in der Fachliteratur Cyber-Governance verstanden werden kann, verdeutlicht aber gleichzeitig auch die Problematik, die mit einem solchen weiten Feld einhergeht. Um sich in wissenschaftlichen Kontexten mit Cyber-Governance in Bezug auf Cybersicherheit auseinandersetzen zu können ist eine Abgrenzung und Definition des Untersuchungsbereichs notwendig. Boeke hat diese getroffen in dem er genau die Cyber-Governance-Struktur betrachtet, welche er als solche in seiner Taxonomie operationalisiert.

Die Taxonomie von Boeke unterteilt die Cyber-Governance-Struktur von Staaten in sieben Attribute, welche Teilbereiche der Cyber-Governance-Struktur darstellen sollen (vgl. Boeke 2018, S. 451 f.). Zu diesen Bereichen zählen „Koordinierung der Cyber-Sicherheitspolitik", „Koordinierung des allgemeinen Krisenmanagements", „die wichtigsten öffentlichen CERTs", „Cyberkapazitäten der Regierung", „Überwachung der Regierungsnetzwerke", „Einbindung der Geheimdienste" und „Netzwerkmodell" (vgl.ebd). Mit Ausnahme von „Cyberkapazitäten der Regierung", „Einbindung der Geheimdienste" sowie „Netzwerksmodell" sind die Ausprägungen der Attribute nicht vordefiniert und können auch mehrere Ausprägungen pro Attribut beinhalten. Für die

drei ausgenommenen Attribute existieren bereits vordefinierte Ausprägungen (vgl. ebd).

Das Attribut „Cyberkapazitäten der Regierung“ hat die Ausprägung „verteilt“ oder „zentralisiert“, während das Attribut „Einbindung der Geheimdienste“ entweder „innerhalb“ oder „außerhalb“ als Ausprägung haben kann (Boeke 2018). Das Attribut „Netzwerkmodell“ hat mit „Participant governed”, „Lead organization” und „Network-administrative” drei verschiedene Ausprägungen (vgl. ebd).

Attribut	**Land**
Koordinierung der Cyber-Sicherheitspolitik	„Individuell“ („ein“ oder „mehrere“)
Koordinierung allgemeines Krisenmanagement	„Individuell“ („ein“ oder „mehrere“)
Die wichtigsten öffentlichen CERTs	„Individuell“ („ein“ oder „mehrere“)
Cyberkapazitäten der Regierung	„verteilt“ oder „zentralisiert“
Überwachung der Regierungsnetzwerke	„Individuell“ („ein“ oder „mehrere“)
Einbindung der Geheimdienste	„innerhalb“ oder „außerhalb“
Netzwerkmodell	„Participant governed”, „Lead organization“, „Network-administrative“

„Tabelle 1: Darstellung der Cyber-Governance-Taxonomie nach Boeke (2018)“

Im Folgenden sollen nun die Attribute der Cyber-Governance-Struktur erläutert und die Vorgehensweise zur Einordnung beschrieben werden. Dabei wird in Kapitel 2.1 auf

alle Attribute bis auf das Attribut „Netzwerkmodell“ eingegangen. Dieses wird aufgrund seiner 3 Ausprägungen in Kapitel 2.2 erläutert.

2.1 Attribute der Cyber-Governance-Struktur

Koordinierung der Cyber-Sicherheitspolitik

Dem Attribut „Koordinierung der Cyber-Sicherheitspolitik“ werden jene Behörden zugeordnet, welche die Cyberpolitik in einem Staat koordinieren (vgl. Boeke 2018). Unter die Koordinierung fallen beispielsweise die Ausarbeitung von Cybersicherheitsgesetzen und damit das Setzen von Sicherheitsstandards, Sicherheitsüberprüfungen und Zertifizierungen von IT-Komponenten oder auch die Überprüfung der Einhaltung von Sicherheitsmaßnahmen bzw. Sicherheitsstandards sowie das Verhängen von Geldstrafen an die Akteure bei Missachtung solcher (vgl. ebd). Die Behörden auf oberster Ebene, welche diese Aufgaben im Staat innehaben werden als Ausprägungen dem Attribut zugeordnet.

Koordinierung des allgemeinen Krisenmanagements

Das Attribut *„Koordinierung des allgemeinen Krisenmanagements“* umfasst das nationale Krisenmanagement eines Staates (vgl. ebd). Der Fokus liegt neben der Reaktion bei Vorfällen auf Prävention, Vorbereitung, Eindämmung, Wiederherstellung sowie institutionelles Lernen (vgl. Boeke 2018, S. 450 ff.). Es soll untersucht werden, welche Behörden in einem Staat diese Aufgabenbereiche innehaben und wie diese dabei vorgehen. Bei der Untersuchung soll auch geschaut werden, welche Behörde für das Cyber-Krisenmanagement zuständig ist, da dieses im nationalen Krisenmanagement integriert ist (vgl. Boeke 2018, S. 451 f.). In das Attribut „Koordinierung des allgemeinen Krisenmanagements“ werden nur die obersten Behörden aufgenommen werden, welche die Aufgaben des nationalen Krisenmanagements innehaben.

Die wichtigsten öffentlichen CERTs

Computer Emergency Response Teams (CERTs) oder *Computer Security Incident Response Teams* (CSIRTs) sind Notfallteams, welche lösungsorientiert an der IT-Sicherheit von Staaten arbeiten und bei Sicherheitsforfällen Hilfe leisten (vgl. Luber

2018). Staaten definieren den Tätigkeitsbereich ihrer CERTs individuell, sodass ein oder mehrere CERTs in einem Land tätig sein können (vgl. Boeke 2018, S. 452). Unter dem Attribut *„die wichtigsten öffentlichen CERTs“* sollen die wichtigsten CERTs eines Staates aufgelistet werden. Als wichtig werden jene CERTs eines Staates angesehen, welche Netzwerke der Regierung, des Militärs oder des privaten Sektors überwachen oder mehrere Ministerien, Betreiber kritischer Infrastrukturen als auch Unternehmen betreuen, bei Cyberangriffen Unterstützung leisten oder viele Informationen über Bedrohungen und deren Abwehr haben (vgl. Boeke 2018). Die Bezeichnung für die Behörde, welche den beschriebenen Aufgabenbereich innehat, kann von Land zu Land variieren. In Estland heißt die Behörde „CERT-EE“, während in Dänemark die Behörde „Center for Cyber Security“ heißt (vgl. Boeke 2018).

Cyberkapazitäten der Regierung

Staaten können ihre Kapazitäten im Cyberbereich auf eine Behörde konzentrieren oder auf mehrere Behörden verteilen (vgl. Boeke 2018, S. 461). Zu Cyberkapazitäten zählen Ressourcen, welche zur Reaktion eines Cyberangriffs eingesetzt werden können, worunter Maßnahmen zur Instandsetzung der angegriffenen Systeme zählen oder Kapazitäten, um einen Cyberangriff aus dem Ausland in der Vorbereitung zu erkennen und ggf. zu stören (vgl. Boeke 2018). Ebenso die Fähigkeit Netzwerke innerhalb des Staates zu Überwachen und Cyberangriffe auf diese Netzwerke zu erkennen, fallen unter Cyberkapazitäten (vgl. Boeke 2018). Für die Einordnung in die Taxonomie soll unter dem Attribut *„Cyberkapazitäten der Regierung“* untersucht werden, ob ein Staat seine Cyberkapazitäten in eine Behörde bündelt und somit zentralisiert oder auf mehrere Behörden verteilt hat (vgl. Boeke 2018, S. 461).

Überwachung der Regierungsnetzwerke

Das Attribut „Überwachung der Regierungsnetzwerke“ zielt darauf ab die staatliche Behörde ausfindig zu machen, welche für die Sicherheit der anderen staatlichen Behörden zuständig ist und deren Netzwerke überwacht (vgl. Boeke 2018). Hierbei können eine oder mehrere Behörden für die Überwachung von Regierungsnetzwerken verantwortlich sein. Beispielsweise ist es auch möglich, dass jede Regierungsbehörde für sich selbst verantwortlich ist und somit seine eigenen Netzwerke überwacht (vgl. ebd).

Einbindung der Geheimdienste

Mit dem Attribut „Einbindung der Geheimdienste“ soll in Boekes Taxonomie die Rolle der Geheimdienste untersucht werden. Speziell geht es darum zu untersuchen, ob die CERTs eines Staates im Geheimdienst verortet sind oder nicht (vgl. Boeke 2018, S. 461). Ob die Geheimdienste eines Landes an den nationalen Computer-Notfallteams (CERTs) beteiligt sind oder nicht macht einen signifikanten Unterschied in Bezug auf die Informationsdichte und den Informationsaustausch (vgl. Boeke 2018, S. 460 f.). Daher kann die Ausprägung dieses Attributs „innerhalb“ oder „außerhalb“ sein.

2.2 Netzwerkmodell

Neben dem institutionellen Aufbau und der Verflechtung innerhalb der staatlichen Institutionen soll die Beziehung und Interaktion zwischen dem öffentlichen und privaten Sektor untersucht werden. Hierfür beinhaltet die Taxonomie von Boeke das Attribut *„Netzwerkmodell“*. Die Ausprägungen dieses Attributs, welche im Folgenden erläutert werden sind theoretische Idealtypen, da sich in der Realität die Merkmale nicht eindeutig kategorisieren lassen aufgrund von unterschiedlichen Kombinationen in den Verfahrensweisen (vgl. Boeke 2018, S. 451).

Participant governed

Das Netzwerkmodell *„Participant governed”* ordnet Boeke in seiner Arbeit den Niederlanden zu (vgl. Boeke 2018, S. 458 f.). Demnach sind eine Konsenskultur und Gleichberechtigung zwischen den öffentlichen und privaten Akteuren bezeichnend für dieses Modell (vgl.ebd). Staatliche Akteure ermöglichen durch freiwillige Teilnahme an Gremien die Vernetzung und Zusammenarbeit unter den Akteuren was den Informationsaustausch untereinander fördert (vgl. Boeke 2018, S. 452 f.). Die Zusammenarbeit in diesem Modell wird nicht erzwungen (vgl. Boeke 2018, S. 453). Es werden den Akteuren keine Aufgaben auferlegt deren Umsetzung kontrolliert wird (vgl. Boeke 2018, S. 458 f.); vielmehr tragen die staatlichen Akteure in diesem Modell dazu bei, dass sich die Akteure vernetzen und selbst organisieren (vgl. ebd).

Lead organization

Das Netzwerkmodell *„Lead organization"* wird in der Arbeit von Boeke Dänemark zugeordnet ist (vgl. Boeke 2018, S. 459) Hier übernimmt ein staatlicher Akteur die zentrale Rolle und koordiniert jegliche Vorgänge (vgl.ebd). Dieser zentrale staatliche Akteur setzt selbst die Regeln und kontrolliert deren Einhaltung durch die anderen Akteure (vgl. Boeke 2018, S.454 f.). Zudem ist der zentrale staatliche Akteur, der erste und einzige Ansprechpartner für die anderen Akteure, da er über viele Informationen verfügt und diese entsprechend an die anderen Akteure verteilen kann (vgl. ebd). Sämtliche Vorgänge werden somit von einem einzigen staatlichen Akteur gesteuert und überwacht (vgl.ebd).

Network-administrative

Das Netzwerkmodell *„Network-administrative"* wird von Estland und der Tschechischen Republik abgebildet (vgl. Boeke 2018, S. 459). Die staatlichen Akteure in diesem Netzwerkmodell sorgen für eine Zusammenarbeit mit den privaten Akteuren und setzen auf eine öffentlich-private Partnerschaft (vgl. ebd). Zudem bestimmen die staatlichen Akteure die Regeln und kontrollieren deren Einhaltung. Bei Nichteinhaltung der Regeln können die staatlichen Akteure Strafen verhängen (vgl. ebd).

3. Die Cyber-Governance-Struktur in Deutschland

Im Folgenden wird die Entwicklung der Cybersicherheitspolitik in Deutschland beschrieben, während im anschließenden Unterkapitel die Einordnung in die Taxonomie stattfindet.

3.1 Die deutsche Cybersicherheitspolitik im zeitlichen Verlauf

Nach der Wiedervereinigung wurde 1991 per Gesetz das Bundesamt für Sicherheit in der Informationstechnik (BSI) gegründet und dem Geschäftsbereich des Bundesministeriums des Innern (BMI) zugewiesen. Das BSI mit Sitz in Bonn löste nach seiner Gründung den Bundesnachrichtendienst (BND) bei der Aufgabe in Bezug auf den technischen Schutz der Regierungsnetzwerke ab (vgl. Schallbruch und Skierka

2018, S. 16 f.). Zudem sollte es die Regierung, Industrie und Gesellschaft bei der IT-Sicherheit beraten (vgl. ebd, S.17), Überprüfung von IT-Systemen vornehmen und anschließend Sicherheitszertifikate vergeben (vgl. Schallbruch 2021c, S. 229). Hierfür wurden dem BSI 213 Mitarbeiter und ein Budget von rund 56 Millionen Deutsche Mark zur Verfügung gestellt (vgl. Deutscher Bundestag 1991, S. 1973 ff.). 1994 folgte die Errichtung des CERT-BUND innerhalb des BSI, um auf IT-Sicherheitsvorfälle reagieren zu können.

Als Reaktion auf das erste Gesetz zum Schutz kritischer Infrastruktur der USA, handelte Deutschland daraufhin ebenfalls und berief 1997 unter Initiative des BMI, eine Arbeitsgruppe aus Vertretern der Ministerien, des BSI und eines Lenkungausschusses (vgl. Schallbruch und Skierka 2018, S. 17). Diese Arbeitsgruppe sollte mögliche Bedrohungen und Verwundbarkeiten für kritische Infrastrukturen ausfindig machen und Gegenmaßnahmen sowie ein Frühwarnsystem entwerfen (vgl. ebd). Der von der Arbeitsgruppe im Jahr 1999 veröffentlichte Bericht unterstrich die Wichtigkeit der IT-Sicherheit und den Schutz der kritischen Infrastruktur vor Ausfällen der IT-Systeme (vgl. ebd).

In Deutschland wurden Cyberangriffe vor der Jahrtausendwende nicht als Bedrohung wahrgenommen. Der „Loveletter-Virus“ der im Mai 2000 über E-Mail-Anhänge verbreitet wurde löste zum ersten Mal eine Debatte im Bundestag aus (vgl. ebd, S. 6). Allerdings gingen die Debatten um die Verringerung der Abhängigkeit von Microsoft Produkten als über die Cybersicherheit (vgl. ebd).
Die Anschläge vom 11. September 2001 und ein Cyberangriff auf die Netze der Bundesregierung im Jahr 2004 veranlassten die Bundesregierung jedoch eine Überprüfung der Cybersicherheitslage durch das BSI durchzuführen (vgl. Schallbruch und Skierka 2018, S. 7 f.). Das Ergebnis der Überprüfung forderte Maßnahmen zum Schutz der IT-Systeme von kritischen Infrastrukturen und die Verbesserung der Prävention in Bezug auf Cyberangriffe (vgl. ebd). Zudem wurde 2004 das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) im Zuständigkeitsbereich des BMI eingerichtet und mit den Aufgaben des Risiko- und Krisenmanagements betraut (vgl. BMI 2017a). Das Krisenmanagement des BBK umfasst die Planung von Maßnahmen, die während einer Krise eingeleitet werden sollen und in denen die Zusammenarbeit von Bund und Ländern festgelegt ist (vgl. BBK 2022a). Das

Risikomanagement analysiert und bewertet die Risiken einer Krise, woraus sich passende Maßnahmen ableiten lassen (vgl. BBK 2022b). Da in Deutschland allerdings aufgrund des Föderalismus der Katastrophenschutz Aufgabe der Bundesländer ist, richten sich die Maßnahmen und Informationen des BBK an die Behörden der Länder, welche die Kommunen und lokalen Behörden unterrichten und darauf einstellen (vgl. BMI 2017b).
Eine weitere Aufgabe, die das BBK erhielt, war die Koordinierung im Bereich der kritischen Infrastrukturen. Das BBK plant und führt regelmäßige Krisenübungen durch, darunter auch Cyberabwehr-Übungen (vgl. Schallbruch und Skierka 2018, S. 36). Daher analysiert das BBK auch die Auswirkungen und Folgen eines Cyberangriffs und gibt Empfehlungen an die Betreiber weiter (vgl. Zedler 2016, S. 75 f.).

