

Bachelorarbeit

BA AI 18/2021

Hilfswerke für die Zivilbevölkerung im Cyber War

angefertigt zur Erlangung des akademischen Grades

Bachelor of Science in Medieninformatik

an der Hochschule Harz

Fachbereich Automatisierung und Informatik

Vorgelegt von:

Yannik Meinhardt
Matrikel-Nr. 25153

Salzwedeler Weg 3
29379 Wittingen-Vorhop
E-Mail: yame@gmx.de

Angefertigt bei:

Erstprüfer:
Prof. Daniel Ackermann

Zweitprüfer:
Manuel Atug

Eingereicht zum: 24.06.2021

**Thema und Aufgabenstellung der Bachelorarbeit
BA AI 18/2021**

für Herrn Yannik Meinhardt

Hilfswerke für die Zivilbevölkerung im Cyber War


Im fortschreitenden Zeitalter der Digitalisierung steigt die Eintrittswahrscheinlichkeit einer Störung katastrophalen Ausmaßes unserer lebensnotwendigen Infrastrukturen durch Cyberangriffe kontinuierlich an. Diese kritischen Infrastrukturen gilt es gegen Attacken zu schützen und vorbereitet auf einen wahrscheinlichen Ernstfall zu sein.

Im Rahmen der Arbeit wird eine Analyse der aktuellen Reaktionsfähigkeit Deutschlands auf einen Cyberangriff auf kritische Infrastrukturen, insbesondere vor dem Hintergrund bestehender Hilfsstrukturen für die Zivilbevölkerung und des bestehenden Völkerrechts sowie anderer Regelungen (z.B. Genfer Konvention oder Tallin Manual) vorgenommen. Analog zum Technischen Hilfswerk, welches bereits im physischen Zivil- und Katastrophenschutz eng mit Bund und Länder zusammenarbeitet, wird überprüft, ob eine ähnliche Institution von Nöten ist, die im Fall eines Cybervorfalls den Staat bei der defensiven Krisenbewältigung unterstützt.

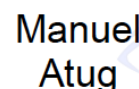
Um eine tatsächliche Umsetzbarkeit zu prüfen, erfolgt der Abgleich des Ergebnisses des Ist-Zustands mit den Potenzialen eines Cyber-Hilfswerks (CHW) (<https://ag.kritis.info/chw-konzept/>), wie von der AG KRITIS vorgeschlagen. Im Konzept des CHW können zivile Helfer und Spezialisten verschiedener Fachbereiche gebündelt werden, um ehrenamtlich in Großschadenslagen unterstützen zu können. Dies bringt neben den Möglichkeiten auch einige Fragestellungen in Themen der Rechtsform, Struktur und Ausbildungsmöglichkeiten mit, die es in dieser Arbeit zu erörtern gilt.

Die Bachelorarbeit beinhaltet folgende Teilaufgaben:

- Analyse des Ist-Zustands
- Recherche von bestehenden Hilfsstrukturen und Regulierungen
- Abgleich des Ist-Zustands mit den Potenzialen eines Cyber-Hilfswerks
- Prüfung einer Umsetzbarkeit im Rahmen bestehender gesetzlicher Regelungen
- Kritische Reflexion und Ausblick


Digital
unterschrieben von
Daniel Ackermann
Datum: 2021.03.08
09:32:16 +01'00'

Prof. Daniel Ackermann
1. Prüfer


Digital signiert von Manuel Atug
DN: cn=Manuel Atug, ou=Seccon,
email=matug@hisolutions.com
Datum: 2021.03.05 14:17:50
+01'00'

Manuel Atug
2. Prüfer

I Inhaltsverzeichnis

Inhaltsverzeichnis	I
Abbildungsverzeichnis	II
Abkürzungsverzeichnis	III
1 Einleitung	1
1.1 Aufbau der Arbeit	2
1.2 Einführung in Kritische Infrastrukturen	2
1.3 Problemstellung	4
2 Rechtlicher Rahmen und Hilfsstrukturen	7
2.1 Anwendung des Völkerrechts auf digitale Kriegsführung	7
2.1.1 Schwelle der Völkerrechtsanwendung	8
2.1.2 Kombattanten-Problematik	9
2.1.3 Attribution von Cyberangriffen	10
2.2 Rechtliche Entwicklungen	11
2.2.1 Tallinn Manual	11
2.2.2 Positionspapiere	14
2.2.3 EU Cybersecurity Act	15
2.2.4 Überarbeitung der EU Richtlinien NIS und ECI	16
2.2.5 Non-Paper on Cyber Diplomacy eines Staatenverbunds	18
2.2.6 Cyber-Sicherheitsstrategie Deutschland für 2021	19
2.2.7 IT-Sicherheitsgesetz 2.0	20
2.2.8 Fazit zur Rechtslage	21
2.3 Bestehende Institutionen	22
2.3.1 Technisches Hilfswerk in Deutschland	23
2.3.2 Estlands Defence League Cyber Unit	24
2.3.3 US amerikanisches C ³ Programm für Volontäre	25
3 Status quo in Deutschland	26
3.1 Vorhandene Kapazitäten und Leistungsfähigkeit	26
3.1.1 Überblick der CERTs	26

3.1.2	<i>BSI MIRT</i>	29
3.1.3	<i>Cyber-Sicherheitsnetzwerk des BSI</i>	29
3.2	Bewusstsein über Gefahrenpotenzial	31
3.3	Gefahrenlage	33
3.3.1	<i>Angriffe in der Vergangenheit</i>	35
3.3.2	<i>Potenzielles Angriffsszenario auf IoT</i>	36
4	Potenziale eines Cyber-Hilfswerks	40
4.1	Einführung in das Cyber-Hilfswerk und die AG KRITIS	40
4.2	Aufgabenbereiche	41
4.3	Anwendungsbereiche	42
4.3.1	<i>Einsatzszenarien</i>	42
4.3.2	<i>IoT Angriffsszenario mit einem CHW</i>	44
5	Umsetzbarkeit eines Cyber-Hilfswerks	46
5.1	Organisatorische Struktur	46
5.2	Rechtsform und Haftung	48
5.3	Externe Bedingungen	51
5.3.1	<i>Behördliche Bedingungen</i>	51
5.3.2	<i>Politische Forderungen und Bedingungen der Community</i>	52
5.4	Erfahrungen aus dem Projekt Cyberwehr des BSI	54
5.5	Vergleich zum Cyber-Sicherheitsnetzwerk des BSI	55
6	Fazit	56
6.1	Kritische Reflexion	56
6.1.1	<i>Herausforderungen und Nachteile</i>	56
6.1.2	<i>Vorteile</i>	56
6.2	Ausblick	57
6.3	Zusammenfassung	59
	Literaturverzeichnis	IV
	Eigenständigkeitserklärung	V

II Abbildungsverzeichnis

Abbildung 1.1: KRITIS-Sektoren	3
Abbildung 3.1: Rollenverständnis im CSN	30
Abbildung 4.1: Bewältigungsdauer mit Cyber-Hilfswerk	44
Abbildung 5.1: Rollen im Cyber-Hilfswerk	47
Abbildung 5.2: Tabelle Mapping Hackerethik auf politische Forderungen	53

III Abkürzungsverzeichnis

ACS	Allianz für Cybersicherheit
AG KRITIS	Arbeitsgruppe Kritische Infrastrukturen
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BCMS	Business Continuity Management System
BGB	Bürgerliches Gesetzbuch
Bitkom	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BKA	Bundeskriminalamt
BMI	Bundesministerium des Innern, für Bau und Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI-KritisV	BSI-Kritisverordnung
C3	Critical Infrastructure Cyber Community
CCD COE	NATO Cooperative Cyber Defence Center of Excellence
CERT	Computer Emergency Response Team
CHW	Cyber-Hilfswerk
CSIRT	Computer Security Incident Response Team
CSN	Cyber-Sicherheitsnetzwerk
DBReg	Deutsche Bundesregierung
DDoS	Distributed Denial of Service Attacke
DRK	Deutsches Rotes Kreuz
DSGVO	Datenschutzgrundverordnung
ECI	Richtlinie European Critical Infrastructure 2008/114/EG
EDL CU	Estonian Defence League Cyber Unit

ENISA	Cybersicherheitsagentur der Europäischen Union für Netz- und Informationssicherheit
EU	Europäische Union
G8	Gruppe der Acht
GG	Grundgesetz
HL7	Health Level 7
ICRC	International Committee of the Red Cross
IGH	Internationaler Gerichtshof
IoT	Internet of Things
ISMS	Information Security Management System
IT-SiG 1.0	Erstes deutsches IT-Sicherheitsgesetz
IT-SiG 2.0	Deutsches IT-Sicherheitsgesetz 2.0
KMU	Kleine und mittlere Unternehmen
KRITIS	Kritische Infrastrukturen
LKA	Landeskriminalamt
MIRT	Mobile Incident Response Team
NATO	North Atlantic Treaty Organization
NCAZ	Nationales Cyber-Abwehrzentrum
NIS	Richtlinie Netz- und Informationssicherheit 2016/1148
NIST	National Institute of Standards and Technology
RCE	Richtlinie Resilience of critical Entities
StGB	Strafgesetzbuch
TA	Technikfolgeabschätzung
THW	Technisches Hilfswerk
THW-Gesetz	Deutsches Gesetz über das Technische Hilfswerk
VCV	Verwaltungs-CERT-Verbund

1 Einleitung

Wer in Deutschland als Privatperson Opfer eines rechtswidrigen Angriffs wird, kann sich nach dem Straf- und Zivilrecht verteidigen. Diese Notwehr ist im privatrechtlichen Bereich unter § 227 des Bürgerlichen Gesetzbuchs (BGB)¹ und sonst in § 32 des Strafgesetzbuchs (StGB)² geregelt. Wenn ein Staat oder seine Bevölkerung angegriffen wird, verletzt diese Handlung das Internationale Völkerrecht mit der Charta der Vereinten Nationen³. Als kriegerische Handlung gewertet, findet nun die Genfer Konvention von 1949⁴ Anwendung, die Regeln für den Schutz von Personen, die nicht oder nicht mehr an Kampfhandlungen teilnehmen (sog. Nicht-KombattantInnen), bietet.

Wie verhält es sich jedoch nun, wenn sich solch ein Konflikt nicht konventionell, sondern verschleiert in Form von Hacks im Cyberraum abspielt?

Wie ist es möglich, insbesondere die Zivilbevölkerung in solchen Situationen zu schützen und Folgen für diese in einem Konflikt abzdämpfen?

Um diesen Fragen auf den Grund zu gehen, beschäftigt sich der Autor mit dem Konzept zur Etablierung eines Cyber-Hilfswerks (CHW)⁵, analog zum bestehenden Technischen Hilfswerk (THW), wie von der Arbeitsgruppe Kritische Infrastrukturen (AG KRITIS) vorgeschlagen. Das Konzept stellt eine mögliche Organisation vor, die im Falle eines Cyberangriffs auf Kritische Infrastrukturen (KRITIS) dem Bund unterstützende Hilfeleistungen bei der Krisenbewältigung und dem Schutz der Grundversorgung der Bevölkerung gewähren könnte.

¹ „Bürgerliches Gesetzbuch“, [gesetze-im-internet.de](https://www.gesetze-im-internet.de/bgb/), zugegriffen 14. Juni 2021, <https://www.gesetze-im-internet.de/bgb/>

² „Strafgesetzbuch“, [gesetze-im-internet.de](https://www.gesetze-im-internet.de/stgb/), zugegriffen 14. Juni 2021, <https://www.gesetze-im-internet.de/stgb/>

³ United Nations, „Charta der Vereinten Nationen“, [lpb-bw.de](https://www.lpb-bw.de/charta), zugegriffen 14. Juni 2021, <https://www.lpb-bw.de/charta>

⁴ „Humanitäres Völkerrecht: Genfer Konventionen“, [humanrights.ch](https://www.humanrights.ch/de/ipf/grundlagen/rechtsquellen-instrumente/humanitaeres-voelkerrecht/genfer-abkommen/), zugegriffen 14. Juni 2021, <https://www.humanrights.ch/de/ipf/grundlagen/rechtsquellen-instrumente/humanitaeres-voelkerrecht/genfer-abkommen/>

⁵ Arbeitsgruppe Kritische Infrastrukturen, „Konzept Cyber-Hilfswerk“, [ag.kritis.info](https://ag.kritis.info/chw-konzept/), zugegriffen 14. April 2021, <https://ag.kritis.info/chw-konzept/>

1.1 Aufbau der Arbeit

Die vorliegende Arbeit ist in mehrere Teilaspekte gegliedert und beschäftigt sich mit der grundlegenden Beantwortung der Frage, ob die Etablierung eines Cyber-Hilfswerks zum Schutz Kritischer Infrastrukturen durch Cyberangriffe sinnvoll ist und wie dies angewendet werden kann. Wie im Exposé zu lesen ist, beinhaltet die Ausarbeitung folgende Teilaufgaben: Bei der Analyse der rechtlichen Rahmenbedingungen und bestehenden Hilfsstrukturen in Deutschland und der Welt liegt der Fokus zunächst auf der Fragestellung, ob es Probleme bei der Anwendbarkeit des humanitären Völkerrechts für den digitalen Raum gibt. Dann werden rechtliche Entwicklungen in diesem Kontext vorgestellt. Es folgt eine Auswertung des Ist-Zustands der Krisenbewältigungsfähigkeit in der Bundesrepublik Deutschland. Im nachfolgenden Kapitel werden die Potenziale des CHW eruiert und anschließend die Umsetzbarkeit des Konzepts überprüft. Unter anderem erfolgt eine hypothetische Modellrechnung zur Veranschaulichung der Auswirkung der Etablierung eines CHW auf die Abwehrbereitschaft während einer Großschadenslage. Abschließend werden Vor- und Nachteile erörtert, um die Arbeit mit einer Zusammenfassung der Ergebnisse und einem Ausblick zu beenden. Dabei liegt der Fokus auf der Prüfung der Notwendigkeit eines solchen Hilfswerks mit dessen Nutzen für die Versorgungssicherheit der Allgemeinheit.

1.2 Einführung in Kritische Infrastrukturen

„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.“⁶

Wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) treffend in ihrer Definition ausweisen, sind

⁶ Bundesamt für Sicherheit in der Informationstechnik, „KRITIS - Definition und Übersicht“, [kritis.bund.de](https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.html), zugegriffen 15. April 2021, https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.html

KRITIS für die Aufrechterhaltung des Allgemeinwohls der Bevölkerung von essenzieller Bedeutung. In Deutschland wurden die kritischen Organisationen 2009 von der Bundesregierung gemäß dem BSI-Gesetz und der BSI-Kritisverordnung (BSI-KritisV)⁷ in Sektoren eingeteilt:

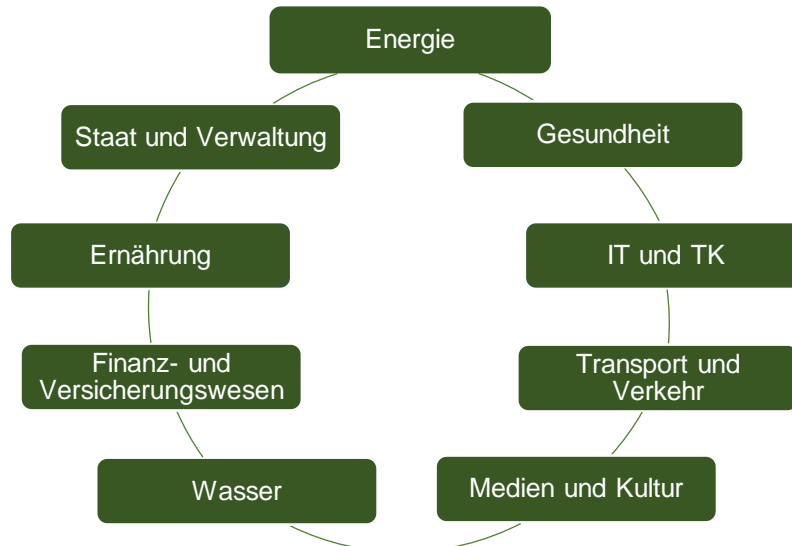


Abbildung 1.1: KRITIS-Sektoren

Dabei muss jedoch beachtet werden, dass diese Sektoren voneinander abhängig sind. Ohne eine gesicherte Energieversorgung lässt sich keine Produktion aufrechterhalten. Mit einem Ausfall der Wasserversorgung wäre die Herstellung von Lebensmitteln nicht denkbar. Ohne Informations- und Kommunikationstechnik kann kein Staat und keine Verwaltung handeln. Diese Interdependenzen verschärfen das Risiko von Ausfällen und können auf diese Weise einen Dominoeffekt auslösen. Die KRITIS-Betreiber, seien es privatwirtschaftliche oder öffentlich-rechtliche Organisationen, erbringen diese Leistungen und müssen dies zu jeder Zeit stabil und störungsfrei tun, um die zwingend erforderliche Versorgung der Bevölkerung aufrechterhalten zu können. In der Einteilung welcher Betrieb tatsächlich als KRITIS Betreiber gewertet werden kann, kommt es jedoch zu Unterscheidungen: Aus europäischer Sicht gibt es mit der Richtlinie Netz- und Informationssicherheit (NIS) 2016/1148 eine Einteilung nach Sektoren und individuellen Kriterien⁸. Die deutsche Sicht gliedert sich gemäß Abbildung 1.1 nach dem BSI-Gesetz und der Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV) und legt Schwellenwerte, wie die Anzahl der zu versorgenden Personen, für sieben der neun Sektoren

⁷ „BSI-KritisV“, [gesetze-im-internet.de, zugegriffen 14. Juni 2021, https://www.gesetze-im-internet.de/bsi-kritisv/](https://www.gesetze-im-internet.de/bsi-kritisv/)

⁸ „NIS 2016/1148 Richtlinie“ (2016), <https://eur-lex.europa.eu/eli/dir/2016/1148/2016-07-19>

fest⁹. Die Sektoren Staat und Verwaltung sowie Medien und Kultur sind über eigene Gesetzgebungen abgedeckt. Das BBK definiert KRITIS nach dem Ansatz, dass jeder Betreiber kritisch ist, wenn bei einem Ausfall von diesem die Bevölkerung gefährdet sein kann. Unter diesem Aspekt kommen zusätzliche Sektoren wie die Chemieproduktion in den Fokus, die über das BSI-KritisV nicht abgedeckt werden¹⁰.

Falls ein Betreiber als kritisch definiert wurde, wird er über das BSI-Gesetz mit einigen Pflichten wie Sicherheitsmaßnahmen, Vorfalle Meldungen und regelmäßigen Prüfungen belegt.

1.3 Problemstellung

Gemäß dem vom Bundesministerium des Innern, für Bau und Heimat (BMI) vorgegebenen All-Gefahren-Ansatz für KRITIS¹¹ können die Betriebe von einer Vielzahl an Gefahren getroffen werden, dessen Handlungsoptionen es im Rahmen einer Risikoanalyse gleichermaßen zu berücksichtigen gilt. Der Versorgungsausfall der Bevölkerung muss zu jeder Zeit ausbleiben. Dabei hilft kein Abschluss einer Versicherung zum Abdämpfen der wirtschaftlichen Folgen. Betreiber müssen alle Risiken adressieren und entsprechende Präventionsmaßnahmen treffen. Neben den alltäglichen Gefahren und Störungen von KRITIS durch technisches oder menschliches Versagen, können diese genauso von Extremereignissen wie beispielsweise Naturkatastrophen oder terroristischen Anschlägen getroffen werden. Darüber hinaus lässt sich ein Trend der Häufung von Cyberattacken auf Einrichtungen der KRITIS erkennen.¹² Trotz mehrerer durch das BSI eingeleiteter Initiativen zum Schutz der Betreiber häufen sich die Angriffe über die letzten Jahre. Wie an der Antwort der Bundesregierung auf eine kleine Anfrage

⁹ Vgl. Bundesamt für Sicherheit in der Informationstechnik, „Sektorspezifische Infos für KRITIS-Betreiber“, bsi.bund.de, zugegriffen 22. Mai 2021, <https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Sektorspezifische-Infos-fuer-KRITIS-Betreiber/sektorspezifische-infos.html>

¹⁰ Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, „Kritische Infrastrukturen“, bbk.bund.de, zugegriffen 15. April 2021, https://www.bbk.bund.de/DE/AufgabenundAusstattung/KritischeInfrastrukturen/kritischeinfrastrukturen_node.html

¹¹ Vgl. Bundesministerium des Innern, „Nationale Strategie zum Schutz kritischer Infrastrukturen“, bmi.bund.de, zugegriffen 21. Mai 2021, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.pdf?__blob=publicationFile&v=3

¹² Vgl. Janina Kröger, „Cyberattacken richten sich verstärkt auf KRITIS“, it-service.network, zugegriffen 20. April 2021, <https://it-service.network/blog/2021/01/13/kritische-infrastrukturen/>

der FDP zu erkennen ist, fokussieren sich Hacker verstärkt auf die vulnerablen KRITIS-Bereiche Energie und Gesundheit.¹³ Wie das Beispiel der Universitätsklinik Düsseldorf aufzeigt, können auch Teilausfälle der IT-Infrastruktur eines KRITIS-Betreibers schnell lebensbedrohlich werden. Eine Ransomware hatte versehentlich nicht die Universität Düsseldorf, sondern die Uniklinik getroffen und dessen Server verschlüsselt. Als Folge dessen kam es zur Störung des Krankenhausbetriebs. Unter anderem mussten Rettungsdienstfahrzeuge zu anderen Kliniken umgeleitet werden.¹⁴

Die zunehmende Digitalisierung findet auch im KRITIS-Sektor statt und stellt die Branche vor sich stetig ändernde Herausforderungen. Die immer stärker werdende Vernetzung der Systeme, gepaart mit der Zunahme an IT-Infrastruktur und der Ablösung von manuellen Aufgaben durch digitale Automatisierung lässt die Eintrittswahrscheinlichkeit eines Sicherheitsvorfalls steigen. Die rasante technische Entwicklung lässt etablierte Technologien schneller obsolet werden, als es bei der Veröffentlichung gedacht war. Von diesem Paradigma spricht auch die AG KRITIS in ihrem Konzeptpapier zur Schaffung eines CHW¹⁵. In der Arbeitsgruppe versammeln sich laut Webseite der Arbeitsgruppe 42 Fachleute und ExpertInnen aus allen Bereichen der Kritischen Infrastruktur, die sich unabhängig von Staat und Wirtschaft das Ziel gesetzt haben, die Versorgungssicherheit der Bevölkerung zu erhöhen.¹⁶

Da laut CHW-Konzept der AG KRITIS die staatlichen Kapazitäten zur Krisenbewältigung einer katastrophalen Großschadenslage in KRITIS nicht ausreichen, fordern sie die Etablierung einer zusätzlichen Organisation. Eine solche Katastrophenlage besteht nach Glossar des BBK¹⁷ dann, wenn Gefahr für Leben und Gesundheit einer Vielzahl an Menschen besteht oder die natürlichen Lebensgrundlagen in Form der KRITIS-Versorgung stark beeinträchtigt werden. In der Folge müssen am Katastrophenschutz mitwirkende Behörden und Einrichtungen aktiv werden. In dieser

¹³ Vgl. Bundesregierung Deutschland, „Drucksache 19/24247: Anfälligkeit kritischer Infrastrukturen vor Hackerangriffen in Deutschland“, zugegriffen am 20. April 2021, <https://dserver.bundestag.de/btd/19/242/1924247.pdf>

¹⁴ „IT-Ausfall an der Uniklinik Düsseldorf“, uniklinik-duesseldorf.de, zugegriffen 20. April 2021, <https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/it-ausfall-an-der-uniklinik-duesseldorf>

¹⁵ Vgl. Arbeitsgruppe Kritische Infrastrukturen, „Konzept Cyber-Hilfswerk“, Seite 4

¹⁶ Vgl. Arbeitsgruppe Kritische Infrastrukturen, „Wer sind wir?“, ag.kritis.info, zugegriffen 20. April 2021, <https://ag.kritis.info/wer-sind-wir/>

¹⁷ Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, „Glossar - A-Z der Katastrophenhilfe“, bbk.bund.de, zugegriffen 21. Mai 2021, <https://www.bbk.bund.de/SubSites/Kritis/DE/Servicefunktionen/Glossar/Functions/glossar.html>

Arbeit wird mit dem Begriff Großschadenslage immer auf die Definition des BBK im Kontext eines Vorfalls mit Auslöser in der Informationstechnik hingewiesen. In dem CHW-Konzept führt die Arbeitsgruppe einen Vorschlag zur Umsetzung einer Organisation zur Erfüllung dieses Katastrophenschutzes im Ehrenamt aus. Die vorliegende Ausarbeitung beschäftigt sich, wie in Kapitel 1.1 Aufbau der Arbeit ausgeführt mit dem Konzeptpapier und erörtert dessen Forderungen.

2 Rechtlicher Rahmen und Hilfsstrukturen

In der Bundesrepublik Deutschland ist für KRITIS der Bund maßgeblich verantwortlich. Betreiber der kritischen Dienstleistungen stellen die Grundversorgung der Bevölkerung sicher. Ein Ausfall oder ein Engpass hätte gravierende Folgen für die BürgerInnen.

