Stiftung Neue Verantwortung

KONRAD ADENAUER STIFTUNG

# Die Beantwortung von staatlich verantworteten Cyberoperationen

**Impuls zur deutschen Cybersicherheitspolitik**

Dr. Sven Herpig

## Impressum

**Herausgeberin:**
Konrad-Adenauer-Stiftung e. V. 2021, Berlin

**Verantwortlicher in der Konrad-Adenauer-Stiftung:**
Johannes Wiggen
Referent Cybersicherheit
Analyse und Beratung
T +49 30 / 26996-3934
johannes.wiggen@kas.de

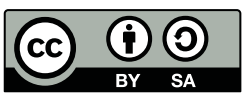


Umschlagfoto: © Unsplash/Marc Schorr
Gestaltung und Satz: yellow too, Pasiek Horntrich GbR

Die Printausgabe wurde bei der Druckerei Kern GmbH, Bexbach, klimaneutral produziert und auf FSC-zertifiziertem Papier gedruckt.

Printed in Germany.

Gedruckt mit finanzieller Unterstützung der Bundesrepublik Deutschland.






ISBN: 978-3-95721-920-6

# Die Beantwortung von staatlich verantworteten Cyberoperationen

**Impuls zur deutschen Cybersicherheitspolitik**

Dr. Sven Herpig

# Auf einen Blick

Spätestens mit dem Bekanntwerden der Cyberoperation gegen den Deutschen Bundestag 2015[1] ist die Bedeutung von Cybersicherheit in Deutschland in den Fokus der Innen-, Verteidigungs- und Außenpolitik geraten. Das Bundesamt für Sicherheit in der Informationstechnik bezeichnete in seinem jährlichen Lagebericht 2020 die Gefährdungslage einmal mehr als „angespannt".[2]

Die Bedrohung durch staatlich verantwortete Operationen im Cyberraum ist deutlich fassbar, und nicht erst seit heute. Es ist daher elementar, sich mit der Frage zu beschäftigen, wie ein Staat diese Operationen beantworten sollte. Mit der Beantwortung von Cyberoperationen können Staaten unterschiedliche Zwecke verfolgen:

1. Normen für staatliches Verhalten aushandeln oder bestehende bestärken, etwa durch das Aufzeigen roter Linien;
2. Signalisieren der eigenen Zurechnungsfähigkeiten;
3. Sanktionieren von Normenverletzungen;
4. Langfristige Herbeiführung von Verhaltensänderungen.

Damit das funktionieren kann, sollte die Beantwortung geeignet sein und zeitnah erfolgen. Im Falle der Cyberoperation gegen den Bundestag dauerte es fünf Jahre, bevor die Bundesregierung öffentlich kommunizierte, auf nationaler[3] und europäischer[4] Ebene gegen die Urheberinnen und Urheber vorzugehen, um durch einen internationalen Haftbefehl eine Verhaltensänderung zu erzielen – oder zumindest das Verhalten niedrigschwellig zu sanktionieren und auf eine rote Linie hinzuweisen. In diesem Fall erfolgte die öffentliche Beantwortung nicht zeitnah. Ob sie geeignet war, wird sich noch zeigen müssen.

Die deutsche Cybersicherheitspolitik steht derzeit vor unterschiedlichen Herausforderungen, die möglicherweise eine entschiedene – insbesondere: zeitnahe und geeignete – Beantwortung von Cyberoperationen in der Vergangenheit verhindert haben. Dazu zählen das Fehlen einer klaren Cybersicherheitspolitikstrategie, die unter anderem definiert, was das Ziel der staatlichen Beantwortung

von Cyberoperationen sein soll, genauso wie Prozesse, um eine geeignete Beantwortung entsprechend den strategischen Zielen – angebunden an die europäische Ebene – zeitnah umzusetzen.

Um die aktuelle Cybersicherheitspolitik zu verbessern und Deutschland bei der Beantwortung von Cyberoperationen handlungsfähiger und anschlussfähiger an die internationale Zusammenarbeit in diesem Bereich – zum Beispiel an die EU Cyber Diplomacy Toolbox – zu machen, sollten folgende Handlungsempfehlungen umgesetzt werden:

1. Entwicklung einer Cybersicherheitspolitikstrategie
2. Einsetzen einer bzw. eines Beauftragten für Cybersicherheitspolitik
3. Einrichten eines interministeriellen Jour fixe „Cybersicherheit“
4. Ausrichtung zu strategischer öffentlicher Zuschreibung, möglichst gemeinsam mit internationalen Partnerstaaten
5. Erarbeitung eines Stufensystems zur Analyse von Auswirkungen der Cyberoperationen als Grundlage für die Beantwortung
6. Informationsweitergabe zwischen den zuständigen Behörden von „Holschuld“ zur „Bringschuld“ entwickeln

1 Sven Herpig (2017), Cyber Operations: Defending Political IT-Infrastructures, online unter: https://www.stiftung-nv.de/sites/default/files/tcf-defending_political_lt-infrastructures-problem_analysis.pdf (letzter Zugriff: 27.4.2021); Florian Flade und Georg Mascolo (2020), Bärenjagd, in: *Süddeutsche Zeitung*, 5.5.2020, online unter: https://www.sueddeutsche.de/politik/hack-bundestag-angriff-russland-1.4891668 (letzter Zugriff: 27.4.2021).

2 Bundesamt für Sicherheit in der Informationstechnik (2020), Die Lage der IT-Sicherheit in Deutschland 2020, online unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf (letzter Zugriff: 27.4.2021).

3 Florian Flade und Georg Mascolo (2020), a. a. O.

4 Handelsblatt (2020), EU sanktioniert Russen für Hackerangriff auf Bundestag, online unter: https://www.handelsblatt.com/politik/international/cyber-attacke-eu-sanktioniert-russen-fuer-hackerangriff-auf-bundestag/26300620.html (letzter Zugriff: 27.4.2021).

# Danksagung

Diese Analyse wurde von Expertinnen und Experten im Rahmen einer Onlinekollaboration und eines virtuellen Workshops unterstützt. Die vertretenen Meinungen und Positionen sind allein die des Autors und geben nicht notwendigerweise die Meinung der Expertinnen und Experten oder der jeweiligen Arbeitgeberinnen und Arbeitgeber wieder.

Besonderer Dank gilt:

1. Manuel Atug, AG KRITIS
2. Florian J. Egloff, Center for Security Studies, ETH Zürich
3. Mark Ennulat, Deutsche Telekom Security GmbH
4. Stefanie Frey, Deutor Cyber Security Solutions
5. Julia Grauvogel, German Institute for Global and Area Studies (GIGA)
6. Henning Lahmann, Digital Society Institute
7. Jens Lange, Stadt Kassel
8. Alexandra Paulus, Technische Universität Chemnitz
9. Thomas Reinhold, Lehrstuhl Wissenschaft und Technik für Frieden und Sicherheit, Technische Universität Darmstadt
10. Julia Schuetze, Stiftung Neue Verantwortung e. V.
11. Marcel Stolz, Cyber Security Analytics Group, University of Oxford
12. Johannes Wiggen, Analyse und Beratung, Konrad-Adenauer-Stiftung e. V.

# Danksagung

Weiterer Dank gilt den Ansprechpartnerinnen und Ansprechpartnern, die für vertrauliche Hintergrundgespräche zur Verfügung standen.

Zusätzlicher Dank gilt Christina Rupp für die Unterstützung bei der Workshopdurchführung.

Die Projektidee entwickelten die Konrad-Adenauer-Stiftung e. V. und die Stiftung Neue Verantwortung e. V. gemeinsam. Das Projekt wurde von der Konrad-Adenauer-Stiftung e. V. finanziert und durch die Stiftung Neue Verantwortung e. V. implementiert.

# Inhaltsverzeichnis


1. Einleitung ..... 8

2. Bereiche bei der Beantwortung von Cyberoperationen ..... 12

2.1 IT-Sicherheit 12
2.1.1 Prävention 12
2.1.2 Detektion 12
2.1.3 Reaktion 13

2.2 Attribution 14
2.2.1 Zurechnung 14
2.2.2 Zuschreibung 15

2.3 Beantwortungsinstrumentarium 15
2.3.1 Weitergabe von Informationen 15
2.3.2 Nachrichten- und geheimdienstliche Operationen 16
2.3.3 Diplomatische Maßnahmen 17
2.3.4 Strafrechtliche Ermittlungen 17
2.3.5 Sanktionen 18
2.3.6 Militäreinsatz 19

3. Herausforderungen der deutschen Cybersicherheitspolitik ..... 23

3.1 (Cyber-)Strategielosigkeit 23

3.2 Kein zentrales Gremium zur strategischen Beurteilung 24

3.3 Fehlender Prozess 25

3.4 Vernachrichtendienstlichung der Zurechnung 27

3.5 Fragmentiertes Lagebild 28

4. Empfehlungen für die Reform der deutschen Cybersicherheitspolitik ..... 32

4.1 Cybersicherheitspolitik-Strategie 32

4.2 Beauftragte bzw. Beauftragter für Cybersicherheitspolitik 33

4.3 Interministerieller Jour fixe „Cybersicherheit“ 34

4.4 Öffentliche Zuschreibung 35

4.5 Stufensystem für Auswirkungen 36

4.6 Von der „Holschuld“ zur „Bringschuld“ 38

5. Prozess für die Beantwortung von Cyberoperationen ..... 41

6. Fazit ..... 44

Quellen- und Literaturverzeichnis ..... 46

Autor ..... 60

# 1. Einleitung

Cybersicherheitspolitik[5] ist ein relativ junges Feld innerhalb der Innen-, Verteidigungs- und Außenpolitik, obwohl „Solar Sunrise“[6], eine Cyberoperation gegen das US-amerikanische Verteidigungsministerium, die oftmals als eine der ersten ihrer Art angeführt wird, bereits über 20 Jahre her ist. Der erste bekannt gewordene Fall von Cyberkriminalität, „Aids Trojan“[7], liegt über 30 Jahre zurück. Mittlerweile finden militärische Auseinandersetzungen[8], Sabotage[9], Einflussnahme auf demokratische Prozesse[10], Spionage[11], Gegenspionage[12] und Kriminalität[13] ganz selbstverständlich auch im Cyberraum statt. Dadurch befindet sich die (Cyber-)Gefährdungslage weltweit – auch in Deutschland – auf einem hohen Niveau.[14]

In der vorliegenden Analyse wird hauptsächlich von Cyberoperationen[15], für die Staaten in unterschiedlichem Ausmaß verantwortlich sind[16] – im Bereich nachrichten- und geheimdienstliche Aktivitäten – gesprochen. Dabei wird die Einbettung einzelner Operationen in Kampagnen[17] mitgedacht. Cyberkriminalität[18] befindet sich außerhalb der Betrachtung dieser Analyse. Von einem Vorfall wird immer dann gesprochen, wenn zu dem entsprechenden Zeitpunkt noch nicht klar ist, was die Ursache für eine Anomalie ist.

In der vorliegenden Analyse wird zwischen Reaktion auf eine Cyberoperation und ihrer Beantwortung in der Gesamtheit unterschieden. Während die Reaktion ein Aspekt der IT-Sicherheit ist, umfasst die Beantwortung alle drei im Folgenden beschriebenen Bereiche „IT-Sicherheit“, „Attribution“ und „Beantwortungsinstrumentarium“. Die (technische und organisatorische) Reaktion zielt darauf ab, Schaden einzudämmen, Schutzziele wiederherzustellen, Prozesse fortzusetzen und Spuren zu analysieren. Die (strategische) Beantwortung von Cyberoperationen beinhaltet wiederum alle Aktivitäten, die

1. Normen für staatliches Verhalten aushandeln oder bestehende bestärken, etwa durch das Aufzeigen roter Linien,
2. die eigenen Aufklärungs- und Zurechnungsfähigkeiten signalisieren,
3. Normenverletzungen sanktionieren und
4. langfristig Verhaltensänderungen herbeiführen.