Eine weitere Reaktion auf die Vorfälle von 2001 und 2004 folgte im Jahr 2005 mit dem Nationalen Plan zum Schutz von Informationsstrukturen (NPSI), der die erste deutsche Cybersicherheitsstrategie war (vgl. Schallbruch und Skierka 2018, S. 7 f.). Der Plan ging auf die Digitalisierung und die Vernetzung von kritischen Infrastrukturen durch IT-Komponenten ein, welche als „Informationsinfrastrukturen“ definiert wurden (vgl. ebd, S. 18). Somit wurde dem Schutz der Informationsinfrastrukturen eine besondere Bedeutung zugesprochen, da er die Funktionalität von Kritischen Infrastrukturen gewährleistet (vgl. Bundesministerium des Innern 2005, S. 3). Daher sah der NPSI größtenteils die Prävention zum Schutz Kritischer Infrastrukturen als Ziel an, wofür das BSI beauftragt wurde IT-Systeme und Produkte auf ihre Sicherheit zu prüfen und zu zertifizieren, damit die Betreiber kritischer Infrastrukturen vertrauenswürdige und sichere Produkte verwenden und den Schutz ihrer Systeme erhöhen (vgl. Zedler 2016, S. 26). Definiert wurden kritische Infrastrukturen im NPSI mit:

„Kritische Infrastrukturen sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“ (Bundesministerium des Innern 2005, S. 21)

Der Plan sah zudem die Kooperation mit den privaten Akteuren vor, zumal diese den größten Teil an Kritischen Infrastrukturen betreiben (vgl. Bundesministerium des

Innern 2005, S. 8). Für die Umsetzung der Maßnahmen ist ein „Umsetzungsplan KRITIS“ vorgesehen worden, der unter Beteiligung von privaten Unternehmen und Wirtschaftsvertretern ausgearbeitet werden sollte (vgl. ebd). Des Weiteren wurde das BSI durch den NPSI mit der Beratung von Unternehmen in Bezug auf Cybersicherheit beauftragt (vgl. ebd). Innerhalb des BSI wurde 2005 zusätzlich ein neu gegründetes nationales IT-Krisenreaktionszentrum (IT-KRZ) angesiedelt (vgl. Astrid Bötticher 2014, S. 91). Dieses sollte schwere IT-Sicherheitsvorfälle analysieren, bewerten und die Informationen an die Stellen weiterleiten, die ebenfalls betroffen sein könnten (vgl. BSI 2021).

Der unter Beteiligung der privaten Akteure ausgearbeitete „Umsetzungsplan KRITIS“ wurde im Jahr 2007 veröffentlicht und enthielt die wesentlichen Punkte Prävention, Reaktion und Nachhaltigkeit aus dem NPSI (Bundesministerium des Innern 2007). Die Unternehmen sollten nach dem Plan ihre Informationsinfrastrukturen schützen, entsprechend IT-Sicherheitsvorfälle bewältigen als auch zukunftsorientiert durch Ausbildung, Forschung und Entwicklung die IT-Sicherheitskompetenzen verbessern (Bundesministerium des Innern 2007). Es wurden auch Aussagen über die Umsetzung. So sollte:

„Die Umsetzung des NPSI erfolgt im Konsens zwischen den privatwirtschaftlichen Zielsetzungen der Betreiber und dem übergeordneten (Fürsorge-)Interesse des Gemeinwesens.“ (Bundesministerium des Innern 2007, S. 5).

Der Austausch von Informationen wurde den Unternehmen selbst überlassen (vgl. Bundesministerium des Innern 2007, S. 30).
Zwei Jahre später im Jahr 2009 folgte die KRITIS-Strategie in welcher die Bedeutung der Zusammenarbeit zwischen Behörden, Unternehmen und Verbänden als wichtiges Ziel für den Erfolg beschrieben wurde (vgl. Bundesministerium des Innern 2009). In der Strategie fand eine Aufteilung der Kritischen Infrastrukturen in zwei Bereiche statt, die jedoch voneinander abhängig sind, was verdeutlichen sollte, dass der Ausfall einer kritischen Infrastruktur, beispielsweise der Ausfall eines Kraftwerkes negative Auswirkungen auf die Funktionalität einer anderen haben kann wie etwa eines Krankenhauses (vgl. ebd, S. 5). Daher wurde betont, dass die Unternehmen ihrer freiwilligen Selbstverpflichtung nachkommen sollten und die entsprechenden

Sicherheitsmaßnahmen umsetzen (vgl. ebd, S. 12). Falls nicht würde der Staat Maßnahmen im Bereich der Gesetzgebung veranlassen, um den Schutz zu gewährleisten (vgl. ebd, S. 13).

Da die Bundesländer für ihre Institutionen eigene IT-Sicherheitsstrukturen haben und auch innerhalb der Bundesbehörden, aufgrund des Ressortprinzips Unterschiede vorhanden waren, wurde 2010 der IT-Planungsrat errichtet der die Zusammenarbeit der Behörden von Bund und Ländern verbessern und ein einheitliches Sicherheitsniveau schaffen sollte (vgl. Zedler 2016, S. 41 f.).
Im Jahr 2011 veröffentlichte das BMI seine ausgearbeitete „Cyber-Sicherheitsstrategie für Deutschland“, welche ein Novum darstellte, da es das erste Mal war, dass der Begriff „Cybersicherheit“ in einem deutschen Regierungsdokument verwendet wurde (vgl. Schallbruch und Skierka 2018, S. 2). Zuvor verwendete man die Begriffe „IT-Sicherheit“ oder „Sicherheit kritischer Informationsinfrastrukturen“ (vgl. ebd). Definiert wurde Cybersicherheit im Strategiepapier mit:

„(Globale) Cyber-Sicherheit in Deutschland ist demnach der anzustrebende Zustand der IT-Sicherheitslage, in welchem die Risiken des deutschen Cyber-Raums auf ein tragbares Maß reduziert sind.“
(Bundesministerium des Innern 2011, S. 15).

Um die allgemeine Sicherheitslage zu verbessern, beinhaltete die Cybersicherheitsstrategie zwei Punkte zur Errichtung neuer Institutionen. Innerhalb dieser Institutionen sollten Strategien und Maßnahmen entworfen werden, welche zum einen das Sicherheitsniveau erhöhen und zum anderen die Zusammenarbeit zwischen den Behörden untereinander, als auch mit den privaten Akteuren der Wirtschaft verbessern sollten (vgl. Stephan Steller 2017, S. 57).
Der in der Strategie vorgesehene Nationale Cybersicherheitsrat (NCS) sollte sich aus Wirtschaftsvertretern und Vertretern einiger Ministerien sowie der Bundesländer zusammensetzen und als Schnittstelle zwischen Wirtschaft und Politik dienen (vgl. ebd). Der Austausch innerhalb des Rates sollte zur Verbesserung der Präventionsmaßnahmen sowie der Zusammenarbeit beitragen (vgl. Bundesministerium des Innern 2011, S. 4). Die Gründung erfolgte im August 2012 durch das BMI. Des Weiteren sollte ein Nationales Cyber-Abwehrzentrum (NCAZ)

geschaffen werden, welches die operative Zusammenarbeit und die Koordinierung von Schutz- und Abwehrmaßnahmen aller staatlichen Institutionen verbessern sollte (vgl. Bundesministerium des Innern 2011, S. 8). Unter Leitung des BSI sollten sich das Bundesamt für Verfassungsschutz (BfV), das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Bundeskriminalamt (BKA), die Bundespolizei (BPol), das Zollkriminalamt (ZKA), der BND sowie die Bundeswehr am NCAZ beteiligen und mitwirken (vgl.ebd, S. 8). Innerhalb des NCAZ sollten IT-Sicherheitsvorfälle analysiert und bewertet werden als auch einheitliche Handlungsempfehlungen verfasst werden (vgl. ebd, S. 8).
Neben der Schaffung von Institutionen betonte die Strategie unter anderem den Schutz kritischer Informationsinfrastrukturen, die Zertifizierung und den Einsatz sicherer IT-Systeme, die europäische und internationale Zusammenarbeit, den Kampf gegen Cyberkriminalität sowie den Ausbau der personellen Kapazitäten in den Behörden (vgl. ebd, S. 12).
Die Bundesregierung versprach die Erreichung der Ziele der Cybersicherheitsstrategie regelmäßig zu prüfen und bei Bedarf Anpassungen vorzunehmen (vgl. ebd, S. 13).

In den Folgejahren gingen 2 Initiativen hervor, welche die Zusammenarbeit mit Akteuren aus dem öffentlichen wie auch privaten Sektor weiter fördern sollen. Das Bundeswirtschaftsministerium gründete 2011 die Initiative „IT-Sicherheit in der Wirtschaft“, welches kleine und mittelständische Unternehmen bei Fragen zur IT-Sicherheit berät und unterstützt (vgl. Bundesministerium für Wirtschaft und Klimaschutz 2022).
Die 2012 vom BSI gegründete Initiative „Allianz für Cybersicherheit“, dient als Austausch- und Beratungsplattform für Unternehmen und Behörden (vgl. Bundesamt für Sicherheit in der Informationstechnik 2021). Die Unternehmen und Behörden werden dort vom BSI über aktuelle Sicherheitsbedrohungen informiert und können selbst ihre Erfahrungen im Bereich der Cybersicherheit mit anderen teilen (vgl. ebd).
Die Enthüllungen des Whistleblowers Edward Snowden lösten im Juni 2013 eine Debatte aus in der die Cybersicherheitspolitik in den Fokus rückte. Die Enthüllungen offenbarten das der BND ausländische Geheimdienste wie die NSA unterstützt hatte, den Auslandsdatenverkehr innerhalb des deutschen Netzes zu überwachen (vgl. Schallbruch und Skierka 2018, S. 23). Die Praktiken des BND verstießen gegen die Verfassung. Zudem wurden deutsche Bürger, Unternehmen und Politiker von der NSA

überwacht (vgl. ebd). Auch das Telefon der damaligen Bundeskanzlerin Angela Merkel wurde überwacht (vgl. ebd). Neben der Opposition, kritisierte auch die Wirtschaft den BND sowie die Bundesregierung und betonte den Vertrauensverlust, der dadurch entstand (vgl. Der Spiegel 2015).Die ausgelöste Debatte um Cybersicherheit und Datenschutz waren vor und nach dem Bundestagswahlkampf ein wichtiges Thema (vgl. Schallbruch und Skierka 2018, S. 9 ff.). So enthielt der Koalitionsvertrag einige Punkte zum Schutz vor Überwachung von Gesellschaft, Wirtschaft und Staat und kündigte Maßnahmen in Form eines IT-Sicherheitsgesetzes und Stärkungen des BSIs an (vgl. ebd).

Die Regierung verabschiedete im August 2014 die „Digitale Agenda 2014-2017“. Sie formulierte darin als eines der wichtigen Ziele „den Erhalt unserer technologischen Souveränität“ (Die Bundesregierung 2014, S. 4). Vor allem die Digitalisierung der Industrie wurde daher als zentrales Mittel angesehen, um dieses Ziel zu erreichen (vgl. Die Bundesregierung 2014, S. 2). Die Regierung würde daher die nötigen Rahmenbedingungen schaffen wie beispielsweise die dafür benötigten Infrastrukturen auszubauen und zu modernisieren bzw. digitalisieren (vgl. Die Bundesregierung 2014, S. 9 f.). Ebenso der Verbraucherschutz im digitalen Bereich wurde als ein wichtiges Thema gesehen bei denen in Bezug auf Datenschutz Maßnahmen versprochen wurden, welche auch als Reaktion auf die Enthüllungen erfolgen sollten (vgl. ebd S. 32). Die Regierung forderte daher auch die Zusammenarbeit von Wirtschaft, Gesellschaft und Wissenschaft und versprach selbst einige Veränderungen in Bezug auf die Sicherheit zu unternehmen (vgl. ebd, S. 32 f.). So wurde ein IT-Sicherheitsgesetz angekündigt, welches den Schutz von kritischen Infrastrukturen durch verstärkte Zusammenarbeit mit den Betreibern als auch gesetzlichen Vorgaben vorsah (vgl. ebd). Neben Ankündigungen den Einsatz sicherer IT-Komponenten mittels Zertifizierungen, Förderungen und Entwicklungen auszubauen, sollten auch Veränderungen auf institutioneller Ebene erfolgen (vgl. ebd, S. 33). Das BKA und die BPol sollten ebenfalls im Kampf gegen Cyberspionage, sowie Cybercrime gestärkt werden (vgl. ebd). Daneben sollte das BBK mehr Kompetenzen beim Schutz kritischer Infrastrukturen erhalten, während das BSI mit besseren Ressourcen ausgestattet werden sollte (vgl. ebd). Das BfV sollte demnach bei seinen Bemühungen gegen Cyberspionage in der Wirtschaft, Terrorismus und Extremismus gestärkt werden und zusätzliche Kapazitäten dafür erhalten (vgl. ebd).

Zwischenzeitlich beschäftigte sich der Bundesrechnungshof mit der Cybersicherheitsstrategie von 2011 und dem erwähnten Punkt zum Personal in den Behörden. Dieser bemängelte die personelle Lage im NCAZ, welche dazu führte das dieses, nach Einschätzung des Bundesrechnungshofs nicht in der Lage sei seiner Aufgabe gerecht zu werden (vgl. Stephan Steller 2017, S. 53). Am NCAZ arbeiteten nach Gründung im Juni 2011 insgesamt 10 Personen aus BSI, BBK und BfV (vgl. Kuhn und Hauck 2011). Der Bundesrechnungshof stellte des Weiteren fest, dass zu den Lagebesprechungen einige Behörden gar anwesend sein würden, und führte dies auf undefinierte Arbeitsabläufe und unklare Kompetenzverteilung zurück (vgl. Goetz und Leyendecker 2014). Allerdings sah das BMI die Situation in Bezug auf Zuordnungen und der Kooperation mit der Wirtschaft im Bereich der Cybersicherheit als unbefriedigend an und arbeitete auf ein neues Gesetz hin (vgl. Zedler 2017, S. 70).
Der im Jahr 2013 verabschiedete Koalitionsvertrag von CDU/CSU und SPD beinhaltete den Vorschlag für ein „IT-Sicherheitsgesetz“, welches strengere Maßnahmen für die Betreiber Kritischer Infrastrukturen vorsah um den Schutz kritischer Infrastrukturen zu verbessern (vgl. Schallbruch und Skierka 2018, S. 22).
Das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ (IT-Sicherheitsgesetz), welches vom BMI ausgearbeitet wurde, ist im Juli 2015 verabschiedet worden. Betreiber kritischer Infrastruktur aus sieben Sektoren wurden durch das Gesetz verpflichtet Meldungen an das BSI bei potenziellen oder tatsächlichen IT-Sicherheitsvorfällen zu machen (vgl. ebd). Die Meldepflicht sollte für IT-Sicherheitsvorfälle bestehen, welche die Funktionalität der kritischen Infrastruktur beeinträchtigen oder zum Ausfall führen könnte (vgl. Bundesministerium des Innern 24.07.2015, S. 1326). Das BSI analysiert und bewertet die Meldungen zu IT-Sicherheitsvorfällen und leitet anschließend Informationen zu Abwehrmaßnahmen an die Unternehmen weiter (vgl. Schallbruch und Skierka 2018, S. 32 f.). Zudem erstellt das BSI mithilfe der Meldungen Lagebilder, welche es veröffentlicht. Neben der Meldepflicht wurden die Betreiber verpflichtet technische Mindeststandards umzusetzen (vgl. Schallbruch und Skierka 2018, S. 32 f.). Da sektoral die benötigten Sicherheitsniveaus variieren können, wurde den Betreibern selbst überlassen, wie diese den Mindeststandard setzen, jedoch nach Absprache mit dem BSI (vgl. ebd). Zudem ist das BSI autorisiert worden, die Einhaltung der Sicherheitsstandards zu

überprüfen und bei Nichteinhaltung Strafen zu verhängen (vgl. ebd). Für die Umsetzung des Gesetzes wurde den Betreibern ein Zeitraum von zwei Jahren nach Inkrafttreten des Gesetzes gewährt (vgl. Bundesministerium des Innern 24.07.2015, S. 1325).
Das IT-Sicherheitsgesetz wies auch dem BKA mehr Aufgaben zu und erweiterte dessen Befugnisse auf Ermittlungen bei Cyberangriffen auf Einrichtungen des Bundes (vgl. Zedler 2016, S.40).