Das Phänomen Cyberwar betrifft grundsätzlich jede vernetzte Gesellschaft und besitzt im Vergleich zur Cyberkriminalität ein höheres Bedrohungspotenzial. Denn Angriffe von Cyberkriminellen oder auch von Cyberterroristen unterliegen der nationalen Rechtsprechung, da sie von Zivilpersonen ausgehen. Falls ein Angriff auf KRITIS von einem staatlichen Akteur ausgeht, kann diese Handlung als kriegerisch angesehen werden und somit das Völkerrecht der Vereinten Nationen verletzen. Staaten haben verstanden, dass im Cyberspace ein großes militärisches und strategisches Potenzial steckt und bauen ihre (offensiven) Kapazitäten dahingehend aus. Dabei findet der Begriff Cyberwar insofern Anwendung, sodass Cyber-Wirkmittel als taktisches Instrument zur Unterstützung in einem hybriden Kriegsszenario dienen.¹⁸

2.1 Anwendung des Völkerrechts auf digitale Kriegsführung

Ob das humanitäre Völkerrecht Anwendung findet, hängt von einigen Aspekten ab. Ob diese auch für einen Konflikt im Cyberraum gelten, wird im Folgenden erörtert. Als Basis der folgenden drei Unterkapitel dient die Ausarbeitung der Wissenschaftlichen Dienste des deutschen Bundestags zur „Anwendbarkeit des humanitären Völkerrechts auf Computernetzwerkoperationen und digitale Kriegsführung (Cyber Warfare)“¹⁹.

¹⁸ Vgl. Andy Greenberg, „What Is Cyberwar? The Complete WIRED Guide“, wired.com, zugegriffen 14. Juni 2021, <https://www.wired.com/story/cyberwar-guide/>

¹⁹ Vgl. Wissenschaftliche Dienste Deutscher Bundestag, „Anwendbarkeit des humanitären Völkerrechts auf Computernetzwerkoperationen und digitale Kriegsführung (Cyber Warfare)“, zugegriffen am 14. April 2021, <https://www.bundestag.de/resource/blob/406028/de1946480e133cf38bbee41d8d3d6898/WD-2-038-15-pdf-data.pdf>

2.1.1 Schwelle der Völkerrechtsanwendung

In der internationalen Gemeinschaft herrscht weitestgehend Einigkeit darüber, dass das humanitäre Völkerrecht auf Cyber-Angriffe während eines bewaffneten Konflikts grundsätzlich Anwendung findet. Gleichzeitig ist festzustellen, dass das Völkerrecht außerhalb bewaffneter Konflikte keine Anwendung findet. Ein bewaffneter Konflikt ist laut Internationalem Gerichtshof (IGH) dann gegeben, wenn in ausgedehnter bzw. andauernder Weise Waffengewalt angewendet wird. Der IGH stellte bereits in Ihrem Rechtsgutachten zu Nuklearwaffen klar:

*“However, it cannot be concluded [...] that the established principles and rules of humanitarian law applicable in armed conflict did not apply to nuclear weapons. Such a conclusion would be incompatible with the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and **applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future.**”²⁰*

Das humanitäre Völkerrecht findet auf jede Form der Kriegsführung und ihren Waffen Anwendung. Das geschieht auch für zukünftige Angriffsformen. Es stellt sich die Frage, ob es sich bei Methoden im Cyberwar um Waffen oder lediglich militärische Wirkmittel handelt. Diese Einstufung der Intensität lässt sich über die Zahl, Dauer und Intensität einzelner Konflikte, über die gewählte Angriffsmethode, über die Zahl der Betroffenen und das Ausmaß der Zerstörung beurteilen. Angriffe auf Kritische Infrastrukturen hätten starke Auswirkungen auf die Zivilbevölkerung und sind somit in ihrem Ausmaß und ihrer Zerstörungskraft mit der konventionellen Kriegsführung zu vergleichen. Dies sehen auch die VerfasserInnen der Ausarbeitung des Deutschen Bundestags so.²¹ Cyberspionage-Aktionen liegen jedoch unterhalb der Schwelle. Es hat sich als gängige Praxis etabliert, Informationen über fremde Nationen und selbst seine Bündnispartner im Friedensfall zu sammeln²². Mehr zum Thema Cyberspionage bringt der Autor in Kapitel 3.3 Gefahrenlage an.

²⁰ Internationaler Gerichtshof, „Legality of the Threat or Use of Nuclear Weapons“, icj-cij.org, zugegriffen 29. April 2021, <https://www.icj-cij.org/en/case/95>

²¹ Vgl. Deutscher Bundestag, „Anwendbarkeit des humanitären Völkerrechts auf Computernetzwerkoperationen und digitale Kriegsführung (Cyber Warfare)“

²² Vgl. Arne Meyer-Fünffinger, „Vor BND-Urteil: So überwacht der Dienst das Internet“, tagesschau.de, zugegriffen 14. Juni 2021, <https://www.tagesschau.de/investigativ/br-recherche/bnd-urteil-101.html>

2.1.2 **Kombattanten-Problematik**

Gemäß der Genfer Konvention von 1949 dürfen sich nur KombattantInnen an Kampfhandlungen beteiligen. Im klassischen Sinne sind KombattantInnen Angehörige der regulären Streitkräfte und auch als solche zu erkennen. Es wird jedoch zunehmend schwieriger KombattantInnen von ZivilistInnen (oder Nicht-KombattantInnen) zu unterscheiden. Dies ist nicht nur im Cyberraum der Fall. Konventionelle Kriege wurden in der Mehrheit längst durch Terrorismus, kriegerische Handlungen gegen die eigene Bevölkerung oder Stellvertreterkriege ersetzt²³. Aber auch bei einem Konflikt über international verteilte IT-Infrastrukturen, in denen sich AngreiferInnen mühelos bewegen können, bilden sich neue Herausforderungen. Zusätzlich können sich in solchen Auseinandersetzungen neben einfachen ZivilistInnen auch zivile Unternehmen als Militär- oder Sicherheitsfirmen am Cyberkrieg beteiligen. Die Vergangenheit hat gezeigt, dass diese privaten Akteure im Auftrag eines Staates immer wieder für Verstöße gegen das Völkerrecht verantwortlich gemacht werden mussten. Ein Beispiel hierfür liefert der Folterskandal durch SoldatInnen und privaten Militärakteuren im Abu Ghraib Gefängnis in Irak²⁴. Eine Anpassung des KombattantInnen-Status für den Cyberwar könnte von staatlichen Akteuren gefordert werden, da diese momentan keinen glaubhaften Beweis für einen Gegenschlag liefern können. In diesem Zusammenhang stellt der Wissenschaftliche Dienst des Bundestages in Ihrer Ausarbeitung klar²⁵: Im Cyberkrieg gibt es für technische Einrichtungen keine Unterscheidungserfordernis, für KombattantInnen jedoch schon. Technische Identifikationsmöglichkeiten wie IP-Adressen lassen sich zu einfach manipulieren, um als Feststellungsurteil dienen zu können.

²³ Vgl. Jost Dülffer, „Alte und neue Kriege. Gewaltkonflikte und Völkerrecht seit dem 19. Jahrhundert“, bpb.de, zugegriffen 14. Juni 2021, <https://www.bpb.de/apuz/232960/alte-und-neue-kriege>

²⁴ Vgl. Noah Bierman, „Few Have Faced Consequences for Abuses at Abu Ghraib Prison in Iraq“, latimes.com, zugegriffen 10. Juni 2021, <https://www.latimes.com/nation/la-na-abu-ghraib-lawsuit-20150317-story.html>

²⁵ Vgl. Deutscher Bundestag, „Anwendbarkeit des humanitären Völkerrechts auf Computernetzwerkoperationen und digitale Kriegsführung (Cyber Warfare)“

2.1.3 Attribution von Cyberangriffen

Die notwendige Transparenz für einen legitimierte Krieg kann bei der Attribution nicht gewährleistet werden²⁶. Hier liegt das Kernproblem der digitalen Kriegsführung, das auch die Kombattanten-Problematik betrifft. Sofern die Konfliktparteien nicht feststehen, bleibt es unklar, ob ein bewaffneter Konflikt im Sinne des Völkerrechts vorliegen kann.

Es bietet sich die einfache Möglichkeit, die Herkunft der Angriffe zu verschleiern oder gar die Aufmerksamkeit auf einen unbeteiligten Drittstaat zu lenken. Des Weiteren besteht bei AngreiferInnen kein unmittelbares Interesse, sich zu einem Cyberangriff zu bekennen. Die Androhung oder Anwendung von Gewalt verbietet die Charta der Vereinten Nationen in Artikel 2. Ein Cyberangriff mit gegebenem Ausmaß würde diesen Artikel verletzen und somit das unter Artikel 51 geregelte Recht zur Selbstverteidigung aktivieren. Wenn man unter diesem Kontext als AngreiferIn unbemerkt und folgenlos bleiben kann, findet eine verschleierte Taktik Anwendung. Auch besteht eine Ungewissheit über den Ort, an dem sich das verwendete Computersystem befindet.

Die Identifizierung eines Angreifers oder einer Angreiferin wird sich zum jetzigen technologischen Stand immer schwierig bis unmöglich gestalten.²⁷ Es wird bereits schwierig sein, einen Angriff von einem übermütigen Jugendlichen, einer kriminellen oder terroristischen Organisation oder von einer gegnerischen Partei in einem bewaffneten Konflikt unterscheiden zu können.

In der Ausarbeitung des deutschen Bundestages wird die Rechtsgrundlage für einen Gegenschlag aufgezeigt: Der Staat, der zu einer militärischen Gegenmaßnahme gemäß seines Rechtes von Artikel 51 der Charta der Vereinten Nationen greift, trägt die Beweislast des Erstschlages und des resultierenden Völkerrechtsverstoßes. Dieser Beweis ist mit forensischer Untersuchung schwer zu erbringen, weshalb die Frage, wem der Angriff am Meisten nützen würde, vorrangig wird. Dadurch können Vermutungen über die Urheberschaft des Angriffes angestellt werden, falls sich ein Akteur weigert, Hilfe bei der Aufklärung zu leisten. Ob diese Vermutungen ausreichen, die Zurechnung einer Attacke zu begründen, bleibt offen. Weitreichendere Vorschläge²⁸ sprechen gar von einem gänzlichen Verzicht der Kausalität einer Zurechnung, sofern sich eine solche Attacke

²⁶ Vgl. Deutscher Bundestag, „Anwendbarkeit des humanitären Völkerrechts auf Computernetzwerkoperationen und digitale Kriegsführung (Cyber Warfare)“, Seite 11 f.

²⁷ Vgl. Peter Schmitz, „Die Urheber von Cyberangriffen erkennen“, security-insider.de, zugegriffen 14. Juni 2021, <https://www.security-insider.de/die-urheber-von-cyberangriffen-erkennen-a-826615/>

²⁸ Vgl. Sean M Condon, „Getting It Right: Protecting American Critical Infrastructure in Cyberspace“ Band 20, Nr. 2 (2007), <https://jolt.law.harvard.edu/assets/articlePDFs/v20/20HarvJLTech403.pdf>

gegen KRITIS richtet. Dort spricht man von der Tatsache, ob ein Staat mit der Gegenmaßnahme leben muss, wenn er toleriert, dass von seinem Boden aus ein Cyberangriff ausgeht. Auswege aus dem Dilemma sollen internationale Kooperationsrichtlinien bieten, die der Autor im Kapitel 2.2 vorstellt.

2.2 Rechtliche Entwicklungen

Wie das vorherige Kapitel aufzeigen konnte, herrscht in der digitalen Kriegsführung Klärungsbedarf. Die Bedrohung durch Cyberkriminelle stellt ein weiteres Problem dar, welches in Kapitel 3.3 näher beleuchtet wird. Im regulatorischen Kontext eines völkerrechtlich relevanten Konflikts befindet sich in den letzten Jahren einiges in Bewegung. Generell herrscht unter den staatlichen Akteuren der westlichen Welt Einigkeit. Staaten wie Russland und China unterscheiden sich, insbesondere hinsichtlich der Cyberkriminalität, von den Sichtweisen der westlichen UN-Mitglieder²⁹.

Das Tallinn Manual bietet einen Startpunkt zur Diskussion einer Anpassung des Völkerrechts. Es ist das erste Dokument für diesen Bereich.

2.2.1 Tallinn Manual

Die akademisch, nicht bindende Studie von 2013³⁰ stellt eine erste maßgebliche Neufassung der Anwendung und Auslegung des Völkerrechts im Cyberkontext dar. Trotz ihres nicht bindenden Charakters war davon auszugehen, dass dieses Handbuch Auswirkungen auf die Ansätze und Positionen von Staaten und Organisationen hat. Die Herangehensweise eines nicht bindenden Handbuchs ist nicht neu. Bereits in den “Manual on International Law Applicable to

²⁹ Vgl. Allison Peters, „Russia and China Are Trying to Set the U.N.’s Rules on Cybercrime“, *foreignpolicy.com*, zugegriffen 14. Juni 2021, <https://foreignpolicy.com/2019/09/16/russia-and-china-are-trying-to-set-the-u-n-s-rules-on-cybercrime/>

³⁰ Vgl. Komitee unter Führung von Michael N. Schmitt nach Einladung der NATO Cooperative Cyber Defence Centre of Excellence, „Tallinn Manual“, *issuu.com*, zugegriffen 14. April 2021, https://issuu.com/nato_ccd_coe/docs/tallinmanual

Armed Conflicts at Sea”³¹ und den “Manual on International Law Applicable to Air and Missile Warfare”³² wurden Grundlagen für eine weitere Entwicklung geschaffen.

Verfasst von einer Expertengruppe um Michael N. Schmitt auf Einladung des NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) legt das Tallinn Manual sogenannte „black letter rules“ fest, die sich analog zu „black letter laws“ verstehen lassen. Dies sind im juristischen Sprachgebrauch Gesetze, die allgemein bekannt und akzeptiert sind und keiner Diskussion mehr ausgesetzt werden sollen.³³ Im Kontext des Manuals heißt das, dass sich das Expertenteam auf die entstandenen Regeln einigen konnte. Zu jeder Regel liegen Kommentare vor, die Meinungsverschiedenheiten der AutorInnen über die genaue Anwendung enthalten und allgemein einen kritischen Zweck haben sollen. Zusätzlich identifizieren die Kommentare Rechtsgrundlagen, gehen auf den Inhalt der Regeln ein und sollen praktische Auswirkungen auf den Cyberkontext liefern.

Als neutrale BeobachterIn im Entwicklungsprozess diente das International Committee of the Red Cross (ICRC). Im Februar 2017 folgte das Tallinn Manual 2.0 in Buchform, das den Umfang auf Cyber-Operationen, nicht nur Konflikte, erweitert.³⁴ Die erste Fassung des Manuals hat den Schwerpunkt in der Diskussion zerstörerischer Cyber-Konflikte, die als bewaffnete Angriffe gelten und Staaten berechtigen, auf diese in Notwehr reagieren zu können und solche, die während eines konventionellen Konflikts eingesetzt werden. Im Tallinn 2.0 Manual wird der internationale Rechtsrahmen untersucht, der für Cyber-Operationen dient, die an der Schwelle zur Anwendung des Völkerrechts liegen.

In der Einleitung des Tallinn Manuals 2.0 stellen die VerfasserInnen direkt klar:

³¹ „Treaties, States parties, and Commentaries - San Remo Manual on Armed Conflicts at Sea“, icrc.org, zugegriffen 14. Juni 2021, <https://ihl-databases.icrc.org/ihl/INTRO/560>

³² „Manual on International Law Applicable to Air and Missile Warfare“, reliefweb.int, zugegriffen 14. Juni 2021, <https://reliefweb.int/sites/reliefweb.int/files/resources/8B2E79FC145BFB3D492576E00021ED34-HPCR-may2009.pdf>

³³ „Definition ‚Black-Letter Law‘“, oxfordreference.com, zugegriffen 21. April 2021, <https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095510675>

³⁴ Vgl. Komitee unter Führung von Michael N. Schmitt nach Einladung der NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0* (Cambridge, Vereinigtes Königreich: Cambridge University Press, 2017)

“Ultimately, Tallinn Manual 2.0 must be understood only as an expression of the opinions of the two International Groups of Experts as to the state of the law... This Manual is meant to be a reflection of the law as it existed at the point of Manual’s adoption by the two International Groups of Expert in June 2016.”³⁵

Das Handbuch stellt und soll auch keinen neuen Standard der Rechtsprechung darstellen. Es ist eine Auslegung der momentanen Strukturen für den digitalen Raum, um eine längere Diskussion in Gang zu setzen.

Eine der wichtigsten Regeln des Handbuchs im Kontext der KRITIS stellt die Nummer 80 dar. Hier wird Rücksicht auf die Zivilbevölkerung gefordert, indem keine KRITIS-Betreiber wie Atomkraftwerke, Staudämme oder auch medizinische Einrichtungen Opfer eines Cyberangriffes werden sollen.

Generell liefern die vorderen Regeln auch einiges an Diskussionsbedarf. Das Manual besagt, dass Staaten keine Hoheit über das gesamte Internet besitzen können. Sie halten die Hoheit nur über Teile des Webs innerhalb ihrer territorialen Grenzen inne.

Das Handbuch liefert eine Vielzahl an Regeln, die als Ansätze für Modifikationen des Völkerrechts dienen können. Es wird zum Beispiel in Regel zehn vorgeschlagen, dass Gewaltanwendung in Form eines Angriffes, egal ob Cyber oder Non-Cyber, stets eine Völkerrechtsverletzung darstellt. Über die elfte Regel wird eine Auswahl an Faktoren mitgeliefert, die zur Bewertung eines solchen Angriffes dienen können, mit.

Wichtig ist in diesem Zusammenhang auch die Definition eines/r HaktivistIn zu nennen, der/die gemäß Glossar des Manuals ein/e private/r BürgerIn darstellt, der/die sich auf eigene Initiative in einen Konflikt einmischt und so den Non-KombattantInnen-Status verliert. Das geschieht auch unter dem Gesichtspunkt der direkten Partizipation. Dies bezeichnet eine Aktion wie das Identifizieren einer Schwachstelle oder das Entwickeln von Malware für eine solche Schwachstelle zur Verwendung in einem Konflikt. Strafbar wäre dies nur nicht, wenn diese Malware öffentlich zur Verfügung gestellt wird.

So wie jeder neue Ansatz unterliegt dieser ebenso einer kritischen Bewertung. Beispielsweise spricht man auf medium.com³⁶ von der Einseitigkeit des Ergebnisses. Staatliche Meinungen, insbesondere von Nicht-NATO-Staaten, seien zu wenig berücksichtigt worden. Außerdem bedarf

³⁵ Komitee unter Führung von Michael N. Schmitt, Tallinn Manual 2.0

³⁶ Vgl. TheCyberDiplomat, „Tallinn Manual — A Brief Review of the International Law Applicable to Cyber Operations“, medium.com, zugegriffen 21. April 2021, <https://medium.com/@cyberdiplomacy/tallinn-manual-a-brief-review-of-the-international-law-applicable-to-cyber-operations-5643c886d9e2>

es einer weiteren Version, in der Rechenschaftspflichten von Staaten für Cyber-Operationen definiert werden, damit Stellvertreterkriege ausgeschlossen werden können. Zusätzlich soll Cyberspionage als rechtswidrig erklärt werden. Eine neue Version in Form des Tallinn Manuals 3.0 befindet sich derzeit in Entwicklung und in einer Vorab-Feedback-Phase für Interessierte und WissensträgerInnen³⁷.

Nichtsdestotrotz stellt das Handbuch einen Startpunkt einer Diskussion über den Umgang mit den neuen Gefahren im digitalen Raum dar. Im nächsten Schritt liegt die Verantwortung bei den Staaten und Staatengemeinschaften weiterzugehen und sich zu positionieren.

2.2.2 Positionspapiere

Als Folge des Tallinn Manuals erschienen diverse Positionspapiere von denen zwei im Folgenden kurz vorgestellt werden.

International Committee of the Red Cross

Das ICRC stellt in ihrem Papier³⁸ klar, dass im Kontext eines bewaffneten Konflikts, zivile Infrastruktur bei Cyberattacken über die existierenden Regeln des humanitären Völkerrechts geschützt ist. Genauer gesagt wird jede Benutzung von Gewalt, ob kinetisch oder Cyber, über die Anwendung der Charta der Vereinten Nationen und die Prinzipien des Völkerrechts geregelt. Sie erklären zudem, dass das Anwenden von Cyber-Operationen in einem Konflikt ein echtes Risiko für die Zivilbevölkerung darstellt. Die Staaten müssen feststellen, ob das geltende Recht angemessen und ausreichend ist, um die Herausforderungen zu bewältigen, die sich aus dem vernetzten und weitgehend digitalen Charakter des Cyberspace ergeben.

³⁷ NATO CCDCOE, „CCDCOE to Host the Tallinn Manual 3.0 Process“, ccdcoe.org, zugegriffen 21. Mai 2021, <https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/>

³⁸ Vgl. International Committee of the Red Cross, „International Humanitarian Law and Cyber Operations during Armed Conflicts“, zugegriffen 14. April 2021, <https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts>

Deutsche Bundesregierung

Die deutsche Bundesregierung (DBReg) ist in Ihrer Ausarbeitung³⁹ vom März 2021 der Überzeugung, dass sich das humanitäre Völkerrecht eins zu eins auf den Cyberraum übertragen lässt. Der digitale Raum besitzt territoriale Grenzen, in denen physische Infrastruktur für digitale Kriegsführung verwendet wird. Gleichzeitig stimmt die DBReg dem Tallinn Manual 2.0 zu, dass Operationen im Cyber-Raum, die zu physischen Auswirkungen und Schäden führen, eine Verletzung der staatlichen Souveränität des Opfers darstellen. Präzisiert legt die Regierung fest, dass jegliche Auswirkung auf Kritische Infrastrukturen eines Staates, eine Verletzung darstellen. Da international jedoch unterschiedliche Definitionen eines KRITIS-Betreibers existieren, kann es bei diesem Punkt zu Streitigkeiten kommen. Bislang überschritt die große Mehrheit an schädlichen Cyber-Operationen nicht die Schwelle zum Verstoß des Völkerrechts. Ein Extremfall kann jedoch absolut im Geltungsbereich des Verbots zur Anwendung von Gewalt liegen und somit zum Verstoß des Völkerrechts führen. Handlungen nicht staatlicher Akteure werden zur Verantwortung eines Staates zugeordnet, wenn der Akteur im Auftrag oder unter Kontrolle des Staates gehandelt hat. Die DBReg stellt fest, dass die internationale Rechtsprechung in der Lage ist, wesentliche Leitlinien für das Verhalten von Staaten im digitalen Raum zur Verfügung zu stellen. Gleichzeitig sollen Unsicherheiten in der Auslegung des Völkerrechts durch die Staatengemeinschaft angegangen und beseitigt werden.

2.2.3 EU Cybersecurity Act

Die europäische Verordnung (EU) 881/2019⁴⁰ oder auch EU Cybersecurity Act, die im Juni 2019 in Kraft trat, hat im Wesentlichen zwei Dinge zum Ziel:

1. Stärkung des Mandats der EU-Cybersicherheitsagentur der Europäischen Union für Netz- und Informationssicherheit (ENISA)
2. Schaffung eines EU-weit geltenden Rahmenwerks für eine IT-Sicherheitszertifizierung von Produkten, Dienstleistungen und Prozessen

³⁹ Vgl. Auswärtiges Amt, Bundesregierung Deutschland, „On the Application of International Law in Cyberspace“, zugegriffen 14. April 2021, <https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf>

⁴⁰ Vgl. Europäische Kommission, „The EU Cybersecurity Act“, [digital-strategy.ec.europa.eu](https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act), zugegriffen 28. April 2021, <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>

Durch die Mandatsstärkung der ENISA sollen finanzielle und personelle Mittel aufgestockt werden. Dadurch wird die Cybersicherheitskapazität und die Abwehrbereitschaft in allen Bereichen gestärkt. Unter anderem soll in diesem Zuge in Form der ENISA ein zentrales Kompetenzzentrum für Unternehmen und BürgerInnen geschaffen werden, in dem Rahmenbedingungen für eine gebündelte Cybersicherheit etabliert und Sensibilisierungsmaßnahmen durchgeführt werden. Diese Form der Zentralisierung spielt auch bei dem Zertifizierungsrahmenwerk eine Rolle. Vereint in einer Anlaufstelle sollen hier die Anforderungen an die Erfüllung der benötigten IT-Sicherheit betrachtet werden. Die Kritikalität des zu zertifizierenden Produktes, der Dienstleistung oder des Prozesses wird mit geprüft. Damit wird in der Europäischen Union das erste Mal „Security by Design“ und „Security bei Default“ in einer gültigen Regelung festgeschrieben. Mit der Anwendung dieser Begriffe legt man laut der Definition Markus Wagners von TÜV NORD fest, dass:

„[...] Sicherheitsanforderungen an Soft- und Hardware schon während der Entwicklungsphase eines Produktes berücksichtigt werden, um spätere Sicherheitslücken zu verhindern.“⁴¹

Dieser Vorstoß ist vergleichbar mit der Datenschutz-Grundverordnung der EU. Mit diesen Maßnahmen soll die Transparenz von IT-Produkten für VerbraucherInnen und deren Sicherheit verbessert werden. Gleichzeitig ist dies ein Ansatz, einer Fragmentierung entgegenzuwirken und eine einheitliche Regelung für die gesamte EU zu bewirken. Nationale Gesetzgebungen wie das jüngst in Kraft getretene IT-Sicherheitsgesetz 2.0 sollen sich daran orientieren.