Damit die Beantwortung von Cyberoperationen, z. B. durch öffentliche Zuschreibung oder Sanktionen, glaubwürdig ist und im günstigen Fall das zukünftige Handeln des Aggressors oder der Aggressorin positiv beeinflusst, muss die Antwort geeignet sein und zeitnah erfolgen. Die Grundlage dafür kann ein strukturierter Prozess bilden, der derzeit in Deutschland allerdings noch nicht existiert. Dieser Prozess kann nicht nur dazu beitragen, dass die Bundesregierung geeignet und zeitnah reagiert. Er ist auch eine Voraussetzung, um parallel entsprechende internationale Maßnahmen vorzubereiten und zu koordinieren – wie zum Beispiel Wirtschaftssanktionen über die Cyber Diplomacy Toolbox[19] auf EU-Ebene oder kollektive öffentliche Zuschreibungen mit gleichgesinnten Partnern.

Während sich Deutschland auf der einen Seite damit beschäftigt, wie digitale Technologie sicherer gemacht werden kann, fehlt es auf der anderen Seite an einem öffentlichen und parlamentarischen Diskurs darüber, wie der Staat mit gegen sich gerichteten Cyberoperationen umgehen, sie beantworten soll. Den Handlungsbedarf in diesen Bereichen kann man unter anderem daran erkennen, dass sich die Gefährdungslage für Deutschland nicht verbessert[20], die Bundesregierung für den „Bundestagshack“ von 2015 erst 2020 Sanktionen gegen Russland auf EU-Ebene vorangetrieben hat[21] und über Beantwortungen der Cyberoperation gegen das Auswärtige Amt (AA) 2017[22] und der seit 2016 laufenden „Winnti“-Kampagne gegen die deutsche Industrie[23] bis heute nichts bekannt ist.

Die vorliegende Analyse[24] beschreibt drei Bereiche – IT-Sicherheit, Attribution und Beantwortungsinstrumentarium – und wie ihre Einzelteile bei der Beantwortung von Cyberoperationen ineinandergreifen. Sie skizziert die aktuellen Herausforderungen der deutschen Cybersicherheitspolitik und welche negativen Auswirkungen sie auf die Funktionalität der einzelnen Bereiche haben. Basierend auf dieser Problemanalyse werden Policyempfehlungen vorgestellt, die die Implementierung eines adäquaten Prozesses zur Beantwortung von Cyberoperationen ermöglichen. Abschließend wird ein möglicher Prozess beispielhaft aufgezeichnet.

5 Cybersicherheitspolitik wird hier als ein Teilbereich der Innenpolitik mit Schnittmengen zu anderen Politikfeldern, v. a. der Außen- und Verteidigungspolitik betrachtet.

6 Fred Kaplan (2016), Dark Territory: The Secret History of Cyber War. New York, Simon & Schuster.

7 Hauke Gierow (2016), Die erste Ransomware: Der Virus des wunderlichen Dr. Popp, in: *golem.de*, 7.7.2016, online unter: https://www.golem.de/news/die-erste-ransomware-der-virus-des-wunderlichen-dr-popp-1607-121809.html (letzter Zugriff: 27.4.2021).

8 z. B. Georgien 2008, siehe: David Hollis (2011), Cyberwar Case Study: Georgia 2008, online unter: https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf (letzter Zugriff: 27.4.2021).

9 z. B. Operation „Stuxnet"/„Olympic Games", siehe: Kim Zetter (2014), Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. New York, Crown.

10 Sven Herpig, Julia Schuetze und Jonathan Jones (2018), Der Schutz von Wahlen in vernetzten Gesellschaften: Wie sich die Sicherheit datenintensiver Wahlen erhöhen lässt. Stiftung Neue Verantwortung, online unter: https://www.stiftung-nv.de/sites/default/files/der_schutz_von_wahlen_in_vernetzten_gesellschaften.pdf (letzter Zugriff: 27.4.2021).

11 z. B. Operation GhostNet, siehe: The SecDev Group (2009), Tracking GhostNet: Investigating a Cyber Espionage Network, online unter: http://www.nartv.org/mirror/ghostnet.pdf (letzter Zugriff: 27.4.2021).

12 z. B. die niederländische Gegenspionage gegen Russland, siehe: Huik Modderkolk (2018), Dutch agencies provide crucial intel about Russia's interference in US-elections, in: *de Volkskrant*, online unter: https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/ (letzter Zugriff: 27.4.2021).

13 z. B. „Revil"/„Sodinokibi Ransomware", siehe: SingCERT (2020), Revil Unravelled, online unter: https://www.csa.gov.sg/singcert/publications/revil-unravelled (letzter Zugriff: 27.4.2021).

14 Bundesamt für Sicherheit in der Informationstechnik (2020), Die Lage der IT-Sicherheit in Deutschland 2020, online unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf (letzter Zugriff: 27.4.2021).

15 Zugrundeliegende Definition für diese Analyse: „the targeted use and hack of digital code by any individual, group, organization or state using digital networks, systems and connected devices [...] in order to steal, alter, destroy information or disrupt and deny functionality with the ultimate aim to weaken and/or harm a targeted political unit", siehe: Sven Herpig (2016), Anti-War and the Cyber Triangle – Strategic Implications of Cyber Operations and Cyber Security for the State, online unter: https://www.stiftung-nv.de/sites/default/files/antiwar_cybertriangle-herpig.pdf (letzter Zugriff: 27.4.2021).

16 Jason Healey (2011), Beyond Attribution: Seeking National Responsibility for Cyber Attacks, in: *Atlantic Council*, online unter: https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF (letzter Zugriff: 27.4.2021).

17 Sven Herpig (2020a), When does a cyber attack/operation become a (cyber) campaign? – Twitter Thread, online unter: https://twitter.com/z_edian/status/1329425489275056132 (letzter Zugriff: 27.4.2021).

18 Zugrundeliegende Definition von Cybercrime im engeren Sinne: „Straftaten, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten", siehe: Bundeskriminalamt (2020), Bundeslagebild Cybercrime 2019, online unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2019.pdf (letzter Zugriff: 27.4.2021).

19 General Secretariat of the Council of the European Union (2017), Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities – approval of the final text, online unter: https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf (letzter Zugriff: 27.4.2021).

20 Vgl. Bundesamt für Sicherheit in der Informationstechnik (2019), Die Lage der IT-Sicherheit in Deutschland 2019, online unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf (letzter Zugriff: 27.4.2021) mit Bundesamt für Sicherheit in der Informationstechnik (2020), Die Lage der IT-Sicherheit in Deutschland 2020, online unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf (letzter Zugriff: 27.4.2021).

21 Catalin Cimpanu (2020), EU sanctions Russia over 2015 German Parliament hack, online unter: https://www.zdnet.com/article/eu-sanctions-russia-over-2015-german-parliament-hack/ (letzter Zugriff: 27.4.2021); Tagesschau (2020), Hackerangriff auf den Bundestag: Russischer Botschafter muss ins Auswärtige Amt, online unter: https://www.tagesschau.de/inland/russische-hacker-101.html (letzter Zugriff: 27.4.2021).

22 Der Spiegel (2018), Hackerangriff auf Regierungsnetz läuft noch, online unter: https://www.spiegel.de/netzwelt/netzpolitik/hackerangriff-auf-regierungsnetz-unter-kontrolle-aber-laeuft-noch-a-1196039.html (letzter Zugriff: 27.4.2021).

23 z. B. Hakan Tanriverdi, Svea Eckert, Jan Lukas Strozyk, Maximilian Zierer und Rebecca Ciesielski (2019), Angriff auf das Herz der deutschen Industrie, online unter: https://web.br.de/interaktiv/winnti/ (letzter Zugriff: 27.4.2021).
Hierzu gab es lediglich eine Informationsweitergabe (u. a. IoCs) ohne Zuschreibung durch das BfV, siehe Bundesamt für Verfassungsschutz (2019), BfV Cyber-Brief Nr. 01/2019 – Hinweis auf aktuelle Angriffskampagne –, online unter: https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/2019/bfv-cyber-brief-2019-1.pdf;jsessionid=F92035623869FAE61FECBA2EE7CC1AD0.intranet231?__blob=publicationFile&v=5 (letzter Zugriff: 27.4.2021), und die generelle Thematisierung von Industriespionage in „direkten Gesprächen mit der chinesischen Führung“, siehe Hakan Tanriverdi, Svea Eckert, Jan Strozyk, Maximilian Zierer und Rebecca Ciesielski (2019), a. a. O.

24 Die inhaltliche Grundlage für die vorliegende Analyse bilden zehn vertrauliche Hintergrundgespräche, ein interdisziplinärer Workshop mit zehn Expertinnen und Experten aus Wissenschaft, Wirtschaft und Zivilgesellschaft sowie weitere Instrumente der Onlinekollaboration mit den genannten Personengruppen.

# 2. Bereiche bei der Beantwortung von Cyberoperationen

## 2.1 IT-Sicherheit[25]

### 2.1.1 Prävention

Als Prävention wird in der IT-Sicherheit der vorbeugende Schutz von Daten in IT-Systemen im Sinne von Vertraulichkeit, Integrität und Verfügbarkeit – auch Schutzziele der IT-Sicherheit[26] genannt – vor Schadenswirkung bezeichnet. Bei der Prävention kommt ein weites Spektrum an technischen und organisatorischen Maßnahmen, wie Software (z. B. Antivirus, Firewall), Policies (z. B. Umgang mit Schwachstellen und Patches) oder Schulungen (z. B. Sensibilisierung zum Erkennen von Phishing) zum Einsatz. Prävention kommt vor allem vor einer Cyberoperation besondere Relevanz zu, da sie einen Vorfall verhindern beziehungsweise den dadurch entstehenden Schaden begrenzen soll. Ist ein solcher erst einmal eingetreten, spielt die Prävention eine leicht untergeordnete Rolle für den von der Cyberoperation betroffenen Akteur. Jedoch können über das Instrument „Weitergabe von Informationen“ bei Akteuren, die noch nicht von dieser Cyberoperation betroffen sind, entsprechend präventive Maßnahmen ergriffen werden, damit dort eine gleichartige Cyberoperation keinen oder geringeren Schaden verursacht.

### 2.1.2 Detektion

Als Detektion wird in der IT-Sicherheit die Erkennung von Anomalien in Prozessen, Datenflüssen, IT-Systemen und Netzwerken bezeichnet, die auf eine Cyberoperation hinweisen können. Bei der Detektion können unterschiedliche technische und organisatorische Maßnahmen zum Einsatz kommen. Diese beinhalten zum Beispiel Angriffserkennungssysteme (Intrusion Detection Systems), Anomalieerkennung auf Systemen und in Netzwerken, Schadsoftwareerkennung, Protokolldatenauswertung, Honeypots[27] und Canarytokens.[28] Eine weitere Maßnahme ist der technische Abgleich von bekannten oder – durch Dritte – übermittelten und veröffent-

lichten Indicators of Compromise (IoCs).[29] Die Detektion ist ein elementarer Baustein bei der Beantwortung von Cyberoperationen, da alle weiteren Elemente darauf aufbauen. Veranschaulicht wird das durch ein geflügeltes Wort im Bereich der Cybersicherheitspolitik, das vermutlich auf Dmitri Alperovitch zurückgeht: „There are only two types of companies – those that know they've been compromised, and those that don't know".[30] Denn Organisationen oder Institutionen, die nicht wissen, dass sie kompromittiert sind, können darauf nicht reagieren[31] – in Deutschland vergingen im Jahr 2020 laut IBM Security um Beispiel durchschnittlich 160 Tage bis zur Identifizierung und Eindämmung eines Vorfalls, der zu einer Datenschutzverletzung führte.[32]

### 2.1.3 Reaktion

Als Reaktion werden in der IT-Sicherheit solche technischen und organisatorischen Maßnahmen bezeichnet, die bei einem Vorfall ergriffen werden, um ihn einzudämmen, die Vertraulichkeit, Integrität und Verfügbarkeit der betroffenen IT-Systeme und Netzwerke wiederherzustellen, die Businessprozesse oder Produktion zeitnah fortzusetzen (Business Continuity Management) und die Spuren des Vorfalls für eine Analyse zu sichern. Hierunter fallen unter anderem das Durchführen von schadensmindernden Maßnahmen (z. B. Abschottung von Netzsegmenten), das Neuaufsetzen von IT-Systemen, das Einspielen von Back-ups und Sicherheitsupdates, aber auch die Analyse des Schadensausmaßes und -umfangs, sowie das Aktivieren eines Krisenmanagements – was natürlich bereits in der Prävention aufgesetzt und kontinuierlich geübt werden muss. Je nach Reaktion können die eingeleiteten Maßnahmen für den Aggressor oder die Aggressorin ein Anzeichen dafür sein, dass sein oder ihr Ziel die Operation bemerkt hat. Es kann daher je nach Situation und strategischen Vorgaben sinnvoll sein, bestimmte Maßnahmen nicht zu ergreifen, um den Aggressor oder die Aggressorin gewähren zu lassen und diesen oder dieser stattdessen – sofern möglich – genauer zu beobachten, wodurch zum Beispiel besserer Aufschluss über das Vorgehen, Ziel und die Herkunft der Operation gewonnen werden kann (vergleiche Abschnitt „Zurechnung"). Hierbei wird jedoch ein möglicherweise erhebliches Risiko eingegangen, dass noch weiterer Schaden angerichtet wird – zum Beispiel zusätzliches Abfließen von Daten oder Gefährdung von Dritten und entsprechende Auswirkungen, wenn das System als Ausgangspunkt für weitere Cyberoperationen oder Ähnliches genutzt wird.