Am 13 Juli 2016 wurde das „Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr“ verabschiedet. Die Auseinandersetzung mit der Cybersicherheit war in diesem Weißbuch deutlich größer als noch zum Vorgängerbuch von 2006. So wurde die größere Bedrohungslage durch Anstieg von Anzahl und Qualität der Cyberangriffe und gleichzeitiger Digitalisierung als Herausforderung beschrieben (vgl. Die Bundesregierung 2016, S. 36). Neben Cyberangriffen benannte das Weißbuch auch die zunehmende Beeinflussung der gesellschaftlichen Meinung durch manipulierte Informationen in sozialen Netzwerken als Bedrohung und Herausforderung (vgl. ebd). Die Aufgabe der Bundeswehr sollte der Aufbau der Cyberverteidigung und der Schutz öffentlicher und privater Akteure sein, wofür im Weißbuch defensive und offensive Cyber-Kriegsfähigkeiten gefordert wurden (vgl. ebd, S. 93).
Die Bundeswehr errichtete ein Jahr nach Veröffentlichung des Weißbuchs das „Kommando Cyber- und Informationsraum“ (KdoCIR) und übertrug ihr die Leitung über den Organisationsbereich „Cyber- und Informationsraum“ (CIR), welcher neu gegründet wurde und alle vorhanden Ressourcen im Cyberbereich der Bundeswehr vereint (vgl. Schulze und Stiftung Wissenschaft und Politik 2020, S. 13). Neben der Funktion als Fort- und Ausbildungsstätte werden im CIR die IT-Systeme der Bundeswehr vor Cyberangriffen geschützt (vgl. Bundeswehr 2022, S. Test). Hierfür wurde das „Zentrum für Cyber-Sicherheit der Bundeswehr“ zuständig.

Im November 2016 stellte das BMI eine neue Cybersicherheitsstrategie vor. In dieser beschränkten sich die Strategie und Maßnahmen auf vier Handlungsfelder, welche alle gesellschaftlichen Bereiche umfassten (vgl. Bundesministerium des Innern 2016, S. 9). Das erste Handlungsfeld bezog sich auf Gesellschaft, Staat sowie Wirtschaft und thematisierte die Sensibilisierung im Umgang mit dem Cyber-Raum, als auch die Sicherheit von IT-Produkten (vgl. Bundesministerium des Innern 2016, S. 12 ff.). Ein

breiteres Bildungsangebot in Schulen und Universitäten sollte ein besseres gesellschaftliches Bewusstsein im Cyber-Raum schaffen und Ausbildung wie auch Forschung im Bereich der Informatik verbessern (vgl. Bundesministerium des Innern 2016, S. 14 ff). Hierfür sollten auch Kooperationen mit Unternehmen entstehen (vgl. ebd). Daneben sollte die Sicherheit von IT-Produkten und Komponenten durch ein Gütesiegel verbessert werden, welches vom BSI vergeben werden sollte (vgl. ebd, S. 17). Das zweite Handlungsfeld betraf den Staat und die Wirtschaft. In diesem wurde die Zusammenarbeit und der Austausch von Staat und Wirtschaft als essenziell angesehen, um Sicherheit zu gewährleisten (vgl. ebd S. 20 f.). Die Regierung betonte die Wichtigkeit des Schutzes von kritischen Infrastrukturen, aber auch von Unternehmen und versprach den Ausbau der bereits vorhandenen Initiativen mit der Wirtschaft (vgl. ebd S. 22). Das dritte Handlungsfeld befasste sich mit der Cyber-Sicherheitsarchitektur von Bund, Ländern und Kommunen. Der Fokus wurde auf die Verbesserung von Zusammenarbeit und Ressourcen gelegt. So sollte beispielsweise der Austausch von Informationen über Cyberangriffe zwischen Bund und Ländern verpflichtend gemacht werden und Fachwissen von Bundesbehörden über die Bundesländer bis zu den Kommunen gelangen (vgl. Bundesministerium des Innern 2016, S. 36). Die Zusammenarbeit und die Ressourcen der Strafverfolgungsbehörden von Bund und Ländern sollten im Kampf gegen Cyber-Kriminalität ebenfalls verbessert werden (vgl. ebd, S. 30). Für die Ressourcen sollte die „Zentrale Stelle für Informationstechnik im Sicherheitsbereich“ (ZITiS) gegründet werden, welche IT-Lösungen und Strategien für die Behörden entwickeln sollte, um deren Cyber-Fähigkeiten zu verbessern (vgl. Bundesministerium des Innern 2016, S. 32). Die Strategie befasste sich auch mit den CERT’s welche über die Jahre in immer mehr Institutionen von Bund und Ländern sowie größeren Unternehmen installiert wurden. Die Strategie befürwortete die weitere Installation von CERTs als auch die Vernetzung dieser untereinander (vgl ebd, S. 34).

Außerdem sah die Strategie vor, dem BMI die Führung über das NCAZ zu übertragen, um die Arbeit des NCAZ weiter zu verbessern (vgl. Bundesministerium des Innern 2016, S. 28). Zudem wurde dem BND eine wichtigere Rolle zugesprochen. Dieser soll Cyberangriffe beobachten, sowohl während ihrer Planung als auch in der Durchführung und die Informationen für Cyberabwehrmaßnahmen entsprechend weiterleiten (vgl. Bundesministerium des Innern 2016, S. 29 ff.). Das vierte und letzte

Handlungsfeld befasste sich mit der europäischen und internationalen Cyber-Sicherheitspolitik.

Die in der Cybersicherheitstrategie erwähnten Beobachtungen von Cyberangriffen durch den BND implizierten das Eindringen des BNDs in ausländische Netze. Die gesetzliche Grundlage für derartige Handlungen des BNDs trat 2017 mit dem BND-Gesetz in Kraft.
Das Bundeskanzleramt erstellte 2016 ein neues Gesetz zu den Befugnissen des BND. Die größtenteils illegalen Praktiken des BNDs die durch Edward Snowden aufgedeckt wurden, sind durch das BND-Gesetz legalisiert worden (vgl. Meister 2016). Dem BND, welcher dem Bundeskanzleramt untersteht, wurde gestattet den Auslandsdatenverkehr im Netz abzuhören und auszuwerten (vgl. Meister 2016) . Die Verwendung des Begriffs „Netz“ innerhalb des Gesetzes war dabei wichtig. Zuvor durfte der BND nur einzelne Leitungen überwachen, doch der Begriff „Netz“ umfasst sämtliche Leitungen und Geräte, die miteinander verbunden sind (vgl. Welchering 2017). Da der Auslandsdatenverkehr auch durch das deutsche Netz fließt (beispielsweise durch den Internetknotenpunkt DE-CIX in Frankfurt), impliziert dies auch eine Überwachung des deutschen Netzes (vgl. Welchering 2017). Das Gesetz wurde von Opposition und NGOs kritisiert (vgl. Meister 2016). Durch die neuen Befugnisse begann der BND Informationen über bevorstehende Cyberangriffe aus dem Ausland zu sammeln und beteiligte sich an der Cyberabwehr (vgl. Schallbruch und Skierka 2018, S. 35).

Das Bundesverfassungsgericht kippte das BND-Gesetz von 2016, da nach Ansicht des BVG die Überwachung des Auslandsdatenverkehrs sowohl gegen das Telekommunikationsgeheimnis als auch gegen die Pressefreiheit verstieß (vgl. Meister 2020).

Die Bundesregierung überarbeitete und erließ 2021 ein neues BND-Gesetz, nachdem die Fassung von 2016 ein Jahr zuvor vom BVG als verfassungswidrig eingestuft wurde. Das neue BND-Gesetz erlaubt es dem BND neben Kommunikationsanbietern auch alle 192 Staaten zu hacken (vgl. Meister 2021).

Ebenso das Abhören deutscher Staatsbürger wird legitimiert (vgl. Meister 2021). Opposition und NGOs kritisierten die neue Novelle des BND-Gesetzes (vgl. Meister 2021). Von Seiten der Wirtschaft wurde das Gesetz nicht so kritisch aufgenommen, da diese den BND als eine wichtige Institution in Bezug auf die Cybersicherheit ansieht (vgl. Bundesverband der Deutschen Industrie e.V. 2020a, S. 3).

Im Mai 2021 trat das IT-Sicherheitsgesetz 2.0 in Kraft. Das Gesetz erweiterte den Bereich der kritischen Infrastrukturen, wodurch mehr Unternehmen unter das Gesetz fallen und sich danach richten müssen (vgl.Schallbruch 2021b, S. 5). So wurde die „Siedlungsabfallentsorgung“ als weiterer Sektor zu den kritischen Infrastrukturen hinzugefügt (vgl. ebd). Ebenso wurden die Befugnisse des BSI gegenüber Betreiber kritischer Infrastrukturen erweitert, sodass das BSI bei größeren Störungen durch Cyberangriffe an der Cyberabwehr mitwirken darf (vgl. Schallbruch 2021b, S. 6). Neben den kritischen Infrastrukturen wurde der Bereich „Unternehmen im besonderen öffentlichen Interesse“ geschaffen, welcher sich aus Rüstungs- und IT-Sicherheitsunternehmen, der Chemie-Industrie und den größten deutschen Unternehmen zusammensetzt (vgl. Schallbruch 2021b, S. 5 ff). Die Regularien für „Unternehmen im besonderen öffentlichen Interesse“ sind allerdings weniger streng als die der kritischen Infrastrukturen (vgl. Schallbruch 2021b, S. 5).
In Bezug auf die Untersuchung von IT-Produkten und Komponenten inländischer Unternehmen auf deren Sicherheit kann das BSI nun Einsicht auf die technischen Unterlagen verlangen muss jedoch bei Befund von Sicherheitsmängeln, die Betreiber kritischer Infrastrukturen und Unternehmen im besonderen öffentlichen Interesse darüber in Kenntnis setzen (vgl. Schallbruch 2021b, S.10). Auch die Befugnisse des BSI gegenüber der Bundesverwaltung wurden erweitert. Das BSI darf verbindliche Mindeststandards für die IT innerhalb der Ministerien und Behörden anordnen und deren Umsetzung kontrollieren (vgl. Schallbruch 2021a, S. 6f). Um die zusätzlichen Aufgaben zu bewältigen, welche durch das IT-Sicherheitsgesetz 2.0 auf das BSI zukommt, ist vorgesehen das Personal des BSI von 1500 auf 2300 zu erhöhen (vgl. Schallbruch 2021a, S. 10).
Von Seiten der Wirtschaftsverbände wurde das Vorhaben der Regierung auch Bereiche zu unterstützen, welche nicht zur kritischen Infrastruktur gehören als positiv empfunden (vgl. ASW Bundesverband 2020, S. 2). Allerdings wurde kritisiert, dass das BSI weiter zu einer zentralen Meldestelle für IT-Sicherheitsvorfälle ausgebaut wird,

jedoch die Weitergabe der Informationen weiterhin im Ermessen des BSI liegt und es keine Verpflichtung gibt (vgl. ASW Bundesverband 2020, S. 4 f.). Ebenso wurde kritisiert, dass das Gesetz im Alleingang vom BMI ohne Beteiligung von Bundesländern und der Wirtschaft entworfen wurde und diesen nur einen Tag für eine Stellungnahme Zeit gelassen wurde (vgl. Schallbruch 2021b, S. 3 f). Von Seiten der Industrie wurde daher gefordert zukünftig mehr Beteiligung am Gesetzgebungsverfahren zu ermöglichen (vgl. Bundesverband der Deutschen Industrie e.V. 2020b, S. 4).

3.2 Einordnung Deutschlands in die Taxonomie

Koordinierung der Cyber-Sicherheitspolitik

Wie aus dem vorherigen Kapitel entnommen werden kann, ist das BMI als oberste Behörde für die Koordinierung der Cyber-Sicherheitspolitik zuständig. Das BMI ist für die Cybersicherheitsstrategien in Deutschland verantwortlich und entwirft Gesetzesvorlagen, wie beispielsweise die des IT-Sicherheitsgesetzes. Das dem BMI unterstellte BSI ist für die Umsetzung und Einhaltung der Gesetze verantwortlich. Es kontrolliert, ob die Betreiber kritischer Infrastrukturen die gesetzlichen Vorgaben umsetzen und kann bei Nichteinhaltung Geldstrafen verhängen. Zudem ist das BSI auch beratend tätig und hilft den Betreibern und Unternehmen dabei ihre Sicherheitsstandards zu verbessern. Da das BSI IT-Produkte und Komponenten auf deren Sicherheit überprüft und zertifiziert, kann es den Unternehmen bei der Auswahl Empfehlungen geben. Das BSI ist somit operativ tätig während das BMI die Cyber-Sicherheitspolitik koordiniert.

Koordination Krisenmanagement:

Das deutsche Krisenmanagement ist vom Föderalismus geprägt. Für die Bewältigung einer Krise sind daher in erster Linie die Bundesländer zuständig. Die Reaktion auf eine Krise erfolgt somit von dem Bundesland, in welchem die Krise entsteht. Die Bundesländer erhalten jedoch im Vorfeld strategische Unterstützung vom BBK. Dieses analysiert und bewertet die Risiken von Krisen und erstellt daraus Maßnahmen und Handlungsempfehlungen für die Bundesländer, welche diese umsetzen. Somit bestimmt das BBK die Strategie des Krisenmanagements, in dem es die Länder auf

die Krisen vorbereitet, beispielsweise durch gemeinsame Krisenübungen oder auch durch Vorgabe von Präventionsmaßnahmen. Das BBK passt sein Krisenmanagement durch ständige Analysen an. Das BBK unterliegt dem BMI, welche die oberste Behörde ist. Im Bereich des Cyber-Krisenmanagements ist das BBK ebenfalls involviert und berät Betreiber kritischer Infrastrukturen. Bei einem schweren Cyberangriff wird allerdings das BSI tätig und unterstützt den Betreiber bzw. das betroffene Unternehmen. Hierfür greift das BSI auf das CERT-Bund und das IT-KRZ zurück, welche innerhalb des BSI angesiedelt sind.

CERT

Unter das Attribut „die wichtigsten öffentlichen CERTs“ fällt das BSI darunter. Das BSI unterstützt sowohl Bundesbehörden, wofür speziell das CERT-Bund zuständig ist, als auch private Akteure wie Betreiber kritischer Infrastrukturen und Unternehmen. Die Unterstützung kann in Form von Cyberabwehrmaßnahmen während oder nach einem Cyberangriff erfolgen mit Unterstützung oder bereits im Vorfeld durch Sicherheitsempfehlungen. Die Bundeswehr überwacht und schützt seine Netzwerke und Systeme selbst und hat mit dem „Zentrum für Cyber-Sicherheit der Bundeswehr“ ein eigenes Notfallteam.

Cyberkapazitäten

Die Cyberkapazitäten der Regierung in Deutschland sind eher verteilt einzuordnen als zentralisiert. Sowohl das BSI verfügt über Ressourcen, welche eingesetzt werden können, um auf einen Cyberangriff zu reagieren als auch die Bundeswehr, die ihre eignen Netzwerke und Systeme überwacht und schützt. Zudem kommt mit dem BND eine dritte Behörde welche Cyberkapazitäten besitzt. Der BND ist in der Lage defensive Cyberoperationen durchzuführen. Das bedeutet, dass der BND in ausländische Netze eindringen und diese ausspionieren kann. Informationen über bevorstehende Cyberangriffe kann der BND an Behörden in Deutschland weiterleiten. Ebenso haben die Ministerien Cyberkapazitäten und überwachen ihre Regierungsnetzwerke.