2.2.4 Überarbeitung der EU Richtlinien NIS und ECI

Ebenso auf der Flughöhe Europa befinden sich derzeit zwei Richtlinien des europäischen Parlaments in Überarbeitung. Die Richtlinie NIS 2016/1148⁴² von 2016 hat sich zum Ziel gesetzt, die IT-Sicherheit in der EU in den Sektoren Energie, Wasserversorgung und Gesundheit zu verbessern. Kernforderungen liegen in der Erstellung einer nationalen Cybersicherheitsstrategie, die Benennung einer national zuständigen Behörde und die Einrichtung von Notfallkontakten in der Behörde und den Kritischen Infrastrukturen zur schnelleren Meldung von Vorfällen. Die

⁴¹ Markus Wagner TÜV NORD, „Security by Design - erklärt“, [tuev-nord.de](https://www.tuev-nord.de), zugegriffen 2. Mai 2021, <https://www.tuev-nord.de/explore/de/erklaert/security-by-design/>

⁴² NIS 2016/1148 Richtlinie

Erneuerung in Form der NIS 2.0⁴³ Direktive soll an aktuelle Bedürfnisse angepasst und zukunftssicher sein. Durch das Hinzufügen von weiteren kritischen Sektoren für Wirtschaft und Gesellschaft und das Schaffen eines Schwellenwerts der KRITIS-Einordnung soll eine klarere Einordnung der Unternehmen stattfinden. Außerdem werden weitere Sicherheitsanforderungen, wie die Einführung eines Risikomanagementsystems, vorgeschlagen. Risiken sollen dann nicht nur für das Unternehmen, sondern auch für dessen Lieferketten erhoben werden. Die Richtlinie peilt die Harmonisierung der Detektion und Registrierung von Sicherheitslücken über alle EU-Mitgliedsstaaten hinweg an und soll dabei auch strengere Durchsetzungsvorschriften, sowie einheitliche Sanktionsregelungen festlegen. Durch die Schaffung eines durch ENISA betriebenen Registers für offene Sicherheitslücken in der EU soll die Resilienz ganzheitlich gestärkt werden. Die aus dem Jahre 2008 stammende European Critical Infrastructure (ECI) 2008/114/EG⁴⁴ Richtlinie wird durch die neue Resilience of critical Entities (RCE)⁴⁵ Direktive ersetzt. Die ECI-Richtlinie beschränkte sich auf die EU-weiten KRITIS-Sektoren Energie und Transport und sollte diese identifizieren und einen Schutz festlegen. In der RCE Fassung wird sich direkt mit der Resilienz kritischer Dienstleistungen befasst. Staaten werden dazu verpflichtet, kritische Einheiten innerhalb ihrer Nation zu identifizieren und Risikoanalysen für die Einrichtungen durchzusetzen. In Folge der Analysen sollen technische und organisatorische Maßnahmen ergriffen werden, welche die Widerstandsfähigkeit erhöhen sollen.

Die AG KRITIS nahm die Änderungspläne des Europäischen Parlaments unter die Lupe und fasst die Erkenntnisse in einer Bewertung zusammen.⁴⁶ Aus dem Ende der Bewertung lässt sich ein Zitat anbringen:

⁴³ Vgl. Europäische Kommission, „Proposal for directive on measures for high common level of cybersecurity across the Union | Shaping Europe’s digital future“, digital-strategy.ec.europa.eu, zugegriffen 9. Mai 2021, <https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union>

⁴⁴ „ECI 2008/114/EG Richtlinie“ (2008), <http://data.europa.eu/eli/dir/2008/114/oj/deu>

⁴⁵ Vgl. Europäische Kommission, „Richtlinie Resilience of critical Entities“, ec.europa.eu, zugegriffen 15. Juni 2021, https://ec.europa.eu/home-affairs/sites/default/files/pdf/15122020_proposal_directive_resilienc_e_critical_entities_com-2020-829_en.pdf

⁴⁶ Vgl. Arbeitsgruppe Kritische Infrastrukturen, „Bewertung der EU-NIS und EU-RCI Richtlinie“, ag.kritis.info, zugegriffen 2. Mai 2021, <https://ag.kritis.info/2021/04/26/bewertung-der-eu-nis-und-eu-rci-richtlinie/>

„Die neuen Entwürfe sind ein Schritt in die richtige Richtung und beinhalten relevante Klarstellungen, insbesondere was die europäische Zusammenarbeit angeht. Auf der technischen Arbeitsebene und dem konkreten Schutz von Kritischen Infrastrukturen, sowie der Vorbereitung auf Großschadenslagen sehen wir allerdings noch deutliches Potenzial, welches hier noch nicht ausgeschöpft wird.“

Die geplanten Maßnahmen werden durch die AG KRITIS positiv aufgenommen. Jedoch gehen sie für einen praktischen Schutz von KRITIS inklusive einer verstärkten Krisenresilienz nicht weit genug.

Zusätzlich widersprechen die geplanten Richtlinien laut VerfasserInnen in einigen Punkten, wie einer rein defensiven Cybersicherheitsstrategie, den politischen Forderungen der Arbeitsgruppe, die näher unter Kapitel 5.3 – Externe Bedingungen erläutert werden.

2.2.5 Non-Paper on Cyber Diplomacy eines Staatenverbunds

Das Diskussionspapier⁴⁷ der Staaten Estland, Frankreich, Polen, Portugal und Slowenien unter der Führung von Deutschland beschäftigt sich mit den ändernden Bedingungen in der Welt und liefert Vorschläge, wie man die Herausforderungen der kommenden Jahre in puncto Cyberspace als Europäische Union angehen könnte.

Neben den Commitments zur Schaffung und Wahrung eines freien und demokratischen Cyberspace, legt dieses Papier nahe, dass die EU vollständig bestätigen soll, dass die Charta der Vereinten Nationen und das Humanitäre Völkerrecht uneingeschränkt im digitalen Raum angewendet werden können. Zusammen mit den Vereinten Nationen soll ein gemeinsamer verantwortungsvoller Verhaltenskodex für Staaten im Cyberraum erarbeitet werden, um zum einen die zentralen Menschenrechte und zum anderen die digitale Souveränität eines jeden Staates sicherstellen zu können. In der EU wurde 2017 hierzu die Cyber Diplomacy Toolbox⁴⁸ ins Leben gerufen. Diese Werkzeugkiste liefert Instrumente, um schadhafte Cyberaktivitäten vorzubeugen,

⁴⁷ Vgl. Auswärtiges Amt, „EU Cyber Diplomacy – Working Together for a Free and Secure Cyberspace“, [auswaertiges-amt.de](https://www.auswaertiges-amt.de/en/aussepolitik/themen/eu-cyber-non-paper/2418984), zugegriffen 2. Mai 2021, <https://www.auswaertiges-amt.de/en/aussepolitik/themen/eu-cyber-non-paper/2418984>

⁴⁸ Vgl. Rat der EU, „Cyberangriffe: EU plant Gegenmaßnahmen, einschließlich Sanktionen“, [europa.eu](https://www.consilium.europa.eu/de/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/), zugegriffen 14. Juni 2021, <https://www.consilium.europa.eu/de/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/>

abzuschrecken oder geeignete und angemessene Gegenmaßnahmen treffen zu können. Dadurch soll das Verhalten von Staaten und anderen Akteuren nachhaltig beeinflusst werden. Das Schreiben verpflichtet sich außerdem zu einer internationalen Vorgehensweise, um einer ansteigenden Fragmentierung des Internets entgegenzuwirken.

2.2.6 Cyber-Sicherheitsstrategie Deutschland für 2021

In eine ähnliche Richtung geht auch die Cyber-Sicherheitsstrategie Deutschlands⁴⁹ für 2021, die sich noch im Erstellungsprozess befindet. In vier Handlungsfelder unterteilt, wird hier laut BMI regulatorisch an einer sicheren und freien Zukunft des Cyberspace geschrieben. Auch hier spricht man von einer benötigten Einbettung der nationalen und europäischen Maßnahmen in internationale Prozesse, um aufgrund der transnationalen Vernetzung ein hohes Niveau der Schadensresilienz erreichen zu können. Zum Ende der Erstellung dieser Arbeit wurde ein erster Entwurf der Cyber-Sicherheitsstrategie zur Kommentierung durch sachkundige Fachleute freigegeben.⁵⁰ Die Inhalte der Strategie gehen in eine ähnliche Richtung wie beim IT-Sicherheitsgesetz 2.0, das im nächsten Kapitel vorgestellt wird. Die Ansätze Deutschlands zum Schutz des Cyberspace laufen Bestrebungen des Tallinn Manuals konträr. Einige Punkte der geplanten Strategie beinhalten unter Kapitel 8.3 die Stärkung von Sicherheitsbehörden zur Überwachung, Grundgesetzänderungen zur Anwendung von Hackbacks und das Entwickeln und Ausnutzen von Zero-Day-Exploits. Diese Exploits sind Schwachstellen, die bei Kenntniserlangung der Existenz einer Lücke für eine spätere Ausnutzung durch Nachrichtendienste oder Strafverfolgungsbehörden geheim gehalten werden. Die angedachte Legitimation von Hackbacks zur Stärkung der deutschen Gefahrenabwehr im Cyberraum kann nicht gültig durchgeführt werden. Wie Kapitel 2.1.3 aufzeigen konnte, ist eine zweifelsfreie Attribution eines Cyberangriffs nach derzeitigem Stand schlicht nicht möglich. Dadurch ist ein völkerrechtlich korrekter Hackback, also ein aktiver Gegenschlag im Cyberkontext, nicht umsetzbar.

⁴⁹ Vgl. Nationaler Cybersicherheitsrat, „Cyber-Sicherheitsstrategie für Deutschland“, bmi.bund.de, zugegriffen 4. Mai 2021, <http://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cyber-sicherheitsstrategie/cyber-sicherheitsstrategie-artikel.html>

⁵⁰ Bundesministerium des Innern, für Bau und Heimat, „Jetzt Stellung nehmen: Entwurf der Cybersicherheitsstrategie 2021“, bmi.bund.de, zugegriffen 10. Juni 2021, <http://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2021/06/css-2021-beteiligungsformat.html>

2.2.7 IT-Sicherheitsgesetz 2.0

Am 23. April 2021 stimmte der Deutsche Bundestag der finalen Fassung des IT-Sicherheitsgesetzes 2.0 (IT-SiG 2.0)⁵¹ zu, das offiziell am 28.05.2021 in Kraft trat. Das vom BMI erarbeitete Gesetz dient der Erhöhung der Sicherheit von informationstechnischen Systemen.

Der Vorgänger, das IT-Sicherheitsgesetz (IT-SiG 1.0)⁵², etablierte nach seinem Inkrafttreten am 25. Juli 2015 Sicherheitsanforderungen für KRITIS, wie die Schaffung eines Mindeststandards für Informationssicherheit in Form der Verpflichtung zur Etablierung eines Information Security Managementsystems (ISMS). In der dazugehörigen KRITIS-Verordnungen BSI-KritisV wird geregelt, welche Einrichtungen und Anlagen unter das Gesetz fallen.

In der neuen Gesetzesversion sollen vier Bereiche gestärkt werden. Das BSI erhält eine erweiterte Kontroll- und Prüfbefugnis. Es soll in der Lage sein, Sicherheitslücken zu detektieren, Schadprogramme zu analysieren und Angriffsmethoden einsetzen zu können. Außerdem soll der Verbraucherschutz durch die Etablierung einer Bestandsdatenauskunft für Hersteller von IT-Produkten gestärkt werden. Zusätzlich wird die unternehmerische Vorsorgepflicht von KRITIS-Betreibern erhöht. Diese sollen Systeme zur Frühwarnerkennung implementieren. Eine Meldepflicht von Vorfällen wird auf weitere Unternehmenszweige der KRITIS ausgeweitet. Im Allgemeinen hat das Gesetz zum Ziel, die staatliche Schutzfunktion der zivilen und wirtschaftlichen Infrastrukturen zu fördern. Da das Gesetz vor der NIS 2.0 Richtlinie verabschiedet wurde, aber auf dieser aufbauen soll, wird eine baldige Anpassung des IT-SiG 2.0 an die Anforderungen der EU-Richtlinie in Form eines dritten Sicherheitsgesetzes erwartet.

Die AG KRITIS meldet sich auch hier wieder mit einer Stellungnahme⁵³ zu Wort und kritisiert das Gesetz auf ganzer Linie. Die Arbeitsgruppe bezeugt dem Entwurf einer unklaren Linie zur tatsächlichen Erhöhung des Sicherheitsniveaus von IT-Systemen und KRITIS. Vielmehr stellt das Gesetz in den Augen der VerfasserInnen eine Ansammlung unabgestimmter und ineffektiver

⁵¹ Vgl. Bundesministerium des Innern, für Bau und Heimat, „Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)“, bmi.bund.de, zugegriffen 22. April 2021, <http://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/entwurf-zweites-it-sicherheitsgesetz.html>

⁵² Vgl. Bundesamt für Sicherheit in der Informationstechnik, „Das IT-Sicherheitsgesetz“, bsi.bund.de, zugegriffen 21. Mai 2021, https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/it_sig.html

⁵³ Vgl. Manuel Atug, „Stellungnahme zum IT-SiG 2.0 für die Anhörung des Bundestagsausschusses für Inneres und Heimat“, bundestag.de, zugegriffen 22. April 2021, <https://www.bundestag.de/resource/blob/825126/c932641828f11342efb2fbf372fa3dbc/A-Drs-19-4-741-C-data.pdf>

Maßnahmen dar. Zusätzlich läuft der Entwurf der EU-Strategie aufgrund seiner Vorveröffentlichung konträr, nationale Gesetzgebungen in europäische und internationale Prozesse einzubetten und eine Strategie der Harmonisierung zu verfolgen. Im Rahmen des IT-SiG 2.0 führt die Anpassung des BSI-Gesetzes dazu, dass das BSI fortwährend den Fokus einer Hackerbehörde einnimmt⁵⁴. Wie die Überarbeitung des BND-Gesetzes, in welcher der Bundesnachrichtendienst (BND) das legitimierte Recht erhält, Freundstaaten auszuhören⁵⁵, schlägt auch das BSI-Gesetz in die gleiche Kerbe und sendet falsche Signale an die Weltgemeinschaft. Mit dem EU Cybersecurity Act und der geplanten NIS 2.0 Richtlinie werden wichtige Schritte hin zu einer gemeinsamen und sichereren IT-Umgebung in Europa gemacht. Die Schaffung eines Registers für offene Sicherheitslücken und eine Zentralisierung von Sicherheitsthemen sind wichtige Schritte. Das IT-SiG 2.0 widerspricht, genauso wie der erste Entwurf der Cyber-Sicherheitsstrategie 2021, diesen Ansätzen dagegen in einigen Punkten, wie das Zurückhalten von Sicherheitslücken. Die Intention verletzt auch die Erkenntnisse des Tallinn Manuals 2.0 zur direkten Partizipation, wie in Kapitel 2.2.1 vorgestellt. Wenn man Schwachstellen identifiziert und nicht der Öffentlichkeit zur Verfügung stellt, wird man im Rahmen eines Cyber Wars zum/zur KombattantIn. Zusätzlich wird das Gesetz um drei Unternehmensbereiche erweitert, was schlussendlich eine Vermengung der deutschen Rüstungsindustrie mit dem Schutz der Zivilbevölkerung zur Folge hat.

2.2.8 Fazit zur Rechtslage

Wie die Analyse des rechtlichen Rahmens aufzeigt, befindet sich zur Erstellungszeit dieser Arbeit viel Bewegung in der Thematik. Viele Staaten sind gewillt, eine vollständige Etablierung des humanitären Völkerrechts für den Cyberraum vorzunehmen. Hier liegt jedoch Handlungsbedarf für die Staatengemeinschaft. Die momentane Definition von KombattantInnen bei kinetischen Wirkmitteln lässt sich nicht auf Digitalwaffen anwenden. Insbesondere wenn Cyber-Operationen unterhalb oder an der Schwelle zu einem bewaffneten Konflikt stehen, sind Unklarheiten vorhanden. Die Attribution von Cyberangriffen und somit die Legitimation von

⁵⁴ Vgl. Andre Meister, „IT-Sicherheitsgesetz 2.0: Seehofer will BSI zur Hackerbehörde ausbauen“, netzpolitik.org, zugegriffen 22. Mai 2021, <https://netzpolitik.org/2020/seehofer-will-bsi-zur-hackerbehoerde-ausbauen/>

⁵⁵ Vgl. Andre Meister, „BND-Gesetz: Bundesnachrichtendienst erhält so viele Überwachungsbefugnisse wie noch nie“, zugegriffen 22. Mai 2021, <https://netzpolitik.org/2021/bnd-gesetz-bundesnachrichtendienst-erhaelt-so-viele-ueberwachungsbefugnisse-wie-noch-nie/>

Gegenmaßnahmen und das Führen eines völkerrechtlich akzeptierten Konflikts ist nach jetzigem technologischen Stand nicht möglich. Das aktive Ausnutzen der Grauzone der Cyberspionage, zu sehen in BND- und BSI-Gesetz, ist gängige Praxis unter einer Mehrheit an Staaten. Dies schafft zunehmend Spannungen in den diplomatischen Beziehungen und bedroht somit auch KRITIS. Es sind eine Vielzahl an weitestgehend übereinstimmenden Richtungsgebungen oder Absichtserklärungen vorhanden. Eine global verpflichtende Regelung, wie eine Verbannung der Digitalwaffen, fehlt jedoch. Deutschland bewegt sich selbst in eine offensivere Cyber-Strategie. Somit muss man dem Internet bis zu einem gewissen Grad die Rechtsfreiheit bezeugen. Auch deswegen ist es ratsam, sich der Gefahrenlage bewusst zu sein und sich entsprechend präventiv auf eine mögliche Großschadenslage im Cyberraum, sei es hervorgerufen durch einen Krieg oder einen Unfall, vorzubereiten und sich bestmöglich selbst zu schützen. Dieser geopolitische Ansatz sollte dann, wie von den politischen EntscheidungsträgerInnen angedacht, in eine globale Harmonisierung eingebettet werden.

2.3 Bestehende Institutionen

Präventive Organisationseinheiten, die auf Freiwilligenbasis beruhen, sind in Deutschland und in der Welt nichts gänzlich Neues. Folglich stellt der Autor drei Institutionen vor, die Deutschland als Inspirationshilfe für eine bessere Cybersicherheit dienen können. Das THW ist für den klassischen Katastrophenfall ein exzellentes Beispiel für ehrenamtliche Mithilfe. Die Cyber Unit Estlands zeigt auf, dass das Prinzip des Ehrenamts auch auf den Cyberraum übertragen werden kann. Anhand des Critical Infrastructure Cyber Community (C3) Volontariat der USA ist zu sehen, dass eine Partnerschaft aus Wirtschaft, WissensträgerInnen und Staat eine Lernkultur mit Verbesserung der Schadensresilienz für alle Beteiligten fördern kann. Die genannten Institutionen werden nun näher erläutert.

2.3.1 Technisches Hilfswerk in Deutschland

Die Zivil- und Katastrophenschutzorganisation THW⁵⁶ ist eine Bundesanstalt des öffentlichen Rechts im Geschäftsbereich des BMI. Als nicht-rechtsfähige⁵⁷ Einheit ist sie einem Träger der öffentlichen Verwaltung zugeordnet und dient dauerhaft einem öffentlichen Zweck. In Form einer Organisation des Zivilschutzes wird sie bei physischen Katastrophenfällen aktiviert und genießt eine hohe Reputation und Akzeptanz in der Bevölkerung und weltweit. Obwohl sie organisatorisch dem BMI zuzuordnen ist, besteht die deutliche Mehrheit (98 %) aus ehrenamtlich tätigen HelferInnen. Laut eigener Webseite passt sich das THW seit sieben Jahrzehnten flexibel den sich ändernden Gefahrenlagen an. Moderne Einsatzgeräte bilden, gepaart mit gut ausgebildeten SpezialistInnen, die Grundsäulen des erfolgreichen Handelns. Mit dem Gesetz über das Technische Hilfswerk (THW-Gesetz)⁵⁸ von 1990 wird der gesetzliche Auftrag der Bundesanstalt festgelegt. Das THW leistet Hilfe, wenn entweder von zuständigen Stellen der Gefahrenabwehr (wie die Feuerwehr) Hilfe ersucht wird oder sie von obersten Bundesbehörden angefordert werden. Dabei zeichnet sich die Bundesanstalt mit ihrer Breite an Einsatzoptionen, Kooperationen und der flächenmäßigen Ausbreitung aus. Sie kann Hilfe in den Bereichen Infrastruktur, Gefahrenabwehr und Versorgung der Bevölkerung leisten. Sie pflegt enge Beziehungen mit dem Deutschen Feuerwehrverband, der Johanniter-Unfall-Hilfe, dem Deutschen Roten Kreuz und vielen mehr. In 668 Ortsverbänden organisiert, die wiederum in Regionalstellen, Landesverbände, drei Ausbildungszentren und einer THW-Leitung verflochten sind, besteht über die gesamte Bundesrepublik ein Sicherheitsnetzwerk. Im Konzept ist für jeden Landkreis und jede kreisfreie Stadt ein Ortsverband vorgesehen. Alle Einheiten und Fachgruppen arbeiten ausschließlich defensiv. Das heißt zum Beispiel für die Fachgruppe Sprengen, dass sich diese trotz hoher Kenntnis in Sprengstofftechnik nicht an kriegerischen Maßnahmen der Bundeswehr beteiligen darf. Dadurch kann sich die Bundesanstalt den Non-KombattantInnen-Status in Konfliktgebieten erhalten.

⁵⁶ Technisches Hilfswerk, „Die Bundesanstalt Technisches Hilfswerk“, thw.de, zugegriffen 29. April 2021, https://www.thw.de/DE/THW/Bundesanstalt/bundesanstalt_node.html?noMobile=1

⁵⁷ Wissenschaftliche Dienste Deutscher Bundestag, „Bundesanstalten als nichtrechtsfähige Anstalt des Öffentlichen Rechts“, bundestag.de, zugegriffen 29. April 2021, <https://www.bundestag.de/resource/blob/413556/1189dabd6fd9f8569aueb35c619fcd06/WD-3-046-12-pdf-data.pdf>

⁵⁸ Vgl. Technisches Hilfswerk, „Gesetzlicher Auftrag des Technischen Hilfswerks“, thw.de, zugegriffen 29. April 2021, https://www.thw.de/DE/THW/Bundesanstalt/Auftrag/auftrag_node.html

2.3.2 Estlands Defence League Cyber Unit

Die Republik Estland gilt als weltweit erstes Opfer einer groß angelegten Cyberattacke, die sehr nah an der Schwelle zu einem Cyberkrieg liegt⁵⁹. Im April 2007 sind als Folge einer Umsetzung eines sowjetischen Kriegsdenkmals 58 Webseiten (darunter Staat, Zeitungen und Banken) mittels über Bot-Netzen ausgeführte Distributed Denial Of Service (DDoS) Attacken lahmgelegt worden. Der Angriff hielt mehrere Wochen an. Zum Ende gab es eine strafrechtliche Verurteilung. Eine schlüssige Schuldzurechnung an einen Staat konnte jedoch nicht bestimmt werden. Diese Attribution eines Cyberangriffs wird auch in Zukunft nur schwer möglich sein, wie Kapitel 2.1.3 aufzeigen konnte.

Seitdem hat das Land viel aus dieser stetigen Gefahr gelernt. Estland ist zu einem Vorreiter in Sachen IT-Sicherheit aufgestiegen. Sie beraten viele Nationen. Die NATO hält ihre größte Cyberübung „Locked Shields“ in Estland ab. Klaid Mägi, Head of Incident Response of Estonia, erklärt in einem Artikel der Regierungsseite e-estonia.com, dass Cybersicherheit nur in Kooperation zwischen Staat, Wirtschaft und BürgerInnen erfolgreich gestaltet werden kann.⁶⁰ Dadurch entstand die estländische „e-Residency“, eine vollständig digitale und sichere Staatsbürgerschaft Estlands. Auch ein 24/7 Monitoring von potenziellen Angriffen durch das Computer Emergency Response Team (CERT) deckt monatlich 300 Vorfälle auf, behandelt sie und schützt vor vielen weiteren Fällen durch frühzeitige Detektion.

Die Cyber Unit der Estonian Defence League (estnisch: *Kaitseliit*) (EDL CU)⁶¹ ist eine auf Freiwilligenbasis aufgestellte Organisation der estnischen Streitkräfte zum Schutz des Cyberspace. Sie setzt sich aus ExpertInnen der KRITIS Informationssicherheit, IT-Fachkräften und weiteren SpezialistInnen wie AnwältInnen und ÖkonomInnen zusammen, um die Resilienz Estlands vor Cyberangriffen zu erhöhen. Neben der Verstärkung des Netzwerks unter CyberexpertInnen und der Aus- und Weiterbildung dieser, wird die Sicherheit insbesondere für Kritische Infrastrukturen erhöht. Bei einem Ernstfall unterstützen die Mitglieder beim Krisenmanagement, indem sie KRITIS beschützen. Da die Cyber Unit innerhalb der Estonian Defence League organisiert ist, stellen ihre Mitglieder im Kriegsfall KombattantInnen nach humanitärem Völkerrecht dar. Sie führen zwar in erster Linie Aufgaben zum Schutz und zur

⁵⁹ Vgl. Thomas Reinhold, „Cyberattacke auf Estland“, cyber-peace.org, zugegriffen 29. April 2021, <https://cyber-peace.org/cyberpeace-cyberwar/relevante-cybervorfaelle/cyberattacke-auf-estland/>

⁶⁰ Vgl. „How Estonia Became a Global Heavyweight in Cyber Security“, investinestonia.com, zugegriffen 29. April 2021, <https://investinestonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/>

⁶¹ Vgl. Estonian Defence League, „EDL Cyber Unit“, kaitseliit.ee, zugegriffen 2. Mai 2021, <https://www.kaitseliit.ee/en/cyber-unit>

Unterstützung der Zivilbevölkerung durch, kooperieren und operieren aber auch auf Befehl der Regierung mit Polizei, anderen Verbänden des Militärs und den Einrichtungen der Gefahrenabwehr.