Schließlich gehört zur Reaktion auch die Auswertung und Analyse der durch die Detektion gewonnenen Erkenntnisse zu Taktiken, Techniken und Vorgehensweise – sogenannte TTPs[33] – des Angreifers oder der Angreiferin sowie das Teilen der gewonnenen Informationen in der IT-Sicherheitsforscherinnen und -forscher-Community, zum Beispiel durch Aufnahme in eine Malware Infor-

mation Sharing Platform.[34] Die rein deskriptive Beschreibung von TTPs oder IoCs bewusst ohne Anteile einer Zurechnung erleichtert die schnelle und effektive Zusammenarbeit der für die IT-Sicherheit zuständigen Stellen (z. B. in einem CERT-Verbund) enorm, da keine zeitaufwändige Zurechnung erfolgen muss und eine darauf aufbauende Zuschreibung meist einem offiziellen Freigabeprozess unterliegt.

Die in einer Organisation festgelegte grundsätzliche Weitergabe von Informationen zur schnellen Information und Warnung Dritter ist bereits die Anwendung des Beantwortungsinstruments „Weitergabe von Informationen“. Es sieht eine Weitergabe von technischen Informationen, ggf. angereichert mit weiteren – zum Beispiel nachrichtendienstlichen – Informationen, vor. Ein Beispiel dafür wären technische Empfehlungen (Technical Advisories), die eine Cyberoperation möglicherweise sogar zuschreiben.[35]

## 2.2 Attribution

### 2.2.1 Zurechnung

Zuschreibung und Zurechnung werden im deutschen und englischen Sprachgebrauch oft als „Attribution“ bezeichnet. Um analytisch genauer arbeiten zu können, ist es sinnvoll, die beiden Termini nicht synonym zu verwenden.[36]

Die Zurechnung (Technical Attribution) beschreibt den Vorgang, bei dem durch technische, nachrichten- und geheimdienstliche sowie geopolitische Erkenntnisse[37] versucht wird, eine Cyberoperation einem bereits bekannten oder neuen Akteur zuzuordnen.[38] Diese Erkenntnisse können zum Beispiel durch forensische Analysen der Daten und betroffenen IT-Systeme gewonnen werden. Eine weitere Quelle kann der Informationsaustausch mit (ausländischen) Akteuren, inklusive öffentlicher Threat Intelligence Reports von Unternehmen und bestehenden technischen Communities (CERT/CSIRT) sowie Sicherheitsbehörden, sein. Auch wenn bei der Zurechnung auf Informationsquellen Dritter zurückgegriffen wird, erfolgt sie zunächst intern, also nicht öffentlich.

Die Zurechnung ist auch erst derjenige Schritt, mit der ein Vorfall zum Beispiel als Cyberoperation eingestuft werden kann. Die Datengrundlage für die Zurechnung wird bereits unter anderem in der Detektion (z. B. Protokolldatenauswertung) und durch Vorfeldaufklärung (z. B. SIGINT Support to Cyber Defense – SSCD[39]) gelegt, während weitere Informationen wie die TTPs im Verlauf der Reaktion, durch technische Maßnahmen Dritter (z. B. aus Warnmeldungen) oder durch nachrichten- und geheimdienstliche Operationen – zum Beispiel Gegenspionage via eigener Cyberoperationen[40], Human Intelligence (HUMINT) oder Open Source

Intelligence (OSINT) – gesammelt werden. Die Zurechnung kann dabei durch manuelle oder technische Analyse der Angriffswege und -mittel erfolgen, oder bei bekannten Indikatoren auch automatisiert im Rahmen der Detektion durch die Sensorik, zum Beispiel aus Angriffserkennungssystemen. Die Zurechnung ist die Grundlage für die Zuschreibung und den Einsatz des Beantwortungsinstrumentariums.

### 2.2.2 Zuschreibung

Die Zuschreibung (Political and Legal Attribution) beschreibt das Anreichern – zum Beispiel die mögliche Zuordnung einer (nachrichten- und geheimdienstlichen) Gruppe zu einem staatlichen Akteur oder eine indirekte Nennung/Eingrenzung[41] – und Kommunizieren dieser Zurechnungsergebnisse gegenüber Dritten. Die Zuschreibung kann dabei öffentlich oder nicht öffentlich geschehen. Eine nicht öffentliche Zuschreibung kann gegenüber dem vermuteten Aggressor oder der Aggressorin aber auch anderen – zum Beispiel Partnerstaaten im NATO-Verbund – erfolgen. Dies hängt von den politischen und strategischen Zielen ab, die mit der Zuschreibung verfolgt werden sollen. Die Zuschreibung kann alleinstehend sein, zum Beispiel durch eine Pressekonferenz oder einen Analysebericht mit Cartoons[42] sowie gemeinsam mit anderen Staaten[43] erfolgen.

Alternativ kann die Zuschreibung im Rahmen anderer Beantwortungsinstrumente erfolgen: Wenn etwa gegen die Urheberin bzw. den Urheber einer Cyberoperation Sanktionen verhängt werden, enthält der entsprechende Vorgang Informationen über die Zuschreibung. Ebenso können nationale Cybersicherheitsbehörden in technischen Empfehlungen nicht nur technische Informationen über Cyberoperationen teilen, sondern diese auch den Urheberinnen bzw. Urhebern zuschreiben.[44] Zuschreibungen signalisieren gegenüber Dritten zusätzlich die eigenen (technischen) Fähigkeiten, diese Zurechnungen entsprechend durchführen zu können.[45] Öffentliche Zuschreibungen können darüber hinaus innerhalb des zuschreibenden Landes zu einem politischen Handlungsdruck führen[46] und der Legitimierung des eingesetzten Beantwortungsinstrumentariums dienen.[47]

## 2.3 Beantwortungsinstrumentarium

### 2.3.1 Weitergabe von Informationen

Der Austausch von technischen Informationen mit Dritten zum Zwecke der Prävention, Detektion und Reaktion auf Cyberoperationen – z. B. in Form von Warnmeldungen[48] – ist Teil des nationalen Beantwortungsinstrumentariums zum Umgang mit Cyberoperationen. Dritte können zum Beispiel Computer Emergency Response Team (CERT) Communities, wie die European

Governments CERTs group (EGC)[49] oder das Computer Security Incident Response Teams (CSIRT) Network[50], andere (ausländische) Sicherheitsbehörden oder Privatunternehmen (zum Beispiel Betreiberinnen oder Betreiber Kritischer Infrastrukturen, Unternehmen im betroffenen Sektor[51] und Incident Response Dienstleister) sein. Die institutionalisierte Festlegung, dass unabhängig vom Einzelfall (technische) Informationen zur Information und Warnung Dritter im Rahmen der „Reaktion“ ausgetauscht werden, ist eine grundsätzliche Festlegung der Organisation zur Anwendung dieses Beantwortungsinstruments. Während die zeitnahe Weitergabe von technischen Informationen in erster Linie für die operative Ebene relevant ist, kann sie auch als politisches Instrument, zum Beispiel als Zuschreibung, genutzt werden.[52] Die weitergegebenen Informationen können implizit oder explizit Daten für eine Zurechnung von Cyberoperationen beinhalten oder sogar als Zuschreibung dienen.

**Beispiel für das Instrument „Weitergabe von Informationen“:**
Am 18. Mai 2020 versendeten der Bundesnachrichtendienst (BND), das Bundesamt für Verfassungsschutz (BfV) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeinsam eine nicht öffentliche Warnmeldung an Betreiberinnen und Betreiber von drei Sektoren in Kritischen Infrastrukturen bezüglich Cyberoperationen durch die Gruppe „Berserk Bear“.[53] Die Meldung enthielt technische Informationen und konkrete Handlungsempfehlungen.

### 2.3.2 Nachrichten- und geheimdienstliche Operationen

Nachrichten- und geheimdienstliche Operationen können im Rahmen des jeweils geltenden nationalen Rechtsrahmens möglicherweise als Spionage-, Sabotage- oder Gegenspionageaktivitäten zur Beantwortung von Cyberoperationen genutzt werden. Diese Maßnahmen müssen nicht notwendigerweise im Cyberraum erfolgen, sondern können auch in anderen Domänen oder domänenübergreifend durchgeführt werden.

Eine nachrichten- und geheimdienstliche Operation kann Informationen zur Zurechnung einer Cyberoperation beitragen – unter anderem durch bestimmte, intrusive, Formen aktiver Cyberabwehr[54] – und damit gegenüber der Urheberin bzw. dem Urheber der Cyberoperation als Zuschreibung dienen. Aktive Cyberabwehr ist hier definiert als „eine aktive Gegenmaßnahme unterhalb der Schwelle des bewaffneten Konflikts, die dazu ausgelegt ist, [eine Cyberoperation] abzuwehren und/oder aufzuklären“.[55]

Nachrichten- und geheimdienstliche Operationen können aber auch ohne vorherigen Vorfall möglicherweise bereits Informationen für präventive Maßnahmen und Detektion liefern – zum Beispiel durch

SSCD. Da nachrichten- und geheimdienstliche Operationen in der Regel klandestin stattfinden, können sie genutzt werden, um eine Antwort außerhalb der Öffentlichkeit zu senden.

**Beispiel für das Instrument „Nachrichten- und geheimdienstliche Operation“:**
Es gibt – qua klandestiner Natur dieser Operationen – so gut wie keine überlieferten nachrichten- und geheimdienstlichen Operationen als Antwort auf Cyberoperationen. Ein mögliches US-amerikanisches Beispiel[56] ist die gezielte Tötung von Junaid Hussain, einem Computerspezialisten, der im Auftrag des „Islamischen Staates“ gehandelt haben soll.[57]

### 2.3.3 Diplomatische Maßnahmen

Staaten stehen im Rahmen ihrer diplomatischen Beziehungen unterschiedliche Instrumente zur Verfügung, um auf eine Cyberoperation zu antworten. So können zum Beispiel eine Botschafterin bzw. ein Botschafter einbestellt oder die oder der eigene zur Berichterstattung zurückgerufen werden. Eine weitere Möglichkeit sind Protestnoten und die Ausweisung von Diplomatinnen und Diplomaten. Diplomatische Maßnahmen können aber auch nicht öffentlich genutzt werden, zum Beispiel im Rahmen von bilateralen Gesprächen. Während diese Aktivitäten immer auch eine Zuschreibung der Cyberoperation darstellen, hat jede öffentliche Zuschreibung – auch als Teil nicht diplomatischer Maßnahmen – ebenfalls immer diplomatische Auswirkungen.