Überwachung der Regierungsnetzwerke

Das BSI überwacht die Regierungsnetze nicht, dafür sind die Bundesministerien selbst verantwortlich.

Einbindung der Geheimdienste

Die CERTs in Deutschland sind nicht in der Geheimdienst- bzw. Nachrichtendienstlandschaft eingebettet. Das BSI hat keine direkte Verbindung zum BND.

Netzwerkmodell

Das Netzwerkmodell, welches Deutschland am nächsten kommt ist das der „Network-administrative". Zwar enthält die Zusammenarbeit Elemente der Freiwilligkeit, wie beispielsweise bei der Initiative „Allianz für Cybersicherheit", bei dem Unternehmen freiwillig zusammenkommen können, sich informieren und austauschen können, allerdings werden den Betreibern kritischer Infrastrukturen durch die IT-Sicherheitsgesetze Bedingungen auferlegt, welche diese umsetzen müssen. Das BSI ist befugt die Umsetzung zu kontrollieren und bei Missachtung Geldstrafen zu verhängen. Dies schließt die Einordnung Deutschlands als „Participant governed" Netzwerkmodel aus. Das BSI ist ein zentraler Akteur bei der öffentlichen-privaten Partnerschaft in Deutschland. Durch die Meldepflichten, die den Betreibern kritischer Infrastrukturen auferlegt werden, erhält das BSI viele Informationen, welche es analysiert und bewertet. Diese kann das BSI entsprechend weiterleiten. Jedoch ist das BSI nicht der einzige Ansprechpartner über alle wichtigen Informationen. Das BSI ist nur für die Unternehmen zuständig, die unter das IT-Sicherheitsgesetz fallen. Innerhalb des gesetzlich festgelegten Zuständigkeitsbereichs ist das BSI dafür zuständig, dass die Unternehmen und Betreiber kritischer Infrastrukturen ihre Funktionalität gewährleisten können. In Bezug auf Cybercrime wird es jedoch nicht tätig. Hier liegen die Kompetenzen und Kapazitäten bei BKA, BPol und bei den Strafverfolgungsbehörden der Bundesländer. Zudem verfügen auch die Bundeswehr und der BND über Kapazitäten im Cyberbereich. Der BND generiert durch seine Arbeit zusätzliche Informationen, welche er an die entsprechenden Stellen weiterleitet. In Deutschland gibt es nicht einen zentralen staatlichen Akteur, sondern mehrere staatliche Akteure welche Kapazitäten, Befugnisse und Informationen besitzen. Um die Zusammenarbeit unter den genannten staatlichen Akteuren zu verbessern, wurde daher das NCAZ gegründet. Somit ist auch das Netzwerkmodel der „Lead organization" auszuschließen. Daher wird Deutschland die „Network-administrative" als Netzwerkmodell zugeordnet.

Nach der Einordnung in die Taxonomie ergibt sich folgende Darstellung.

	Deutschland
Koordinierung der Cyber-Sicherheitspolitik	BMI
Koordinierung allgemeines Krisenmanagement	BMI
Die wichtigsten öffentlichen CERTs	CERT-BUND, Zentrum für Cyber-Sicherheit der Bundeswehr
Cyberkapazitäten der Regierung	verteilt
Überwachung der Regierungsnetzwerke	Ministerien haben eigene Verantwortung
Einbindung der Geheimdienste	außerhalb
Netzwerkmodell	Network-administrative

„Tabelle 2: Eigene Darstellung der Cyber-Governance-Struktur Deutschlands in Anlehnung an Boeke (2018)“

4. Die Cyber-Governance-Struktur Frankreichs

Im Folgenden wird die Entwicklung der Cybersicherheitspolitik in Frankreich beschrieben, während im anschließenden Unterkapitel die Einordnung in die Taxonomie stattfundet.

4.1 Die französische Cybersicherheitspolitik im zeitlichen Verlauf

Die Gefahren von Cyber-Attacken und die daraus resultierende Bedrohung für die Sicherheit ist in Frankreich 2008 verstärkt in den Fokus gerückt (vgl. Jonas und Ondarza 2010, S. 34 ff.). Im Weißbuch „Livre Blanc de la Défense“ von 2008, welches die strategische Ausrichtung der nationalen Sicherheitspolitik definiert, wurde die Cybersicherheit als wichtiger Bestandteil aufgeführt (vgl. Vitel und Bilddal 2015, S. 3209-3). Zudem empfahl das Weißbuch die Entwicklung von defensiven als auch offensiven Cyber-Kriegsfähigkeiten (vgl. Hathaway et al. 2016, S. 15 f). Hintergrund war der Cyberangriff auf Estland im Jahr 2007 (vgl. Vitel und Bilddal 2015, S. 3209-11) sowie Berichte zweier französischer Senatoren in den Jahren 2006 und 2008, welche die nationale Lage der Cyberverteidigung als unzureichend und mangelhaft bewerteten (vgl. Baumard 2017, S. 55 f.). Die Berichte legten offen, dass Frankreich sowohl organisatorisch als auch ressourcentechnisch im Vergleich zu Nachbarländern wie beispielsweise Deutschland rückschrittlich sei (vgl. ebd). Dieses Urteil galt für den öffentlichen wie für den privaten Sektor gleichermaßen (vgl. ebd). Daher wurden im Weißbuch von 2008 die Cybersicherheitskapazitäten im Bereich der Industrie als wichtiger Punkt aufgeführt und die Förderung dieser Kapazitäten als Ziel verankert (vgl. Calcara und Marchetti 2021, S. 10 ff.).

Als Reaktion auf die Berichte und das Weißbuch wurde 2009 zudem die „Agence nationale de la sécurité des systèmes d ' information“ (ANSSI) gegründet (vgl. Vitel und Bilddal 2015, S. 3209-3). Diese Behörde wurde im „Secrétariat général de la défense et de la sécurité nationale“, dem Generalsekretariat für Verteidigung und nationale Sicherheit (SGDSN) angesiedelt. Nach der Gründung wurde die ANSSI mit 120 Mitarbeitern und einem Budget von 45 Mio. € ausgestattet und hatte den Auftrag, die Sicherheit von Informationssystemen zu koordinieren, während die SGDSN den Premierminister in Bezug auf die Sicherheit berät und unterstützt (vgl. Brangetto 2015,

S. 11). Innerhalb der ANSSI wurde das „Centre opérationnel de la sécurité des systèmes d'information“ (COSSI) installiert, welches Bedrohungen und Schwachstellen identifizieren sowie Gegenmaßnahmen durchführen und Schadensbegrenzung betreiben bzw. Schäden beheben soll (vgl. Vitel und Bilddal 2015, S. 3209-6). Um in Notfallsituationen Hilfe leisten zu können, wird das COSSI vom Computer-Securit-incident-response-team „CERTA“ unterstützt (vgl. ebd). CERTA veröffentlicht auch Meldungen zu Bedrohungen und Schwachstellen.

Das SGDSN ist dem Premierminister unterstellt und unterstützt diesen im Falle einer Krise in dem es die „cellule interministérielle de crise“ (CIC), eine Interministerielle Kriseneinheit einberuft (vgl. Secrétariat général de la défense et de la sécurité nationale 2022). Der Premierminister kann daraufhin je nach Art der Krise einem Minister die Verantwortung für die Bewältigung der Krise übertragen (vgl. Secrétariat général de la défense et de la sécurité nationale 2022). In der Regel sind das jedoch der Innenminister, wenn es sich um eine Krise im Inland handelt oder der Minister für auswärtige Angelegenheiten, wenn die Krise außerhalb des französischen Staatsgebiets liegt (vgl. Secrétariat général de la défense et de la sécurité nationale 2022). Die im Innenministerium angesiedelte „Direction générale de la sécurité civile et de la gestion des crises“ (DGSCGC) ist für die Prävention als auch die Überwachung von Krisen zuständig (vgl.European Civil Protection and Humanitarian Aid Operations 2022). Nationale Krisenübungen, darunter auch im Cyberbereich werden von der SGDSN organisiert und alle zwei Jahre unter strenger Geheimhaltung durchgeführt (vgl. Hathaway et al. 2016, S. 9). Für die Durchführung der Übungen wird im Vorfeld ein Plan erstellt, bei dem die SGDSN, Vertreter der Ministerien und private Akteure beteiligt sind (vgl. ebd).

Das französische Verteidigungsministerium widmet sich der Cyberverteidigung in dem es das militärische System und Netzwerke wartet und beschützt (vgl. Baezner et al. 2018, S. 13). Dass das Militär von Cyberattacken nicht verschont ist, bewahrheitete sich im Jahr 2009 als der „Cornficker-Wurm“ das Computersystem der französischen Marine infizierte und dadurch die Kampfflugzeuge nicht starten konnten (vgl. Brangetto 2015, S. 11).

Unter der Präsidentschaft von Nicolas Sarkozy wurde im Jahr 2010 ein Strategierat (CSFRS) mit Akteuren aus Wirtschaft, Militär, Staat, Wissenschaft und dem zivilen Bereich einberufen, der sich mit der Organisation der Cybersicherheit beschäftigen sollte (vgl. Baumard 2017, S. 57 ff.). Der Strategierat unterstrich in ihrem Bericht die Wichtigkeit der Informationstechnologie und deren Sicherheit und forderte weitere Maßnahmen Frankreichs, da die bisherigen noch nicht ausreichend seien (vgl. ebd). Der Bericht machte deutlich, dass es sowohl an Normen und deren Kontrolle als auch an Fachkräften und Fachwissen im Bereich der Cyberverteidigung in Frankreich mangele (vgl. ebd). Der Strategierat empfahl daher die Förderung von Forschung und Entwicklung im Bereich der Cyberverteidigung, die Installation von Koordinierungsstellen, welche die Umsetzung von Sicherheitsstandards von öffentlichen und privaten Akteuren kontrollieren sollte und machte sich für die Ausweitung der Kompetenzen der ANSSI stark (vgl. ebd). Des Weiteren stellte der Bericht fest, dass Frankreich über keinerlei offensive Cyberfähigkeiten verfüge und forderte diesbezüglich zum Handeln auf (vgl. Baumard 2017, S. 59). Die ANSSI wurde daraufhin von der SGDSN mit der Ausarbeitung einer nationalen Cybersicherheitsstrategie beauftragt, welche 2011 veröffentlicht wurde (vgl. Brangetto 2015, S. 7 f.).

Die Cybersicherheitsstrategie von 2011 war die erste reine Cyberstrategie für Frankreich. In dieser stellte Frankreich klar, dass es zu einer Weltmacht in der Cyberverteidigung werden möchte (vgl. Agence Nationale de la Sécurité des Systèmes d'Information 2011, S. 5 ff.). Ebenso sollte die Cybersicherheit von kritischen Infrastrukturen verbessert werden und der Cyberraum für alle Bürger sicher gemacht werden (vgl. Agence Nationale de la Sécurité des Systèmes d'Information 2011, S. 7). Die Strategie sah zudem konkrete Maßnahmen für den Schutz der Industrie vor Cyberangriffen vor (vgl. Calcara und Marchetti 2021, S. 10 ff.). Das Verteidigungsministerium sollte als Ansprechpartner für militärisch relevante Partner zuständig sein, während die ANSSI alle anderen öffentlich und privaten Partner unterstützt, welche nicht vom Verteidigungsministerium abgedeckt werden (vgl. Baezner et al. 2018, S. 18).

Als 2011 und 2012 Frankreich Opfer von Cyberangriffen wurde stand die Organisation der Cybersicherheit erneut auf dem Prüfstand, zumal es sich bei den Zielen um das

Finanzministerium und einem wichtigen Unternehmen im Bereich der Kernenergie handelte (vgl. Baumard 2017, S. 60). Ein neu verfasster Bericht von Senatoren im Jahr 2012 bemängelte erneut die Cybersicherheit in Frankreich und forderte unter anderem mehr Investitionen in die ANSSI, welche zu diesem Zeitpunkt mit 230 Mitarbeitern und einem Budget von 75 Mio. € ausgestattet war, was im Vergleich zu ähnlichen Behörden in Nachbarländern wie beispielsweise Deutschland wenig war (vgl. ebd).

Im Jahr 2013 erschien eine neue Version des Weißbuchs. Dieses betonte die Wichtigkeit des Aufbaus von Cybersicherheitskapazitäten aufgrund des Voranschreitens des technologischen Fortschritts und der zunehmenden Abhängigkeit von Informationssystemen (vgl. Vitel und Bilddal 2015, S. 3209-4 ff.). Daher müssten deutlich größere Investitionen vorgenommen werden. Speziell in die Ausbildung und Rekrutierung von Fachpersonal wie auch in starke Sicherheitssysteme sollte investiert werden, um die wachsende Bedrohung von Cyberangriffen bewältigen zu können (vgl. ebd). Hierbei sieht das Weißbuch die Förderung von Wissenschaft und Industrie in Bezug auf Cybersicherheit als wichtigen Punkt an (vgl. ebd). Frankreich müsse zudem in der Lage sein sich vor Cyberangriffen zu schützen und diese zu attribuieren, d.h. die Herkunft des Angriffs festzustellen (vgl. ebd). Im Weißbuch von 2013 wurde des Weiteren gefordert, dass rechtliche Normen für die Cybersicherheit in Frankreich getroffen werden sollen. Es müssten klare Sicherheitsstandards für die Sektoren der nationalen kritischen Infrastruktur definiert werden an diese sich die Betreiber zu halten haben (vgl. ebd). Eine weitere Forderung des Weißbuchs ist die Sensibilisierung der Bevölkerung in Bezug auf die Cybersicherheit, mittels Kampagnen (vgl. Vitel und Bilddal 2015, S 3209-5). Wie schon das vorherige Weißbuch aus dem Jahr 2008, forderte die neue Version die Entwicklung von offensiven Cyberfähigkeiten (vgl. Brangetto 2015, S. 8). Als einen letzten wichtigen Punkt sollte eine gemeinsame europäische Cybersicherheitspolitik vorangetrieben werden (vgl. Vitel und Bilddal 2015, S. 3209-5).

Um die Punkte des Weißpapiers von 2013 umzusetzen, wurden einige Maßnahmen veranlasst. So investierte die Regierung zwischen 2013 und 2014 ca. 150 Mio. € in die Forschung und Entwicklung im Bereich der Cybersicherheit (vgl. Calcara und Marchetti 2021, S. 10 f.). Das Ministerium für Wirtschaft, Finanzen und die industrielle und digitale Souveränität initiierte 2013 34 Projekte, um Frankreichs Wirtschaft zu

modernisieren. Eines dieser Projekte unter der Leitung des ANSSI zielte darauf, französische Unternehmen bei der Entwicklung von Cybersicherheitslösungen zu unterstützen (vgl. Vitel und Bilddal 2015, S. 3209-7). Der französische Verteidigungsminister Jean-Yves Le Drian ging auf die im Weißbuch geforderte Entwicklung von offensiven Cyberfähigkeiten ein und wollte sich dieser annehmen (vgl. Vitel und Bilddal 2015, S. 3209-5).
Der Premierminister wurde durch das Militärplanungsgesetz „Loi de Programmation Militaire“ von 2013 mit mehr Befugnissen ausgestattet. Die Politik und deren Durchsetzung in Bezug auf die französische Cybersicherheitspolitik ging vollständig in die Obhut des Premierministers über (vgl. Brangetto 2015, S. 9 f.). Das SGDSN sollte dabei Gesetzesvorlagen ausarbeiten und dem Premierminister vorschlagen (vgl. ebd). Die Umsetzung wurde ebenfalls der SGDSN auferlegt die dafür die Unterstützung der ANSSI hat (vgl. ebd). Zudem wurde im Jahr 2013 das „CIIP-Gesetz“ erweitert. Dieses Gesetz bezieht sich auf die kritische Infrastruktur und ihre Betreiber. Frankreich definiert kritische Infrastrukturen wie folgt:

„Critical infrastructures are institutions, structures or facilities that provide the essential goods and services forming the backbone of French society and its way of life.“
(Secrétariat général de la défense et de la sécurité nationale 2017).