Laut Analyse der NATO CCD COE⁶² funktioniert dieses Konzept, weil es in Estland zwei Komponenten gibt, die zu einem Erfolg beitragen: Zum einen die stark ausgeprägte privat-öffentliche Kooperation in der IT-Sicherheit und zum anderen das schon lange existierende Konzept der Freiwilligenverbände der EDL mit der Bevölkerung. Bedenken liefern die AutorInnen bei dem Problem, dass ein Mitglied des Freiwilligenverbands im Kriegsfall als KombattantIn zu werten ist, da die EDL im Krieg direkt den estnischen Streitkräften unterstellt wird.

2.3.3 US amerikanisches C³ Programm für Volontäre

Die Cyber Unit Estlands stellt einen bislang einzigartigen Fall der privaten Mitwirkung bei der Cybersicherheit dar. Das C³⁶³ Volontariat der US amerikanischen Homeland Security wurde im Februar 2014 nach einer sogenannten Executive Order des damaligen Präsidenten Obama gestartet. Das Programm soll die Partnerschaft des privaten mit dem öffentlichen Sektor in Form der Homeland Security stärken, indem Organisationen geholfen werden, das durch das National Institute of Standards and Technology (NIST) entworfene Cybersecurity Framework zu etablieren und somit das Risikomanagement zu verbessern. Das auf Freiwilligenbasis bestehende System zielt darauf ab, die Kritischen Infrastrukturen des Landes zu schützen und ein Netzwerk der Partnerschaft zwischen Unternehmen, WissensträgerInnen und dem Staat aufzubauen⁶⁴. Dadurch sollen sich Best Practices besser und flächendeckender umsetzen lassen und eine Lernkultur etabliert werden.

⁶² Vgl. NATO CCDCOE: Kadri Kaska, Anna-Maria Osula, und LTC Jan Stinissen, „The Cyber Defence Unit of the Estonian Defence League“, ccdcoe.org, zugegriffen 7. Mai 2021, https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf

⁶³ Vgl. Cybersecurity & Infrastructure Security Agency, „Critical Infrastructure Cyber Community C³ Voluntary Program“, cisa.gov, zugegriffen 9. Mai 2021, <https://www.cisa.gov/ccubedvp>

⁶⁴ Vgl. Cybersecurity & Infrastructure Security Agency, „Resources Cybersecurity Framework“, us-cert.cisa.gov, zugegriffen 9. Mai 2021, <https://us-cert.cisa.gov/resources>

3 Status quo in Deutschland

3.1 Vorhandene Kapazitäten und Leistungsfähigkeit

Mit dem THW besteht in Deutschland für den klassischen, nicht-digitalen Katastrophenfall bereits eine gut funktionierende Einrichtung, die flächendeckend und schnell mit ihren rund 80.000 ehrenamtlichen HelferInnen Unterstützung leisten kann. Für eine Großschadenslage mit digitalem Hintergrund sehen vorhandene Kapazitäten deutlich rarer aus. Nach Anfrage eines Abgeordneten der FDP-Bundestagsfraktion lässt sich dies genau an der Antwort der Bundesregierung (Drucksache 19/2645 vom Juni 2018)⁶⁵ erkennen. Die beiden folgenden Kapitel beziehen sich auf diese Drucksache.

3.1.1 Überblick der CERTs

Zunächst sind in Deutschland verschiedene, dem BMI unterstellte, CERTs vorhanden. Diese Einheiten stellen Teams von SicherheitsexpertInnen und IT-Fachleuten dar, die an der Lösung von konkreten Sicherheitsvorfällen arbeiten oder davor warnen bzw. präventive Lösungsansätze liefern.⁶⁶

Als Erstes wäre hier das CERT-Bund⁶⁷ zu nennen, das hauptsächlich für Bundesbehörden tätig ist. Neben einer 24-Stunden-Rufbereitschaft, einem Analyse- und Lagezentrum und der aktiven Alarmierung der Bundesverwaltung unterstützt das CERT-Bund bei Sicherheitsvorfällen in der IT-Landschaft des Bundes. Anfragen aus der Privatwirtschaft werden zwar aufgenommen, aber

⁶⁵ Vgl. Bundesregierung Deutschland, „Drucksache 19/2645: Cyberabteilungen im Zuständigkeitsbereich der Bundesministerien“, bundestag.de, zugegriffen 14.04.2021, <https://dserver.bundestag.de/btd/19/026/1902645.pdf>

⁶⁶ Vgl. Stefan Lubert, „Was ist ein CERT?“, security-insider.de, zugegriffen 10. Mai 2021, <https://www.security-insider.de/was-ist-ein-cert-a-702654/>

⁶⁷ „CERT-Bund“, cert-bund.de, zugegriffen 14. Juni 2021, <https://www.cert-bund.de/>

nur nach verfügbaren Mitteln bearbeitet. Das CERT-Bund ist momentan mit etwa 20 Kräften besetzt.

Daran angegliedert existiert mit dem Bürger-CERT⁶⁸ eine Institution, die lediglich umfangreiche Informationen über aktuelle Angriffe, Sicherheitslücken und gefährliche Schadsoftware aufbereitet und für die Bevölkerung aufbereitet.

Auf europäischer Ebene liefert die Task Force CSIRT⁶⁹ (Computer Security Incident Response Team – synonym zu CERT) ein Netzwerk der Kooperation der nationalen CERTs, ohne geschlossen für die Zivilbevölkerung aktiv zu werden.

Das Nationale Cyber-Abwehrzentrum⁷⁰ (NCAZ) stellt einen Zusammenschluss deutscher Sicherheitsstellen wie BBK, BSI und BND dar, das Tätigkeiten zur Prävention, Information und Frühwarnung über Cyber-Angriffe durchführt.

Auch der Verwaltungs-CERT-Verbund⁷¹ (VCV) stellt eine Informationsaustauschplattform der CERTs des Bundes und der einzelnen Bundesländer dar. Inwieweit vorhanden und wie hoch die Bewältigungskapazitäten der unterschiedlichen CERTs der Bundesländer sind, ist der Öffentlichkeit nicht bekannt. Im Rahmen der Informationssicherheitsleitlinie in der öffentlichen Verwaltung von 2013⁷² haben sich jedoch alle Bundesländer zur Etablierung eines CERTs innerhalb von fünf Jahren verpflichtet. Das VCV lässt sich als behördliches Pendant zur Allianz für Cyber-Sicherheit⁷³ (ACS) verstehen. Die ACS beschäftigt sich hauptsächlich mit dem wirtschaftlichen Sektor und den privaten Betreibern von Kritischen Infrastrukturen. Als Initiative von BSI und dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom) hervorgegangen, verbinden sich über 4.000 Institutionen, um aktuelle und valide Informationen zu Gefährdungslagen bereitstellen zu können. Insbesondere Klein- und

⁶⁸ „Bürger-CERT“, [bsi.bund.de](https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html), zugegriffen 14. Juni 2021, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html

⁶⁹ „TF-CSIRT: Computer Security Incident Response Teams“, [geant.org](https://www.geant.org), zugegriffen 14. Juni 2021, https://www.geant.org:443/People/Community_Programme/Task_Forces/Pages/TF-CSIRT.aspx

⁷⁰ „BKA - Nationales Cyber-Abwehrzentrum“, [bka.de](https://www.bka.de), zugegriffen 14. Juni 2021, https://www.bka.de/DE/UnsereAufgaben/Kooperationen/NCAZ/ncaz_node.html

⁷¹ Oliver Wege, „Verwaltungs-CERT-Verbund“, [secupedia.info](https://www.secupedia.info), zugegriffen 13. Mai 2021, <https://www.secupedia.info/wiki/Verwaltungs-CERT-Verbund>

⁷² Deutscher IT-Planungsrat, „Leitlinie Informationssicherheit in der öffentlichen Verwaltung“, zugegriffen 13. Mai 2021, https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/10_Sitzung/Leitlinie_Informationssicherheit_Hauptdokument.html

⁷³ „Allianz für Cyber-Sicherheit - ACS“, [allianz-fuer-cybersicherheit.de](https://www.allianz-fuer-cybersicherheit.de), zugegriffen 13. Mai 2021, https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/home_node.html

Mittelständler stehen hier im Fokus, da diese häufig kein eigenes Know-how in der Cybersecurity aufgebaut haben. VCV und ACS haben zum Ziel, den Informationsaustausch zwischen den TeilnehmerInnen zu verstärken, um so eine effektivere und schnellere Antwort auf einen IT-Angriff durchführen zu können.

Mit dem CERT-Verbund⁷⁴ ist eine weitere Organisation zum Informationsaustausch zu nennen. Auch hier liegt der Fokus der TeilnehmerInnen auf den Informationsaustausch und einem koordinierten Response. Neben dem CERT-Bund befinden sich in dieser Vereinigung über 40 Mitglieder einschließlich der CERTs einiger DAX-Konzerne wie der Siemens AG und der Lufthansa Group.

Die öffentlich-private Kooperation UP KRITIS⁷⁵ bildet einen Zusammenschluss der Betreiber Kritischer Infrastrukturen mit den zuständigen staatlichen Stellen. Acht der neun KRITIS-Sektoren werden in der Kooperation abgebildet. Der Sektor „Staat und Verwaltung“ wird über den UP BUND abgedeckt. Das Ziel ist die Versorgungssicherheit von KRITIS für Deutschland aufrechtzuerhalten. Dabei will die Kooperation in präventiven Themen wie Informationsaustausch, Ausbau von Krisenmanagementsystemen und der Durchführung von Notfall- und Krisenübungen Synergien bilden. Gleichzeitig soll aber auch die koordinierte Krisenreaktion und -bewältigung verbessert werden. Streng nach Zielvorgabe der Bundesregierung „Prävention, Reaktion und Nachhaltigkeit“ gemäß nationalem Plan zum Schutz der Informationsinfrastrukturen werden konkrete Maßnahmen auch für engagierte Betreiber unter der Schwelle zum KRITIS-Unternehmen nach KritisV durchgeführt. Dabei gehen die zu behandelnden Themen auch über Informationstechnik in Richtung physischer Sicherheit hinaus. Wie das Kapitel zeigt, beschäftigen sich die Institutionen mit präventiven und informationstechnischen Themen. Reaktive Bewältigungsstrukturen sind nur für die eigenen Systeme vorhanden. Ein flächendeckendes System, das bei allen Szenarien helfen kann, ist nicht etabliert.

⁷⁴ Juergen Sander, „Überblick des CERT-Verbunds“, [cert-verbund.de](https://www.cert-verbund.de/), zugegriffen 9. Mai 2021, <https://www.cert-verbund.de/>

⁷⁵ Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, „Vorstellung UP KRITIS“, [kritis.bund.de](https://www.kritis.bund.de/), zugegriffen 13. Mai 2021, https://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/upk_node.html

3.1.2 BSI MIRT

In einem Ernstfall kann das BSI mit einem Mobile Incident Response Team (MIRT) den Bund, KRITIS oder reguläre Unternehmen aktiv im Feld unterstützen. Das MIRT soll sich dafür als Vor-Ort-Einsatztruppe aus ExpertInnen des CERT-Bunds zusammensetzen.⁷⁶ Dem MIRT stehen für ein KRITIS Einsatzszenario laut AG KRITIS⁷⁷ 15 MitarbeiterInnen zur Verfügung, die möglicherweise aus anderen Teilen des BSI, beispielsweise den Fachbereich Wirtschaft und Gesellschaft 1 für KRITIS⁷⁸, noch aufgestockt werden könnten. Das MIRT stellt somit die einzige Abteilung des BSI und des Bundes dar, die bei einer Großschadenslage aktiv bei Betreibern Kritischer Infrastrukturen tätig werden könnte.

3.1.3 Cyber-Sicherheitsnetzwerk des BSI

Das mit Start Oktober 2021 geplante Cyber-Sicherheitsnetzwerk (CSN) des BSI soll die reaktiven Handlungsfähigkeiten bei IT-Sicherheitsvorfällen für kleine und mittlere Unternehmen (KMU) sowie BürgerInnen steigern. Mit dem „BSI für Bürger“ und der ACS bestehen laut BSI ausreichend präventive Informationsplattformen für die Bevölkerung.⁷⁹ Durch die Schaffung des CSN soll eine dezentrale Struktur aufgebaut werden, die bestehende Dienstleistungen ergänzt und schnell und kostengünstig Hilfe leisten kann.

⁷⁶ Bundesamt für Sicherheit in der Informationstechnik, „Vorfallunterstützung – Mit CERT-Bund und MIRT“, bsi.bund.de, zugegriffen 10. Mai 2021, <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/CyberSicherheitslage/Reaktion/Vorfallunterstuetzung/MIRT/mirt.html>

⁷⁷ Vgl. Arbeitsgruppe Kritische Infrastrukturen, „Konzept Cyber-Hilfswerk“, Seite 6

⁷⁸ Bundesamt für Sicherheit in der Informationstechnik, „Abteilung WG - Cyber-Sicherheit für Wirtschaft und Gesellschaft“, bsi.bund.de, zugegriffen 13. Mai 2021, <https://www.bsi.bund.de/DE/Das-BSI/Organisation-und-Aufbau/Abteilungen-inkl-Organigramm/Abteilung-WG/abteilung-wg.html>

⁷⁹ Vgl. Bundesamt für Sicherheit in der Informationstechnik, „Cyber-Sicherheitsnetzwerk des BSI“, bsi.bund.de, zugegriffen 9. Mai 2021, <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/cyber-sicherheitsnetzwerk.html>

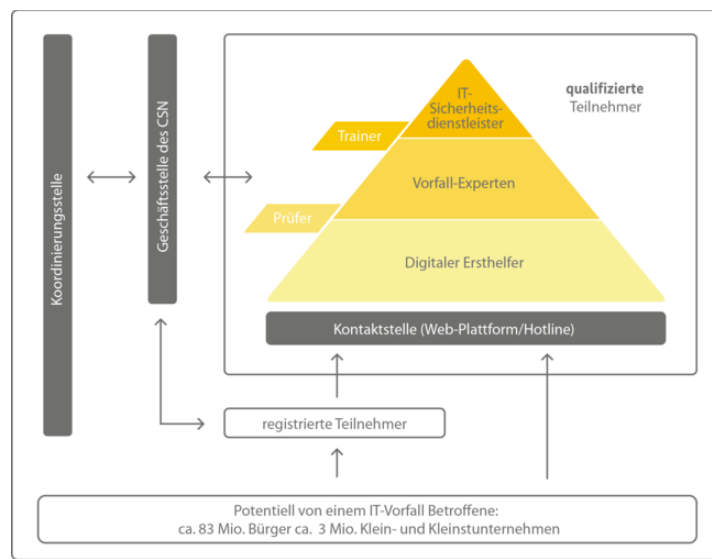


Abbildung 3.1: Rollenverständnis im CSN

Der auf Freiwilligenbasis beruhende Zusammenschluss von ExpertInnen führt reaktiv eine Vorfallbehandlung je nach Anwendungsbereich und Zielgruppe durch. Die Grundlage der Rekrutierung bildet ein Schulungsprogramm für qualifizierte TeilnehmerInnen, um diese zu eine/r Digitalen ErsthelferIn oder Vorfall-ExpertIn auszubilden und mit einem Zertifikat auszuzeichnen. Für diese Workshops konnte man sich als Interessierte oder Interessierter während der Erstellung dieser Arbeit anmelden.⁸⁰ Über eine Kontaktstelle können BürgerInnen und KMUs Kontakt zu den Digitalen ErsthelferInnen aufnehmen. Vorfall-ExpertInnen können für Vor-Ort-Einsätze ausrücken. Diese Einsätze können über die Koordinierungsstelle des BSI mit lokalen Initiativen gebündelt werden, um Synergien zu schaffen. Zertifizierte IT-Sicherheitsdienstleister könnten so mit einem Team an Vorfall-ExpertInnen des CSN bei größeren und komplexeren IT-Sicherheitsvorfällen helfen. Zusätzlich sollen im Nachgang eines Vorfalls über einen Erfahrungsaustausch zwischen allen Vorfall-ExpertInnen Erfahrungen gesammelt und analysiert werden, um Optimierungspotenzial am Cyber-Sicherheitsnetzwerk zu identifizieren. Ein Vergleich zwischen dem CSN und dem unter Kapitel 4 vorgestellten Cyber-Hilfswerk wird in Kapitel 5.5 durchgeführt.

⁸⁰ „Workshop zum Vorfall-Experten des CSN des BSI“, qskills.de, zugegriffen 9. Mai 2021, www.qskills.de/qs/workshops/governance/sc580vorfall-expertedescybersicherheitsnetzwerksdesbsi

3.2 Bewusstsein über Gefahrenpotenzial

Die politischen EntscheidungsträgerInnen haben Handlungsbedarf erkannt. Dies ist nicht nur an den neuen Richtlinien und Gesetzen wie EU Cybersecurity Act, IT-SiG 2.0 und der deutschen Cyber-Sicherheitsstrategie 2021 zu erkennen. Durch die kommende Etablierung des CSN wird die Resilienz Deutschlands im KMU- und Bürgersektor auch im reaktiven Umfeld gestärkt. Außerdem hält Deutschland mit der Krisenübung LÜKEX zweijährlich eine Übung zur Bewältigung von digitalen Angriffen und einem Ausfall der Versorgungsinfrastruktur ab. Die auf 2022 verschobene LÜKEX 21⁸¹ befasst sich beispielsweise mit dem Szenario „Cyberangriff auf Regierungshandeln“. Da diese Übung lediglich eine Stabsrahmenübung ist, kommt sie über planerische und organisatorische Bewältigungsansätze nicht hinaus. Die tatsächliche Ausführung von Maßnahmen wird nicht getestet. Zusätzlich beteiligt sich Deutschland an der durch das CCDCOE durchgeführte Übung „Locked Shields“⁸², die auf NATO-Ebene Angriffe auf Anlagen simuliert. KRITIS steht dort jedoch nicht im Fokus. Ein Positivbeispiel, in dem neben der Krisenkommunikation auch zusätzlich das Responseverhalten geprobt wird, liefern Nationen wie die USA. Mit der GridEx-Übung⁸³ für den Stromsektor findet alle zwei Jahre ein simulierter Cyberangriff auf das nordamerikanische Stromnetz statt. Neben der Krisenkommunikation wird hier auch das Responseverhalten geprobt. Zusätzlich zu der wenig vorhandenen praktischen Erfahrung im Umgang mit größeren Cyberangriffen hat das Kapitel 3.1 aufgezeigt, dass es nicht genügend personelle Kapazitäten für eine ausreichende Reaktion geben würde. Die fast 2.000 KRITIS-Unternehmen in Deutschland stehen 15 MitarbeiterInnen des BSI MIRT gegenüber. Die verschiedenen CERT Zusammenschlüsse stellen keine Organisationen dar, die in einer KRITIS-Schadenslage schnell und koordiniert Hilfe leisten können. Eine Aufstockung der Kapazitäten des BSI aus anderen Bereichen der Behörde wäre hinsichtlich der tatsächlich benötigten Ressourcen immer noch unzureichend. Wie eine solche Krisensituation aussehen könnte, wird vom Verfasser in Kapitel 3.3.2 thematisiert.

⁸¹ Vgl. „LÜKEX 21“, [bbk.bund.de](https://www.bbk.bund.de/DE/AufgabenundAusstattung/Krisenmanagement/Luekex/LUEKEX_21/LUEKEX_21_node.html), zugegriffen 14. Juni 2021, https://www.bbk.bund.de/DE/AufgabenundAusstattung/Krisenmanagement/Luekex/LUEKEX_21/LUEKEX_21_node.html

⁸² Vgl. „Locked Shields“, [bundeswehr.de](https://www.bundeswehr.de/organisation/cyber-und-informationsraum/uebungen/locked-shields-119136), zugegriffen 14. Juni 2021, <https://www.bundeswehr.de/organisation/cyber-und-informationsraum/uebungen/locked-shields-119136>

⁸³ Vgl. North American Electric Reliability Corporation, „Allgemeines Zu GridEx“, [nerc.com](https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx), zugegriffen 15. Mai 2021, <https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx>

Zudem sei das Verhalten zur IT-Resilienz für weite Teile der Wirtschaft desaströs, meint der Computerwissenschaftler Hartmut Pohl in einem zdf-Beitrag⁸⁴. Die AG KRITIS nennt im selben Beitrag die Gründe: Für das Aufspielen von Sicherheitsupdates und somit das System bestmöglich vor Sicherheitslücken zu bewahren, fehlt es an Budget und Zeit. Zusätzlich fehlt ein Mindesthaltbarkeitsdatum für Software. Dieses Problem hat sich jüngst in der im März 2021 aufgetretenen Hafnium-Sicherheitslücke für Microsoft Exchange gezeigt⁸⁵. Dort war es möglich über eine Schwachstelle E-Mails abzugreifen, Backdoors zu platzieren und unter Umständen Vollzugriff auf das System zu erhalten. Wenn nicht schnell genug gepatched wurde, war der/die AnwenderIn höchstwahrscheinlich kompromittiert. Neben dem unzureichenden Verhalten der Wirtschaft, kommt außerdem eine Konkurrenzlandschaft unter der Vielzahl an Behörden dazu, wird in dem zdf-Beitrag⁸⁶ argumentiert. Wie der Überblick der CERTs aus 3.1.1 gezeigt hat, gibt es bereits dort eine starke Varietät an Verbänden. Zusätzlich kommen mit Bundeskriminalamt (BKA), 16 Landeskriminalämter (LKA), dem Verfassungsschutz und dem Kommando Cyber- und Informationsraum der Bundeswehr weitere Akteure hinzu, die teils ganz andere Ziele verfolgen. Ein Beispiel stellt hier das Offenlegen oder auch Zurückhalten von Sicherheitslücken dar. Allgemein entsteht der Eindruck, dass noch nicht vollständig akzeptiert wurde, dass zu jeder menschlichen oder juristischen Person ein digitales Abbild existiert, das nicht nur als Anhängsel der analogen Welt betrachtet werden sollte. Man muss als Staat oder Unternehmen beide dieser Welten sicher und störungsfrei abdecken.

In ihrer Erklärung zur Lage der IT-Sicherheit in Deutschland für 2020⁸⁷ zeichnet das BSI ein anderes Bild und sieht die Situation weniger kritisch. Insbesondere die KRITIS-Unternehmen sind mit der Etablierung der Information Security Management und Business Continuity Management Systeme (BCMS) sowie der Nachweispflicht gegenüber dem BSI gut auf die Gefahren des digitalen Wandels vorbereitet. Der Bund und das BSI hätten die Voraussetzung geschaffen, den Betrieb von KRITIS sicher zu gestalten. Nichtsdestotrotz identifiziert das BSI in

⁸⁴ Vgl. „Experten: IT-Sicherheit in Deutschland ‚desaströs‘“, zdf.de, zugegriffen 10. Mai 2021, <https://www.zdf.de/uri/6b5e5843-d5e4-4971-9c28-372d1f249356>

⁸⁵ Vgl. Stefan Krempl, „Exchange-Lücken: BSI sieht hierzulande zehntausende Server betroffen“, heise.de, zugegriffen 14. Juni 2021, <https://www.heise.de/news/Exchange-Luecken-BSI-sieht-hierzulande-zehntausende-Server-betroffen-5073716.html>

⁸⁶ Vgl. zdf.de, „Experten: IT-Sicherheit in Deutschland ‚desaströs‘“

⁸⁷ Vgl. Bundesamt für Sicherheit in der Informationstechnik, „Die Lage der IT-Sicherheit in Deutschland 2020“, bsi.bund.de, zugegriffen 10. Mai 2021, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2

einigen Sektoren Verbesserungspotenziale. Der Einsatz veralteter Soft- und Hardware, insbesondere im Bereich Kritische Infrastruktur, wird jedoch nicht thematisiert.

3.3 Gefahrenlage

Dabei steigt die Eintrittswahrscheinlichkeit einer Großschadenslage durch einen Cyberangriff kontinuierlich an. Das Bundeslagebild Cybercrime 2020 des BKA⁸⁸ zeigt: Angriffe von Cyberkriminellen nehmen deutlich zu. Für den Zeitraum von 2016 bis 2020 hat sich die jährlich erfasste Anzahl an Fällen um gerundet 31 Prozent erhöht. Die COVID-19-Pandemie hat die Digitalisierung stark voranschreiten lassen. Dies geschah aufgrund der Kritikalität in einem schnellen Tempo, was auch zu Lasten der Informationssicherheit gehen könnte⁸⁹. Die AG KRITIS nennt in ihrem Konzept weitere Problemfelder⁹⁰: Unternehmen sind immer stärker untereinander vernetzt, um die Effizienz zu steigern und Kosten zu sparen. Ursprünglich autarke Systeme können mittlerweile durch Angriffe aus dem Internet betroffen sein. Die Anzahl und Variation an Informationstechnik steigt rapide an. Soft- und Hardware werden zu lange verwendet. Dadurch, dass die Geschwindigkeit des technologischen Fortschritts ansteigt, sollten Programme und Sicherungssysteme schneller als obsolet betrachtet werden. Das „Internet of Things“ (IoT) liefert eine weitere Variable, dessen mögliches Ausmaß der Verfasser in einem potenziellen Angriffsbeispiel in Kapitel 3.3.2 erfassen möchte. Dadurch, dass es Soft- und Hardware gibt, die flächendeckend eingesetzt wird, können auf einen Schlag eine Vielzahl an KRITIS-Betrieben betroffen sein. Ein Beispiel bietet hier die bereits angesprochene Hafnium-Sicherheitslücke, in der laut BSI zehntausende deutsche Systeme betroffen waren und sind. Zusätzlich zu den allgemein geltenden Entwicklungen kommen noch weitere Gründe zur Sorge um KRITIS hinzu.⁹¹

⁸⁸ Vgl. „Bundeslagebild Cybercrime 2020“, bka.de, zugegriffen 21. Juni 2021, <https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2020.html>

⁸⁹ Vgl. Bundesministerium für Wirtschaft und Energie, „Auswirkungen von COVID-19 auf die IT-Sicherheit und Handlungsempfehlungen“, it-sicherheit-in-der-wirtschaft.de, zugegriffen 21. Mai 2021, <https://www.it-sicherheit-in-der-wirtschaft.de/ITS/Redaktion/DE/Meldungen/2020/2020-03-19-auswirkungen-covid-19-auf-it-sicherheit.html>

⁹⁰ Arbeitsgruppe Kritische Infrastrukturen, „Konzept Cyber-Hilfswerk“, Seite 4 f.