**Beispiel für das Instrument „Diplomatische Maßnahmen“:**
Als Antwort auf die Cyberoperation gegen den Deutschen Bundestag 2015 verurteilte das Auswärtige Amt im Namen der Bundesregierung am 28. Mai 2020 diese Aktivität gegenüber dem geladenen Botschafter der Russischen Föderation „auf das Schärfste“.[58]

### 2.3.4 Strafrechtliche Ermittlungen

Als Antwort auf eine Cyberoperation können außerdem Strafverfahren eingeleitet werden – auch gegen unbekannt.[59] Für ein erfolgreiches Strafverfahren ist eine belastbare und gerichtsverwertbare Zurechnung der Cyberoperation zu einzelnen natürlichen Personen notwendig; eine Zurechnung nur zu juristischen Personen oder Organisationseinheiten reicht nicht aus. Dies stellt von Beginn an hohe Anforderungen an die Beweissicherung im Rahmen der Vorfallsanalyse im Bereich der IT-Sicherheit. Auf Basis von strafrechtlichen Ermittlungen kann ein nationaler oder internationaler Haftbefehl – zum Beispiel ein Europäischer Haftbefehl (EuHB) – erlassen werden.[60] Während die Einleitung von Ermittlungen in

einem Strafverfahren als Antwort auf eine Cyberoperation möglicherweise erst einmal nur symbolische bzw. diplomatische Wirkung hat, kann ein bestehender (internationaler) Haftbefehl durchaus direkten Einfluss auf das Verhalten der dort benannten Personen haben (z. B. Eingrenzung der Reisefreiheit wegen Auslieferungsabkommen).[61]

**Beispiel für das Instrument „Strafrechtliche Ermittlungen“:**
Im Januar 2016 leitete der deutsche Generalbundesanwalt (GBA) beim Bundesgerichtshof wegen des Verdachts der geheimdienstlichen Agententätigkeit im Rahmen der Cyberoperation gegen den Deutschen Bundestag 2015 ein Strafverfahren gegen unbekannt ein.[62] Im Mai 2020 beantragte der Generalbundesanwalt daraufhin wegen „geheimdienstlicher Agententätigkeit“ und dem „Ausspähen von Daten“ einen internationalen Haftbefehl gegen den russischen Bürger Dmitrij Badin, der Teil dieser Cyberoperation des russischen Militärgeheimdienstes Glawnoje Raswedywatelnoje Uprawlenije (GRU) gegen den Deutschen Bundestag gewesen sein soll.[63]

### 2.3.5 Sanktionen

Sanktionen sind ein weiteres Instrument, das als Antwort auf eine Cyberoperation genutzt werden kann. Es beinhaltet zum Beispiel das Einfrieren von Vermögen gelisteter natürlicher oder juristischer Personen, das Verbot, einem Personenkreis finanzielle Vermögenswerte bereitzustellen (Finanzsanktionen, sogenannte Listungen), Einreisebeschränkungen für natürliche Personen, aber auch Import- und Exportbeschränkungen von Waren und Dienstleistungen (sektorale Wirtschaftssanktionen). Wirtschafts- und Finanzsanktionen können, wie alle Beantwortungsinstrumente, auch unbeabsichtigte Auswirkungen nach sich ziehen.[64] Deutschland verhängt Sanktionen in der Regel nicht unilateral, sondern über die VN- oder die EU-Ebene. Es gibt auch noch unübliche Ziele, die mit Finanzsanktionen verfolgt werden können, wie die Beschlagnahmung von Kryptowährung.[65]

Das bestehende EU-Cybersanktionsregime erfordert keine Zuschreibung zu einem Staat. Dennoch können Informationen über die staatliche Verantwortung einer Cyberoperation wichtig sein, um Partnerstaaten von der Notwendigkeit der Sanktionen zu überzeugen. Weiterhin kann die Zuschreibung einer bestimmten Aktivität zu einem Land geeignet sein, um ein Sanktionsregime aufzusetzen. Für die Listung einzelner Personen oder Entitäten ist darüber hinaus aber erforderlich, dass diese eine spezifische Verbindung zu den sanktionsauslösenden Aktivitäten aufweisen. Die europäischen Gerichte überprüfen, ob der Rat der EU das Vorliegen dieser Listungsgründe hinreichend substantiiert hat und belegen kann.

**Beispiel für das Instrument „Sanktionen“:**
Auf Basis der Ermittlungen des Generalbundesanwalts hat die Bundesregierung auf EU-Ebene im Oktober 2020 Listungen in einem bestehenden Sanktionsregime als Antwort auf die Cyberoperation gegen den Bundestag 2015 erreicht.[66] Der Rat der EU hat im Rahmen des Cybersanktionsregimes – gemäß Verordnung (EU) 2019/796 – Finanzsanktionen gegen zwei natürliche Personen (Igor Kostjukow und Dmitri Badin) und den GRU, sowie – gemäß Ratsbeschluss (GASP) 2019/797 – EU-Einreiseverbote gegen die beiden natürlichen Personen verhängt.

### 2.3.6 Militäreinsatz

Als Antwort auf eine Cyberoperation ist auch ein Militäreinsatz innerhalb und außerhalb des Cyberraums sowie domänenübergreifend denkbar.[67] Es bedarf dazu jedoch aller Voraussetzungen, die auch sonstigen Militäreinsätzen in der jeweiligen Situation zugrunde liegen (zum Beispiel Parlamentsvorbehalt, UN-Mandat oder völkerrechtliche Rechtmäßigkeit der staatlichen Selbstverteidigung und anderer Faktoren, wie die Geeignetheit der Beantwortung).[68] Während ein Militäreinsatz niedrigschwellig ausgestaltet sein kann (zum Beispiel Erhöhung der Einsatzbereitschaft der Truppe oder Truppenverlegung), kann er in seiner extremen Ausprägung schwerwiegende Folgen, wie den Verlust von Menschenleben, haben. Daher bedarf es hierbei eines sehr hohen Grades an Gewissheit bezüglich Zurechnung zu der Urheberin bzw. dem Urheber der Cyberoperation. Dies gilt sowohl im nationalen als auch im internationalen Rahmen, zum Beispiel im NATO-Bündnisfall. Ein Militäreinsatz bedeutet gleichzeitig auch die Zuschreibung einer Cyberoperation – da sie in der Regel als Ausgangspunkt für den Militäreinsatz angeführt werden muss.[69]

In der Vergangenheit haben reine Cyberoperationen je nach Auslegung nicht, beziehungsweise selten,[70] die Schwelle zur völkerrechtlichen Gewaltanwendung überschritten, sondern fanden grundsätzlich im Rahmen nachrichten- und geheimdienstlicher Operationen oder bereits bestehender bewaffneter Konflikte statt. Auch wenn es international vereinzelt Militäroperationen als Antwort auf Cyberoperationen gegeben hat, käme eine Normalisierung dessen einem Paradigmenwechsel gleich.

**Beispiel für das Instrument „Militäreinsatz“:**
Am 4. Mai 2019 haben die Israelischen Verteidigungsstreitkräfte als Antwort auf eine vorhergehende Cyberoperation der Hamas einen Luftschlag gegen ein Gebäude durchgeführt, in dem sich Mitglieder der Hamas-internen Gruppe für Cyberoperationen befunden haben sollen.[71] Dieser Militäreinsatz fand innerhalb eines bestehenden bewaffneten Konflikts zwischen Israel und der Hamas statt.

25 Laut Bundesamt für Sicherheit in der Informationstechnik (2021), Glossar der Cyber-Sicherheit ist IT-Sicherheit wie folgt definiert: „IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind". Online unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html;jsessionid=0E6EA6061B01579E0B665831030639F5.internet461?nn=522504&cms_lv2=132764 (letzter Zugriff: 27.4.2021).
Im Verlauf der letzten Dekade nahm v. a. im anglo-amerikanischen, aber auch im europäischen Raum, der Gebrauch des Wortes Cybersicherheit zu. Der Begriff „Cybersicherheit" ist breiter angelegt als „IT-Sicherheit" und umfasst zusätzlich auch soziokulturelle, politische, rechtliche und weitere Dimensionen, vgl. Sven Herpig (2016), Anti-War and the Cyber Triangle – Strategic Implications of Cyber Operations and Cyber Security for the State, online unter: https://www.stiftung-nv.de/sites/default/files/antiwar_cybertriangle-herpig.pdf (letzter Zugriff: 27.4.2021).

26 Bundesamt für Sicherheit in der Informationstechnik (2021), IT-Grundschutz: Glossar, a. a. O.

27 Stefan Luber und Peter Schmitz (2018), Was ist ein Honeypot?, in: *Security-Insider* (18.4.2018), online unter: https://www.security-insider.de/was-ist-ein-honeypot-a-703883/ (letzter Zugriff: 27.4.2021).

28 Thinkst Canary (2021), Canarytokens, online unter: https://canary.tools/help/canarytokens (letzter Zugriff: 27.4.2021).

29 Timo Steffens (2016), Threat Intelligence: IT-Sicherheit zum Selbermachen?, in: *Heise online* (7.11.2016), online unter: https://www.heise.de/security/artikel/Threat-Intelligence-IT-Sicherheit-zum-Selbermachen-3453595.html (letzter Zugriff: 27.4.2021).

30 Michael Joseph Gross (2011), Enter the Cyber-Dragon, in: *Vanity Fair* (2.8.2011), online unter: https://www.vanityfair.com/news/2011/09/chinese-hacking-201109 (letzter Zugriff: 27.4.2021).

31 Es gibt jedoch bestehende Security-Design-Prinzipien, die von einer zukünftigen Kompromittierung ausgehen. Siehe z. B. Stefan Luber und Peter Schmitz (2018), Definition Zero Trust – Was ist ein Zero-Trust-Modell?, in: *Security Insider* (4.10.2018), online unter: https://www.security-insider.de/was-ist-ein-zero-trust-modell-a-752389/ (letzter Zugriff: 27.4.2021) und Ray Pompon (2017), Living in an Assume Breach world, in: *Helpnet Security*, online unter: https://www.helpnetsecurity.com/2017/08/24/assume-breach-world/ (letzter Zugriff: 27.4.2021).

32 IBM Security (2020), Cost of a Data Breach Report 2020, online unter: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/de [Anmeldung erforderlich].

33 Tactics, Techniques, and Procedures (TTPs) sind gemäß National Institute of Standards and Technology – NIST (2021), Tactics, Techniques, and Procedures (TTPs) definiert als „The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique", online unter: https://csrc.nist.gov/glossary/term/Tactics_Techniques_and_Procedures (letzter Zugriff: 27.4.2021).

34 Siehe z. B. MISP (2021), MISP – Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing, online unter: https://www.misp-project.org/index.html (letzter Zugriff: 27.4.2021).

35 Siehe z. B. National Security Agency (2020), Russian State-Sponsored Actors Exploiting Vulnerability in VMware Workspace ONE Access Using Compromised Credentials, online unter: https://media.defense.gov/2020/Dec/07/2002547071/-1/-1/0/CSA_VMWARE%20ACCESS_U_OO_195076_20.PDF (letzter Zugriff: 27.4.2021).

36 Florian J. Egloff (2020a), Public attribution of cyber intrusions, in: *Journal of Cybersecurity*, Vol. 6, Iss. 1, 2020, online unter: https://academic.oup.com/cybersecurity/article/6/1/tyaa012/5905454 (letzter Zugriff: 27.4.2021).

37 Timo Steffens (2021), Auf Tätersuche: Herausforderungen bei der Analyse von Cyber-Angriffen, in: *Heise online* (8.2.2021), online unter: https://www.heise.de/hintergrund/Auf-Taetersuche-Herausforderungen-bei-der-Analyse-von-Cyber-Angriffen-5043620.html (letzter Zugriff: 27.4.2021) und Sven Herpig und Thomas Reinhold (2018), Spotting the bear: credible attribution and Russian operations in cyberspace, in: Hacks, Leaks and Disruptions. Russian Cyper Strategies, in: *Chaillot Papers* No. 148, S. 33–43 (letzter Zugriff: 27.4.2021).

38 Weiterführende Informationen zu Attribution in Timo Steffens (2018), Auf der Spur der Hacker: Wie man die Täter hinter der Computer-Spionage enttarnt. Wiesbaden, Springer.

39 Bundesnachrichtendienst (2021), Cybersicherheit, online unter: https://www.bnd.bund.de/DE/Die_Themen/Cybersicherheit/cybersicherheit_node.html (letzter Zugriff: 27.4.2021).

40 Huik Modderkolk (2018), Dutch agencies provide crucial intel about Russia's interference in US-elections, in: *de Volkskrant*, online unter: https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/ (letzter Zugriff: 27.4.2021).

41 Vergleiche z. B. „There are only a few countries in the world who have the level of sophistication shown during the cyberattack campaign", hier: Kevin Kwang (2018), Singapore health system hit by ‚most serious breach of personal data' in cyberattack; PM Lee's data targeted, in: *Channel News Asia* (20.7.2018), online unter: https://www.channelnewsasia.com/news/singapore/singhealth-health-system-hit-serious-cyberattack-pm-lee-target-10548318 (letzter Zugriff: 27.4.2021).