Die Betreiber von kritischen Infrastrukturen sind durch das CIIP-Gesetz angewiesen worden ihre kritischen Bereiche „kritische Informationssysteme“ zu identifizieren und an die ANSSI zu übermitteln (vgl. ANSSI 2022h). Im CIIP-Gesetz wurde entsprechend definiert was unter „kritische Informationssysteme“ fällt. Das Gesetz galt für 200 öffentliche und private Betreiber aus 12 Sektoren (vgl. ANSSI 2022h). Diese Betreiber wurden definiert als:

„operator[s] whose unavailability could strongly threaten the economical or military potential, the security or the resilience of the Nation”.
(ANSSI 2022f)

Das Militärplanungsgesetz und das CIIP erweiterten auch die Befugnisse der ANSSI. Die Agentur sollte die Sicherheitsmaßnahmen für die Betreiber von kritischer

Infrastruktur festlegen und deren Einhaltung überprüfen (vgl. Vitel und Bilddal 2015, S. 3209-7). Die Sicherheitsmaßnahmen erarbeitete die ANSSI gemeinsam mit den Betreibern, da beide ihr Wissen und ihre Erfahrungen einbringen konnten (vgl. ANSSI 2022f). Hierfür gründete die ANSSI eine Arbeitsgruppe für öffentlich und privater Betreiber kritischer Infrastrukturen, Ministerien sowie Regierungsbehörden. Unter freiwilliger Teilnahme konnten sich die einzelnen Vertreter an der Ausarbeitung von Sicherheitsregeln beteiligen und Fachwissen aus den jeweiligen Sektoren einbringen (vgl. ANSSI 2022h).
Für die Einhaltung der Sicherheitsmaßnahmen wurde die ANSSI autorisiert, auch andere Behörden anzuordnen, eine Überprüfung durchzuführen (vgl. ANSSI 2022h).
Die Sicherheitsmaßnahmen zielen auf den Schutz der gemeldeten kritischen Bereiche und soll das Sicherheitsniveau der Betreiber auf ein gleich hohes Level bringen. Die entstehenden Kosten für die Umsetzung der auferlegten Sicherheitsmaßnahmen müssen die Betreiber selbst tragen (vgl. ANSSI 2022h). Sollten die Betreiber die Sicherheitsmaßnahmen nicht umsetzen, wurde im Militärgesetz ein Bußgeld von 150.000€ bzw. 750.00€ festgeschrieben (vgl.ANSSI 2022c).
Die Betreiber sind zudem verpflichtet worden Meldung über Zwischenfälle an die ANSSI zu erstatten (vgl. ANSSI 2022c). Die ANSSI bewertet und analysiert die gemeldeten Zwischenfälle und greift bei einer hohen Gefahrenlage unterstützend ein (vgl. ANSSI 2022c). Zudem informiert es andere Betreiber, Unternehmen und Ministerien über den Zwischenfall (vgl. ANSSI 2022c). Die Zahl der Mitarbeiter der ANSSI wurde dafür bis 2014 auf 350 und das Budget auf 83,4 Mio. aufgestockt € (vgl. Baumard 2017, S. 57). Des Weiteren führte die ANSSI das Siegel „FRANCE CYBER SECURITY“ ein. Französische Unternehmen können dort ihre IT-Produkte überprüfen und anschließend zertifizieren lassen (vgl. Calcara und Marchetti 2021, S. 11).

Die ANSSI aktualisierte 2014 auch einen Teil des „VIGIPIRATE-Plan“, einen Präventionsplan gegen Terrorismus, welcher Ende der siebziger Jahre entstand (vgl. Brangetto 2015, S. 13 f). Hierbei gab die ANSSI Empfehlungen im Bereich der Cybersicherheit für Betreiber und Behörden, welche nicht zu kritischen Infrastruktur zählen (vgl. ANSSI 2022d). Die ANSSI erhielt die Befugnis diesen Plan bei Bedarf zu aktualisieren. Die Verantwortung für den VIGIPIRATE-Plan allerdings trägt das SGDSN (vgl. Brangetto 2015, S. 13 f.).

Im Februar 2014 stellte der Verteidigungsminister Jean-Yves Le Drian den Cyberverteidigungspakt „pacte défense cyber“ vor. In diesem wurde das Verteidigungsministerium offiziell mit der Cyberverteidigung betraut was zuvor nur informell galt (vgl. Baezner et al. 2018, S. 13). Zudem sollen Investitionen in Höhe von bis zu 1 Milliarde € in die Cyberverteidigung erfolgen. Neben der Erhöhung des Sicherheitsniveaus der eigenen Systeme und militärischen Netze soll der Ausbau der Forschung und Ausbildungsstätten vorangetrieben werden (vgl. Vitel und Bilddal 2015, 3209-8 f.). So wurde in der Bretagne ein Exzellenz-Zentrum für Cyberverteidigung „pôle d'excellence cyber“ geschaffen, um Personal auszubilden und eine nationale Cyberindustrie in der Region zu entwickeln (vgl. ebd). Des Weiteren wurden COSSI und das Analysezentrum des Verteidigungsministerium „Le Centre d’analyse de lutte informatique défensiv“ CALID im Jahr 2014 ins gleiche Gebäude in Paris untergebracht um die Koordinierung sowie den Austausch von Informationen zu verbessern (vgl. ebd, S. 3209-8). CALID ist das CERT des französischen Militärs und schützt dieses vor Cyberangriffen (vgl. Hathaway et al. 2016, S. 17). Außerdem wurde das Computer-Securit-incident-response-team „CERTA“ 2014 in CERT-FR umbenannt.

Das Innenministerium unternahm ebenfalls im Jahr 2014 einige Maßnahmen in Bezug auf die Cybersicherheit. So wurde die Position des „Cyber-Präfekten“ geschaffen, dessen Aufgabe in der Verbesserung der Strukturen gegen Cyberbedrohungen liegt (vgl. Vitel und Bilddal 2015, S. 3209-10 f.). Der „Cyber-Präfekt“ sollte sicherstellen, dass Polizei und Gendarmerie bestens aufgestellt und abgestimmt sind, um auch Verbrechen im Internet zu bekämpfen (vgl. ebd). Das Innenministerium verstärkte zudem die Zusammenarbeit und den Austausch mit anderen Ministerien innerhalb Frankreichs als auch mit Partner und Verbündeten außerhalb Frankreichs (vgl. Vitel und Bilddal 2015, S. 3209-11).

Im Januar 2015 ereignete sich der Terroranschlag auf die Zeitschrift Charlie Hebdo, auf den zusätzlich zahlreiche Cyberangriffe von Extremisten auf staatliche Websites erfolgte (vgl. Vitel und Bilddal 2015, S. 3209-2 f.). Die Regierung veranlasste daraufhin im Juli ein neues Nachrichtengesetz „Loi relative au renseignement“, welches die Befugnisse der Nachrichtendienste erweiterte und diese bei Terrorverdacht ermächtigte, Personen zu überwachen und die gesammelten Daten für eine bestimmte Zeit zu speichern (vgl. Hathaway et al. 2016, S. 10). Das Gesetz wurde scharf kritisiert,

was besonders an den 434 Änderungsanträgen aus dem Parlament und den 227 Änderungsanträgen aus dem Senat deutlich wurde (vgl. Baumard 2017, 62). Dennoch trat das Gesetz am 24. Juli 2015 in Kraft.

Im Oktober 2015 brachte Manuel Valls, damaliger Premierminister Frankreichs die neue nationale Strategie für digitale Sicherheit „strategie nationalité pour la securite du numerique“ auf den Weg. Dabei ersetzt die neue Strategie größtenteils den Begriff der „Cybersicherheit“, welche in der Strategie von 2011 verwendet wurde durch „digitale Sicherheit“ (vgl. Baezner et al. 2018, S. 12). Sicherheit im Allgemeinen wird allumfassend definiert und beinhaltet sowohl den Schutz der Bevölkerung als auch den des militärischen Sektors (vgl. Baumard 2017, S. 60 ff). Die neue Strategie beschäftigt sich zudem sehr mit der Internetnutzung. Themen wie Datenschutz und Privatsphäre sowie der Kampf gegen Propaganda im Internet werden aufgegriffen (vgl. Baezner et al. 2018, S. 13). Das Innenministerium soll sich daher um die Strafverfolgung im Internet kümmern und beispielsweise eine „nationale Anlaufstelle für Cyberverbrechensopfer“ errichten (vgl. Premier Ministre 2015, S. 21 ff.).

Eine Gesetzesänderung im Jahr 2016 ermöglichte es der ANSSI Meldungen über Schwachstellen bei kritischen Informationssystemen entgegenzunehmen und diese entsprechend weiterzuleiten (vgl. ANSSI 2022a).
Zudem führte die ANSSI unter Beteiligung von Unternehmen, Verbänden, Universitäten und dem Bildungsministerium ein neues Label ein, welches Studiengänge zertifiziert, die essenzielle Kernpunkte der Cybersicherheit in ihren Modulen enthalten (vgl. ANSSI 2022g).

Um die Cyberkapazitäten des Verteidigungsministeriums zu bündeln gab im Dezember 2016 der französische Verteidigungsminister Jean-Yves Le Drian das Vorhaben für die Errichtung eines Cyber-Kommandos der Streitkräfte für Frankreich bekannt (vgl. Guibert 2016).
Im Mai 2017 wurde daraufhin das „Le commandement de la cyberdéfense“ (COMCYBER) gegründet. Im Cyber-Kommando COMCYBER sind alle Cyberabwehreinheiten der französischen Streitkräfte vereint (vgl. Baezner et al. 2018, 16). Das Cyber-Kommando umfasste nach Errichtung rund 2600 Mitarbeiter (vgl. ebd). Das COMCYBER ist für sämtliche militärische Cyberoperation zuständig (vgl. ebd).

Unterstützt wird es dabei vom Analysezentrum des Verteidigungsministerium CALID, das COMCYBER im Bereich der Cyber-Risiko Bewertung Informationen liefert (vgl. Laudrain 2019a, S. 25 f.).

Während der Präsidentschaftswahl zwischen dem 23. April und dem 7. Mai 2017 wurde Frankreich die Gefahr von ausländischer Einmischung vor Augen geführt. Zwei Tage vor der Wahl wurden gestohlene Dokumente aus dem Wahlkampf von Emmanuel Macron veröffentlicht (vgl. Toucas 2017).

Im Oktober 2017 veröffentlichte das SGDSN ein Papier zur Strategischen Überprüfung der Verteidigung und der nationalen Sicherheit. In diesem wird die Trennlinie zwischen offensiven und defensiven Cyberoperationen in der französischen Cyberverteidigung verdeutlicht (vgl. Laudrain 2019a, S. 7 f.). So wird zwischen den Behörden unterschieden, welche zum Schutz und zur Verteidigung defensive Cyberoperationen durchführen und denen welche nachrichtendienstliche oder offensive Cyberoperationen durchführen (vgl. Delerue und Géry 2018). Demnach sind ANSSI und COMCYBER für defensive Cyberoperationen in ihren jeweiligen Bereichen, dem nicht-militärischen, bzw. dem militärischen Bereich zuständig (vgl. Laudrain 2019a, S. 25 f.). Die Trennung betrifft auch den französischen Auslandsnachrichtendienst DGSE, der ebenfalls eigenständig operiert (vgl. Liebetrau 2022, S. 9). Obwohl diese drei Institutionen für sich genommen eigenständig arbeiten, unterstützt sowohl COMCYBER (vgl. Laudrain 2019a, S. 25 f.) , als auch die DGSE die ANSSI bei defensiven Cyberoperationen (vgl. Liebetrau 2022, S. 9 f.).

Das Frankreich neben defensiven auch über offensive Cyber-Kriegsfähigkeiten verfügt machte die französische Verteidigungsministerin Florence Parly im Januar 2019 bei der Vorstellung der neuen Doktrin für offensive und defensive Cyberoperationen erstmals publik (vgl. Laudrain 2019a, S. 11). Sie machte zudem deutlich, dass Frankreich „keine Angst“ vor dem Gebrauch ihrer offensiven Cyberfähigkeiten habe (vgl. Laudrain 2019a, S. 11). Welche Institutionen über offensive Cyber-Kriegsfähigkeiten verfügen ist offiziell nicht bekannt jedoch lässt sich vermuten, dass sowohl das COMCYBER als auch die DGSE in der Lage sind offensive Cyberoperationen durchzuführen (vgl. Liebetrau 2022, S. 11).

Das neue Militärplanungsgesetz für den Zeitraum 2019-2025 sieht 1,6 Milliarden Euro für Cyber-Operationen und Personal vor (vgl. Laudrain 2019b). Daneben erweiterte das Militärplanungsgesetz die Befugnisse der ANSSI. Bislang hatte die ANSSI keine Legitimität für die Überwachung der Informationssysteme der Ministerien, da diese für ihre eigene Sicherheit verantwortlich sind (vgl. Sénat 2021). Allerdings wurde der ANSSI durch das Gesetz gestattet bei Feststellung einer Bedrohung der Systeme, Netzwerksonden zu installieren, welche die Netzwerke überwachen und eine bessere Reaktion ermöglichen (vgl. ANSSI 2022b).
Diese Befugnis gilt für die Ministerien und Behörden, als auch für die öffentlichen und privaten Betreiber kritischer Infrastrukturen (vgl. ANSSI 2022b).

Für die Zukunft investiert Frankreich weiterhin in seine Cybersicherheit. So soll die Bretagne ein Budget von 130 Millionen Euro bis 2025 bereitgestellt bekommen, um die dortige Cyberindustrie weiter zu unterstützen (vgl. Calcara und Marchetti 2021, S. 11). Die Bereiche künstliche Intelligenz, Megadaten, Nanotechnologie und Cybersicherheit werden von der Regierung mit rund 5 Milliarden im Zeitraum von 2018 – 2022 gefördert (vgl. Calcara und Marchetti 2021, S. 9). Am 15 Februar 2022 wurde ein zukunftweisendes Projekt im Bereich der Cybersicherheit eröffnet. Der „Cyber Campus“ in Paris soll Akteure der französischen Cybersicherheit an einem Ort vereinen. So sollen sich Unternehmen, Start-ups und Forschungszentren dort ansiedeln und sich dort austauschen können (vgl. ANSSI 2022e).Durch den persönlichen Kontakt soll Vertrauen geschaffen werden, um einen gemeinsamen Datenaustausch zu fördern und Wissen zu vermitteln (vgl.ANSSI 2022e). Zudem sollen Aus- und Weiterbildungsprogramme für staatliches Personal auf dem Campus stattfinden (vgl.ANSSI 2022e). Die ANSSI hat bereits ihre Beteiligung an dem Projekt angekündigt (vgl.ANSSI 2022e).

4.2 Einordnung Frankreichs in die Taxonomie

Koordinierung der Cyber-Sicherheitspolitik
Für die Koordinierung der Cyber-Sicherheitspolitik ist in Frankreich offiziell seit Inkrafttreten des Militärplanungsgesetz der Premierminister zuständig. Allerdings ist dies eher symbolisch, da die Gesetzesentwürfe von der SGDSN erarbeitet und dem Premierminister anschließend vorgelegt werden. Auch die Umsetzung koordiniert das

SGDSN mit Hilfe der ANSSI. Die ANSSI legt die Sicherheitsmaßnahmen fest und kontrolliert deren Einhaltung. Bei Verstößen kann die ANSSI Bußgelder verhängen. Die ANSSI führt auch Zertifizierungen von IT-Produkten durch und vergibt das Siegel „FRANCE CYBER SECURITY“. Die Koordinierung der Cyber-Sicherheitspolitik ist somit Aufgabe des SGDSN.