⁹¹ Vgl. Peter Schmitz, „5 Gründe, die das Risiko Kritischer Infrastrukturen erhöhen“, security-insider.de, zugegriffen 15. Mai 2021, <https://www.security-insider.de/5-gruende-die-das-risiko-kritischer-infrastrukturen-erhoehen-a-850951/>

Neben der Tatsache, dass laut Analyse der Telekom gemäß des Artikels von Peter Schmitz Cyberangriffe exponentiell zunehmen, sind KRITIS-Betreiber attraktive Ziele für HackerInnen. Hier würde sich bei einer Verschlüsselung wahrscheinlicher und höheres Lösegeld erpressen lassen. Nach einer Studie von Tenable und dem Ponemon Institute⁹² haben 90% aller Unternehmen mit Operational Technology in den letzten 24 Monaten einen schädlichen Cyberangriff erlebt. Bei 62% waren es sogar mindestens zwei Angriffe.

Neben den kriminell motivierten Angriffen können KRITIS auch staatliche Konflikte im Sinne eines Cyber Wars zum Opfer fallen. Kapitel 2 dieser Arbeit hat aufgezeigt, dass es dort Unklarheiten und Probleme in der Rechtsprechung gibt, die diese Angriffe begünstigen könnten. Gerade bei Operationen, die unterhalb der Schwelle zu einer Völkerrechtsanwendung liegen, wie die Cyberspionage, ist kein Verbot, sondern eine aktive Ausnutzung durch Staaten vorhanden. Zusätzlich wird diese Gefahr mit den Tendenzen zu einer aktiven Cyberabwehr mittels Hackback verstärkt. Nachrichtendienste und das Militär würden im Verteidigungsfall gegenüber eine/r AngreiferIn mit Gegenmaßnahmen reagieren. Wie das Kapitel 2.1.3 Attribution von Cyberangriffen jedoch aufzeigen konnte, ist eine solche Schuldzurechnung mit legitimiertem Gegenschlag aus technologischer Sicht nicht möglich. Dies gefährdet die Kritischen Infrastrukturen und die Bevölkerung zunehmend. Wenn man davon ausgehen muss, dass man im Falle einer katastrophalen Großschadenslage nicht die benötigten Bewältigungskapazitäten stellen kann, trägt das nicht zu einer gemilderten Situation bei.

Wie in der Einleitung erwähnt, schrecken Aggressoren nicht davor zurück, die vulnerabelsten Sektoren der KRITIS anzugreifen. Ganz im Gegenteil sogar: Sie fokussieren sich aktiv auf die Bereiche Energie und Gesundheit⁹³.

In die Karten eine/r AngreiferIn spielt auch die COVID-19-Pandemie, meint BSI Präsident Arne Schönbohm in einer Stellungnahme vom 12. April 2021⁹⁴. Diese können sich die besondere Lage mit einer Vielzahl an Möglichkeiten zunutze machen, um BürgerInnen und auch KRITIS zu schaden. Neben dem Anstieg von Social-Engineering-Angriffen machen sich HackerInnen auch die erschwerten Bedingungen, die aus der Homeoffice Situation folgen, zunutze. Die

⁹² Vgl. Ted Gary, „Cybersecurity-Fachkräfte sind mit erheblichen Schwierigkeiten bei der OT-Sicherheit konfrontiert: Ponemon-Bericht“, [tenable.com](https://de.tenable.com/blog/cybersecurity-pros-face-significant-challenges-with-ot-security-ponemon-report), zugegriffen 15. Mai 2021, <https://de.tenable.com/blog/cybersecurity-pros-face-significant-challenges-with-ot-security-ponemon-report>

⁹³ Vgl. Bundesregierung Deutschland, „Drucksache 19/24247: Anfälligkeit kritischer Infrastrukturen vor Hackerangriffen in Deutschland“

⁹⁴ Vgl. Arne Schönbohm, „Stellungnahme des BSI-Präsidenten, Bilanzierung des Bevölkerungsschutzes angesichts der Corona-Pandemie“, [bundestag.de](https://www.bundestag.de/resource/blob/833204/f80fedb9c35706c289a79fd85eb3d132/A-Drs-19-4-793-F-data.pdf), zugegriffen 9. Mai 2020, <https://www.bundestag.de/resource/blob/833204/f80fedb9c35706c289a79fd85eb3d132/A-Drs-19-4-793-F-data.pdf>

Angriffsfläche hat sich mit dem Digitalisierungsschub massiv vergrößert, um den Unternehmensbetrieb in der Krise aufrechterhalten zu können. Diese Mehrnutzung digitaler Infrastruktur bietet AngreiferInnen zusätzliches Potenzial.

3.3.1 Angriffe in der Vergangenheit

Glücklicherweise blieb Deutschland und die Welt bislang von katastrophalen Großschadenslagen verschont. Wie in der Einleitung erwähnt, gab es in der Universitätsklinik Düsseldorf im September 2020 eine Vollverschlüsselung der Systeme, die eigentlich die örtliche Universität treffen sollte. Der Krankenhausablauf wurde stark gestört.

Ein weiteres Beispiel aus Deutschland, ebenfalls ein Krankenhaus, fand am 10. Februar 2016 in Neuss statt⁹⁵. Das Lukaskrankenhaus wurde auch von einer Ransomware getroffen. Die Abläufe waren stark gestört und es fiel ein wirtschaftlicher Schaden von ungefähr einer Millionen Euro an. Durch ein gutes Abwehrverhalten mit der Einbindung von BSI, BeraterInnen und weiteren SicherheitsexpertInnen konnten Folgen für PatientInnen ausgeschlossen werden. Über mehrere Wochen dauerte die Beseitigung der Folgen an, ehe sie auf eine teils gänzlich neue IT-Sicherheitsstruktur umstiegen.

Besorgniserregender ist ein Angriff auf die Wasserversorgung in Oldsmar, Florida (USA) aus dem Februar 2021⁹⁶. Dort hatten HackerInnen versucht, über den Fernwartungsdienst TeamViewer, die Menge an Natriumhydroxid im Leitungswasser zu erhöhen. Die Lauge wird normalerweise in geringen Mengen zur Kontrolle des Säuregehalts angewendet. Eine erhöhte Dosis hätte gesundheitliche Folgen für die 15.000 Abnehmer der Wasseraufbereitungsanlage. Die AngreiferInnen konnten die Konzentration kurzzeitig erhöhen, ehe ein Mitarbeiter den Eingriff bemerkte. Zusätzlich hätte laut dem Bürgermeister der Stadt auch ein anderer Kontrollmechanismus verhindert, dass das kontaminierte Wasser in die Versorgung gelangt wäre. Das Beispiel zeigt aber gut und erschreckend auf, wie leicht eine solche Gefahr entstehen kann. Wäre der kontrollierende Mitarbeiter aus dem System ausgesperrt und die Kontrollmechanismen der Aufbereitungslagen manipuliert worden, wären so die Änderungen länger unbemerkt

⁹⁵ Vgl. Nicolas Krämer, „Trojaner im KIS“, [bibliomedmanager.de](https://www.bibliomedmanager.de), zugegriffen 21. Mai 2021, <https://www.bibliomedmanager.de/fw/artikel/31425-trojaner-im-kis>

⁹⁶ Vgl. Christopher Bing, „Hackers Try to Contaminate Florida Town’s Water Supply through Computer Breach“, [reuters.com](https://www.reuters.com), zugegriffen 10. Mai 2021, <https://www.reuters.com/article/us-usa-cyber-florida-idUSKBN2A82FV>

geblieben und die AngreiferInnen hätten über den Einfallspunkt größeren Schaden anrichten können.

Auch von einer Ransomware betroffen war im Mai 2021 die größte US amerikanische Pipeline. In einer Vielzahl von Bundesstaaten blieb die Versorgung von Benzin und anderen Erdölprodukten über Tage aus, sodass die Regierung einen Notstand ausrufen musste⁹⁷. Besonders prekär ist hier die Tatsache, dass der KRITIS-Betreiber wirtschaftliche Interessen über die Versorgungssicherheit der Bevölkerung gestellt hat. Das Unternehmen hat infolge der Verschlüsselung von nicht kritischen Systemen des Betriebes die Pipelines abgestellt, um eine kostenfreie Verteilung des Benzins zu verhindern.

Wie die genannten Beispiele zeigen, liefert aktuell besonders die Angriffsmethode einer Ransomware Verschlüsselung im kriminellen Kontext ein verstärktes Bedrohungspotenzial für alle Institution mit Informationstechnik.

3.3.2 Potenzielles Angriffsszenario auf IoT

Mit dem Internet of Things oder IoT werden alle möglichen Geräte über ein Netzwerk miteinander verbunden⁹⁸. Damit können zwischen den Geräten Daten ausgetauscht werden. Heutzutage reichen diese Geräte von SmartPlugs bis zu anspruchsvollen Industriewerkzeugen. Es lassen sich Anwendungen automatisieren und Aufgaben ohne händischen Eingriff erledigen. Dies bringt ein großes Potenzial für das eigene Zuhause und auch der Wirtschaft mit. Leider entsteht dadurch aber auch eine neue Gefahrenquelle, welche die AG KRITIS in ihrem CHW-Konzept⁹⁹ thematisiert hat und hier weiter unter die Lupe genommen wird.

IoT-Geräte der Kategorie weiße Ware, also Geschirrspüler oder Waschmaschinen, könnten beim Ausnutzen einer Sicherheitslücke über ihre hohe Schaltleistung Skaleneffekte entstehen lassen. In diesen Geräten sind üblicherweise 3kW Heizelemente verbaut. Geht man von einer Million Geräte dieses Typus in Deutschland aus, ergebe das nach einfacher Rechnung eine potenzielle Schaltleistung von 3 Gigawatt. Wenn ein/e AngreiferIn nun Zugang zu einer Sicherheitslücke erhalten könnte, bei der er/sie die Geräte mit 3 Gigawatt synchron ein- und ausschalten kann, beeinflusst das die Netzfrequenz in Deutschland so stark, dass nach Einschätzung der AG KRITIS

⁹⁷ Vgl. tagesschau.de, „Hackerangriff auf Pipeline: USA erklären regionalen Notstand“, tagesschau.de, zugegriffen 13. Mai 2021, <https://www.tagesschau.de/ausland/usa-notstand-pipeline-101.html>

⁹⁸ Vgl. „Was ist das Internet of Things?“, oracle.com, zugegriffen 23. Mai 2021, <https://www.oracle.com/de/internet-of-things/what-is-iot/>

⁹⁹ Vgl. Arbeitsgruppe Kritische Infrastrukturen, „Konzept Cyber-Hilfswerk“, Seite 17

keine der aktuell vorhandenen Technologien zur Netzfrequenzstabilisierung den Ausfall des Stromnetzes verhindern kann. Es folgt nicht nur ein Stromausfall, sondern ein flächendeckender Blackout. Dabei reichen nach dieser Einschätzung möglicherweise auch schon 300.000 Geräte. Wobei eine Millionen Geräte nur 2,4% der deutschen Haushalte ausmachen. Gemäß einer Technikfolgeabschätzung (TA) des Ausschusses für Bildung, Forschung und TA in Form der Drucksache 17/5672 vom 27.04.2011¹⁰⁰ attestiert der Bericht eine außerordentliche Verletzbarkeit der modernen Gesellschaft Deutschlands im Rahmen eines Blackouts. Abseits von wirtschaftlichen Folgen, die in einer Vielzahl an Milliarden Euro steigen würden, fällt bereits nach wenigen Tagen ohne Stromversorgung die flächendeckende und bedarfsgerechte Versorgung der Bevölkerung aus. Auch die öffentliche Sicherheit, mit der Schutzpflicht des Staates, ist nicht mehr aufrechtzuerhalten. Eine nationale Katastrophenlage historischen Ausmaßes wäre die Folge, in der Strom-, Wasser- und Lebensmittelversorgung zum Erliegen kämen. Mit dem Ausfall der Grundversorgung und der staatlichen Schutzfunktion sind bürgerkriegsähnliche Zustände zu erwarten. Diese Ansätze sind jedoch nur theoretischer Natur. Glücklicherweise ist es noch zu keinem realen Blackout gekommen. Das heißt aber auch, dass dies noch nie gelebt oder auch getestet wurde. Der Bericht liefert Vorschläge, wie das Schaffen von Inselnetzen, um die Resilienz der Stromversorgung nach einem Stromausfall zu stärken. Nach diesem Prinzip würden im Katastrophenfall Eigenstrominsellösungen für einzelne Gebiete die Stromversorgung z. B. über erneuerbare Energien sicherstellen. Oberstes Gebot ist aber auch hier die allgemeine Resilienz der Kritischen Infrastrukturen auf kurz- oder mittelfristiger Sicht zu erhöhen.

Das solche Sicherheitslücken durchaus möglich sind und keine utopischen Szenarien darstellen, zeigt die „TR-069-Sicherheitslücke“ der Speedport-Router¹⁰¹. Dort gab es 2016 eine Sicherheitslücke im Fernwartungsdienst. 900.000 Geräte waren betroffen und sollten über den vorhandenen Exploit mit einer Schaddatei infiziert werden. Die Infizierung schlug jedoch aufgrund eines Versehens der HackerInnen fehl. Stattdessen hatten die vielen Versuche der AngreiferInnen, die Schaddatei von den Routern laden zu lassen, einen Absturz der Geräte in Form eines Denial Of Service zur Folge, woraufhin es zum Ausfall der Geräte und des Internets bei den BesitzerInnen der Speedports kam. Die eigentliche Attacke schlug fehl, der Vorfall ging

¹⁰⁰ Vgl. Ausschuss für Bildung, Forschung und Technikfolgeabschätzung, „Drucksache 17/5672: Gefährdung und Verletzbarkeit moderner Gesellschaften - am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung“, bundestag.de, zugegriffen 17. Mai 2021, <https://dipbt.bundestag.de/dip21/btd/17/056/1705672.pdf>

¹⁰¹ Vgl. Linus Neumann, „TR-069, die Telekom, und das, was wirklich geschah“, netzpolitik.org, zugegriffen 23. Mai 2021, <https://netzpolitik.org/2016/tr-069-die-telekom-und-das-was-wirklich-geschah/>

glimpflich aus – Folgen waren trotzdem zu spüren. Glücklicherweise besitzen diese Geräte auch keine hohe Schaltleistung, was zu einem Kollaps des Stromnetzes hätte führen können.

Wenn man bei dem Szenario der Waschmaschinen bleibt, hätte das wie beschrieben einen flächendeckenden und anhaltenden Stromausfall in Form eines Blackouts zur Folge. Davon abgesehen, dass wenn das deutsche Stromnetz zusammenbrechen würde, auch die Netze benachbarter Staaten kollabieren würden, stellt ein solches Szenario eine große Herausforderung für den Katastrophenschutz dar. Im schlimmsten Szenario müsste die Firmware der betroffenen Geräte händisch aktualisiert oder alle Geräte sofort vom Netz genommen werden, bevor der Prozess zur Wiederkehr aus einem Blackout starten kann. Da man hier von einem Szenario ohne Stromversorgung spricht, muss zunächst einmal die Bevölkerung flächendeckend aufgefordert werden, den Anweisungen zum Entfernen der Geräte Folge zu leisten. Da ein Update der Firmware nicht über das Internet verbreitet werden könnte, müssten mit erheblichem Personalaufwand die einzelnen Geräte bis zu einem Break-Even-Point vor Ort durch geeignetes Personal aktualisiert werden. Dieser Break-Even-Point wäre dann erreicht, wenn genügend Geräte bereinigt wurden, um das Stromnetz wieder stabil laufen lassen zu können. Das eingesetzte Personal müsste effizient und strukturiert vorbereitet und in den Einsatz geschickt werden. Ausgestattet mit Akku oder Generator, müssten sie von Tür zu Tür und die befallenen Geräte patchen. Um dieses Szenario besser veranschaulichen zu können, bringt der Verfasser eine vereinfachte Modellrechnung für den entstehenden Skaleneffekt an:

Bei einer Anzahl X an HelferInnen, die der Staat nach derzeitigem Stand maximal für eine solche Aktion bereitstellen kann und einer Veranschlagung von 30 Minuten Reparaturzeit mit benötigter Anfahrt für ein Gerät, lässt sich mit diesen Annahmen eine theoretische Formel aufstellen. Da das Kapitel 3.1 aufgezeigt hat, dass in einem solchen Fall momentan gutgewollt ca. 45 Personen des BSI MIRT koordiniert und strukturiert für eine solche Tätigkeit in einem Katastrophenszenario für KRITIS und die Bevölkerung zusammengezogen werden können, ergibt sich gepaart mit einem veranschlagten Break-Even-Point von 300.000 Geräten eine vereinfachte Berechnung der benötigten Bewältigungsdauer:

$$300.000 \text{ Geräte} / 45 \text{ Helfer} / 7 \text{ Tage/Woche} / 10 \text{ Stunden/Tag} / 2 \text{ Geräte/Stunde} \\ = 47,62 \text{ Arbeitstage}$$

Zu dieser Bearbeitungszeit kommt das Finden und Bereitstellen einer Lösung in Form eines Updates hinzu sowie die Zeit, die man braucht, um aus einem vollständigen Blackout wieder

anzulaufen. Für dieses Problem liefert die TA der Drucksache 17/5672¹⁰² im Kapitel 2.3.4 eine Vielzahl an sektorspezifischen Gründen zu einer langsamen Rückkehr in den Normalbetrieb. Beispielsweise ist in der Wasserversorgung ein langsames Anfahren vonnöten, um Rohrbrüche zu vermeiden. Zudem muss das gesamte System zunächst durchgespült werden, um möglicher Keimbildung in den Leitungen entgegenzuwirken. Die veranschlagte Modellrechnung kommt zu dem Ergebnis einer Bearbeitungszeit von gerundet 47 Tagen, was im Hinblick auf ein Katastrophenszenario solchen Ausmaßes gravierende Folge für die Gesellschaft hätte. Auf das Ergebnis der Modellrechnung mit möglicher Verbesserung der Bewältigungsdauer geht der Autor weiter in Kapitel 4.3.2 ein.

¹⁰² Vgl. Ausschuss für Bildung, Forschung und Technikfolgeabschätzung, „Drucksache 17/5672: Gefährdung und Verletzbarkeit moderner Gesellschaften - am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung“

4 Potenziale eines Cyber-Hilfswerks

4.1 Einführung in das Cyber-Hilfswerk und die AG KRITIS

Das Konzept¹⁰³ mit dem Arbeitstitel Cyber-Hilfswerk wurde durch die AG KRITIS entworfen, um bei Großschadenslagen, welche die Bewältigungskapazitäten des Staates überschreiten, eine schnelle und effektive Hilfe zur Wiederherstellung der kritischen Dienstleistungen bereitstellen zu können. Diese Hilfe soll wie bei anderen Hilfsorganisationen auf zivile KatastrophenhelferInnen beruhen. Die AG KRITIS besteht momentan aus ungefähr 42 Fachleuten und ExpertInnen, die sich täglich mit Angelegenheiten der KRITIS beschäftigen¹⁰⁴. Die Arbeitsgruppe besitzt Mitglieder aus allen KRITIS-Sektoren und bringt eine breit gefächerte Ansammlung an ExpertInnen mit. Sie sehen sich nicht als Wirtschaftsverband, haben keine Sponsoren und organisieren sich auch nicht als Unternehmen. Sie haben sich gegründet, um gemeinsam am Ziel einer nachhaltigen Verbesserung der IT-Sicherheit zu arbeiten. Laut eigener Aussage vereint die Gruppe, dass sie unabhängig voneinander zu der Erkenntnis gelangt sind, dass die Bundesrepublik mit ihren jetzigen Kapazitäten auf einen Angriff und eine resultierende Großschadenslage auf Kritische Infrastrukturen unzureichend vorbereitet ist, die Folgen eines solchen Szenarios zu bewältigen. Zu dieser Erkenntnis kommt auch der Verfasser dieser Arbeit in Kapitel 3.3.2.

Wegen dieser unzureichenden Kapazität strebt die AG KRITIS die Gründung eines Cyber-Hilfswerks an¹⁰⁵. Im klassischen Katastrophenfall dienen bereits überwiegend ehrenamtliche HelferInnen bei der Katastrophenbewältigung. Für den digitalen Katastrophenfall gibt es eine solche Struktur nicht. Da es heutzutage Fakt ist, dass ein digitales Abbild der analogen Welt existiert, muss sich die Frage gestellt werden, ob die Etablierung eines digitalen Abbilds eben einer solchen Hilfsorganisation gefordert ist.

Analog zur AG KRITIS für den deutschen Raum, besteht in Österreich mit dem Cyber Security Austria ein gemeinnütziger Verein, der sich auch unabhängig und überparteilich für die

¹⁰³ Arbeitsgruppe Kritische Infrastrukturen, „Konzept Cyber-Hilfswerk“

¹⁰⁴ Vgl. Arbeitsgruppe Kritische Infrastrukturen, „Wer sind wir?“

¹⁰⁵ Vgl. Arbeitsgruppe Kritische Infrastrukturen, „Konzept Cyber-Hilfswerk“, Seite 12

Verbesserung der IT-Sicherheit von Kritischen Infrastrukturen einsetzt¹⁰⁶. Die beiden folgenden Kapitel vier und fünf orientieren sich am Konzept der AG KRITIS zur Schaffung des Cyber-Hilfswerks¹⁰⁷ und führen zusätzliche Informationen des Verfassers an.

4.2 Aufgabenbereiche

Die erklärten Hauptaufgaben des CHW liegen in der Bündelung ziviler HelferInnen und SpezialistInnen der verschiedenen Fachbereiche für Kritische Infrastrukturen sowie in der Bereitstellung der benötigten Rahmenbedingungen, um unterstützende Tätigkeiten für die behördlichen Organisationen leisten zu können. Die Einrichtung soll eine Organisation aus Freiwilligen und Ehrenamtlichen darstellen, welche die unzureichenden Bewältigungskapazitäten des Staates ergänzen. Hierbei liegt der Schutz der Bevölkerung im Fokus. Die zivilen HelferInnen sollen bei konkreten Großschadenslagen als Einsatztruppe in der Lage sein, operative Tätigkeiten an den betroffenen Anlagen und Systemen durchzuführen. Im Zuge dieser Thematik soll zur Veranschaulichung eine Analogie zur Arbeitsteilung der Feuerwehr herangezogen werden: Das BSI MIRT ist als Berufsfeuerwehr zu sehen, das zuerst ausrückt. Das CHW kann dann nachgerufen werden, um als freiwillige Feuerwehr die Kapazitäten zu ergänzen. Sie dienen als digitale KatastrophenhelferInnen. Positive Nebeneffekte einer solchen Vereinigung liegen in der Möglichkeit zur Nachwuchsförderung und -generierung sowie das Vernetzen der ExpertInnen untereinander. Das Schaffen von Know-how in der Ereignisbewältigung von IT-Großschadenslagen kann eine Rückkopplung ergeben, die auch den Abteilungen der ArbeitgeberInnen dieser ExpertInnen nützen kann.

¹⁰⁶ „Cyber Security Austria“, zugegriffen 23. Mai 2021, <https://www.cybersecurityaustria.at/>

¹⁰⁷ Vgl. Arbeitsgruppe Kritische Infrastrukturen, „Konzept Cyber-Hilfswerk“, Seite 12 f.

4.3 Anwendungsbereiche

4.3.1 Einsatzszenarien

Laut einer Umfrage in Deutschland zur Verbreitung der ehrenamtlichen Tätigkeit bis 2020¹⁰⁸ stieg diese über die Jahre stetig an. Das ehrenamtliche Engagement ist in der letzten Generation deutlich gestiegen¹⁰⁹. Die Bereitschaft zur Hilfe in einer katastrophalen Lage ist da, sie muss jedoch strukturiert und koordiniert erfolgen. Die HelferInnen müssen wissen, wie und wo sie helfen können. Medizinisches Fachpersonal kann sich anders einbringen als eine ausgebildete InformatikerIn. Bei Bedarf der freiwilligen HelferInnen müssen Konstrukte zur Koordinierung schon davor bestehen¹¹⁰.