42 Shannon Vavra (2020), How the Pentagon is trolling Russian, Chinese hackers with cartoons, in: *Cyberscoop* (12.11.2020), online unter: https://www.cyberscoop.com/pentagon-cyber-command-trolling-russian-chinese-hackers-cartoons/ (letzter Zugriff: 27.4.2021).

43 European Parliament (2018), Attribution of the NotPetya attack, online unter: https://www.europarl.europa.eu/doceo/document/E-8-2018-001005_EN.html (letzter Zugriff: 27.4.2021).

44 Siehe z. B. National Security Agency (2020), Russian State-Sponsored Actors Exploiting Vulnerability in VMware Workspace ONE Access Using Compromised Credentials, online unter: https://media.defense.gov/2020/Dec/07/2002547071/-1/-1/0/CSA_VMWARE%20ACCESS_U_OO_195076_20.PDF (letzter Zugriff: 27.4.2021).
In Deutschland setzt dies eine vorherige ministerielle Befassung und Entscheidung voraus.

45 Gil Baram (2020), Indicting Russia's Most Destructive Cyberwar Unit: The Implications of Public Attribution, in: *Council on Foreign Relations* (23.11.2020), online unter: https://www.cfr.org/blog/indicting-russias-most-destructive-cyberwar-unit-implications-public-attribution (letzter Zugriff: 27.4.2021).

46 Sven Herpig und Thomas Reinhold (2018), a. a. O.

47 Julia Schuetze (2020), EU-US Cybersecurity Policy Coming Together: Recommendations for instruments to accomplish joint strategic goals, EU Cyber Direct, online unter: https://eucyberdirect.eu/wp-content/uploads/2020/11/rif_eu-us-cybersecurity-final.pdf (letzter Zugriff: 29.04.2021).

48 Bundesamt für Sicherheit in der Informationstechnik (2021), Cyber-Sicherheit: Warn- und Informationsdienst (WID), online unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Technische-Sicherheitshinweise-und-Warnungen/Technische-Sicherheitshinweise/technische-sicherheitshinweise.html (letzter Zugriff: 27.4.2021).

49 European Government CERTs Group (2020), EGC group: European Government CERTs group, online unter: http://www.egc-group.org/ (letzter Zugriff: 27.4.2021).

50 European Union Agency for Cybersecurity (2021), CSIRTs Network, online unter: https://csirtsnetwork.eu/ (letzter Zugriff: 27.4.2021).

51 Timo Steffens (2021), a. a. O.

52 Siehe z. B. United States of America Office of the Director of National Intelligence (2017), Background to „Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution, online unter: https://www.dni.gov/files/documents/ICA_2017_01.pdf (letzter Zugriff: 27.4.2021).

53 Sean Lyngaas (2020), German intelligence agencies warn of Russian hacking threats to critical infrastructure, in: *Cyberscoop* (26.5.2020), online unter: https://www.cyberscoop.com/german-intelligence-memo-berserk-bear-critical-infrastructure/ (letzter Zugriff: 27.4.2021) und Hakan Tanriverdi (2020), Behörden warnen vor Angriffen: Russische Bären unter Hackerverdacht, in: *tagesschau.de* (27.5.2020), online unter: https://www.tagesschau.de/investigativ/br-recherche/hacker-angriff-infrastruktur-101.html (letzter Zugriff: 27.4.2021).

54 Sven Herpig (2018), Aktive Cyber-Abwehr/Hackback. Stiftung Neue Verantwortung, online unter: https://www.stiftung-nv.de/de/publikation/hackback-ist-nicht-gleich-hackback (letzter Zugriff: 27.4.2021).

55 ebd.

56 Es ist unklar, ob es sich hierbei um einen Einsatz des US-Militärs oder des Geheimdienstes CIA gehandelt hat.

57 Spencer Ackerman, Ewen MacAskill und Alice Ross (2015), Junaid Hussain: British hacker for Isis believed killed in US air strike, in: *The Guardian* (27.8.2015), online unter: https://www.theguardian.com/world/2015/aug/27/junaid-hussain-british-hacker-for-isis-believed-killed-in-us-airstrike (letzter Zugriff: 27.4.2021).

58 Auswärtiges Amt (2020), Auswärtiges Amt zum Hackerangriff auf den Deutschen Bundestag, Pressemitteilung vom 28.5.2020, online unter: https://www.auswaertiges-amt.de/de/newsroom/hackerangriff-bundestag/2345542 (letzter Zugriff: 27.4.2021).

59 Vermutlich eine der bisher umfassendsten Ermittlungen wegen Cyberoperationen: United States Department of Justice (2020), Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace, online unter: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and (letzter Zugriff: 27.4.2021).

60 Bundesamt für Justiz (2021), Internationale Rechtshilfe in Strafsachen, online unter: https://www.bundesjustizamt.de/DE/Themen/Gerichte_Behoerden/IRS/Rechtshilfe_node.html (letzter Zugriff: 27.4.2021).

61 Siehe z. B. Chimène I. Keitner (2019), Attribution by Indictment, in: *American Journal of International Law*, Vol. 113, S. 207–212 (letzter Zugriff: 27.4.2021).

62 Maik Baumgärtner und Sven Röbel (2016), Hacker-Angriff auf den Bundestag: Generalbundesanwalt übernimmt Ermittlungen, in: *Der Spiegel* (20.1.2016), online unter: https://www.spiegel.de/politik/deutschland/hacker-angriff-auf-bundestag-generalbundesanwalt-uebernimmt-ermittlungen-a-1073041.html (letzter Zugriff: 27.4.2021).

63 Florian Flade und Georg Mascolo (2020), a. a. O.

64 Eine Einführung zum Thema bietet Sascha Lohmann (2018), Sanktionen in den internationalen Beziehungen. Bundeszentrale für politische Bildung, online unter: https://www.bpb.de/apuz/275108/sanktionen-in-den-internationalen-beziehungen (letzter Zugriff: 27.4.2021).

65 Catalin Cimpanu (2020), US sues to recover cryptocurrency funds stolen by North Korean hackers, in: *ZDNet*, online unter: https://www.zdnet.com/article/us-sues-to-recover-cryptocurrency-funds-stolen-by-north-korean-hackers/ (letzter Zugriff: 27.4.2021).

66 Handelsblatt (2020), Cyber-Attacke: EU sanktioniert Russen für Hackerangriff auf Bundestag, online unter: https://www.handelsblatt.com/politik/international/cyber-attacke-eu-sanktioniert-russen-fuer-hackerangriff-auf-bundestag/26300620.html (letzter Zugriff: 27.4.2021).

67 Verteidigungsausschuss des Deutschen Bundestages (2021), Protokoll der öffentlichen Anhörung zum Thema „Verfassungs- und völkerrechtliche Fragen im militärischen Cyber- und Informationsraum unter besonderer Berücksichtigung des Parlamentsvorbehaltes, der Zurechenbarkeit von Cyberangriffen sowie einer möglichen Anpassung nationaler und internationaler Normen“, online unter: https://www.bundestag.de/resource/blob/828966/e4383b79a21f05de18f0495c453022d3/protokoll-data.pdf (letzter Zugriff: 27.4.2021).

68 Deutscher Bundestag (2021), Im Cyberraum verschwimmen die Grenzen zwischen Angriff und Verteidigung, online unter: https://www.bundestag.de/dokumente/textarchiv/2021/kw11-pa-verteidigung-806470 (letzter Zugriff: 27.4.2021).

69 Vergleiche z. B. Art. 2 Abs. 4 und 51, United Nations Regional Information Centre for Western Europe (1973), Charta der Vereinten Nationen und Statut des Internationalen Gerichtshofs, online unter: https://unric.org/de/wp-content/uploads/sites/4/2020/01/charta-1.pdf (letzter Zugriff: 27.4.2021).

70 Ausnahmen hiervon waren u. a. die Cyberoperationen gegen das iranische Nuklearprogramm („Stuxnet“/„Olympische Spiele“) – siehe z. B. Kim Zetter (2014), a. a. O. sowie gegen das ukrainische Stromnetz („BlackEnergy 3“/„Sandworm“) – siehe z. B. Andy Greenberg (2019), Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin’s Most Dangerous Hackers. New York, Doubleday und gegen industrielle Steueranlagen, erstmals entdeckt in einer petrochemischen Anlage in Saudi Arabien („Triton“/„Trisis“) – siehe z. B. Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker und Christopher Glyer (2017), Attackers Deploy New ICS Attack Framework „TRITON“ and Cause Operational Disruption to Critical Infrastructure, in: *Fire Eye*, online unter: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html (letzter Zugriff: 27.4.2021).

71 International Cyber Law in Practice (2021), Israeli attack against Hamas cyber headquarters in Gaza (2019), online unter: https://cyberlaw.ccdcoe.org/wiki/Israeli_attack_against_Hamas_cyber_headquarters_in_Gaza_(2019) (letzter Zugriff: 27.4.2021).

# 3. Herausforderungen der deutschen Cyber-sicherheitspolitik

## 3.1 (Cyber-)Strategielosigkeit

Um Cyberoperationen zukünftig geeignet und zeitnah beantworten zu können, steht Deutschland gegenwärtig vor einigen Herausforderungen. Es fehlt Deutschland an einer umfassenden Strategie, wie das Land von anderen Staaten verantwortete Cyberoperationen beantworten will.[72] Weder das Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr (Bw)[73] noch die aktuelle deutsche Cybersicherheitsstrategie 2016 enthalten Antworten auf diese Frage.[74] Momentan ist unklar, ob und warum Deutschland Cyberoperationen beantworten sollte, was die langfristigen Ziele sind und welche Maßnahmen eingesetzt werden können und sollen, um diese zu erreichen.

Kernpunkt einer solchen außenpolitisch eingebetteten nationalen Strategie sollte daher sein, zu klären, ob Deutschland Normen – und wenn ja, welche – für staatliches Verhalten aushandeln[75] oder bestehende bestärken[76] möchte sowie, ob es die eigenen Zurechnungsfähigkeiten signalisieren, Normenverletzungen sanktionieren und/oder Verhaltensveränderungen herbeiführen möchte. Eine solche Strategie muss cybersicherheitspolitische Ziele samt Wege zu ihrer Erreichung identifizieren. Das ist die notwendige Grundlage, um zu entscheiden, welche Beantwortungsinstrumente in einer konkreten Situation eingesetzt werden sollten. Diese Strategie sollte weiterhin bestehende[77] und zukünftige Zielkonflikte erfassen und ausbalancieren oder, wenn möglich, auflösen.[78]

In den Entwurf einer solchen Strategie sollten neben der Bundesregierung auch andere Akteure intensiv eingebunden werden. Dazu zählen Industrie, Wissenschaft, Zivilgesellschaft und Bundesländer. Aber auch die „öffentliche Meinung“ sollte berücksichtigt werden.[79]

Die staatliche Beantwortung von Cyberoperationen berührt zwangsläufig angrenzende Politikfelder. Daher sollte eine cybersicherheitspolitische Strategie nicht auf die Innenpolitik verengt werden, sondern zumindest auch eine außen- und verteidigungspolitische Strategie zum Umgang mit Bedrohungen im Cyberraum darstellen. Darüber hinaus sollte sie eng verzahnt werden mit größeren politischen Fragestellungen jenseits des Cyberraums. Domänenübergreifendes, politisches Denken – wie werden einzelne Staaten die gegen sie eingesetzten Instrumente auffassen und wie ist der Einsatz dieser Instrumente in die deutsche Geopolitik diesen Staaten gegenüber eingebettet – ist bei der Planung der Beantwortung (Cross-Domain Response) notwendig. Joshua Rovner spricht hierbei von einer Grand Strategy: „Grand strategy, in contrast, is a theory of security. It describes how various foreign policy instruments help the state achieve durable national security. Grand strategy deals with questions about the nature of world politics, the underlying sources of national power, and the utility of both military and non-military tools“.[80]

Ohne eine solche Strategie wird die „richtige“ Instrumentenauswahl für Entscheidungsträgerinnen und Entscheidungsträger erschwert. Im Ergebnis verhindern unterschiedliche Politikfelder möglicherweise gegenseitig ihre Zielerreichung.