Koordinierung des allgemeines Krisenmanagement

Die Bewältigung von Krisen in Frankreich ist Aufgabe der „cellule interministérielle de crise“ (CIC), einer Interministeriellen Kriseneinheit. Diese wird vom SGDSN auf Anordnung des Premierministers einberufen und setzt sich in der Regel aus dem Innenminister und dem Minister für auswärtige Angelegenheiten zusammen. Je nach Art der Krise kann der Premierminister die Bewältigung der Krise auf einen der beiden Minister oder einen beliebigen Minister delegieren. Die Koordinierung des allgemeinen Krisenmanagements kann somit Aufgabe des Innenministerium oder das Ministerium für Europa und auswärtige Angelegenheiten sein. Das Cyber-Krisenmanagement liegt jedoch im Aufgabenbereich der ANSSI. Im Vorfeld analysiert und bewertet diese Cyberbedrohungen und leitet diese an die Akteure weiter. Während eines Cyberangriffs verfügt die ANSSI über die entsprechenden Kapazitäten und Informationen um Hilfe leisten zu können. Dabei informiert die ANSSI auch andere Akteure über den Angriff und warnt diese entsprechend.

Die wichtigsten öffentlichen CERTs

Ein wichtiges öffentliches CERT ist das CERT-FR, welches in der ANSSI angesiedelt ist. Es leistet Hilfe nach Cyberangriffen, gibt Sicherheitswarnungen sowie Sicherheitshinweise heraus und veröffentlicht Berichte über Bedrohungen und Vorfälle. Neben dem zivilen CERT-FR besitzt das französische Militär mit CALID ein eigenes CERT das die Netzwerke des Militärs überwacht und schützt.

Cyberkapazitäten der Regierung

Frankreichs Cyberkapazitäten sind eher „verteilt“ als zentralisiert. Jeder Bereich hat seine eigenen Kapazitäten aufgebaut. Die ANSSI kümmert sich im Rahmen seiner Kapazitäten um den öffentlichen und privaten Sektor und kann dabei auf die Hilfe, der ihr unterstellten, COSSI, CERT-FR und CTG zurückgreifen. Das

Verteidigungsministerium hat für die Überwachung und den Schutz seiner Netze das COMCYBER. Innerhalb des COMCYBER ist das Analysezentrum CALID angesiedelt. Hinzu kommt als dritte Institution der Auslandsnachrichtendienst DGSE der ebenfalls Cyberkapazitäten besitzt. Auch die Regierungsnetzwerke werden von den Ministerien selbst überwacht, wofür es Kapazitäten braucht.

Überwachung der Regierungsnetzwerke

Für die Sicherheit der Regierungsnetzwerke sind die Ministerien selbst verantwortlich.

Einbindung der Geheimdienste

Das CERT-FR ist nicht innerhalb der französischen Geheimdienste bzw. Nachrichtendienste angesiedelt, sondern untersteht der ANSSI. Frankreichs größter Nachrichtendienst die DGSE ist außerhalb der ANSSI und außerhalb des COMCYBER angesiedelt und operiert unabhängig.

Netzwerkmodel

Die ANSSI ist ein wichtiger zentraler staatlicher Akteur in Frankreich im Bereich der Cybersicherheit, welcher über viele Cyberkapazitäten und Informationen verfügt. Dabei wird die ANSSI sowohl von Seiten des Militärs als auch von Seiten des Nachrichtendienstes unterstützt und erhält so viele Informationen. Die ANSSI ist damit der wichtigste Ansprechpartner für die öffentlichen und privaten Akteure. Trotz dieser Stellung ist die ANSSI sehr um Kooperationen und Partnerschaften mit den Akteuren bemüht. Ein Beispiel ist die von der ANSSI gegründete Arbeitsgruppe, bei der öffentliche und private Betreiber kritischer Infrastrukturen freiwillig an der Ausarbeitung von Sicherheitsregeln teilnehmen konnten. Ebenso das Label für Studiengänge mit Bezug zur Cybersicherheit hat die ANSSI gemeinsam mit öffentlichen und privaten Akteuren ins Leben gerufen und dabei die Verbindung zwischen den Akteuren hergestellt. Selbst wenn man davon absieht, dass die ANSSI nicht der einzige zentrale staatliche Akteur ist, welcher alle Informationen und Kapazitäten bündelt, so ist das Netzwerkmodell der “Lead organization” durch die Bereitschaft der ANSSI für Kooperationen und Partnerschaften eher auszuschließen. Inwieweit die Zusammenarbeit auf Konsens und Gleichberechtigung basiert ist nicht bekannt, allerdings tendieren die Kontroll- und Sanktionsbefugnisse eher zu einer stärkeren Rolle der ANSSI. Es ist generell wahrscheinlicher anzunehmen, dass die Beteiligungen

und Investitionen in die Projekte das angesprochene Ziel verfolgen, Frankreich zu einer Weltmacht in der Cyberverteidigung werden zu lassen. Daher lässt sich bezweifeln, dass die Behörden dabei Kontrolle abgeben und eine Zusammenarbeit anstreben, welche nur auf Basis von Konsens und Gleichberechtigung beruht. Demnach ist das Netzwerkmodell der “Network-administrative” am wahrscheinlichsten.
Nach der Einordnung in die Taxonomie ergibt sich folgende Darstellung.

	Frankreich
Koordinierung der Cyber-Sicherheitspolitik	SGDSN
Koordinierung allgemeines Krisenmanagement	Ministère de l’intérieur, Ministère de l’Europe et des Affaires étrangères
Die wichtigsten öffentlichen CERTs	CERT-FR, CALID
Cyberkapazitäten der Regierung	verteilt
Überwachung der Regierungsnetzwerke	Ministerien haben eigene Verantwortung
Einbindung der Geheimdienste	außerhalb
Netzwerkmodell	Network-administrative

„Tabelle 3: Eigene Darstellung der Cyber-Governance-Struktur Frankreichs in Anlehnung an Boeke (2018)“

5. Vergleich der Cyber-Governance-Struktur

Stellt man beide Länder in der Taxonomie gegenüber ergibt sich folgende Tabelle

	Deutschland	Frankreich
Koordinierung der Cyber-Sicherheitspolitik	BMI	SGDSN
Koordinierung allgemeines Krisenmanagement	BMI	Ministère de l'intérieur, Ministère de l'Europe et des Affaires étrangères
Die wichtigsten öffentlichen CERTs	CERT-BUND, Zentrum für Cyber-Sicherheit der Bundeswehr	CERT-FR, CALID
Cyberkapazitäten der Regierung	verteilt	verteilt
Überwachung der Regierungsnetzwerke	Ministerien haben eigene Verantwortung	Ministerien haben eigene Verantwortung
Einbindung der Geheimdienste	außerhalb	außerhalb
Netzwerkmodell	Network-administrative	Network-administrative

„Tabelle 4: Eigene Darstellung der Cyber-Governance-Struktur von Deutschland und Frankreich in Anlehnung an Boeke (2018)"

Die Gegenüberstellung der Taxonomie der Cyber-Governance-Struktur beider Länder zeigt die besondere Rolle des BMI. Das BMI ist sowohl für die Koordinierung der Cyber-Sicherheitspolitik als auch für die Koordinierung des allgemeinen Krisenmanagements zuständig. Das BSI, welches dem BMI untersteht ist die nationale Cybersicherheitsbehörde und beheimatet das CERT-BUND, welches wichtige Unterstützung bei Cyberangriffen leistet. Deutschland hat damit viele Aufgaben und Kapazitäten in sein Innenministerium zentralisiert. In Frankreich dagegen verteilen sich die Aufgabenbereiche der Cyber-Sicherheitspolitik und des Krisenmanagements auf 3

Behörden, darunter das Innenministerium, dass sich die Koordination des allgemeinen Krisenmanagements mit dem Außenministerium teilt. Die Rolle des Innenministeriums ist in Frankreich daher nicht ganz so bedeutend wie in Deutschland. Frankreich hat seine nationale Cybersicherheitsbehörde die ANSSI nicht innerhalb des Innenministeriums eingebettet, sondern im Generalsekretariat für Verteidigung und nationale Sicherheit, das dem Premierminister unterstellt ist. Trotz der unterschiedlichen Verortung von ANSSI und BSI gibt es Ähnlichkeiten zwischen den beiden Behörden. So sind beide Behörden für das Cyber-Krisenmanagement in ihren Ländern zuständig und helfen in Notfällen den dort öffentlichen und privaten Akteuren. Allerdings lässt sich anhand der historischen Rekonstruktion sehen, dass beide Behörden anfangs hauptsächlich für den technischen Schutz der Regierungsnetzwerke zuständig und beratend bei technischen Schutzmaßnahmen waren. Erst mit der Zeit erlangten beide Behörden mehr Aufgaben und Befugnisse.

Bei der ANSSI war es vor allem das „CIIP-Gesetz“ und das Militärplanungsgesetz im Jahr 2013, welche die ANSSI maßgeblich mit Kontroll- und Sanktionsbefugnissen ausstattete und diese zu einem wichtigen zentralen staatlichen Akteur im Bereich der Cybersicherheit machte. Beim BSI waren es die IT-Sicherheitsgesetze von 2015 und 2021. In beiden Ländern sind die öffentlichen und privaten Akteure verpflichtet worden der ANSSI und dem BSI Meldung über Sicherheitsvorfälle zu machen, welche diese dann bewerten, analysieren und die Informationen entsprechend weiterleiten. Jedoch gibt es Unterschiede in der Zusammenarbeit mit anderen Behörden. Die ANSSI kann zur Unterstützung auf das COMCYBER des Militärs und auf den Auslandsnachrichtendienst DGSE zurückgreifen. Das BSI dagegen kann offiziell nicht auf die Unterstützung von Militär und Nachrichtendienst zurückgreifen.

Das BSI, die ANSSI und die jeweiligen CERTs nicht zu stark mit dem BND bzw. DGSE zu verknüpfen und diese außerhalb der nationalen Cybersicherheitsbehörden zu lassen kann als Reaktion auf den Vertrauensverlust nach Veröffentlichungen der Snowden Dokumente gewertet werden. Dennoch haben beide Länder ihre Nachrichtendienste von der Gesetzgebung gestärkt und die Befugnisse erweitert. Beide Länder taten dies nicht unmittelbar nach den Enthüllungen der Snowden Dokumente, sondern warteten damit bis 2015 bzw. 2016. In beiden Ländern ist dies geschehen trotz großer Kritik innerhalb der Gesellschaft. Speziell am Beispiel in

Deutschland lässt sicher erkennen, dass die Regierung durch das BND-Gesetz die Praktiken, die zum Zeitpunkt der Enthüllungen nach deutschem Gesetz illegal waren, legalisiert hat. Zwar kippte das Bundesverfassungsgericht das BND-Gesetz doch die Regierung ließ von diesem Vorhaben nicht ab und verabschiedete erneut ein Gesetz zur Stärkung des BND. Daraus lässt sich vermuten, dass die Arbeit der Nachrichtendienste besondere Wichtigkeit in Bezug auf die Cybersicherheit haben. Dennoch scheint die Angst vor Vertrauensverlust durch die Einbindung der Nachrichtendienste zu groß zu sein. Die FDP in Deutschland geht sogar noch weiter. In ihrem Wahlprogramm zur Bundestagswahl 2021 verspricht sie, das BSI vom BMI zu lösen und begründet dies damit, dass durch die Zugehörigkeit des BSI's zum BMI, Unternehmen ihre Sicherheitslücken nicht an das BSI melden, aus Angst, ihre Sicherheitslücken würden vom BMI zur Überwachung und Online-Durchsuchung verwendet (vgl. FDP 2021).

Dass die Zusammenarbeit mit den öffentlichen und privaten Akteuren in Deutschland unbefriedigend zu sein scheint, lässt sich aus der historischen Rekonstruktion ableiten. Bis 2015 beruhten Meldungen und Umsetzung von Sicherheitsmaßnahmen auf Freiwilligkeit bzw. auf freiwilliger Selbstverpflichtung. Mit dem IT-Sicherheitsgesetz von 2015 wurden die Akteure per Gesetz verpflichtet. Zudem wurden Kontrollen eingeführt und bei Missachtung der Pflichten Bußgelder verhängt. Belief sich die Geldbuße im Gesetz von 2015 noch zwischen fünfzig- und hunderttausend Euro, so waren die Bußgelder mit dem zweiten IT-Sicherheitsgesetz auf zwischen einhunderttausend und zwei Millionen Euro angehoben worden. Zudem wurde das zweite IT-Sicherheitsgesetz vom BMI im Alleingang entworfen und den Akteuren dabei nur einen Tag für eine Stellungnahme Zeit gelassen.
In Frankreich scheint die Zusammenarbeit besser zu sein. Zwar führt die ANSSI ebenfalls Kontrollen durch und kann Bußgelder verhängen allerdings setzt die ANSSI auf freiwillige Zusammenarbeit. Sie steht in engem Austausch mit den jeweiligen Akteuren und bindet diese in Prozesse und Projekte mit ein. Zwar sind Deutschland und Frankreich dem Netzwerkmodel der "Network-administrative" am nächsten, jedoch bewegt Frankreich sich derzeit in Richtung eines „Participant governed".
Dennoch stärkt Frankreich weiterhin seine Behörden. Beide Länder haben im Untersuchungszeitraum viel in ihre Cybersicherheitsbehörden investiert. Sowohl das Budget als auch das Personal stieg über die Jahre an. Allerdings lässt sich daraus

nicht auf die Qualität der Cybersicherheit schließen. Die Anzahl des Personals der beiden Behörden sind zwar zugänglich, jedoch lässt sich nicht sagen, welche Art von Fachkräften in den Behörden tätig sind. Es ist keine Auskunft darüber möglich, ob es sich um Informatiker, Kryptographen oder um normale Beamte ohne Bezug zur Informatik oder Cybersicherheit handelt. Ein Interview von Dominika Zedler mit dem BKA machte dies deutlich. Das BKA beschäftigte zum Zeitpunkt des Interviews 120 Mitarbeiter im Cybersicherheitsbereich von denen nur 8 einen Bachelorabschluss in Informatik besaßen (vgl. Zedler 2017, S. 73 f.). Daher könnte man einem Trugschluss erliegen, bewerte man die Qualität der Cybersicherheit an der Höhe des Budgets und des Personals. Jedoch ging aus dem Interview ein Problem hervor, dass sowohl Deutschland als auch Frankreich betrifft. Der Bedarf an qualifizierten Informatikern in der Wirtschaft ist hoch und gleichzeitig die Verfügbarkeit an Informatikern gering (vgl. Merat 2022; vgl. Specht 2022).Somit ist es für die Behörden schwierig Personal zu gewinnen, zumal das Personalbudget zu gering ist, als dass die Behörden in Bezug auf das Salär mit der freien Wirtschaft konkurrieren könnten (vgl. Zedler 2017, S. 71). In Deutschland ist diese Problematik noch ein wenig größer zu bewerten als in Frankreich.