Eine Großschadenslage, welche die Hilfe von ehrenamtlichen HelferInnen bedarf, kann in einem Verteidigungsfall oder infolge einer Katastrophe im Frieden auftreten. Im Verteidigungsfall liegt die rechtliche Verantwortung nach Artikel 73 des Grundgesetzes¹¹¹ (GG) beim Bund, im Friedensfall nach Artikel 70 GG bei den Ländern. In der Praxis findet diese starre Unterscheidung aber nicht statt. Bund und Länder arbeiten in den verschiedenen Szenarien zusammen. Beispielsweise stellt der Bund den Ländern im friedlichen Katastrophenfall das in Kapitel 2.3.1 vorgestellte THW zur Verfügung. Das THW darf sich nach dem THW-Gesetz¹¹² an keiner kriegerischen Handlung beteiligen. Als Organisation des Zivilschutzes liegt die Zielsetzung in defensiven Handlungen darin, die Zivilbevölkerung zu schützen und zu unterstützen. Auch ein aufgestelltes CHW soll diesen Status erhalten, um als Non-Kombattant klassifiziert zu sein und somit nicht für die Vorbereitung, Unterstützung oder Durchführung von Cyberangriffen inklusive

¹⁰⁸ Vgl. „Verbreitung ehrenamtlicher Arbeit in Deutschland 2020“, statista.com, zugegriffen 23. Mai 2021, <https://de.statista.com/statistik/daten/studie/173632/umfrage/verbreitung-ehrenamtlicher-arbeit/>

¹⁰⁹ Vgl. D. I. W. Berlin, „Wachsendes ehrenamtliches Engagement : Generation der 68er häufiger auch nach dem Renteneintritt aktiv“, diw.de, zugegriffen 23. Mai 2021, https://www.diw.de/de/diw_01.c.683556.de/publikationen/wochenberichte/2019_42/wachsendes_ehrenamtliches_engagement_generation_der_68er_haeufiger_auch_nach_dem_renteneintritt_aktiv.html

¹¹⁰ Vgl. BMBF-Internetredaktion, „Freiwillige Helfer besser koordinieren“, bmbf.de, zugegriffen 23. Mai 2021, <https://www.bmbf.de/de/freiwillige-helfer-besser-koordinieren-3398.html>

¹¹¹ „Grundgesetz für die Bundesrepublik Deutschland“, gesetzte-im-internet.de, zugegriffen 14. Juni 2021, <https://www.gesetze-im-internet.de/gg/BJNR000010949.html>

¹¹² „THWG - Gesetz über das Technische Hilfswerk“, gesetzte-im-internet.de, zugegriffen 23. Mai 2021, <https://www.gesetze-im-internet.de/thw-helfrg/BJNR001180990.html>

Hackback missbraucht zu werden. Darunter fällt auch die Bereitstellung von über im Rahmen der Tätigkeit gewonnen Informationen zu Sicherheitslücken und Angriffswerkzeugen an staatliche Stellen wie BMI und BND.

Die konkreten Einsatzszenarien können sehr vielseitig aussehen. Ein mögliches Szenario im Rahmen der IoT-Technologie wird in den Kapiteln 3.3.2 und 4.3.2 genauer erläutert. Das Konzept der AG KRITIS nennt weitere Einsatzmöglichkeiten¹¹³: Bei einem flächendeckenden Befall von Infrastruktur mit Schadsoftware, wie dem mittlerweile zerschlagenen Emotet Virus¹¹⁴, der Ransomware in einer Größenordnung einschleusen konnte, welche die momentanen Bewältigungskapazitäten von Staat und Incident Response Dienstleistern an ihre Belastungsgrenzen hätte führen können. Die Bewältigung einer solchen Verschlüsselung ist möglich, wird aber schon in einem geringen Ausmaß sehr personalintensiv, da jedes betroffene Gerät im Netzwerk analysiert und bereinigt werden muss. Genauso müssen dann meistens in der Folge einer Kompromittierung alle NutzerInnen des Systems mit neuen Passwörtern und Zertifikaten ausgestattet werden, was wie im Beispiel der Universität Gießen¹¹⁵ schnell in die Anzahl der Zehntausender wachsen kann. Ein CHW könnte bei diesen Tätigkeiten allein in der Quantität eine große Hilfe bedeuten. Dabei gibt es Tätigkeiten, wie das Anlegen von Passwörtern, die keine tiefen Kenntnisse benötigen. Bei der Analyse und Bereinigung muss jedoch das Personal geschult sein, um auch tatsächlich helfen zu können. Die Anforderungen an die HelferInnen sind unterschiedlich: Von der Art der zu leistenden Tätigkeit bis zum benötigten Kenntnisstand.

Ein weiteres Beispiel liefert ein möglicher Angriff auf Krankenhausprotokolle in Form des Datenaustauschs mit dem Health Level 7 (HL7) Standard¹¹⁶. Bei einem Fehler in der Definition oder Implementierung des Standards für z. B. den HL7-Nachrichtentypen, kann es in der Folge zu weitreichenden Datenmanipulationen kommen. Da der HL7 Standard überregional in Deutschland eingesetzt wird, wäre ein breiter Ausfall des Krankenhausinformationssystems denkbar, was die staatlichen Kapazitäten wieder um ein Vielfaches ausreizen könnte.

¹¹³ Vgl. Arbeitsgruppe Kritische Infrastrukturen, „Konzept Cyber-Hilfswerk“, Seite 13 f.

¹¹⁴ Vgl. Bundeskriminalamt, „Infrastruktur der Emotet-Schadsoftware zerschlagen“, bka.de, zugegriffen 23. Mai 2021, https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html

¹¹⁵ Vgl. Friedhelm Greis, „Hackerangriff auf Uni Gießen: Lange Schlangen für 38.000 neue E-Mail-Passwörter - Golem.de“, golem.de, zugegriffen 23. Mai 2021, <https://www.golem.de/news/hackerangriff-auf-uni-giessen-lange-schlangen-fuer-38-000-neue-e-mail-passwoerter-1912-145593.html>

¹¹⁶ HL7 International, „Health Level Seven International - Homepage“, hl7.org, zugegriffen 23. Mai 2021, <http://www.hl7.org/>

4.3.2 IoT Angriffsszenario mit einem CHW

Betrachtet man nun das Angriffsszenario aus Kapitel 3.3.2 mit einem etablierten Cyber-Hilfswerk, lassen sich deutliche Verbesserungen in der Responsezeit attestieren. Zuvor bräuchten die verfügbaren staatlichen Kapazitäten in der vereinfachten Modellrechnung 47,62 Tage für das Patchen der 300.000 Waschmaschinen zum Break-Even-Point. Geeignete HelferInnen des CHW könnten die 45 staatlichen HelferInnen nun sinnvoll ergänzen. Die Gesamtzahl der HelferInnen würde stark ansteigen und die Variable X in der Gleichung signifikant erhöhen. Um den Unterschied in der Dauer im Vergleich zur Anzahl der vorhandenen HelferInnen darzustellen, bringt der Verfasser eine Modellierung an:

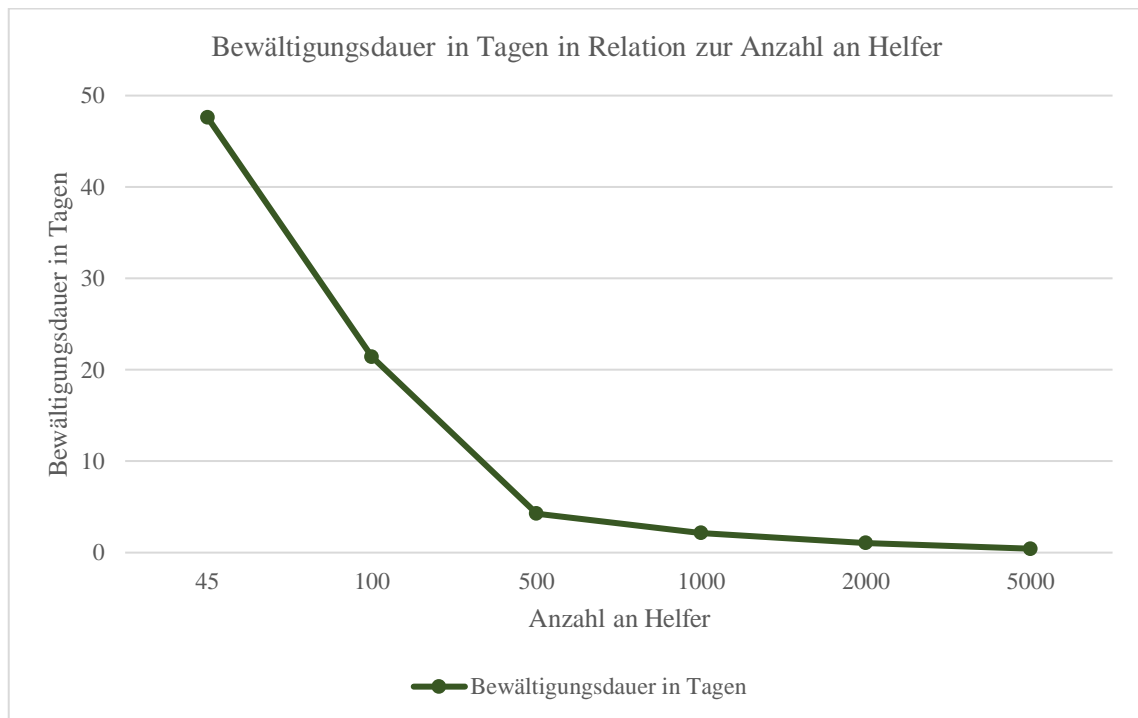


Abbildung 4.1: Bewältigungsdauer mit Cyber-Hilfswerk

Wie die Visualisierung aufzeigt, kann die Bearbeitungsdauer deutlich reduziert werden. Auch bei den vor- und nachgeschalteten Aufgaben, wie das Finden einer Lösung und des langsamen Wiederanlaufens aus dem Blackout, kann das CHW mitwirken. Einer erfolgreichen Mitwirkung von CHW-HelferInnen bedarf der Füllung des vorhandenen Vertrauensdefizits. In einer solch prekären Lage, wie dem Blackout mit bürgerkriegsähnlichen Zuständen mit möglichem Diebstahl und anderen Straftaten, muss für die Gewährung des Zutritts zur Gefahrenquelle in den eigenen vier Wänden staatliche Autorität in Form von Polizei oder Bundeswehr vorhanden sein. Die Bundeswehr sollte man jedoch als letzte Kriseninstanz hinzuziehen, wenn tatsächlich alle anderen Mittel ausgereizt sind. Möglicherweise kann man den CHW-HelferInnen diese Autorität auch

über die Schaffung eines CHW-Gesetzes, analog zum THW-Gesetz, geben. Als VerwaltungshelferInnen in einem Amtshilfeverfahren könnte dies ausreichen. Erfahrungswerte hierzu sind jedoch nicht vorhanden. Mehr zu der Rechtsform eines CHW folgt in Kapitel 5.2.

5 Umsetzbarkeit eines Cyber-Hilfswerks

5.1 Organisatorische Struktur

Die AG KRITIS erwähnt in Ihrem Konzept treffend, dass jede staatliche Reaktionskapazität automatisch auch ein potenzielles Missbrauchsrisiko mit sich bringt¹¹⁷. Unternehmen und Betreiber könnten sich auf staatliche Organisationen wie ein CHW verlassen und in der Folge ihre eigene IT-Sicherheit vernachlässigen. Um dem vorzubeugen, darf ein CHW nicht durch Unternehmen oder kritische Betreiber alarmiert werden. Nur Behörden im Rahmen einer Notlage dürfen die Einsatztruppen des CHW anfordern. Wer diesen Befehl erteilen kann, hängt von der Behörde ab, die diese erweiterte Befugnis erhalten soll. Das Konzept nennt unterschiedliche Möglichkeiten, die jeweils Ihre Vorteile mit sich bringen können:

- BMI: Erteilt derzeit bereits dem THW den Einsatzbefehl
- BSI: Kann über das NCAZ verfrüht über Cyber-Großschadenslagen informiert sein und die Bedrohungslage, insbesondere für KRITIS, besser abschätzen. Das CHW könnte auch parallel zur Aktivierung des CERT-Bunds aktiviert werden.
- BBK: Kann zusammen mit dem gemeinsamen Melde- und Lagezentrum von Bund und Ländern informieren.

Die AG KRITIS stellt in diesem Zuge fest, dass eine Alarmierung durch Militär oder Rüstungsunternehmen sowie andere militärisch agierende Unternehmen und im besten Fall auch Behörden ausgeschlossen sein sollte. Diese Organisationen dienen nicht der Sicherstellung der Versorgung der Bevölkerung mit KRITIS. Außerdem würde dies einen möglichen Non-KombattantInnen-Status des CHW gefährden.

Bei einer Großschadenslage kann, wie in Kapitel 4.3.2 zu lesen ist, das CHW bei der Betreuung von Geräten und Systemen außerhalb der Kritischen Infrastruktur in Berührung kommen, wenn von diesen Systemen die Störung ausgeht. Auch möglich ist eine Bedienung von Geräten außerhalb der Kritisverordnung, die für das Wiederanlaufen benötigt werden oder dass das CHW beim Verteilen von neuen Passwörtern assistiert¹¹⁸.

¹¹⁷ Vgl. Arbeitsgruppe Kritische Infrastrukturen, „Konzept Cyber-Hilfswerk“, Seite 18

¹¹⁸ Vgl. Arbeitsgruppe Kritische Infrastrukturen, „Konzept Cyber-Hilfswerk“, Seite 18 f.

Die Arbeitsgruppe hat sich in ihrem Konzept verschiedene Rollen innerhalb des CHW überlegt, um bei Schadenslagen in KRITIS bestmöglich helfen zu können. Der Verfasser visualisiert diese Rollenverteilung¹¹⁹ anhand folgender Grafik:

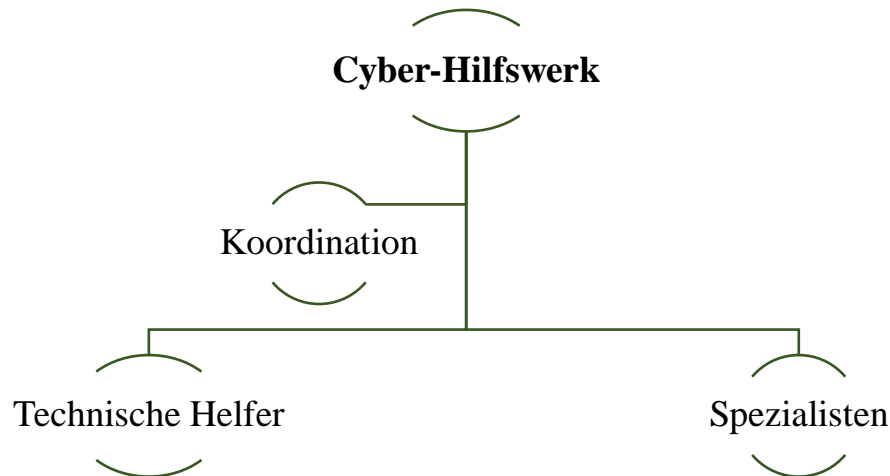


Abbildung 5.1: Rollen im Cyber-Hilfswerk

Es sind drei Rollen angedacht. Die Koordinationsstelle oder der Krisenstab ist die als Erstes zu besetzende Rolle in einem Anwendungsfall. Wie in einem klassischen Krisenstab fungiert die Stelle zur Organisation der HelferInnen und das Anordnen der Maßnahmen. Technisches Wissen für den Anwendungsfall ist nicht zwingend vonnöten. Mitglieder der Koordination sollten über planerische Fähigkeiten und Stressresilienz verfügen. Sie können zusätzlich als externes Kommunikationsorgan zu staatlichen Stellen, den Medien und anderen Hilfsorganisationen dienen. Sie sollten sich in dem betroffenen Sektor der KRITIS auskennen, um Folgen und mögliche Gegenmaßnahmen prioritär einschätzen zu können.

In der fachlichen und hierarchischen Sicht folgt darunter der/die SpezialistIn. Diese hilft bei der Koordination der breiten Maße an technischen HelferInnen. Als technische KompetenzträgerInnen haben die SpezialistInnen die Aufgabe, als Führungskraft zu agieren und den technischen HelferInnen beispielsweise Arbeitsanweisungen zu geben. Um sich als SpezialistIn qualifizieren zu können, sollten beruflichen Fähigkeiten vorliegen oder Fortbildungen durchgeführt werden.

In der niedrigsten Einstiegsqualifikation folgen die technischen HelferInnen. Mit technischem Grundwissen, einer Notfallsensibilisierung und Grundfitness ausgestattet, bilden die technischen HelferInnen die wichtigste Komponente. Sie gehen im größten Anteil operativ ins Feld und

¹¹⁹ Vgl. Arbeitsgruppe Kritische Infrastrukturen, „Konzept Cyber-Hilfswerk“, Seite 19 f.

arbeiten nach Anweisung der SpezialistInnen die zu leistenden Tätigkeiten in der Großschadensbewältigung ab. In dem Beispiel aus Kapitel 4.3.2 wären es die technischen HelferInnen, welche die Aktualisierungen an den Waschmaschinen vornehmen.

Wie die AG KRITIS in Ihrem Konzept¹²⁰ feststellt, stellt die benötigte Ausbildung der verschiedenen Rollen eine Herausforderung dar. Das Themenfeld der IT-Sicherheit unterliegt einer schnellen Entwicklung, die in letzter Zeit noch zugenommen hat. Fachkenntnisse erwirbt man in diesem Feld hauptsächlich durch praktische Tätigkeiten. Die Arbeitsgruppe schlägt vor, Praxiserfahrung für den Ernstfall durch das Durchführen von Aus- und Fortbildungen in Form von Krisenübungen in Trainingszentren anzureichern. Für Einrichtungen wie THW und Feuerwehr ist dies bereits erfolgreich etabliert. Die Trainings- oder Kompetenzzentren sollen praktische Übungen an realistischen Anlageaufbauten und auch theoretische Grundlagen vermitteln. In Anlehnung an die existierenden Übungszentren der spezifischen THW-Fachgruppen kann ein eigenes CHW-Trainingszentrum aktuelle und eingesetzte Systeme und Anlagen der KRITIS bereitstellen. HelferInnen können dann an diesen Anlagen trainieren, um Expertise in dem Fachsektor aufzubauen. Dadurch, dass diese Anlagen sehr speziell und exklusiv sind, würde sich die Attraktivität des CHW für potenzielle HelferInnen erhöhen. In diesem Zuge ist eine Grundausbildung einer jeden HelferIn des CHW ratsam. Mögliche Inhalte beschreibt die Arbeitsgruppe in ihrem Konzept.

Des Weiteren schlagen sie eine Bescheinigung der vermittelten Kenntnisse in Form von Zertifikaten vor, um den HelferInnen auch einen persönlichen Mehrwert für Ihr Engagement in der Arbeitswelt zu bescheren. Kooperationen bei der Fachausbildung mit bereits existierenden Ausbildungsträgern und KRITIS-Betreibern hält die AG KRITIS für sinnvoll und wahrscheinlich.

5.2 Rechtsform und Haftung

Bei der Wahl der geeigneten Rechtsform eines möglichen Cyber-Hilfswerks werden von der Arbeitsgruppe im groben vier Möglichkeiten genannt¹²¹, die der Verfasser im Folgenden erläutern möchte. Es wirken eine Vielzahl an regulatorischen und politischen Bedingungen auf die Frage der Rechtsform ein, die der Verfasser im folgenden Kapitel 5.3 größtenteils nennt. Wenn es um Fragen der Haftung, Versicherung sowie Freistellung und Kostenerstattung der ArbeitgeberInnen geht, dreht es sich um finanzielle Mittel. Als Organisation des Katastrophenschutzes sollte in

¹²⁰ Vgl. Arbeitsgruppe Kritische Infrastrukturen, „Konzept Cyber-Hilfswerk“, Seite 20 f.

¹²¹ Vgl. Arbeitsgruppe Kritische Infrastrukturen, „Konzept Cyber-Hilfswerk“, Seite 23 ff.

einer solchen Angelegenheit die Übernahme von finanziellen Summen der Staat übernehmen, bei dem auch die Schutzverantwortung liegt. Auf genauere Vorschläge der Arbeitsgruppe geht der Autor am Ende dieses Kapitels ein. Die AG KRITIS räumt aber auch ein, dass die genauen Modalitäten in Einklang mit behördlichen Anforderungen zu lösen seien, sodass ein rechtlich einwandfreier Vorschlag vertieft diskutiert werden muss.

Teil des Deutschen Roten Kreuzes

Das Cyber-Hilfswerk könnte als Teil des Bevölkerungsschutzes des Deutschen Roten Kreuzes (DRK) etabliert werden. Das DRK ist ein gemeinnütziger, eingetragener Verein¹²² der sich in breiter Linie für die Bevölkerung Deutschlands und der Welt einsetzt. Als unabhängige Hilfsorganisation ist der Verein freiwillig über das DRK-Gesetz vom 05.12.2008¹²³ in enger Zusammenarbeit mit dem Bund getreten. Sie sind flächendeckend in Deutschland strukturiert und bekennen sich zu den Rotkreuzgrundsätzen wie Menschlichkeit, Unabhängigkeit und Freiwilligkeit. Finanziert wird das DRK hauptsächlich durch Spenden der vier Millionen Mitglieder. Aber auch Bund, Länder und Kommunen stellen Mittel bereit, wenn diese im öffentlichen Interesse liegen. Bei der Finanzierung liegt laut CHW-Konzept der Nachteil, da Vorhaltungen für den Katastrophenschutz und der Ausbildung der Freiwilligen die Hauptaktivität des CHW darstellen. Diese müssten durch Spendengelder vorgestreckt werden, falls der Bund nicht im Ganzen dafür aufkommen möchte. Das DRK kann für Streitkräfte, aufgrund staatlicher Beauftragung, auf eigene Initiative oder wegen privatrechtlicher Vereinbarungen in den Einsatz gehen.

Teil einer Behörde

Es ist auch möglich das CHW direkt an eine Behörde anzugliedern. Dies würde Vorteile bei den Themen der Haftung, Versicherung und Entschädigung mitbringen, die später in diesem Kapitel erläutert werden. Infrage kommen hier laut AG KRITIS das BBK oder das BSI. Beim BSI bilden sich jedoch Interessenkonflikte, die im Kapitel 5.3.2 beschrieben werden. Die Leitung des BSI

¹²² Deutsches Rotes Kreuz, „Das DRK“, drk.de, zugegriffen 24. Mai 2021, <https://www.drk.de/das-drk/>

¹²³ Vgl. Deutsches Rotes Kreuz, „DRK-Gesetz“, drk.de, zugegriffen 24. Mai 2021, <https://www.drk.de/das-drk/auftrag-ziele-aufgaben-und-selbstverstaendnis-des-drk/drk-gesetz/>

MIRT signalisierte der Arbeitsgruppe, dass eine Zusammenarbeit „*machbar klingt*“¹²⁴. Das BBK sieht sich laut Arbeitsgruppe nicht beteiligt¹²⁵.

Teil des Technischen Hilfswerks

Die Analogie im Namen des Cyber-Hilfswerks wurde gemäß AG KRITIS nicht zufällig gewählt. Die Angliederung an das Technische Hilfswerk ist eine weitere Umsetzungsmöglichkeit. Wie Kapitel 2.3.1 beschreibt, besitzt das THW eine hohe Reputation und den Non-KombattantInnen-Status, wodurch ehrenamtliche HelferInnen geschützt werden könnten. Das CHW könnte eine eigene THW-Fachgruppe bilden, die den Bereich IT und OT für KRITIS abdeckt. Fachgruppen im THW sind dezentral organisiert und erreichen die Fläche des Landes einfacher. Das THW hat über Ihre Ortsverbände ein lückenloses Netz über der Bundesrepublik gespannt. Man könnte von dem existierenden Mantra der regelmäßigen Übungen und der angereicherten Erfahrung in der Krisenabwicklung profitieren.

Schaffung einer neuen Bundesanstalt

Die letzte Möglichkeit wäre ein CHW analog zum THW in Form einer Bundesanstalt zu gründen. Dies bringt jedoch viel politische und regulatorische Arbeit mit, wie das Schaffen eines CHW-Gesetzes. Eine Umsetzung dieser Lösung scheint sehr langwierig und am Wenigsten praktikabel.

In Haftungsfragen werden im Konzept drei Optionen aufgezeigt¹²⁶, die bereits in anderen Konstrukten aktiv Anwendung finden:

- Als VerwaltungshelferInnen¹²⁷ haftet das Land oder der Bund. Nur bei grob fahrlässigen Handlungen oder Vorsatz ist eine persönliche Haftung denkbar.
- Als HelferInnen im THW haftet immer der Bund. Dies ist über das THW-Gesetz¹²⁸ geregelt.

¹²⁴ Vgl. Arbeitsgruppe Kritische Infrastrukturen, „Konzept Cyber-Hilfswerk“, Seite 24

¹²⁵ Vgl. Arbeitsgruppe Kritische Infrastrukturen, „Konzept Cyber-Hilfswerk“, Seite 30

¹²⁶ Vgl. Arbeitsgruppe Kritische Infrastrukturen, „Konzept Cyber-Hilfswerk“, Seite 25

¹²⁷ Vgl. „Verwaltungshelfer: Definition, Begriff und Erklärung“, juraforum.de, zugegriffen 15. Juni 2021, <https://www.juraforum.de/lexikon/verwaltungshelfer>

¹²⁸ Vgl. „THWG - Gesetz über das Technische Hilfswerk“

- Als SpontanhelferInnen¹²⁹ kann man für den Einsatz kurzfristig Mitglied des DRK werden, um so die gleichen Rechte wie reguläre Mitglieder zu erhalten.