**Auswirkung auf die Bereiche:**
Während ein fehlender strategischer Rahmen nicht notwendigerweise Auswirkungen auf den Bereich IT-Sicherheit hat, so führt er zu fundamentalen Herausforderungen in den Bereichen Attribution und Beantwortungsinstrumentarium. Ohne klar formulierte strategische Ziele bleibt unklar, wozu Maßnahmen aus diesen Bereichen dienen sollen. Das reicht von fehlender Ressourcenallokation für die Zurechnung bis zu unklaren Rahmenbedingungen und Grenzwerten für die Zuschreibung und den geeigneten Einsatz von Instrumenten.

## 3.2 Kein zentrales Gremium zur strategischen Beurteilung

Um die Erkenntnisse des operativen Bereichs in geeignete und zeitnahe strategische Entscheidungen der Bundesregierung zu überführen, bedarf es eines übergreifenden Gremiums mit einem geeigneten technischen Grundverständnis, um die Folgen der staatlichen Beantwortung umfassend abschätzen zu können. Die deutsche Cybersicherheitsarchitektur zeichnet sich durch eine Vielzahl an Akteuren aus, die arbeitsteilig agieren.[81] Auf operativer Ebene sollen diese Akteure durch das Nationale Cyber-Abwehrzentrum (Cyber-AZ), auf strategischer Ebene durch den Cyber-

Sicherheitsrat (Cyber-SR) zusammengehalten werden. Jedoch ist keine dieser Institutionen derzeit mit den notwendigen Kompetenzen ausgestattet, oder de facto in der Lage, als strategisches Gremium zu fungieren.

In einem solchen zentralen Gremium, das als Beratungsgremium der Bundesregierung ressortübergreifend auszugestalten wäre und alle zentralen Akteure umfassen müsste, müsste im Rahmen der übergeordneten Strategie (vgl. Herausforderung „(Cyber-) Strategielosigkeit“) und unter Berücksichtigung der Erkenntnisse aus der operativen Arbeit (vgl. Bereiche IT-Sicherheit und Attribution) entschieden werden, mit welchen Instrumenten (vgl. Bereich Beantwortungsinstrumentarium) Operationen beantwortet werden sollen. Dieses Gremium müsste auch die operative Durchführung der Beantwortung überblicken. Hier würde unter anderem die Beurteilung der Bedeutung von einzelnen Operationen und Kampagnen für die nationale und internationale Sicherheit und Geeignetheit der Beantwortung stattfinden – zum Beispiel: Wann rechtfertigt eine Operation welche Art von Sanktionen, und wie hoch muss die Gewissheit der Zurechnung dafür sein (vgl. Empfehlung „Stufensystem für Auswirkungen“). Dies setzt einen funktionierenden Bottom-up-Prozess voraus (vgl. Herausforderung „Fehlender Prozess“), der unter anderem definiert, ab wann und in welcher Form dieses Gremium über Cyberoperationen und -kampagnen informiert wird.

**Auswirkung auf die Bereiche:**
Ein fehlendes zentrales Gremium zur strategischen Beurteilung führt vor allem zu Defiziten und Inkonsistenzen bei der Abstimmung von Instrumenten. Nur ein funktionsfähiges, mit den erforderlichen Kompetenzen ausgestattetes Gremium ermöglicht dagegen erst eine tatsächlich handlungsfähige staatliche Beantwortung. Es dient als Schnittstelle zwischen den Bereichen IT-Sicherheit, Attribution und Beantwortungsinstrumenten.

## 3.3 Fehlender Prozess

Es kommt nicht von ungefähr, dass es fünf Jahre dauerte, bis die Bundesregierung öffentlich auf die Cyberoperation gegen den Bundestag reagiert hat[82], und bisher noch keine Antworten auf die 2017 erfolgte Cyberoperation gegen das Auswärtige Amt[83] und die seit 2016 laufende „Winnti“-Kampagne gegen die deutsche Industrie[84] bekannt geworden sind. Natürlich ist denkbar, wenn auch unwahrscheinlich, dass eine strategische Abwägung eine Nichtantwort beziehungsweise sehr verspätete Beantwortung ergab. Es braucht eine gewisse Zeit, bis die Auswirkungen einer Cyberoperation bewertet und eine Zurechnung zu einer Urheberin bzw.

einem Urheber durchgeführt werden können. Auf der Grundlage der Zurechnung, des Risikos weiterer Operationen im Rahmen einer Kampagne und der Einordnung in die weitere Sicherheitspolitik muss zeitnah der Einsatz von geeigneten Instrumenten diskutiert und entschieden werden. Das muss deutlich schneller erfolgen als bislang.

Es mangelt Deutschland bisher an einem klaren nationalen Entscheidungsprozess und einer entsprechenden nationalen Instanz für die Beantwortung von Cyberoperationen, und damit auch an der notwendigen Schnittstelle zur EU und zu internationalen Partnerinnen und Partnern wie der NATO, gleichgesinnten Einzelstaaten, wie den USA, und Ad-hoc-Gruppen (vgl. „Kein zentrales Gremium zur strategischen Beurteilung"). Der Verbesserungsbedarf scheint hierbei vor allem am Prozess der Lagefeststellung und Lagebeurteilung sowie einer hierauf aufbauenden Entscheidungskompetenz zu liegen, also der Verknüpfung von Details zu Wirkung und Herkunft einer Operation mit den entsprechenden Instrumenten zur Beantwortung und ihren Konsequenzen.

Während hierbei in den letzten Jahren oft über aktive Cyberabwehr (auch verkürzt bekannt als „Hackback") gesprochen wurde[85], greift das zu kurz. Ciaran Martin, ehemaliger Leiter des britischen National Cyber Security Centre sagte dazu: „The Obama administration's ingenious innovation of issuing criminal indictments against hostile state actors did more to deter hostile state activity than any retaliatory cyber attack: not just by embarrassing the states they accused, but by removing, for life, the prospect of traveling to the West for any of those indicted".[86] Stattdessen lassen sich schon jetzt mehrere weitere Beantwortungsinstrumente jenseits von Cyberoperationen identifizieren. Doch damit diese auch zum Einsatz kommen können, ist ein Prozess nötig, der dem Gremium zur strategischen Beurteilung und Entscheidung zeitnah und unaufgefordert Informationen und Analysen über Vorfälle zuliefert.

**Auswirkung auf die Bereiche:**
Ein fehlender Prozess führt zur Trennung der Bereiche voneinander, aber auch zwischen den einzelnen Maßnahmen innerhalb des jeweiligen Bereichs, was die Wirksamkeit einschränkt. Werden zum Beispiel Erkenntnisse über einen Akteur bei der Detektion nicht weitergegeben oder erst gar nicht erfasst, können weder Reaktion noch Zurechnung bei anderen Aktionen stattfinden – von der Anwendung des Beantwortungsinstrumentariums ganz abgesehen. Kurzum: Ohne einen solchen strukturierten Prozess von Lagefeststellung, Lagebeurteilung und Entwicklung von Handlungsoptionen ist eine strategisch ausgerichtete staatliche Beantwortung von Cyberoperationen nicht möglich.

## 3.4 Vernachrichtendienstlichung der Zurechnung

Neben der Detektion einer Cyberoperation bildet die Zurechnung zu den Verantwortlichen die Grundlage für jede Beantwortung durch den Staat.

Eine Kleine Anfrage hat 2019 bestätigt, dass der zugrundeliegende Prozess hinterfragt werden muss: „Die Attribution von Cyberangriffen erfolgt aktuell durch die jeweils zuständigen Behörden, die sich abstimmen. Der Abstimmungsprozess wird derzeit überprüft“.[87] Das ist nicht unbedingt verwunderlich, denn Deutschland hat mit dem BSI zwar eine gut aufgestellte technische Behörde zuständig für IT- und Cybersicherheit auf Bundesebene, die Zurechnung von Cyberoperationen obliegt jedoch zuständigkeitshalber dem BfV.

Für einen Bereich, in dem ein Großteil der Arbeit über technische Erkenntnisse und Austausch mit Dritten (vergleiche „Zurechnung“) erfolgt, erscheint dies nicht mehr zeitgemäß. Vor allem dann nicht, wenn die Zuständigkeiten für alle anderen operativen, technischen Aufgaben – wie die Detektion und Reaktion – zumindest auf Bundesebene hauptsächlich[88] beim BSI liegen beziehungsweise bei ihm zusammenlaufen.

Nachrichtendienstliche Erkenntnisse sollten eine technische Zurechnung anreichern, aber sie definieren diese nicht.[89] Es gibt zwischen dem BfV und dem BSI sowie weiteren Sicherheitsbehörden, wie dem BND, eine bilaterale Zusammenarbeit und einen Austausch über das Cyber-AZ[90], aber die Zurechnungsberichte werden im Rahmen seines Zuständigkeitsbereichs (unter anderem Spionageabwehr und Wirtschaftsschutz) vom BfV erstellt, unter anderem auch mit Informationen aus dem SSCD des BND und von internationalen Partnerorganisationen. Möglicherweise ist gerade diese „Vernachrichtendienstlichung“ der Zurechnung der Grund, warum in Deutschland solche Berichte selten und nur in Teilen veröffentlicht werden.[91] Die Offenlegung dieser Informationen ermöglicht und legitimiert bestimmte (multilaterale) Antworten auf Cyberoperationen, die auch eine Signalwirkung an die Urheberinnen bzw. Urheber haben können und die Herausbildung von Normen befördern (vgl. z. B. Voraussetzungen für das Beantwortungsinstrument „Sanktionen“). Gleichzeitig birgt es das Risiko, dass Dritte hierdurch Kenntnis über nachrichten- und geheimdienstliche Quellen erlangen und diese gefährdet werden und/oder nicht mehr genutzt werden können. Es muss daher eine entsprechende Abwägung und Abstraktion stattfinden.

**Auswirkung auf die Bereiche:**
Die Vernachrichtendienstlichung der Zurechnung kann für alle öffentlichen Maßnahmen (vergleiche „Auswirkungen auf die Bereiche“ bei Herausforderung „Fragmentiertes Lagebild“), aber auch die Reaktion und die Weitergabe von Informationen eine Herausforderung darstellen.

## 3.5 Fragmentiertes Lagebild

Es gibt in Deutschland kein gemeinsames Lagebild zur Situation der Cybersicherheit.[92] Daraus ergeben sich Herausforderungen für Entscheidungsträgerinnen und Entscheidungsträger zur strategischen Beurteilung der Gesamtlage und deren Entwicklung sowie damit verbunden unter anderem die Entwicklung eines leistungsfähigen, sach- und zeitgerechten Beantwortungsprozesses und der zugrunde liegenden Strategie. Zudem wird auf EU-Ebene ein halbjähriges, EU-weites Lagebild („Biennial report on the state of cybersecurity in the Union“) angestrebt.[93] Hierfür könnte Deutschlands Gesamtlagebild als Grundlage der Informationsweitergabe dienen.

Neben dem BSI erstellen mindestens noch das Bundeskriminalamt (BKA), das BfV und die Bw eigene Lagebilder für ihren Zuständigkeitsbereich des Cyberraums. Während zwar eine fallbezogene Abstimmung zwischen den Behörden im Cyber-AZ erfolgt, gibt es kein gemeinsames Lagebild. Darüber hinaus fehlt auch die systematische Einbindung der Erkenntnisse von Telekommunikationsunternehmen, aus Industrie, Kommunen und Ländern.[94] Ausnahmen bilden die Bereiche, die von der Berichtspflicht Kritischer Infrastrukturen betroffen sind und über Landeskriminalämter (LKÄ) und Landesämter für Verfassungsschutz (LfVs) von Länderebene über die Zentralstellenfunktionen von BKA und BfV berücksichtigt werden.