Wie aus Kapitel 3 hervor geht, gibt es neben den Behörden auf Bundesebene auch auf Länderebene Behörden, die für Cybersicherheit zuständig sind. Ein Beispiel hierfür ist das Cyber-Allianz-Zentrum Bayern (CAZ), das im Jahr 2013 vom Bayrischen Landesamt für Verfassungsschutz errichtet wurde und als Aufgabe hat, in Bayern ansässige Unternehmen, Hochschulen und Betreiber kritischer Infrastruktur vor Cyberangriffen zu unterstützen (vgl. Bayerisches Landesamt für Verfassungsschutz 2022). Die Unterstützung reicht von Beratung, Prävention bis hin zur Abwehr von Cyberangriffen (Bayerisches Landesamt für Verfassungsschutz 2022). Das Aufgabenfeld ähnelt damit stark dem des BSI. Somit konkurrieren in Deutschland zusätzlich Behörden des Bundes und der Länder um Fachkräfte aus dem IT-Bereich. Frankreich wirkt dem Problem durch große Investitionen und Projekte entgegen. Der „Cyber Campus“ in Paris oder das Exzellenz-Zentrum für Cyberverteidigung in der Bretagne welches vom Verteidigungsministerium gegründet wurde sind Beispiele wie Frankreich dem Personalmangel im IT-Sicherheitsbereich bewältigen möchte. Das französische Verteidigungsministerium investiert seit 2014 in seine Cybersicherheit. Daher hat die französische Armee auch eine starke Rolle in diesem Bereich eingenommen und unterstützt die ANSSI bei Cyber-Operationen. Die Verflechtung und

Zusammenarbeit des Verteidigungsministeriums mit der ANSSI wird auch durch die Unterbringung von CALID und COSSI im gleichen Gebäude deutlich. Die Bundeswehr dagegen hat erst 2016 begonnen sich dem Thema der Cybersicherheit stärker zu widmen. Allerdings beschränkt sich die Cybersicherheit der Bundeswehr auf die eigenen Netzwerke und Systeme, wofür die Bundeswehr entsprechend Kapazitäten aufgebaut hat. Vergleicht man die Rolle des Militärs beider Länder im Cyberbereich so fällt auf, dass die Bundeswehr eine weniger starke Stellung hat als die französische Armee besitzt. Ein Grund hierfür könnte sein, dass die Bundeswehr eine reine Verteidigungsarmee ist und per Gesetz nur die eignen Systeme schützen darf (vgl. Schallbruch und Skierka 2018, S. 36 f.).
Nur in Ausnahmefällen wie beispielweise bei Ersuchen von Amtshilfe einer Behörde, darf die Bundeswehr unterstützen (vgl. ebd). Das die Verteidigungsministerien beider Länder in der Taxonomie nur unter „Die wichtigsten öffentlichen CERTs“ vertreten sind und diese CERTs in erster Linie dem Schutz der eigenen Netzwerke dienen zeigt, dass die Cyber-Governance in beiden Ländern unter ziviler Führung stattfindet. Gerade in Frankreich, wo die Cyberkapazitäten und -Fähigkeiten der Armee recht groß zu sein scheinen, leistet dieses nur Unterstützung bei Aufforderung.

6. Fazit

Zielsetzung dieser Arbeit war es, zu untersuchen, wie Deutschland und Frankreich ihre Cyber-Governance-Struktur aufgebaut haben. Hierfür wurde die Taxonomie von Boeke verwendet, welche Cyber-Governance-Strukturen kategorisierbar und für Untersuchungen zugänglich macht. Die Taxonomie wurde dafür erläutert. Anschließend wurde zuerst für Deutschland und dann für Frankreich die Cyber-Governance-Strukturen analysiert, ehe diese miteinander verglichen wurden.
Beim Vergleich und der Einordnung war zu sehen, dass die Kategorisierung beider Länder keine Eindeutigkeit ihrer Cyber-Governance-Strukturen hervorbrachte. Dies betrifft vor allem das Attribut des „Netzwerkmodells“. So musste in dieser Arbeit bei der Einordnung abgewogen werden, zu welchem Netzwerkmodell Deutschland und Frankreich gehören, da beide Länder Merkmale unterschiedliche Netzwerkmodell-Ausprägungen aufweisen. Insbesondere bei Frankreich war dies komplex, da Frankreich stark in Richtung „Participant governed“ tendiert. Boeke wies, wie in Kapitel

2.2 beschrieben darauf hin, dass sich die Länder nicht eindeutig kategorisieren lassen, allerdings ließ Boeke offene Fragen bezüglich der Gewichtung der Befunde. Es fehlte eine genaue Erläuterung für die Einordnung der Staaten in das Netzwerkmodell. Ab wann ein Staat dem „Participant governed“, der „Lead organization“ oder der „Network-administrative“ zugeordnet wird, wurde in dieser Arbeit durch Untersuchung der Länderfallbeispiele und den daraus resultierenden Unterschieden bzw. Gemeinsamkeiten abgeleitet. Daher musste die Operationalisierung der Taxonomie von Boeke größtenteils aus den Fallbeispielen der Studie abgleitet werden, da diese im Vorfeld seiner Arbeit nicht klar definiert wurden. Beispielsweise wurde nicht definiert, ab wann die Cyberkapazitäten der Regierung „Zentralisiert“ sind und ab wann diese als „Verteilt“ gelten. So wurde aus dem Fallbeispiel Dänemark abgleitet, dass die Cyberkapazitäten zentralisiert sind, wenn ein Ministerium sämtliche Kapazitäten im Cyberbereich in sich vereint, was am Beispiel des dänischen Verteidigungsministeriums deutlich wurde. Sobald jedoch eine Cyberkapazität in einem anderen Ministerium angesiedelt wurde, sind die Cyberkapazitäten der Regierung als verteilt einzuordnen, was am Fallbeispiel der Tschechischen Republik zu sehen war.

Ein anderes Problem dieser Arbeit war der Literaturstand. Die Einordnungen in die Taxonomie stützen sich auf die ausgewerteten Literaturteile. Die Auswahl an Literatur zur Cyber-Governance beider Länder nahm mit dem Jahr 2018 stark ab, sodass auf wenige Internetdokumente zugegriffen werden musste. Dies machte es schwierig, die Cyber-Governance der Länder weiter zu verfolgen. Jedoch ist anzunehmen, dass es Maßnahmen und Veränderungen gegeben haben muss, da die Anzahl an Cyberangriffen insbesondere auf kritische Infrastrukturen in der Pandemie zugenommen haben.

Der Mangel an Fachliteratur ist ein bekanntes Problem, welches Boeke in seiner Arbeit ebenfalls thematisierte. Er beschreibt eine Zurückhaltung und Geheimhaltung von Informationen durch Regierungen und Unternehmen, welche die Datenlage für die Cybersicherheitsforschung einschränkt (vgl. Boeke 2018, S. 452). Er selbst konnte dieses Problem durch anonyme Interviews mit Beamten aus den nationalen Cybersicherheitszentren und der Nachrichtendienstgemeinschaft umgehen (vgl. ebd). Es lässt sich vermuten, dass die Zurückhaltung und Geheimhaltung von Informationen unter dem Aspekt der Cybersicherheit stattfinden, um die Angreifbarkeit zu verringern. Denn die Analyse der Cyber-Governance-Struktur liefert, wie sich gezeigt hat Wissen

über die Verfahrensweisen der Länder in Bezug auf ihre Cybersicherheit. Daher könnten sich Schwachstellen ausfindig machen lassen. Speziell vor dem Hintergrund der Pandemie ließe sich dieses Verhalten damit erklären.Dennoch konnte sich diese Arbeit der Fragestellung widmen und die Cyber-Governance-Strukturen offenlegen. So zeigte sich, dass beide Länder ihre nationale Cybersicherheitsbehörde zu einem zentralen Akteur in der Cybersicherheit aufgebaut haben. Die auferlegten Aufgaben beider Behörden sind identisch, lediglich die rechtlichen Befugnisse weichen leicht voneinander ab. Beide Länder haben ihr Militär nicht stark in ihre Cyber-Governance-Struktur eingebunden und die Cybersicherheit zivilen Behörden überlassen. Auch die Geheim- bzw. Nachrichtendienste sind kaum eingebunden und die CERTs dort nicht angesiedelt. Jedoch wurden beiden Nachrichtendiensten per Gesetz mehr Befugnisse gewährt und dass trotz großer Kritik innerhalb der Länder. Boeke beschrieb in seiner Arbeit, dass die Einbindung der CERTs innerhalb der Geheimdienste mehr Daten und Informationen mit sich bringt, allerdings rechtliche, politische und ethische Auswirkungen haben. Es lässt sich vermuten, dass Frankreich und Deutschland die Befugniserweiterung ihrer Nachrichtendienste als Mittelweg angesehen haben. Beide Länder haben sich ebenfalls dazu entschieden die Überwachung der Regierungsnetzwerke den Ministerien zu überlassen. So sind auch die Cyberkapazitäten der Regierung verteilt.

Beide Länder folgen dem gleichen Netzwerkmodell, jedoch wurden Unterschiede festgestellt die Fragen aufwerfen.

In Deutschland, wo Ressortprinzip und Föderalismus die Zusammenarbeit der Akteure unübersichtlich macht und dadurch erschwert, muss sich die Frage gestellt werden, wie in Zukunft damit verfahren werden soll. Das betrifft auch die angesprochene Problematik um Fachkräfte aus dem IT-Bereich für die Behörden. Martin Schallbruch, ehemaliger Abteilungsleiter für Informationstechnik im BMI, äußerte sich über seine Zeit als Staatsbeamter kritisch zur Aus- und Fortbildung von Staatsbeamten im Bereich der Digitalisierung und dem Erschweren von Wechseln in die freie Wirtschaft, obwohl sich das Berufsverhalten von Menschen geändert hat (vgl.Schallbruch 2018, S. 247 f.). Zudem sind die Wechsel zwischen Staat und Wirtschaft nicht gern gesehen. Während in anderen Ländern wie in Frankreich dies die Normalität sei (vgl. ebd). Das Verhältnis von Privatwirtschaft und Staat in Frankreich scheint befreiter zu sein und die Bereitschaft zur Kooperation größer. Ein weiteres Argument dafür wäre der Cyber

Campus in Paris an dem sich die privaten Akteure mit 50% beteiligt haben (ANSSI 2022e).

Diese Tatsachen bekräftigen die im Vergleich beschriebene Aussage, dass Deutschland und Frankreich dem Netzwerkmodell der "Network-administrative am nahesten stehen, obwohl Frankreich eher in Richtung eines “Participant governed” als Deutschland tendiert. Frankreich hat einige Projekte veranlasst und kann hinsichtlich der Zusammenarbeit mit den anderen Akteuren als Vorbild für Deutschland dienen.

Damit konnte unter Berücksichtigung und Erweiterung des Boekeschen Modells gezeigt werden, wie Deutschland und Frankreich ihre Cyber-Governance-Struktur organisiert haben.

Zudem konnten die Definitionen der Attribute und Ausprägungen präzisiert werden, wodurch die Taxonomie für weitere Forschung im Cyber-Sicherheitsdiskurs verwendbar und ergänzbar wird.

7.Literaturverzeichnis

Agence Nationale de la Sécurité des Systèmes d'Information (2011): Verteidigung und Sicherheit der Informationssysteme Frankreichs Strategie. Online verfügbar unter https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Verteidigung_und_Sicherheit_der_Informationssysteme_-_Frankreichs_strategie.pdf.

ANSSI (2022a): Alertes aux vulnérabilités et failles de sécurité. Online verfügbar unter https://www.ssi.gouv.fr/en-cas-dincident/vous-souhaitez-declarer-une-faille-de-securite-ou-une-vulnerabilite/, zuletzt aktualisiert am 05.01.2022, zuletzt geprüft am 30.06.2022.

ANSSI (2022b): LPM 2019 – 2025 : la publication du décret d'application de l'article 34 renforce les missions de l'ANSSI. Online verfügbar unter https://www.ssi.gouv.fr/actualite/lpm-2019-2025-la-publication-du-decret-dapplication-de-larticle-34-renforce-les-missions-de-lanssi/, zuletzt aktualisiert am 05.01.2022, zuletzt geprüft am 30.06.2022.

ANSSI (2022c): Foire aux questions. Online verfügbar unter https://www.ssi.gouv.fr/administration/protection-des-oiv/foire-aux-questions/, zuletzt aktualisiert am 17.02.2022, zuletzt geprüft am 30.06.2022.

ANSSI (2022d): Plans gouvernementaux. Online verfügbar unter https://www.ssi.gouv.fr/agence/cybersecurite/plans-gouvernementaux/, zuletzt aktualisiert am 11.05.2022, zuletzt geprüft am 30.06.2022.

ANSSI (2022e): Un Campus dédié à la cybersécurité. Online verfügbar unter https://www.ssi.gouv.fr/agence/cybersecurite/un-campus-dedie-a-la-cybersecurite/, zuletzt aktualisiert am 11.05.2022, zuletzt geprüft am 30.06.2022.

ANSSI (2022f): FAQ. Online verfügbar unter https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/faq/#2-3, zuletzt aktualisiert am 19.05.2022, zuletzt geprüft am 30.06.2022.

ANSSI (2022g): SecNumedu, Labeling of higher education courses in cybersecurity. Online verfügbar unter https://www.ssi.gouv.fr/en/cybersecurity-in-

france/formations/secnumedu-labeling-of-higher-education-courses-in-cybersecurity/, zuletzt aktualisiert am 19.05.2022, zuletzt geprüft am 30.06.2022.

ANSSI (2022h): The French CIIP Framework. Online verfügbar unter https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/, zuletzt aktualisiert am 19.05.2022, zuletzt geprüft am 30.06.2022.

Astrid Bötticher (2014): Die Strukturlandschaft der Inneren Sicherheit der Bundesrepublik Deutschland. In: Hans-Jürgen Lange und Astrid Bötticher (Hg.): Cyber-Sicherheit. 1. Aufl. s.l.: Springer VS (Studien zur Inneren Sicherheit, v.18), S. 69–102.

ASW Bundesverband (2020): Positionspapier Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0). ALLIANZ FÜR SICHERHEIT IN DER WIRTSCHAFT E.V. Online verfügbar unter https://www.aswwest.de/fileadmin/images/ASW_20201210_-_IT-SiGe_2.0_-_Positionspapier.pdf, zuletzt geprüft am 22.06.2022.

Baezner, Marie; Dewar, Robert S.; Cordey, Sean; Robin, Patrice (2018): National Cybersecurity and Cyberdefense Policy Snapshots. ETH Zürich. Online verfügbar unter https://css.ethz.ch/en/services/digital-library/publications/publication.html/0689441d-67a0-4476-8b36-b6f7f964545c, zuletzt geprüft am 30.06.2022.

Baumard, Philippe (2017): Cybersecurity in France. Cham: Springer International Publishing.

Bayerisches Landesamt für Verfassungsschutz (2022): Cyber-Allianz-Zentrum Bayern (CAZ). Online verfügbar unter https://www.verfassungsschutz.bayern.de/spionageabwehr/cyber_allianz_zentrum/, zuletzt aktualisiert am 30.06.2022, zuletzt geprüft am 30.06.2022.

BBK (2022a): Krisenmanagement. Online verfügbar unter https://www.bbk.bund.de/DE/Themen/Krisenmanagement/krisenmanagement_node.html, zuletzt aktualisiert am 26.06.2022, zuletzt geprüft am 26.06.2022.

BBK (2022b): Risikomanagement. Online verfügbar unter https://www.bbk.bund.de/DE/Themen/Risikomanagement/risikomanagement_node.html, zuletzt aktualisiert am 26.06.2022, zuletzt geprüft am 26.06.2022.

BMI (2017a): Bundes-amt für Bevölkerungs-schutz und Katastrophen-hilfe. Online verfügbar unter https://www.bmi.bund.de/SharedDocs/behoerden/DE/bbk.html, zuletzt aktualisiert am 25.09.2017, zuletzt geprüft am 26.06.2022.

BMI (2017b): Wer macht was beim Zivil- und Katastrophenschutz? Online verfügbar unter https://www.bmi.bund.de/DE/themen/bevoelkerungsschutz/zivil-und-katastrophenschutz/gefahrenabwehr-und-katastrophenschutz/gefahrenabwehr-und-katastrophenschutz-node.html, zuletzt aktualisiert am 25.09.2017, zuletzt geprüft am 26.06.2022.

Boeke, Sergei (2016): First responder or last resort? The role of the ministry of defence in national cyber crisis management in four European countries. Online verfügbar unter https://scholarlypublications.universiteitleiden.nl/access/item%3a2887288/view.

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

Brangetto, Pascal (2015): National Cyber Security Organisation: France. Tallin. Online verfügbar unter https://ccdcoe.org/library/publications/national-cyber-security-organisation-france/.

BSI (2021): IT-Krisenreaktionszentrum - Das Nationale IT-Krisenreaktionszentrum im BSI. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/IT-Krisenreaktionszentrum/itkrisenreaktionszentrum.html, zuletzt aktualisiert am 09.12.2021, zuletzt geprüft am 26.06.2022.

Bundesamt für Sicherheit in der Informationstechnik (2021): Allianz für Cyber-Sicherheit - ACS. Häufige Fragen zur Allianz für Cyber-Sicherheit. Online verfügbar unter https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/home_node.html, zuletzt aktualisiert am 08.03.2021, zuletzt geprüft am 29.06.2022.