Für das CHW sind all diese Optionen, von Modifikation eigener Haftungsregeln über ein Gesetz bis hin zur Regelung als VerwaltungshelferIn, denkbar. Hier liegt es im Ermessensbereich des Staates eine praktikable Lösung zu finden, die Mitglieder des CHW nicht zusätzlich zu belasten. Auch beim Thema Unfallversicherung hängt die Entscheidung von der gewählten Rechtsform ab. Der Staat befindet sich, wie bei THW und Feuerwehr, in der Verantwortung über die jeweiligen Kassen des Bundes oder der Länder eine Versicherung der HelferInnen zu gewährleisten. Dabei spielt auch eine Rolle, ob die HelferIn im öffentlichen Sinne handelt oder hoheitliche Aufgaben erfüllt, wie das CHW-Konzept¹³⁰ beschreibt.

Bei der Entschädigung und Kostenerstattung für ArbeitgeberInnen gibt es mit dem THW eine Vorbildstruktur. ArbeitgeberInnen der ehrenamtlichen HelferInnen sollte eine Kostenerstattung gewährt werden.

5.3 Externe Bedingungen

5.3.1 Behördliche Bedingungen

Die AG KRITIS kann nach ersten Gesprächen mit VertreterInnen des BSI und BBK eine Bedingung seitens der Behörden anbringen: Für HelferInnen eines CHW muss die fachliche Qualifikation sichergestellt werden¹³¹. Dafür möchte die Arbeitsgruppe wie in Kapitel 5.1 im Abschnitt Ausbildung beschrieben, ein Übungs- und Trainingskonzept etablieren, das berufliche Vorkenntnisse mit angeeigneten Fähigkeiten in den Trainingszentren kombiniert und dies über Zertifikate bescheinigt. Als Vorbild dient hier das System „THWin“¹³² des THW.

¹²⁹ Vgl. Harald Erkens, „Rechtliche Koordinaten für den Einsatz von Spontanhelfern“, bbk.bund.de, zugegriffen 15. Mai 2021, https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Sonstiges/Buerger_und_Buergerinnen.pdf?blob=publicationFile

¹³⁰ Vgl. Arbeitsgruppe Kritische Infrastrukturen, „Konzept Cyber-Hilfswerk“, Seite 26

¹³¹ Vgl. Arbeitsgruppe Kritische Infrastrukturen, "Konzept Cyber-Hilfswerk", Seite 27

¹³² „THWin“, thwiki.org, zugegriffen 15. Juni 2021, <https://thwiki.org/t=THWin>

5.3.2 Politische Forderungen und Bedingungen der Community

Bedingungen aus der IT- und OT-Security Gemeinschaft führt die AG KRITIS in ihrem Konzept aus¹³³. Mit der Bereitschaft dieser Community für das CHW tätig zu werden, steht und fällt das Anliegen. Wenn man die Forderungen nicht berücksichtigt, werden sich nicht genügend ehrenamtliche HelferInnen finden lassen.

Ein CHW muss ausschließlich defensiv wirken. Das Ehrenamt wird für den Zivilschutz verwendet und darf nicht zur Erweiterung der offensiven Wirkmittel in einem Cyber War oder zur Spionage ausgenutzt werden. Die Arbeitsgruppe betont die strikte Trennung zu Sicherheitsbehörden. CHW-HelferInnen dürfen nicht als Personalpool für diese Behörden gelten, ebenso wie die Werkzeuge eines CHW. Das bedeutet, dass Werkzeuge und auch entdeckte Sicherheitslücken nicht an Sicherheitsbehörden weitergegeben werden dürfen, da dort immer die Gefahr des Dual-Use (offensiv und defensiv) besteht.

In diesem Zuge ist die Hackerethik, aufgegriffen durch den Chaos Computer Club (CCC), zu nennen¹³⁴. Potenzielle Mitglieder eines CHW aus der Community handeln privat und in ihrem Beruf nach ethischen und sozialen Devisen. Die Grundsätze dieser Ethik lassen sich auf Forderungen an die Sicherheitsstrategie Deutschlands und ein CHW abbilden:

¹³³ Vgl. Arbeitsgruppe Kritische Infrastrukturen, „Konzept Cyber-Hilfswerk“, Seite 27 f.

¹³⁴ Vgl. „Hackerethik“, ccc.de, zugegriffen 24. Mai 2021, <https://www.ccc.de/de/hackerethik>

Hackerethik Grundsatz	Konkrete Forderung
Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.	Open-Source-Software verwenden, die frei verfügbar ist oder wenigstens durch staatliche und unabhängige Stellen kontrolliert wird.
Alle Informationen müssen frei sein.	Erkannte Sicherheitslücken offenlegen und schließen.
Misstrau Autoritäten – fördere Dezentralisierung.	Eine ehrenamtliche Krisenbewältigungsstruktur etablieren, die in der Fläche der Bundesrepublik unabhängig und dezentral arbeitet.
Beurteile einen Hacker nach dem, was er tut, und nicht nach üblichen Kriterien wie Aussehen, Alter, Herkunft, Spezies, Geschlecht oder gesellschaftlicher Stellung.	Wenn die Bundesregierung bewilligt, offensive Wirkmittel wie Cyberspionage bei befreundeten Staaten einzusetzen, muss man auch mit solchen Gegenmaßnahmen rechnen. Deswegen: Staatliche Akteure müssen rein defensiv im digitalen Raum agieren.
Man kann mit einem Computer Kunst und Schönheit schaffen.	Diese beiden Grundsätze lassen sich zu einer Forderung zusammenfassen: Die IT ausschließlich für den guten Zweck, also niemals offensiv, verwenden.
Computer können dein Leben zum Besseren verändern.	
Mülle nicht in den Daten anderer Leute.	Auch hier kann man eine Forderung nennen: Cyber-Spionage muss verboten werden.
Öffentliche Daten nützen, private Daten schützen.	

Abbildung 5.2: Tabelle Mapping Hackerethik auf politische Forderungen

Die AG KRITIS formuliert zusätzlich auf Ihrer Webseite politische Forderungen¹³⁵. Eine dieser Forderungen ist die Etablierung des Cyber-Hilfswerk. Sie fordern die Unabhängigkeit des BSI vom BMI. Sicherheitslücken von KRITIS werden an das BSI gemeldet. Da das BMI Weisungsbefugnis gegenüber dem BSI besitzt, kann es anordnen, Sicherheitslücken geheim und offen zu halten und diese an Sicherheitsbehörden zu melden, damit diese sie im späteren Verlauf aktiv ausnutzen können. Um Vertrauen in das BSI zu entwickeln und damit das BSI auf

¹³⁵ Vgl. Arbeitsgruppe Kritische Infrastrukturen, „Politische Forderungen der AG KRITIS“, ag.kritis.info, zugegriffen 24. Mai 2021, <https://ag.kritis.info/politische-forderungen/>

Augenhöhe mit anderen Aufsichtsbehörden agieren kann, muss die Weisungsbefugnis des BMI aufgehoben werden. Mit den jüngsten Entwicklungen des IT-SiG 2.0 wird das BSI jedoch zunehmend offensiver¹³⁶ und mutiert zu einer weiteren Sicherheitsbehörde wie BND oder BKA. Des Weiteren fordert die AG KRITIS angemessene Personal- und Budgetausstattung für BSI, BBK und THW, um den Schutz von IT-Systemen in KRITIS erhöhen zu können. Ein weiterer wichtiger, bereits genannter, Punkt liegt in der Verwendung von Open-Source-Software im KRITIS-Umfeld. Wenn der Quellcode offen ist, kann Software für KRITIS auf weite Sicht sicherer betrieben werden. Auch nach Existenzverlust des Software-Herstellers ist dann ein Beheben von Sicherheitslücken möglich. Weiter fordern sie eine strikt defensive Cybersicherheitsstrategie für Staat und Wirtschaft und drängen auf ein internationales Verbot von Digitalwaffen per Sperrvertrag. Dabei muss Deutschland vorangehen und nicht wie mit dem BND-Gesetz und dem IT-SiG 2.0 falsche Signale an die Weltgemeinschaft senden. Eine defensive Cyberstrategie soll Deutschland auch im Rahmen der EU-Mitgliedschaft durchsetzen. Die Arbeitsgruppe verlangt eine erweiterte staatliche Verantwortung und Aufsicht der KRITIS-Betreiber, wie sie im IT-SiG 2.0 zum Teil durchgesetzt wird. Hersteller von KRITIS-Software sollen zur Entwicklung eines Patches zum Schließen einer Sicherheitslücke verpflichtet werden können. Zu guter Letzt setzt sich die AG KRITIS für eine bessere Kooperation nationaler und europäischer Cybersicherheitsinstitutionen ein, um eine Harmonisierung der Informationen und Strategien voranzutreiben.

5.4 Erfahrungen aus dem Projekt Cyberwehr des BSI

Die Arbeitsgruppe führt in ihrem Konzept¹³⁷ die Erfahrungen aus dem gescheiterten Projekt der Cyberwehr des BSI an. Das Projekt weist Ähnlichkeiten zum CHW auf und sollte eine Kooperation von Unternehmen und dem BSI darstellen. Gescheitert ist die Idee an einigen Problemstellen, die aus dem vertraglichen Charakter zwischen den Unternehmen beruhen. HelferInnen sollten ihre eigene Ausrüstung verwenden, bei möglichen KonkurrentInnen Ihrer ArbeitgeberInnen Hilfe leisten und weiter von der ArbeitgeberIn bezahlt werden. Die AG KRITIS liefert in ihrem Konzept Antworten zu den entstandenen Problemen, die sich über die Rechtsform als ehrenamtliche Organisation mit Vorbild des THW lösen lassen. Weitere, auch für das CHW

¹³⁶ Vgl. Meister, netzpolitik.org, „IT-Sicherheitsgesetz 2.0: Seehofer will BSI zur Hackerbehörde ausbauen“

¹³⁷ Vgl. Arbeitsgruppe Kritische Infrastrukturen, „Konzept Cyber-Hilfswerk“, Seite 29 f.

relevante Probleme, liegen in den Feldern Haftung, Fortbildung und Datenschutz. Eine Fortbildung der HelferInnen lässt sich über THW-ähnliche Strukturen durchführen. Die Haftungsfrage lässt sich nach Wahl der Rechtsform eindeutig mit der zuständigen Behörde klären. Datenschutzfragen würden sich bestmöglich über die Etablierung eines eigenen Gesetzes oder der Erweiterung bestehender Gesetzgebungen wie das THW-Gesetz umsetzen.

5.5 Vergleich zum Cyber-Sicherheitsnetzwerk des BSI

Das im Kapitel 3.1.3 vorgestellte CSN des BSI ist ein auf Freiwilligenbasis beruhender Zusammenschluss von ExpertInnen, um BürgerInnen und KMU bei der Vorfallbehandlung eines IT-Sicherheitsvorfalls zu unterstützen. Das CHW richtet sich in erster Linie an die Steigerung der Bewältigungskapazitäten in Cyber-Großschadenslagen für KRITIS. Beide Konstrukte sind dezentral organisiert und sollen flächendeckend in Deutschland wirken. Bei Beiden gibt es mehrere Stufen an HelferInnen mit Ihren eigenen Anforderungen. Im CSN übernehmen digitale ErsthelferInnen einen Firstlevel-Support an der Hotline und geben Ersthilfe. Vorfall-ExpertInnen können tiefergehende Analysen durchführen und bei Bedarf ausrücken, um lokal tätig zu werden. Das CHW hingegen stellt technische HelferInnen auf, die vor Ort die Arbeiten durchführen und hat mit den SpezialistInnen geschultes Fachpersonal mit der Expertise zur Lösungsfindung. Die Anforderungen an die HelferInnen der jeweiligen Einrichtungen unterscheiden sich aufgrund der Zielgruppe. Ein IT-Sicherheitsvorfall bei einer BürgerIn bringt andere Aufgaben mit als das Bewältigen eines Ausfalls von Kritischer Infrastruktur. Das CSN möchte IT-Sicherheitsdienstleister einbinden, das CHW plant eine Hilfsorganisation ohne wirtschaftlichen Einfluss. Die strategische Ausrichtung des CSN wird durch eine Koordinierungsstelle des BSI übernommen¹³⁸. Das CHW arbeitet nach Alarmierung durch eine Behörde im Austausch mit anderen Hilfsorganisationen und staatlichen Stellen weitestgehend eigenständig. Bei beiden Einrichtungen sollen über Schulungen die fachliche Eignung aufgebaut und geprüft werden. Da sich die Zielgruppen unterscheiden und das BSI dem CSN Weisungen erteilt, welche wiederum vom BMI kommen können, ist eine Verschmelzung oder Erweiterung des CSN mit dem CHW ohne weitere Anpassungen nur schwer möglich. Eine Symbiose der beiden Konstrukte kann jedoch durchaus zu Vorteilen führen.

¹³⁸ Vgl. Bundesamt für Sicherheit in der Informationstechnik, „Cyber-Sicherheitsnetzwerk des BSI“

6 Fazit

6.1 Kritische Reflexion

6.1.1 Herausforderungen und Nachteile

Wenn es um Themen der Prävention geht, kann man diese immer schlecht an die Außenwelt vermitteln. Krisenprävention will nicht gebraucht werden, sie sollte aber allzeit verfügbar und funktionsfähig sein. Die vorgehaltenen Mittel kommen bei Katastrophen zum Einsatz und sind somit stets mit etwas Negativem verbunden. Tatsächlich gibt es aber wenige Nachteile bei der Etablierung von Präventionsmechanismen wie dem CHW.

Eine der Herausforderungen ist der damit verbundene Aufwand für die Einführung eines solchen Hilfswerks. Auch stellen die Ausbildung der HelferInnen und das Schaffen der Ausbildungsumgebung Negativpunkte dar. Zusätzlich wurde diese Arbeit unter der Prämisse verfasst, dass sich ausreichend ehrenamtliches Personal finden lässt. Dies ist sehr an eine zielbewusste Ausführung des Konzepts mit den einhergehenden moralischen und ethischen Bedingungen der Community gekoppelt. Die Möglichkeiten, die einem eine solche Katastrophenorganisation bieten, übertrumpfen die Nachteile jedoch bei Weitem. Die Vorsorgepflicht des Staates zwingt diesen dazu, dessen Bevölkerung vor möglichen Bedrohungsszenarien zu schützen.

6.1.2 Vorteile

Mit denen im Kapitel 3 des Status quos ausgeführten Erkenntnissen in der Gefahrenlage und der momentanen Leistungsfähigkeit Deutschlands bei einer Cyber-Katastrophe lässt sich eine Verbesserung der Response-Möglichkeiten in Form einer ehrenamtlichen Institution annehmen. Der Cyberraum unterliegt noch keinem international verpflichtenden Abkommen. Wirkmittel der Informationstechnik, wie die Cyberspionage oder Maßnahmen unter einer Schwelle zur Anwendung des Völkerrechts, sind nicht gesperrt. Sie werden durch alle Staaten genutzt und auch die Bundesrepublik geht mit neuen Gesetzgebungen in eine offensivere Cyberstrategie.

Zusätzlich dazu verstärkt sich die Cyber-Kriminalität gegen KRITIS. Dies sind gute Gründe um bei einem kommenden Angriff und einer darauffolgenden potenziellen Krise gewappnet zu sein. Mit dem THW existiert gemäß der Vorstellung aus Kapitel 2.3.1 für den klassischen Katastrophenfall eine beispiellos funktionierende Organisation. Das THW passt sich laut eigener Webseite bereits seit sieben Jahrzehnten an die sich ändernden Gefahrenlagen an. Die Bedrohungssituation im Cyberraum stellt eine solche Art neuer Gegebenheiten dar. Diese bestehende Struktur kann man sich zunutze machen und sie um ein CHW erweitern.

Die Cyber Unit Estlands präsentiert darüber hinaus ein funktionierendes Konstrukt einer Kooperation staatlicher mit privater Strukturen im Kontext der IT-Sicherheit.

Die stattfindende COVID-19 Pandemie zeigt der Welt, welchen Unterschied es machen würde, auf eine weitreichende Krise vorbereitet zu sein. Die Versorgungssicherheit des Gesundheitssektors fällt unter KRITIS und geriet im Laufe des Geschehens immer wieder an seine Grenzen, bis hin zum Einsatz von Triage. Der Schutz und die Resilienz vor Versorgungsausfällen der Bevölkerung stellt einen Grundpfeiler einer modernen Gesellschaft dar, den es um jeden Preis zu bewahren gilt. Ein CHW würde die nicht ausreichende Bewältigungskapazität sinnvoll ergänzen. Auch im Vergleich zum klassischen Katastrophenfall zeigt sich: Es ist nicht sinnvoll eine Armee aus behördlichen MitarbeiterInnen für eine Extremlage vorzuhalten. Eine skalierbare Struktur aus ehrenamtlichen HelferInnen liefert eine umsetzbare und sinnvolle Alternative. Wie das Kapitel 4.3.1 gezeigt hat und die AG KRITIS in ihrem Konzept bezeugt, ist ein breites Interesse an ein Ehrenamt in Deutschland generell und auch für das CHW vorhanden. Es muss nur dem richtigen Zweck dienen. Eine absolute Sicherheit wird jedoch nie möglich sein. Dies bezeugt auch die TA in der Drucksache 17/5672¹³⁹ in ihrem Fazit. Politische EntscheidungsträgerInnen müssen sich die Frage stellen, wie sicher sicher genug ist. Der derzeitige Stand im Juni 2021 ist, wie diese Arbeit aufzeigen konnte, nicht sicher genug.

6.2 Ausblick

Die AG KRITIS nennt in ihrem Konzept¹⁴⁰ die aus ihrer Sicht fälligen nächsten Schritte:

- Verhandlungen mit Behörden und Organisationen wie THW

¹³⁹ Vgl. Ausschuss für Bildung, Forschung und Technikfolgeabschätzung, „Drucksache 17/5672: Gefährdung und Verletzbarkeit moderner Gesellschaften - am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung“

¹⁴⁰ Vgl. Arbeitsgruppe Kritische Infrastrukturen, „Konzept Cyber-Hilfswerk“, Seite 30

- Verfassen eines Manifest für das CHW mit Aufgaben, Zuständigkeiten, Rahmenbedingungen und Handlungsspielräumen im Einsatzfall

Vom BSI MIRT kamen bereits durchaus positive Signale. Die Christlich-Demokratische Union Rheinland-Pfalz hat in ihrem Regierungsprogramm 2021-2026 unter Abschnitt 01.07¹⁴¹ erklärt, dass sie die gesetzliche Grundlage zur Etablierung eines CHW schaffen wollen. Die Bundestagsfraktion der Freien Demokratische Partei forderte bereits am 24.11.2020 in der Drucksache 19/24632¹⁴² die Erweiterung der Bewältigungskapazitäten für Großschadenslagen im Cyberraum, indem man eine Organisation nach Vorbild des THW schafft, ohne das CHW namentlich zu nennen. In diesem Schriftstück fordern sie auch die Unabhängigkeit des BSI vom BMI und eine strikt defensive Cybersicherheitsstrategie.

Die gesetzlichen Entwicklungen laufen jedoch in eine andere Richtung. Die Bundesrepublik etabliert eine offensivere Ausrichtung seiner Behörden. Im IT-SiG 2.0 gibt es einen Beschluss, der die deutsche Rüstungsindustrie mit dem Schutz der Zivilbevölkerung vermengt und diese als Folge in Gefahr bringt. Die offensivere Ausrichtung könnte eine Signalwirkung für Europa und die Welt nach sich ziehen. Die Bundesrepublik gilt in Themen der Ethik als Vorbild und ist ein Mitglied der Gruppe der Acht (G8-Staaten). Die mächtige Position Deutschlands mit einer potenziellen Beeinflussung der europäischen Politik durch nationale Bestrebungen hat sich schon bei der Datenschutzgrundverordnung (DSGVO) gezeigt. Sie kam als Vorgabe aus Deutschland und wurde schlussendlich in der EU übernommen¹⁴³. Möglicherweise wiederholt sich ein solches Signal und weitere EU-Mitgliedsstaaten geben ihren Behörden umfassende Rechte zum Abhören Ihrer Freunde, einschließlich Kritischer Infrastrukturen. Dann würde eine Entspannung der Lage im Cyberraum in die Ferne rücken.

Falls es in Zukunft zur Umsetzung eines Cyber-Hilfswerk kommen sollte und die Politik die nötigen Mittel beschließt, könnte es trotzdem noch mehrere Monate, wenn nicht sogar Jahre dauern, bis es in der Fläche einsatzbereit wäre.

¹⁴¹ Vgl. Christlich Demokratische Union Rheinland Pfalz, „Regierungsprogramm der CDU RLP für 2021-26“, cdurlp.de, zugegriffen 26. Mai 2021, https://www.cdurlp.de/sites/www.cdu-rlp.de/files/antraege/cdu-rlp-regierungsprogramm_210126_2.pdf

¹⁴² Vgl. Bundestagsfraktion der freien Demokraten, „Drucksache 19/24632: Pandemie als digitalen Weckruf ernstnehmen“, bundestag.de, zugegriffen 27. Mai 2021, <http://dipbt.bundestag.de/dip21/btd/19/246/1924632.pdf>

¹⁴³ Vgl. Ruth Berschens, „Jan-Philipp Albrecht: Das ist der Vater der DSGVO“, handelsblatt.com, zugegriffen 27. Mai 2021, <https://www.handelsblatt.com/politik/international/jan-philipp-albrecht-das-ist-der-vater-der-dsgvo/22605018.html>

6.3 Zusammenfassung

Wie diese Arbeit belegen konnte, steigt die Gefahr, die durch potenzielle Cyberkriminalität, Cyberspionage oder auch einen potenziellen Cyberkrieg ausgeht, stetig an. Dabei steht KRITIS im Fokus von Kriminellen und staatlichen Akteuren. Es besteht kein international verpflichtendes Abkommen wie eine Verbannung von Digitalwaffen. Völkerrechtliche Aspekte der digitalen Kriegsführung sind nicht allumfassend geklärt. Es sind lediglich Absichtserklärungen und lokale Gesetzgebungen vorhanden. Das Internet ist derzeit bis zu einem gewissen Grad rechtsfrei. IT-Sicherheit wird in Teilen der Wirtschaft immer noch für weniger wichtig erachtet. Die Politik hat den Handlungsbedarf erkannt und mit der Anpassung von Gesetzen begonnen, die jedoch, wenn es um den Bevölkerungsschutz und somit um die Kernaufgabe des Staates geht, in eine falsche Richtung gehen. Die derzeitigen staatlichen Kapazitäten für die Bewältigung einer Großschadenslage reichen schlicht nicht aus. Ein Cyber-Hilfswerk würde durch seine Skalierbarkeit mit dem erfolgreichen Vorbild des THW eine umsetzbare Gelegenheit bieten, die Versorgungssicherheit der Bevölkerung zu erhöhen und die Response-Zeit in der Folge einer Beeinträchtigung Kritischer Infrastrukturen deutlich zu reduzieren. Eine Umsetzung der Organisation bedarf eines langfristigen Prozesses, in dem politische EntscheidungsträgerInnen, in behördlicher Sicht das BMI, in der Verantwortung stehen.