Die fehlende Konsolidierung wird bereits an Unterschieden im Kleinen deutlich. So veröffentlichen BSI und BKA jedes Jahr fast zeitgleich ihre Lagebilder mit ähnlichem Erfassungszeitraum.[95] Es fällt dabei aber auf, dass das BSI Lagebild die aktuelle Jahreszahl trägt, während das vom BKA die Jahreszahl des vergangenen Jahres führt. Während BSI und BKA Lagebilder veröffentlichen, die sich dediziert auf den Cyberraum beziehen, integriert das BfV seine Erkenntnisse in den jährlichen Verfassungsschutzbericht.[96] Im Gegensatz zu den vorgenannten Behörden stellt die Bw ihr Lagebild dem BSI zur Verfügung und verzichtet auf ein eigenes, separates, öffentliches Lagebild.[97]

**Auswirkung auf die Bereiche:**
Ein fragmentiertes nicht öffentliches Lagebild stellt vor allem die Zuschreibung und den langfristigen, strategischen Einsatz der Beantwortungsinstrumente vor Herausforderungen. Ein konsolidiertes, öffentliches Lagebild wiederum könnte die Legitimität für den Einsatz öffentlicher Instrumente – Diplomatische Maßnahmen, Strafrechtliche Ermittlungen, Sanktionen und Militäreinsatz – gegenüber der eigenen Bevölkerung erhöhen.

72 Siehe z. B. Matthias Schulze und Sven Herpig (2018), Germany Develops Offensive Cyber Capabilities Without A Coherent Strategy of What to Do With Them, in: *Council on Foreign Relations*, online unter: https://www.cfr.org/blog/germany-develops-offensive-cyber-capabilities-without-coherent-strategy-what-do-them (letzter Zugriff: 27.4.2021) und Sven Herpig (2019), Strategielos im Cyber- und Informationsraum? (6.8.2019), in: *Tagesspiegel*, online unter: https://background.tagesspiegel.de/digitalisierung/strategielos-im-cyber-und-informationsraum (letzter Zugriff: 27.4.2021).

73 Die Bundesregierung (2016), Weissbuch 2016 zur Sicherheitspolitik und Zukunft der Bundeswehr, online unter: https://www.bundesregierung.de/resource/blob/975292/736102/64781348c12e4a80948ab1bdf25cf057/weissbuch-zur-sicherheitspolitik-2016-download-data.pdf (letzter Zugriff: 27.4.2021).

74 Möglicherweise wird die für Sommer 2021 geplante Cybersicherheitsstrategie diese Herausforderung adressieren.

75 Siehe z. B. Alexandra Paulus und Sven Herpig (2020), Covid-19: Why states now need to consider self-restraint in the cyber domain, in: *About Intel* (9.4.2020), online unter: https://aboutintel.eu/covid-cyber-china/ (letzter Zugriff: 27.4.2021).

76 Siehe z. B. Matthias C. Kettemann und Alexandra Paulus (2020), Ein Update für das Internet: Reform der globalen digitalen Zusammenarbeit 2021. Stiftung Entwicklung und Frieden, online unter: https://www.sef-bonn.org/de/publikationen/global-governance-spotlight/42020/ (letzter Zugriff: 27.4.2021).

77 Siehe z. B. Sven Herpig (2017), Staatliches Hacken in Deutschland: Öffentliche Sicherheit kontra IT-Sicherheit, in: *Security Insider*, online unter: https://www.security-insider.de/oeffentliche-sicherheit-kontra-it-sicherheit-a-658471/ (letzter Zugriff: 27.4.2021).

78 Myriam Dunn Cavelty und Florian J. Egloff (2019), The Politics of Cybersecurity: Balancing Different Roles of the State. In: *St Antony's International Review*, Vol. 15, 2019, No.1, S. 37–57, https://www.researchgate.net/publication/338572624_The_Politics_of_Cybersecurity_Balancing_Different_Roles_of_the_State (letzter Zugriff: 27.4.2021).

79 Leah Matchett, Lauren Sukin und Kathryn Hedgecock (2021), American Public Reticent to Retaliate Against SolarWinds Hack, in: *The National Interest*, online unter: https://nationalinterest.org/feature/american-public-reticent-retaliate-against-solarwinds-hack-176459 (letzter Zugriff: 27.4.2021);
Ryan Shandler, Michael L. Gross und Daphna Canetti (2021), A fragile public preference for cyber strikes: Evidence from survey experiments in the United States, United Kingdom, and Israel. In: *Contemporary Security Policy*, Vol. 42, 2021, Iss. 2, online unter: https://www.tandfonline.com/doi/abs/10.1080/13523260.2020.1868836 (letzter Zugriff: 27.4.2021); Sven Herpig und Thomas Reinhold (2018), a. a. O.

80 Joshua Rovner (2021), Warfighting in Cyberspace, in: *War on the Rocks* (17.3.2021), online unter: https://warontherocks.com/2021/03/warfighting-in-cyberspace/ (letzter Zugriff: 27.4.2021).

81 Stiftung Neue Verantwortung (2021), Deutschlands staatliche Cybersicherheitsarchitektur. Impulse, online unter: https://www.stiftung-nv.de/de/publikation/akteure-und-zustaendigkeiten-der-deutschen-cybersicherheitspolitik (letzter Zugriff: 4.5.2021) und Bundesministerium des Innern, für Bau und Heimat (2020), Online-Kompendium Cybersicherheit in Deutschland, online unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/it-digitalpolitik/online-kompendium-nationaler-pakt-cybersicherheit.pdf (letzter Zugriff: 27.4.2021).

82 Ausnahme hiervon bildet die nicht abgestimmte öffentliche Attribution durch den damaligen Präsidenten des Bundesamtes für Verfassungsschutz.

83 Hackerangriff auf Regierungsnetz läuft noch, in: *Spiegel.de* (1.3.2018), online unter: https://www.spiegel.de/netzwelt/netzpolitik/hackerangriff-auf-regierungsnetz-unter-kontrolle-aber-laeuft-noch-a-1196039.html (letzter Zugriff: 27.4.2021).

84 z. B. Hakan Tanriverdi, Svea Eckert, Jan Strozyk, Maximilian Zierer und Rebecca Ciesielski (2019), a. a. O. Hierzu gab es lediglich eine Informationsweitergabe (u. a. IoCs) ohne Zuschreibung durch das BfV, siehe Bundesamt für Verfassungsschutz (2019), a. a. O. und die Thematisierung von Industriespionage in „direkten Gesprächen mit der chinesischen Führung", siehe Hakan Tanriverdi, Svea Eckert, Jan Strozyk, Maximilian Zierer und Rebecca Ciesielski (2019), a. a. O.

85 Stiftung Neue Verantwortung (2020), Aktive Cyberabwehr/Hackback in Deutschland. Leseliste 2017–2020 – Version 3.0 | Stand: 06.03.2020, online unter https://www.stiftung-nv.de/sites/default/files/leseliste-cyberabwehrhackback_in_deutschland.pdf (letzter Zugriff 27.4.2021).

86 Ciaran Martin (2020), Cyber weapons are called viruses for a reason: statecraft, security and safety in the digital age, in: *The Strand Group*, online unter: https://thestrandgroup.kcl.ac.uk/event/ciaran-martin-cyber-weapons-are-called-viruses-for-a-reason-statecraft-security-and-safety-in-the-digital-age/ (letzter Zugriff: 27.4.2021).

87 Die Bundesregierung (2019), Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz, Agnieszka Brugger, Tabea Rößner, weiterer Abgeordneter und der Fraktion Bündnis 90 / Die Grünen – Drucksache 19/11755 – IT-Sicherheit durch mehr Transparenz und Standardisierung bei Zählweisen und Klassifizierungen von Angriffen, online unter: https://dip21.bundestag.de/dip21/btd/19/122/1912280.pdf (letzter Zugriff: 27.4.2021).

88 Im Rahmen ihrer Befugnisse und internationalen Beziehungen können durch das Bundesamt für den Militärischen Abschirmdienst (BAMAD), das Bundesamt für Verfassungsschutz, das Bundeskriminalamt und den Bundesnachrichtendienst z. B. bei der forensischen Analyse eines Vorfalls oder SIGINT Support to Cyber Defense natürlich auch Spuren zu Vorfällen detektiert werden.

89 Sven Herpig und Thomas Reinhold (2018), a. a. O.

90 Um Silos entgegenzuwirken soll das Cyber-AZ eigentlich als zentrale operative Austauschplattform in der deutschen Cybersicherheitsarchitektur (vgl. Sven Herpig und Clara Bredenbrock (2019), Cybersicherheitspolitik in Deutschland. Akteure, Aufgaben und Zuständigkeiten. Im Fokus: Das Cyber-Abwehrzentrum. Stiftung Neue Verantwortung, online unter: https://www.stiftung-nv.de/sites/default/files/cybersicherheitspolitik_in_deutschland.pdf (letzter Zugriff: 27.4.2021)) fungieren. Jedoch ist das Cyber-AZ seit Jahren reformbedürftig (vgl. Sven Herpig (2020b), IT-Sicherheitsgesetz 2.0. Eine vertane Chance für die IT-Sicherheit in Deutschland. In: *netzpolitik.org*, 20.6.2020, https://netzpolitik.org/2020/eine-vertane-chance-fuer-die-it-sicherheit-in-deutschland/ (letzter Zugriff: 27.4.2021)). Aufgrund mangelnder öffentlich-verfügbarer Informationen ist unklar, ob die 2019er-Reform des Cyber-AZ tatsächlich zu einer Verbesserung beigetragen hat. Klar ist jedoch, dass das BSI als Cybersicherheitsbehörde des Bundes mittlerweile keine leitende Rolle mehr innerhalb der Plattform hat und weiterhin weder Vertreterinnen und Vertreter aus Kommunen oder der Industrie involviert sind (vgl. Bundesamt für Sicherheit in der Informationstechnik (2021), Das Nationale Cyber-Abwehrzentrum, online unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/Nationales-IT-Lagezentrum/Nationales-Cyber-Abwehrzentrum/nationales-cyber-abwehrzentrum_node.html (letzter Zugriff: 27.4.2021)).

91 Bundesamt für Verfassungsschutz (2021), Cyberabwehr, online unter: https://web.archive.org/web/20210118163638/https:/www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/pb-cyber-abwehr (letzter Zugriff: 27.4.2021).

92 Das Erheben der notwendigen Informationen und Aggregieren dieser ist eine notwendige Voraussetzung, um die reale Entwicklung der Gefährdungslage besser erfassen zu können. Ohne die technische Kompetenz in den betroffenen Institutionen, Cyberoperationen detektieren zu können und entsprechende Informationen zur Aggregation „nach oben“ weitergeben zu können, wird eine sinnvolle Analyse und entsprechende Beantwortung erschwert.

93 European Commission (2020), Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, 16.12.2020, COM(2020) 823 final, online unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0823 (letzter Zugriff: 29.04.2021).

94 Eine weitere Beurteilung des nicht öffentlichen, gemeinsamen Lagebilds ist aufgrund der Einstufung des Produkts nicht möglich.

95 Vergleiche Bundesamt für Sicherheit in der Informationstechnik (2021), Die Lage der IT-Sicherheit in Deutschland, online unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Jahreslageberichte/jahreslageberichte_node.html (letzter Zugriff: 27.4.2021) mit Bundeskriminalamt (2021), Bundeslagebilder Cybercrime, online unter: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html (letzter Zugriff: 27.4.2021).

96 Bundesamt für Verfassungsschutz (2021), Publikationen, online unter: https://www.verfassungsschutz.de/SiteGlobals/Forms/Suche/Publikationensuche_Formular (letzter Zugriff: 27.4.2021).

97 Bundesministerium der Verteidigung (2021), FAQ: Cyber-Abwehr, online unter: https://www.bmvg.de/de/themen/cybersicherheit/cyber-verteidigung/cyber-abwehr (letzter Zugriff: 27.4.2021).