Bundeskriminalamt (2021): Bundeslagebild Cybercrime 2020. Bundeskriminalamt. Wiesbaden. Online verfügbar unter https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2020.html;jsessionid=011B5DF5BC87A028F871ED1907D6AE87.live302?nn=28110, zuletzt geprüft am 29.06.2022.

Bundesministerium des Innern (2005): Nationaler Plan zum Schutz der Informationsinfrastrukturen. NPSI. Online verfügbar unter https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/05-12-09/05-12-09-anlage-nr-16.pdf?__blob=publicationFile&v=2, zuletzt geprüft am 26.06.2022.

Bundesministerium des Innern (2007): Umsetzungsplan KRITIS. des Nationalen Plans zum Schutz der Informationsinfrastrukturen. Online verfügbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/umsetzungsplan-kritis.html, zuletzt geprüft am 29.06.2022.

Bundesministerium des Innern (Hg.) (2009): Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). Bundesministerium des Innern. Online verfügbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.html, zuletzt geprüft am 29.06.2022.

Bundesministerium des Innern (2011): Cyber-Sicherheitsstrategie für Deutschland. Online verfügbar unter https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_download.pdf?__blob=publicationFile, zuletzt geprüft am 29.06.2022.

Bundesministerium des Innern (24.07.2015): Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme. IT-Sicherheitsgesetz. Fundstelle: Bundesministerium des Innern. In: *Bundesgesetzblatt* 2015 (31), S. 1324–1331. Online verfügbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/gesetzestexte/it-sicherheitsgesetz.pdf?__blob=publicationFile&v=1, zuletzt geprüft am 29.06.2022.

Bundesministerium des Innern (2016): Cyber-Sicherheitsstrategie für Deutschland 2016. Bundesministerium des Innern. Online verfügbar unter https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf, zuletzt geprüft am 29.06.2022.

Bundesministerium für Wirtschaft und Klimaschutz (2022): Initiative "IT-Sicherheit in der Wirtschaft". Online verfügbar unter https://www.bmwk.de/Redaktion/DE/Artikel/Digitale-Welt/it-sicherheit-in-der-wirtschaft.html, zuletzt aktualisiert am 29.06.2022, zuletzt geprüft am 29.06.2022.

Bundesverband der Deutschen Industrie e.V. (2020a): Stellungnahme Zum Referentenentwurf vom 25. November 2020 für ein Gesetz zur Änderung des BND-Geset-zes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts (BVerfG) und des Bundesverwaltungsgerichts (BVerwG). Online verfügbar unter https://bdi.eu/media/publikationen/#/publikation/news/aenderung-des-bundesnachrichtendienstgesetzes-bndg/, zuletzt geprüft am 29.06.2022.

Bundesverband der Deutschen Industrie e.V. (2020b): Stellungnahme zum Referentenentwurf vom 9. Dezember 2020 für ein Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0). Online verfügbar unter https://bdi.eu/publikation/news/referentenentwurf-fuer-ein-it-sicherheitsgesetz-2-0/, zuletzt geprüft am 29.06.2022.

Bundeswehr (2022): Cyber- und Informationsraum. Online verfügbar unter https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum, zuletzt aktualisiert am 29.06.2022, zuletzt geprüft am 29.06.2022.

Calcara, Antonio; Marchetti, Raffaele (2021): State-industry relations and cybersecurity governance in Europe. In: *Review of International Political Economy*, S. 1–26. DOI: 10.1080/09692290.2021.1913438.

Delerue, François; Géry, Aude (2018): The French Strategic Review of Cyber Defense. In: *ISPI*, 02.05.2018. Online verfügbar unter https://www.ispionline.it/it/pubblicazione/french-strategic-review-cyber-defense-20376, zuletzt geprüft am 30.06.2022.

Der Spiegel (2015): BDI-Chef über BND-Affäre: "Verhältnis zwischen Staat und Industrie ist erheblich belastet". Online verfügbar unter https://www.spiegel.de/wirtschaft/soziales/bnd-affaere-bdi-kritisiert-bundesregierung-scharf-a-1031290.html, zuletzt aktualisiert am 29.04.2015, zuletzt geprüft am 29.06.2022.

DER STANDARD (2021): Sensible Daten von 500.000 Patienten in Frankreich landeten im Netz. In: *DER STANDARD*, 27.02.2021. Online verfügbar unter https://www.derstandard.de/story/2000124528665/sensible-daten-von-500-000-patienten-in-frankreich-landeten-im, zuletzt geprüft am 16.05.2022.

Deutscher Bundestag (Hg.) (1991): Plenarprotokoll 12/27. Deutscher Bundestag, Stenographischer Bericht. 27. Sitzung Bonn, Mittwoch, den 5. Juni 1991. Online

verfügbar unter https://dserver.bundestag.de/btp/12/12027.pdf, zuletzt geprüft am 26.06.2022.

Die Bundesregierung (2014): Digitale Agenda 2014 – 2017. Hg. v. Bundesministerium für Wirtschaft und Energie, Bundesministerium des Innern und Bundesministerium für Verkehr und digitale Infrastruktur. Online verfügbar unter https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-agenda.pdf?__blob=publicationFile&v=3, zuletzt geprüft am 29.06.2022.

Die Bundesregierung (2016): Weissbuch 2016. Zur Sicherheitspolitik und zur Zukunft der Bundeswehr. Hg. v. Bundesministerium der Verteidigung. Online verfügbar unter https://www.bmvg.de/resource/blob/13708/015be272f8c0098f1537a491676bfc31/weissbuch2016-barrierefrei-data.pdf, zuletzt geprüft am 29.06.2022.

European Civil Protection and Humanitarian Aid Operations (2022): The national disaster management system. Online verfügbar unter https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/national-disaster-management-system_en, zuletzt aktualisiert am 29.06.2022, zuletzt geprüft am 30.06.2022.

FDP (2021): BSI unabhängig vom BMI machen. Online verfügbar unter https://www.fdp.de/forderung/bsi-unabhaengig-vom-bmi-machen, zuletzt aktualisiert am 30.06.2022, zuletzt geprüft am 30.06.2022.

Goetz, John; Leyendecker, Hans (2014): Rechnungsprüfer kritisieren Cyber-Abwehrzentrum für "nicht gerechtfertigt". In: *Süddeutsche Zeitung* 2014, 07.06.2014. Online verfügbar unter https://www.sueddeutsche.de/digital/behoerde-in-bonn-rechnungspruefer-halten-cyber-abwehrzentrum-fuer-nicht-gerechtfertigt-1.1989433, zuletzt geprüft am 29.06.2022.

Guibert, Nathalie (2016): L’armée française consolide son commandement cyber. In: *Le Monde*, 12.12.2016. Online verfügbar unter https://www.lemonde.fr/international/article/2016/12/12/l-armee-francaise-consolide-son-commandement-cyber_5047780_3210.html, zuletzt geprüft am 30.06.2022.

Hathaway, Melissa; Spidalieri, Francesca; Demchak, Chris; Kerben, Jason; McArdle, Jennifer (2016): CYBER READINESS AT A GLANCE. Online verfügbar unter https://securitydelta.nl/media/com_hsd/report/139/document/cri-netherlands-profile-pips.pdf.

Jonas, Alexandra; Ondarza, Nicolai von (2010): Chancen und Hindernisse für die europäische Streitkräfteintegration. Grundlegende Aspekte deutscher, französischer und britischer Sicherheits- und Verteidigungspolitik im Vergleich. 1. Aufl. Wiesbaden: VS Verl. für Sozialwiss (Schriftenreihe des Sozialwissenschaftlichen Instituts der Bundeswehr, 9). Online verfügbar unter http://www.loc.gov/catdir/enhancements/fy1405/2010395061-b.html.

Kuhn, Johannes; Hauck, Mirjam (2011): Behörden-Sheriffs gegen Hacker-Attacken. In: *Süddeutsche Zeitung* 2011, 17.06.2011. Online verfügbar unter https://www.sueddeutsche.de/digital/nationales-cyber-abwehrzentrum-bei-hackerangriff-ruf-den-minister-1.1109300, zuletzt geprüft am 29.06.2022.

Laudrain, Arthur P. B. (2019a): French Cyber Security and Defence: Strategy, Policy-Making and Coordination.

Laudrain, Arthur P.B. (2019b): France's New Offensive Cyber Doctrine. Lawfare. Online verfügbar unter https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine, zuletzt aktualisiert am 31.10.2019, zuletzt geprüft am 30.06.2022.

Liebetrau, Tobias (2022): Cyber conflict short of war: a European strategic vacuum. In: *European Security*, S. 1–20. DOI: 10.1080/09662839.2022.2031991.

Luber, Stefan (2018): Was ist ein CERT? Definition Computer Emergency Response Team (CERT). Security-Insider. Online verfügbar unter https://www.security-insider.de/was-ist-ein-cert-a-702654/, zuletzt aktualisiert am 09.04.2018, zuletzt geprüft am 29.06.2022.

Meister, Andre (2016): Neues BND-Gesetz: Alles, was der BND macht, wird einfach legalisiert. Und sogar noch ausgeweitet. netzpolitik.org e. V. Online verfügbar unter https://netzpolitik.org/2016/neues-bnd-gesetz-alles-was-der-bnd-macht-wird-einfach-legalisiert-und-sogar-noch-ausgeweitet/, zuletzt aktualisiert am 29.06.2022, zuletzt geprüft am 29.06.2022.

Meister, Andre (2020): Bundesverfassungsgericht: Massenüberwachung im BND-Gesetz ist verfassungswidrig. netzpolitik.org e. V. Online verfügbar unter https://netzpolitik.org/2020/das-neue-bnd-gesetz-ist-verfassungswidrig/, zuletzt aktualisiert am 29.06.2022, zuletzt geprüft am 29.06.2022.

Meister, Andre (2021): BND-Gesetz: Bundesnachrichtendienst erhält so viele Überwachungsbefugnisse wie noch nie. netzpolitik.org e. V. Online verfügbar unter https://netzpolitik.org/2021/bnd-gesetz-bundesnachrichtendienst-erhaelt-so-viele-ueberwachungsbefugnisse-wie-noch-nie/, zuletzt aktualisiert am 29.06.2022, zuletzt geprüft am 29.06.2022.

Merat, Victor (2022): Les entreprises sont confrontées à une pénurie de talents dans les métiers du numérique, selon un rapport. le Figaro. Online verfügbar unter https://etudiant.lefigaro.fr/article/les-entreprises-sont-confrontees-a-une-penurie-de-talents-dans-les-metiers-du-numerique-selon-un-rapport_9fa81aa0-8e62-11ec-90fa-661da1828997/, zuletzt aktualisiert am 30.06.2022, zuletzt geprüft am 30.06.2022.

Premier Ministre (2015): Französische Nationale Strategie Für Digitale Sicherheit. Online verfügbar unter https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_de.pdf, zuletzt geprüft am 30.06.2022.

Savaş, Serkan; Karataş, Süleyman (2022): Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. In: *Int. Cybersecur. Law Rev.* 3 (1), S. 7–34. DOI: 10.1365/s43439-021-00045-4.

Schallbruch, Martin (2018): Schwacher Staat im Netz. Wiesbaden: Springer Fachmedien Wiesbaden.

Schallbruch, Martin (2021a): Das IT-Sicherheitsgesetz 2.0 – Befugnisse des BSI und Schutz der Bundesverwaltung — Neue Rechtslage im ITSicherheitsrecht (Teil II). In: *Computer und Recht* 37 (8), S. 516–523. DOI: 10.9785/cr-2021-370809.

Schallbruch, Martin (2021b): Das IT-Sicherheitsgesetz 2.0 – neue Regeln für Unternehmen und IT-Produkte — Neue Rechtslage im IT-Sicherheitsrecht (Teil I). In: *Computer und Recht* 37 (7), S. 450–458. DOI: 10.9785/cr-2021-370709.

Schallbruch, Martin (2021c): Mehr Unabhängigkeit für das BSI? In: *Datenschutz Datensich* 45 (4), S. 229–233. DOI: 10.1007/s11623-021-1424-3.

Schallbruch, Martin; Skierka, Isabel (2018): Cybersecurity in Germany. Cham: Springer International Publishing.

Schulze, Matthias; Stiftung Wissenschaft und Politik (2020): Militärische Cyber-Operationen. Nutzen, Limitierungen und Lehren für Deutschland. Hg. v. Stiftung

Wissenschaft und Politik. Berlin. Online verfügbar unter https://www.swp-berlin.org/publications/products/studien/2020S15_she_CyberOperationen.pdf, zuletzt geprüft am 29.06.2022.

Secrétariat général de la défense et de la sécurité nationale (2017): THE CRITICAL INFRASTRUCTURE PROTECTION IN FRANCE. Online verfügbar unter http://www.sgdsn.gouv.fr/uploads/2017/03/plaquette-saiv-anglais.pdf, zuletzt geprüft am 30.06.2022.

Secrétariat général de la défense et de la sécurité nationale (2022): Réagir en cas de crise. Online verfügbar unter http://www.sgdsn.gouv.fr/missions/reagir-en-cas-de-crise/, zuletzt aktualisiert am 28.06.2022, zuletzt geprüft am 30.06.2022.

Sénat (2021): La cyberdéfense : un enjeu mondial, une priorité nationale. Online verfügbar unter https://www.senat.fr/rap/r11-681/r11-68122.html, zuletzt aktualisiert am 19.03.2021, zuletzt geprüft am 30.06.2022.

Specht, Frank (2022): IT-Berufe: Die Fachkräftelücke ist so groß wie nie zuvor. In: *Handelsblatt*, 07.02.2022. Online verfügbar unter https://www.handelsblatt.com/politik/deutschland/arbeitsmarkt-fachkraefteluecke-in-den-it-berufen-so-gross-wie-nie/28046062.html, zuletzt geprüft am 30.06.2022.

Stephan Steller (2017): Die Cyber-Sicherheitsstrategie für Deutschland. Arbeitspapiere zur Internationalen Politik und Außenpolitik. AIPA 1/2017. Lehrstuhl Internationale Politik. Köln. Online verfügbar unter https://ib.uni-koeln.de/fileadmin/templates/Allgemeines/AIPA_Die_Cyber-Sicherheitsstrategie_fuer_Deutschland_Stephan_Steller.2017.pdf, zuletzt geprüft am 29.06.2021.

tagesschau (2021): Immer mehr Cyberangriffe: Kliniken im Visier der Hacker. In: *tagesschau.de*, 28.06.2021. Online verfügbar unter https://www.tagesschau.de/wirtschaft/technologie/cybersicherheit-infrastruktur-hacker-kliniken-cybercrime-101.html, zuletzt geprüft am 16.05.2022.

Toucas, Boris (2017): The Macron Leaks: The Defeat of Informational Warfare. Center for Strategic and International Studies. Online verfügbar unter https://www.csis.org/analysis/macron-leaks-defeat-informational-warfare, zuletzt aktualisiert am 30.06.2022, zuletzt geprüft am 30.06.2022.

Vitel, Philippe; Bilddal, Henrik (2015): French Cyber Security and Defence: An Overview. In: *ISIJ* 32, S. 29–41. DOI: 10.11610/isij.3209.

Welchering, Peter (2017): Überwachung: Bundesnachrichtendienst soll Cybersicherheit gewährleisten. Hg. v. Deutschlandfunk.de. Online verfügbar unter https://www.deutschlandfunk.de/ueberwachung-bundesnachrichtendienst-soll-cybersicherheit-100.html, zuletzt geprüft am 29.06.2022.

Zedler, Dominika (2016): Zur strategischen Planung von Cyber Security in Deutschland. Arbeitspapiere zur Internationalen Politik und Außenpolitik. AIPA 2/2016. Lehrstuhl Internationale Politik. Köln. Online verfügbar unter https://ib.uni-koeln.de/fileadmin/templates/publikationen/aipa/AIPA_2016_2.pdf, zuletzt geprüft am 29.06.2022.

Zedler, Dominika (2017): Zur strategischen Planung von cyber security in Deutschland. In: *Z Außen Sicherheitspolit* 10 (1), S. 67–85. DOI: 10.1007/s12399-016-0606-9.