IV Literaturverzeichnis

Buchquellen

- [34] Komitee unter Führung von Michael N. Schmitt: *Tallinn Manual 2.0*, NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, 2017, Cambridge, Vereinigtes Königreich
- [35] *Siehe 34*

Internetquellen

- [1] [gesetz-im-internet.de](https://www.gesetze-im-internet.de/bgb/), 2021: *Bürgerliches Gesetzbuch*, <https://www.gesetze-im-internet.de/bgb/> (Zugriff: 14. Juni 2021)
- [2] [gesetz-im-internet.de](https://www.gesetze-im-internet.de/stgb/), 2021: *Strafgesetzbuch*, <https://www.gesetze-im-internet.de/stgb/> (Zugriff: 14. Juni 2021)
- [3] [lpb-bw.de](https://www.lpb-bw.de/charta), 2021: *Charta der Vereinten Nationen*, <https://www.lpb-bw.de/charta> (Zugriff: 14. Juni 2021)
- [4] [humanrights.ch](https://www.humanrights.ch/de/ipf/grundlagen/rechtsquellen-instrumente/humanitaeres-voelkerrecht/genfer-abkommen/), 2021: *Humanitäres Völkerrecht: Genfer Konventionen*, <https://www.humanrights.ch/de/ipf/grundlagen/rechtsquellen-instrumente/humanitaeres-voelkerrecht/genfer-abkommen/> (Zugriff: 14. Juni 2021)
- [5] [ag.kritis.info](https://ag.kritis.info/chw-konzept/), 2020: Arbeitsgruppe Kritische Infrastrukturen: *Konzept Cyber-Hilfswerk*, <https://ag.kritis.info/chw-konzept/> (Zugriff: 14. April 2021)
- [6] [kritis.bund.de](https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.html), 2021: *KRITIS - Definition und Übersicht*, https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.html (Zugriff: 15. April 2021)
- [7] [gesetz-im-internet.de](https://www.gesetze-im-internet.de/bsi-kritisv/), 2021: „BSI-KritisV“, <https://www.gesetze-im-internet.de/bsi-kritisv/> (Zugriff: 14. Juni 2021)
- [8] [eur-lex.europa.eu](https://eur-lex.europa.eu/eli/dir/2016/1148/2016-07-19), 2016: *NIS 2016/1148 Richtlinie*, <https://eur-lex.europa.eu/eli/dir/2016/1148/2016-07-19> (Zugriff: 02. Mai 2021)
- [9] [bsi.bund.de](https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Sektorspezifische-Infos-fuer-KRITIS-Betreiber/sectorspezifische-infos.html), 2021: *Sektorspezifische Infos für KRITIS-Betreiber*, <https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Sektorspezifische-Infos-fuer-KRITIS-Betreiber/sectorspezifische-infos.html> (Zugriff 22. Mai 2021)
- [10] [bbk.bund.de](https://www.bbk.bund.de/DE/AufgabenundAusstattung/KritischeInfrastrukturen/kritischeinfrastrukturen_node.html), 2021: *Kritische Infrastrukturen*, https://www.bbk.bund.de/DE/AufgabenundAusstattung/KritischeInfrastrukturen/kritischeinfrastrukturen_node.html (Zugriff 15. April 2021)

- [11] bmi.bund.de, 2021: *Nationale Strategie zum Schutz Kritischer Infrastrukturen*, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.pdf?__blob=publicationFile&v=3 (Zugriff 21. Mai 2021)
- [12] it-service.network, 2021: *Cyberattacken richten sich verstärkt auf KRITIS*, <https://it-service.network/blog/2021/01/13/kritische-infrastrukturen/> (Zugriff 20. April 2021)
- [13] bundestag.de, 2020: *Drucksache 19/24247: Anfälligkeit Kritischer Infrastrukturen vor Hackerangriffen in Deutschland*, <https://dserver.bundestag.de/btd/19/242/1924247.pdf> (Zugriff 20. April 2021)
- [14] uniklinik-duesseldorf.de, 2020: *IT-Ausfall an der Uniklinik Düsseldorf*, <https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/it-ausfall-an-der-uniklinik-duesseldorf> (Zugriff: 20. April 2021)
- [15] *Siehe 5, Seite 4*
- [16] ag.kritis.info, 2021: *Wer sind wir?*, <https://ag.kritis.info/wer-sind-wir/> (Zugriff: 20. April 2021)
- [17] bbk.bund.de, 2021: *Glossar - A-Z der Katastrophenhilfe*, <https://www.bbk.bund.de/SubSites/Kritis/DE/Servicefunktionen/Glossar/Functions/glossar.html> (Zugriff: 21. Mai 2021)
- [18] wired.com, 2019: *What Is Cyberwar? The Complete WIRED Guide*, <https://www.wired.com/story/cyberwar-guide/> (Zugriff: 14. Juni 2021)
- [19] bundestag.de, 2015: *Anwendbarkeit des humanitären Völkerrechts auf Computernetzwerkoperationen und digitale Kriegsführung (Cyber Warfare)*, <https://www.bundestag.de/resource/blob/406028/de1946480e133cf38bbec41d8d3d6898/WD-2-038-15-pdf-data.pdf> (Zugriff: 14. April 2021)
- [20] icj-cij.org, 1994: *Legality of the Threat or Use of Nuclear Weapons*, <https://www.icj-cij.org/en/case/95> (Zugriff: 29. April 2021)
- [21] *Siehe 19*
- [22] tagesschau.de, 2020: *Vor BND-Urteil: So überwacht der Dienst das Internet*, <https://www.tagesschau.de/investigativ/br-recherche/bnd-urteil-101.html> (Zugriff: 14. Juni 2021)
- [23] bpb.de, 2016: *Alte und neue Kriege. Gewaltkonflikte und Völkerrecht seit dem 19. Jahrhundert*, <https://www.bpb.de/apuz/232960/alte-und-neue-kriege> (Zugriff: 14. Juni 2021)
- [24] latimes.com, 2015: *Few Have Faced Consequences for Abuses at Abu Ghraib Prison in Iraq*, <https://www.latimes.com/nation/la-na-abu-ghraib-lawsuit-20150317-story.html> (Zugriff: 10. Juni 2021)
- [25] *Siehe 19*
- [26] *Siehe 19, Seite 11 f.*

- [27] security-insider.de, 2019: *Die Urheber von Cyberangriffen erkennen*, <https://www.security-insider.de/die-urheber-von-cyberangriffen-erkennen-a-826615/> (Zugriff: 14. Juni 2021)
- [28] law.harvard.edu, Harvard Journal, Band 20, Nr. 2, 2007: *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, <https://jolt.law.harvard.edu/assets/articlePDFs/v20/20HarvJLTech403.pdf> (Zugriff: 29. April 2021)
- [29] foreignpolicy.com, 2019: *Russia and China Are Trying to Set the U.N.'s Rules on Cybercrime*, <https://foreignpolicy.com/2019/09/16/russia-and-china-are-trying-to-set-the-u-n-s-rules-on-cybercrime/> (Zugriff: 14. Juni 2021)
- [30] issuu.com, 2013: *Tallinn Manual*, https://issuu.com/nato_ccd_coe/docs/tallinnmanual (Zugriff: 14. April 2021)
- [31] icrc.org, 1994: *Treaties, States parties, and Commentaries - San Remo Manual on Armed Conflicts at Sea*, <https://ihl-databases.icrc.org/ihl/INTRO/560> (Zugriff: 14. Juni 2021)
- [32] reliefweb.int, 2009: *Manual on International Law Applicable to Air and Missile Warfare*, <https://reliefweb.int/sites/reliefweb.int/files/resources/8B2E79FC145BFB3D492576E00021ED34-HPCR-may2009.pdf> (Zugriff: 14. Juni 2021)
- [33] oxfordreference.com, 2021: *Definition 'Black-Letter Law'*, <https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095510675> (Zugriff: 21. April 2021)
- [36] medium.com, 2019: *Tallinn Manual — A Brief Review of the International Law Applicable to Cyber Operations*, <https://medium.com/@cyberdiplomacy/tallinn-manual-a-brief-review-of-the-international-law-applicable-to-cyber-operations-5643c886d9e2> (Zugriff: 21. April 2021)
- [37] ccddcoe.org, 2020: *CCDCOE to Host the Tallinn Manual 3.0 Process*, <https://ccddcoe.org/news/2020/ccddcoe-to-host-the-tallinn-manual-3-0-process/> (Zugriff: 21. Mai 2021)
- [38] icrc.com, 2019: *International Humanitarian Law and Cyber Operations during Armed Conflicts*, <https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts> (Zugriff: 14. April 2021)
- [39] auswaertiges-amt.de, 2021: *On the Application of International Law in Cyberspace*, <https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf> (Zugriff: 14. April 2021)
- [40] digital-strategy.ec.europa.eu, 2021: *The EU Cybersecurity Act*, <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act> (Zugriff: 28. April 2021)
- [41] tuev-nord.de, 2017: *Security by Design - erklärt*, <https://www.tuev-nord.de/explore/de/erklaert/security-by-design/> (Zugriff: 2. Mai 2021)
- [42] *Siehe 8*

- [43] digital-strategy.ec.europa.eu, 2021: *Proposal for directive on measures for high common level of cybersecurity across the Union | Shaping Europe's digital future*, <https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union/> (Zugriff: 9. Mai 2021)
- [44] data.europa.eu 2008: *ECI 2008/114/EG Richtlinie*, <http://data.europa.eu/eli/dir/2008/114/oj/deu> (Zugriff: 02. Mai 2021)
- [45] ec.europa.eu, 2020: *Richtlinie Resilience of critical Entities*, https://ec.europa.eu/home-affairs/sites/default/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf (Zugriff: 15. Juni 2021)
- [46] ag.kritis.info, 2021: *Bewertung der EU-NIS und EU-RCI Richtlinie*, <https://ag.kritis.info/2021/04/26/bewertung-der-eu-nis-und-eu-rci-richtlinie/> (Zugriff: 2. Mai 2021)
- [47] auswaertiges-amt.de, 2020: *EU Cyber Diplomacy – Working Together for a Free and Secure Cyberspace*, <https://www.auswaertiges-amt.de/en/aussenpolitik/themen/eu-cyber-non-paper/2418984> (Zugriff 2. Mai 2021)
- [48] europa.eu, 2017: *Cyberangriffe: EU plant Gegenmaßnahmen, einschließlich Sanktionen*, <https://www.consilium.europa.eu/de/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/> (Zugriff: 14. Juni 2021)
- [49] bmi.bund.de, 2021: *Cyber-Sicherheitsstrategie für Deutschland*, <http://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cyber-sicherheitsstrategie/cyber-sicherheitsstrategie-artikel.html> (Zugriff: 4. Mai 2021)
- [50] bmi.bund.de, 2021: *Jetzt Stellung nehmen: Entwurf der Cybersicherheitsstrategie 2021*, http://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2021/06/css-2021-beteiligung_sformat.html (Zugriff: 10. Juni 2021)
- [51] bmi.bund.de, 2021: *Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)*, <http://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/entwurf-zweites-it-sicherheitsgesetz.html> (Zugriff: 22. April 2021)
- [52] bsi.bund.de, 2021: *Das IT-Sicherheitsgesetz*, https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/it_sig.html (Zugriff: 21. Mai 2021)
- [53] bundestag.de, 2021: *Stellungnahme zum IT-SiG 2.0 für die Anhörung des Bundestagsausschusses für Inneres und Heimat*, <https://www.bundestag.de/resource/blob/825126/c932641828f11342efb2fbf372fa3dbc/A-Drs-19-4-741-C-data.pdf> (Zugriff: 22. April 2021)
- [54] netzpolitik.org, 2020: *IT-Sicherheitsgesetz 2.0: Seehofer will BSI zur Hackerbehörde ausbauen*, <https://netzpolitik.org/2020/seehofer-will-bsi-zur-hackerbehoerde-ausbauen/> (Zugriff: 22. Mai 2021)

- [55] netzpolitik.org, 2021: *BND-Gesetz: Bundesnachrichtendienst erhält so viele Überwachungsbefugnisse wie noch nie*, zugegriffen, <https://netzpolitik.org/2021/bnd-gesetz-bundesnachrichtendienst-erhaelt-so-viele-ueberwachungsbefugnisse-wie-noch-nie/> (Zugriff: 22. Mai 2021)
- [56] thw.de, 2021: *Die Bundesanstalt Technisches Hilfswerk*, https://www.thw.de/DE/THW/Bundesanstalt/bundesanstalt_node.html?noMobile=1 (Zugriff: 29. April 2021)
- [57] bundestag.de, 2012: *Bundesanstalten als nichtrechtsfähige Anstalt des Öffentlichen Rechts*, <https://www.bundestag.de/resource/blob/413556/1189dabd6fd9f8569aaeb35c619fcd06/WD-3-046-12-pdf-data.pdf> (Zugriff: 29. April 2021)
- [58] thw.de, 2021: *Gesetzlicher Auftrag des Technischen Hilfswerks*, https://www.thw.de/DE/THW/Bundesanstalt/Auftrag/auftrag_node.html (Zugriff: 29. April 2021)
- [59] cyber-peace.org, 2021: *Cyberattacke auf Estland*, <https://cyber-peace.org/cyberpeace-cyberwar/relevante-cybervorfalle/cyberattacke-auf-estland/> (Zugriff: 29. April 2021)
- [60] investinestonia.com, 2017: *How Estonia Became a Global Heavyweight in Cyber Security*, <https://investinestonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/> (Zugriff: 29. April 2021)
- [61] kaitseliit.ee, 2021: *EDL Cyber Unit*, <https://www.kaitseliit.ee/en/cyber-unit> (Zugriff: 2. Mai 2021)
- [62] ccdcoe.org, 2013: *The Cyber Defence Unit of the Estonian Defence League*, https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf (Zugriff: 7. Mai 2021)
- [63] cisa.gov, 2020: *Critical Infrastructure Cyber Community C3 Voluntary Program*, <https://www.cisa.gov/ccubedvp> (Zugriff: 9. Mai 2021)
- [64] us-cert.cisa.gov, 2021: *Resources Cybersecurity Framework*, <https://us-cert.cisa.gov/resources> (Zugriff: 9. Mai 2021)
- [65] bundestag.de, 2018: *Drucksache 19/2645: Cyberabteilungen im Zuständigkeitsbereich der Bundesministerien*, <https://dserver.bundestag.de/btd/19/026/1902645.pdf> (Zugriff: 14. April 2021)
- [66] security-insider.de, 2018: *Was ist ein CERT?*, <https://www.security-insider.de/was-ist-ein-cert-a-702654/> (Zugriff: 10. Mai 2021)
- [67] cert-bund.de, 2021: *CERT-Bund*, <https://www.cert-bund.de/> (Zugriff: 14. Juni 2021)
- [68] bsi.bund.de, 2021: *Bürger-CERT*, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html (Zugriff: 14. Juni 2021)
- [69] geant.org, 2021: *TF-CSIRT: Computer Security Incident Response Teams*, https://www.geant.org:443/People/Community_Programme/Task_Forces/Pages/TF-CSIRT.aspx (Zugriff: 14. Juni 2021)

- [70] bka.de, 2021: *BKA - Nationales Cyber-Abwehrzentrum*, https://www.bka.de/DE/UnsereAufgaben/Kooperationen/NCAZ/ncaz_node.html (Zugriff: 14. Juni 2021)
- [71] secupedia.info, 2021: *Verwaltungs-CERT-Verbund*, <https://www.secupedia.info/wiki/Verwaltungs-CERT-Verbund> (Zugriff: 13. Mai 2021)
- [72] it-planungsrat.de, 2013: *Leitlinie Informationssicherheit in der öffentlichen Verwaltung*, https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/10_Sitzung/Leitlinie_Informationssicherheit_Hauptdokument.html (Zugriff: 13. Mai 2021)
- [73] allianz-fuer-cybersicherheit.de, 2021: *Allianz für Cyber-Sicherheit - ACS*, https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/home_node.html (Zugriff: 13. Mai 2021)
- [74] cert-verbund.de, *Überblick des CERT-Verbunds*, <https://www.cert-verbund.de/> (Zugriff: 9. Mai 2021)
- [75] kritis.bund.de, 2021: *Vorstellung UP KRITIS*, https://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/upk_node.html (Zugriff: 13. Mai 2021)
- [76] bsi.bund.de, *Vorfallunterstützung – Mit CERT-Bund und MIRT*, <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/CyberSicherheitslage/Reaktion/Vorfallunterstuetzung/MIRT/mirt.html> (Zugriff: 10. Mai 2021)
- [77] *Siehe 5, Seite 6*
- [78] bsi.bund.de, 2021: *Abteilung WG - Cyber-Sicherheit für Wirtschaft und Gesellschaft*, <https://www.bsi.bund.de/DE/Das-BSI/Organisation-und-Aufbau/Abteilungen-inkl-Organigramm/Abteilung-WG/abteilung-wg.html> (Zugriff: 13. Mai 2021)
- [79] bsi.bund.de, 2021: *Cyber-Sicherheitsnetzwerk des BSI*, <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/cyber-sicherheitsnetzwerk.html> (Zugriff: 9. Mai 2021)
- [80] qskills.de, 2021: *Workshop zum Vorfall-Experten des CSN des BSI*, <https://www.qskills.de/qs/workshops/governance/sc580vorfall-expertedescybersicherheitsnetzwerksdesbsi/> (Zugriff: 9. Mai 2021)
- [81] bbk.bund.de, 2021: *LÜKEX 21*, https://www.bbk.bund.de/DE/AufgabenundAusstattung/Krisenmanagement/Luekex/LUEKEX_21/LUEKEX_21_node.html (Zugriff: 14. Juni 2021)
- [82] bundeswehr.de, 2019: *Locked Shields*, <https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/uebungen/locked-shields-119136> (Zugriff: 14. Juni 2021)
- [83] nerc.com, 2021: *Allgemeines Zu GridEx*, <https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx> (Zugriff: 15. Mai 2021)
- [84] zdf.de, 2021: *Experten: IT-Sicherheit in Deutschland ‚desaströs‘*, <https://www.zdf.de/uri/6b5e5843-d5e4-4971-9c28-372d1f249356> (Zugriff: 10. Mai 2021)

- [85] heise.de, 2021: *Exchange-Lücken: BSI sieht hierzulande zehntausende Server betroffen*, <https://www.heise.de/news/Exchange-Luecken-BSI-sieht-hierzulande-zehntausende-Server-betroffen-5073716.html> (Zugriff: 14. Juni 2021)
- [86] *Siehe 84*
- [87] bsi.bund.de, 2020: *Die Lage der IT-Sicherheit in Deutschland 2020*, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2 (Zugriff: 10. Mai 2021)
- [88] bka.de, 2021: *Bundeslagebild Cybercrime 2020*, <https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2020.html> (Zugriff: 21. Juni 2021)
- [89] it-sicherheit-in-der-wirtschaft.de, 2020: *Auswirkungen von COVID-19 auf die IT-Sicherheit und Handlungsempfehlungen*, <https://www.it-sicherheit-in-der-wirtschaft.de/ITS/Redaktion/DE/Meldungen/2020/2020-03-19-auswirkungen-covid-19-auf-it-sicherheit.html> (Zugriff: 21. Mai 2021)
- [90] *Siehe 5, Seite 4 f.*
- [91] security-insider.de, 2019: *5 Gründe, die das Risiko Kritischer Infrastrukturen erhöhen*, <https://www.security-insider.de/5-gruende-die-das-risiko-kritischer-infrastrukturen-erhoehen-a-850951/> (Zugriff: 15. Mai 2021)
- [92] tenable.com, 2019: *Cybersecurity-Fachkräfte sind mit erheblichen Schwierigkeiten bei der OT-Sicherheit konfrontiert: Ponemon-Bericht*, <https://de.tenable.com/blog/cybersecurity-pros-face-significant-challenges-with-ot-security-ponemon-report> (Zugriff: 15. Mai 2021)
- [93] *Siehe 13*
- [94] bundestag.de, 2021: *Stellungnahme des BSI-Präsidenten, Bilanzierung des Bevölkerungsschutzes angesichts der Corona-Pandemie*, <https://www.bundestag.de/resource/blob/833204/f80fedb9c35706c289a79fd85eb3d132/A-Drs-19-4-793-F-data.pdf> (Zugriff: 9. Mai 2021)
- [95] bibliomedmanager.de, 2017: *Trojaner im KIS*, <https://www.bibliomedmanager.de/fw/artikel/31425-trojaner-im-kis> (Zugriff: 21. Mai 2021)
- [96] reuters.com, 2021: *Hackers Try to Contaminate Florida Town's Water Supply through Computer Breach*, <https://www.reuters.com/article/us-usa-cyber-florida-idUSKBN2A82FV> (Zugriff: 10. Mai 2021)
- [97] tagesschau.de, 2021: *Hackerangriff auf Pipeline: USA erklären regionalen Notstand*, <https://www.tagesschau.de/ausland/usa-notstand-pipeline-101.html> (Zugriff: 13. Mai 2021)
- [98] oracle.com, 2021: *Was ist das Internet of Things?*, <https://www.oracle.com/de/internet-of-things/what-is-iot/> (Zugriff: 23. Mai 2021)

- [99] *Siehe 5, Seite 17*
- [100] bundestag.de, 2011: *Drucksache 17/5672: Gefährdung und Verletzbarkeit moderner Gesellschaften - am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung*, <https://dipbt.bundestag.de/dip21/btd/17/056/1705672.pdf> (Zugriff: 17. Mai 2021)
- [101] netzpolitik.org, 2016: *TR-069, die Telekom, und das, was wirklich geschah*, <https://netzpolitik.org/2016/tr-069-die-telekom-und-das-was-wirklich-geschah/> (Zugriff: 23. Mai 2021)
- [102] *Siehe 100*
- [103] *Siehe 5*
- [104] *Siehe 16*
- [105] *Siehe 5, Seite 12*
- [106] cybersecurityaustria.at, 2021: *Cyber Security Austria*, <https://www.cybersecurityaustria.at/> (Zugriff: zugegriffen 23. Mai 2021)
- [107] *Siehe 5, Seite 12 f.*
- [110] bmbf.de, 2016: *Freiwillige Helfer besser koordinieren*, <https://www.bmbf.de/de/freiwillige-helfer-besser-koordinieren-3398.html> (Zugriff: 23. Mai 2021)
- [111] gesetze-im-internet.de, 2021: *Grundgesetz für die Bundesrepublik Deutschland*, <https://www.gesetze-im-internet.de/gg/BJNR000010949.html> (Zugriff: 14. Juni 2021)
- [112] gesetze-im-internet.de, 2021: *THWG - Gesetz über das Technische Hilfswerk*, <https://www.gesetze-im-internet.de/thw-helfrg/BJNR001180990.html> (Zugriff: 23. Mai 2021)
- [113] *Siehe 5, Seite 13 f.*
- [114] bka.de, 2021: *Infrastruktur der Emotet-Schadsoftware zerschlagen*, https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html (Zugriff: 23. Mai 2021)
- [115] golem.de, 2019: *Hackerangriff auf Uni Gießen: Lange Schlangen für 38.000 neue E-Mail-Passwörter*, www.golem.de/news/hackerangriff-auf-uni-giessen-lange-schlangen-fuer-38-000-neue-e-mail-passwoerter-1912-145593.html (Zugriff: 23. Mai 2021)
- [116] hl7.org, 2021: *Health Level Seven International - Homepage*, <http://www.hl7.org/> (Zugriff: 23. Mai 2021)
- [117] *Siehe 5, Seite 18*
- [118] *Siehe 5, Seite 18 f.*
- [119] *Siehe 5, Seite 19 f.*
- [120] *Siehe 5, Seite 20 f.*
- [121] *Siehe 5, Seite 23 ff.*

- [122] drk.de, 2021: *Das DRK*, <https://www.drk.de/das-drk/> (Zugriff: 24. Mai 2021)
- [123] drk.de, 2021: *DRK-Gesetz*, <https://www.drk.de/das-drk/auftrag-ziele-aufgaben-und-selbstverstaendnis-des-drk/drk-gesetz/> (Zugriff: 24. Mai 2021)
- [124] *Siehe 5, Seite 24*
- [125] *Siehe 5, Seite 30*
- [126] *Siehe 5, Seite 25*
- [127] juraforum.de, 2021: *Verwaltungshelfer: Definition, Begriff und Erklärung*, <https://www.juraforum.de/lexikon/verwaltungshelfer> (Zugriff: 15. Juni 2021)
- [128] *Siehe 112*
- [129] bbk.bund.de, 2016: *Rechtliche Koordinaten für den Einsatz von Spontanhelfern*, https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Sonstiges/Buerger_und_Buergerinnen.pdf?__blob=publicationFile (Zugriff: 15. Mai 2021)
- [130] *Siehe 5, Seite 26*
- [131] *Siehe 5, Seite 27*
- [132] thwiki.org, 2017: *THWin*, <https://thwiki.org/t=THWin> (Zugriff: 15. Juni 2021)
- [133] *Siehe 5, Seite 27 f.*
- [134] ccc.de, 2021: *Hackerethik*, <https://www.ccc.de/de/hackerethik> (Zugriff: 24. Mai 2021)
- [135] ag.kritis.info, 2021: *Politische Forderungen der AG KRITIS*, <https://ag.kritis.info/politische-forderungen/> (Zugriff: 24. Mai 2021)
- [136] *Siehe 54*
- [137] *Siehe 5, Seite 29 f.*
- [138] *Siehe 79*
- [139] *Siehe 100*
- [140] *Siehe 5, Seite 30*
- [141] cdurlp.de, 2021: *Regierungsprogramm der CDU RLP für 2021-26*, https://www.cdurlp.de/sites/www.cdu-rlp.de/files/antraege/cdu-rlp-regierungsprogramm_210126_2.pdf (Zugriff: 26. Mai 2021)
- [142] bundestag.de, 2020: *Drucksache 19/24632: Pandemie als digitalen Weckruf ernstnehmen*, <http://dipbt.bundestag.de/dip21/btd/19/246/1924632.pdf> (Zugriff: 27. Mai 2021)
- [143] handelsblatt.com, *Jan-Philipp Albrecht: Das ist der Vater der DSGVO*, <https://www.handelsblatt.com/politik/international/jan-philipp-albrecht-das-ist-der-vater-der-dsgvo/22605018.html> (Zugriff: 27. Mai 2021)

Studien

- [108] statista.com, 2020: *Verbreitung ehrenamtlicher Arbeit in Deutschland 2020*, <https://de.statista.com/statistik/daten/studie/173632/umfrage/verbreitung-ehrenamtlicher-arbeit/> (Zugriff 23. Mai 2021)
- [109] diw.de, 2019: *Wachsendes ehrenamtliches Engagement: Generation der 68er häufiger auch nach dem Renteneintritt aktiv*, https://www.diw.de/de/diw_01.c.683556.de/publikationen/wochenberichte/2019_42/wachsendes-ehrenamtliches-engagement-generation-der-68er-haeufiger-auch-nach-dem-renteneintritt-aktiv.html (Zugriff 23. Mai 2021)

Bildquellen

- [1.1] Eigene Abbildung der KRITIS-Sektoren nach KritisV der Bundesrepublik Deutschland
- [3.1] Rollenverständnis im CSN
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/cyber-sicherheitsnetzwerk_node.html
(Zugriff 09.05.2021)
- [4.1] Eigene Visualisierung zur Bewältigungsdauer eines Angriffsszenarios mit CHW
- [5.1] Eigene Visualisierung zu den Rollen im Cyber-Hilfswerk nach Konzept der AG KRITIS
- [5.2] Eigene Tabelle Mapping der CCC Hackerethik auf politische Forderungen an ein CHW

V Eigenständigkeitserklärung

Hiermit versichere ich, dass ich die vorliegende Arbeit bisher bei keiner anderen Prüfungsbehörde eingereicht, sie selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt sowie Zitate kenntlich gemacht habe.

A handwritten signature in black ink, reading 'Yannik Meinhardt'. The signature is written in a cursive style with a large initial 'Y'.

Yannik Meinhardt

Berlin, 23.06.2021