# 4. Empfehlungen für die Reform der deutschen Cyber-sicherheitspolitik

## 4.1 Cybersicherheitspolitik-Strategie

Deutschland muss eine klare Whole of Society oder zumindest Whole of Government Cybersicherheitspolitikstrategie mit nationalen und internationalen Komponenten, klaren Zuständigkeiten und Befugnissen formulieren. Hierbei sollten die Ambitionen größer sein als bei der gegenwärtigen und der gerade in Abstimmung befindlichen neuen deutschen Cybersicherheitsstrategie. Wenige, klar definierte rote Linien bei (Arten von)[98] staatlich verantworteten Cyberoperationen gegen Deutschland – zum Beispiel dass die Manipulation demokratischer Entscheidungsprozesse oder nachrichten- und geheimdienstliche Operationen gegen Kritische Infrastrukturen in jedweder Art und Weise nicht toleriert werden – sollten den Kern einer solchen Strategie formen. Dabei dürfen die Formulierungen nicht so uneindeutig sein wie in der Vergangenheit („Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“[99]). Während zu viele oder zu scharfe rote Linien zu Herausforderungen führen, die wenig strategische Ambiguität zulassen,[100] sind Normen gleichzeitig elementar für die Legitimierung von Gegenmaßnahmen, die ohne Verweis auf eine Normverletzung Gefahr laufen, willkürlich zu werden.[101]

Es müssen SMARTe (spezifische, messbare, akzeptierte, realistische und terminierte) strategische Ziele formuliert werden, die zukünftig haushaltswirksam von den zuständigen Ministerien umgesetzt werden. Die Ziele könnten vorgeben, dass Deutschland seine Ressourcen überwiegend für IT-Sicherheit und Resilienz einsetzen soll, sich Selbstverpflichtungen auferlegt – zum Beispiel keine Steuergelder für den Kauf von Exploits und Schwachstellen zu verwenden oder

keine zivilen IT-Infrastrukturen anzugreifen –, führender Staat bei dem Schutz von industriellen Steueranlagen wird, Rüstungskontrolle im Cyberraum[102] vorantreibt oder sich vorbehält, auf Cyberoperationen mit einem breiten, domänenübergreifenden Instrumentenkasten zu antworten – „there's no need to fight cyber with cyber".[103]

Es sind klare Zuständigkeiten auf Bund-Länder-Ebene und ressortübergreifend innerhalb der Bundesregierung festzulegen, entsprechende leistungsstarke und resiliente Strukturen zu schaffen, Veränderungen an der Cybersicherheitsarchitektur vorzunehmen[104] sowie ausreichend Ressourcen bereitzustellen. Eine regelmäßige, transparente und unabhängige Evaluation dieser Strategie sollte mit eingeplant werden. Auch gilt es, die normativen Kernelemente einer solchen Strategie Partnerstaaten und Nichtpartnerstaaten gegenüber klar zu kommunizieren.[105]

**Adressiert Herausforderungen:**

- (Cyber-)Strategielosigkeit
- Kein zentrales Gremium zur strategischen Beurteilung
- Fehlender Prozess
- Fragmentiertes Lagebild
- Vernachrichtendienstlichung der Zurechnung

## 4.2 Beauftragte bzw. Beauftragter für Cybersicherheitspolitik

Zuständigkeiten für einzelne Bereiche der deutschen Cybersicherheitspolitik erstrecken sich über die Ressorts des Bundesministeriums des Innern, für Bau und Heimat (BMI), des Bundesministeriums für Verteidigung (BMVg), des Auswärtigen Amts, des Bundeskanzleramts (BKAmt) und einiger mehr.[106] Herausforderungen wie das Fehlen eines zentralen Prozesses und einer echten Cybersicherheitspolitikstrategie sowie die Fragmentierung des (öffentlichen) Cyberlagebildes können daher unter Umständen darauf zurückgeführt werden, dass es in Deutschland keine ressortübergreifende Beauftragte bzw. keinen ressortübergreifenden Beauftragten für Cybersicherheitspolitik gibt, die bzw. der die operative und strategische Ebene miteinander verknüpfen kann. Für eine kohärente, ressortübergreifende Politik, die zur Erreichung der Cybersicherheitspolitikstrategie beitrüge und Zielkonflikte auflöste, wäre ein solche Rolle aber notwendig, was zum Beispiel die Schweiz[107] und die USA[108] bereits erkannt haben. Eine solche Beauftragte bzw. ein solcher Beauftragter – flankiert von einer Arbeitseinheit mit technischer und politischer Expertise und entsprechender Sicherheitsüberprüfung – sollte Kernaufgaben wie

die technisch politische Prüfung der Vorfalls- und Zurechnungsberichte sowie Strategie- und Policyentwicklung oder die Evaluierung der Wirksamkeit des Einsatzes von Beantwortungsinstrumenten[109] übernehmen.

Hierbei sollten – auch ad hoc – Länder und Vertreterinnen und Vertreter aus Wirtschaft, Wissenschaft und Zivilgesellschaft einbezogen und die Zusammenarbeit auf politischer Ebene ermöglicht werden. Das ist eine Rolle, die – in der Theorie – teilweise dem Nationalen Cyber-Sicherheitsrat zukommt. Die Beauftragte bzw. der Beauftragte würde daher zusammen mit ihrer bzw. seiner entsprechenden Arbeitseinheit den Nationalen Cyber-Sicherheitsrat – dessen Mehrwert für Deutschland trotz Reform auf Basis der Cybersicherheitsstrategie für Deutschland 2016 unklar geblieben ist – in der Cybersicherheitsarchitektur[110] ersetzen.

Diese Rolle sollte aber weder im BKAmt, AA, BMI oder BMVg angesiedelt sein, damit sie bzw. er möglichst unabhängig von den Partikularinteressen der obersten Bundesbehörden und ihren nachgeordneten Bereichen ist.[111] In einem solchen Rahmen könnte diese Funktion auf Vorschlag der Kanzlerin oder des Kanzlers vom Deutschen Bundestag oder aufgrund der Relevanz für die Bundesländer sogar von Bundestag und Bundesrat ernannt werden. Entscheidend wäre außerdem, dass für die genannten Ressorts entsprechende Bringpflichten definiert würden, um die Beauftragte bzw. den Beauftragten bei ihren bzw. seinen Aufgaben zu unterstützen sowie diese bzw. diesen mit den notwendigen Weisungsbefugnissen auszustatten.

**Adressiert Herausforderungen:**
- (Cyber-)Strategielosigkeit
- Kein zentrales Gremium zur strategischen Beurteilung

## 4.3 Interministerieller Jour fixe „Cybersicherheit“

Um Entscheidungen zum Einsatz von Instrumenten und zur öffentlichen Zuschreibung zu fällen und zwischen den Ministerien abzustimmen, braucht es auf ministerieller Ebene eine Austauschplattform, ein Äquivalent zu dem, was auf operativer Ebene das Nationale Cyber-Abwehrzentrum ist. Hierfür sollte unter Vorsitz der Beauftragten bzw. des Beauftragten (vergleiche Empfehlung „Beauftragte bzw. Beauftragter für Cybersicherheitspolitik“) ein interministerieller Jour fixe auf Referatsleiterinnen- bzw. Referatsleiterebene[112] geschaffen werden.[113] Teilnehmen sollten an diesem Jour fixe folgende Ministerien: BKAmt, AA, BMI, BMVg, Bundesministerium für Wirtschaft und Energie (BMWi) und das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) – sowie

die relevanten Sicherheitsbehörden BSI, BfV, BND, BKA, Bw und BAMAD. Vorfallsbedingt können natürlich ad hoc weitere Akteure aus Verwaltung (zum Beispiel Bundesländer), Wissenschaft, Wirtschaft und Zivilgesellschaft hinzugezogen werden.

Der interministerielle Jour fixe sollte dauerhaft und proaktiv von der operativen Ebene mit allen aktuellen Analysen zu Auswirkungen von Cyberoperationen und Zurechnung zu Urheberinnen und Urhebern versorgt werden. Ebenso wie die Arbeitseinheit der Beauftragten bzw. des Beauftragten müssten entsprechende Sicherheitsüberprüfungen bei den Beteiligten vorliegen beziehungsweise durchgeführt werden. Der Einsatz von Beantwortungsinstrumenten kann darauf aufbauend abgesprochen und in den entsprechenden Ministerien geprüft werden.

**Adressiert Herausforderungen:**
- Kein zentrales Gremium zur strategischen Beurteilung
- Fehlender Prozess

## 4.4 Öffentliche Zuschreibung

Deutschland agiert bisher sehr verhalten, wenn es um die öffentliche Zuschreibung von Cyberoperationen zu Gruppen und entsprechender staatlicher Verantwortung geht.[114] Während andere Länder wie die USA oder das Vereinigte Königreich Cyberoperationen häufiger öffentlich zuschreiben – entweder unilateral[115] oder multilateral[116] –, geschieht das in Deutschland eher verhalten.

Hierbei handelt es sich gegenüber Partnerstaaten um eine wichtige Grundlage, um den Einsatz bestimmter Beantwortungsinstrumente – zum Beispiel innerhalb der Europäischen Union als Basis für Sanktionen – zu begründen. Auch gegenüber der eigenen Gesellschaft kann öffentliche Zuschreibung zur Legitimierung des Einsatzes von Beantwortungsinstrumenten beitragen[117], was jedoch nicht ohne Risiko ist.[118] Darüber hinaus kann öffentliche Zuschreibung gegenüber anderen möglichen Aggressoren die eigenen Zurechnungsfähigkeiten signalisieren und zur internationalen Normenbildung beitragen. Natürlich kann die öffentliche Zuschreibung als diplomatische Maßnahme auch ein Beantwortungsinstrument an sich sein, „to deter camera shy countries from engaging in a particular kind of covert activity“.[119]

Eine Strategie, die explizit öffentliche Zuschreibungen verfolgt, muss notwendigerweise Ressourcen in verbesserte Detektion und Zurechnung (inklusive Threat Intelligence[120]) – die Grundlagen für Zuschreibung – von Cyberoperationen investieren. Gleichzeitig

muss der Rechtsrahmen Behörden und Unternehmen ermöglichen, Protokolldaten zu erfassen, ausreichend lange vorzuhalten und mit dem Ziel der Zurechnung von Cyberoperationen auswerten zu dürfen. Damit eine öffentliche Zuschreibung möglich ist, sollte zusätzlich zum BfV auch das BSI die Befugnisse für die Zurechnung von Cyberoperationen bekommen. Dadurch kann sowohl öffentliche Zuschreibung – zum Beispiel über die Beauftragte bzw. den Beauftragten für Cybersicherheitspolitik – besser ermöglicht werden als auch das BfV weiterhin seinen Vorgaben bezüglich Geheimhaltung bestimmter Informationen – zum Beispiel von Partnerländern – nachkommen.

Auf Basis der in der Strategie festgelegten Ziele (vergleiche Empfehlung „Cybersicherheitspolitikstrategie“) muss geprüft werden, ob die öffentliche Zuschreibung staatlich verantworteter Cyberoperationen gegen Deutschland als Instrument häufiger erfolgen sollte.[121] Dies kann zum Beispiel in öffentliche „Cyberverhaltensberichte“ bestimmter Gruppen münden, – die auch auf europäischer Ebene zusammengefasst werden könnten[122] –, und kann unter anderem die normenorientierte (deutsche/europäische) Politik im Cyberraum informieren.[123]

**Adressiert Herausforderungen:**
- Fragmentiertes Lagebild
- Vernachrichtendienstlichung der Zurechnung

## 4.5 Stufensystem für Auswirkungen

Um eine konsistente Beantwortung von Cyberoperationen zu ermöglichen, sollte ein Stufensystem (vgl. Abb. 1) geschaffen werden, das Lagefeststellung (IT-Sicherheit), Lagebeurteilung (IT-Sicherheit und Attribution) und Entwicklung von Handlungsoptionen (Beantwortungsinstrumentarium) miteinander verbindet. Konkret müssen die Auswirkungen einer Cyberoperation oder -kampagne mit der (Gewissheit) der Zurechnung zusammengebracht werden, um als Entscheidungsbasis für den Einsatz des Beantwortungsinstrumentariums zu dienen. Dieses Stufensystem sollte dann die Debatte über Handlungsoptionen im interministeriellen Jour fixe „Cybersicherheit“ leiten, die dem Kabinett anschließend vorgelegt werden. Die Entwicklung eines solchen Stufensystems könnte über eine Reihe von Policyübungen (Exercises) erfolgen.[124]

Auswirkungen anhand der Schwere könnten zum Beispiel auf Basis von Kategorien wie „Kompromittierung kritischer Infrastrukturen gemäß IT-Sicherheitsgesetz/KRITIS-Verordnungen“

(das beinhaltet den Sektor „Staat und Verwaltung"), „Vorfall führte zu Ausrufen des Katastrophenfalls", „Cyberoperation zielte auf Beeinträchtigung demokratischer Prozesse ab", „Schwere ist oberhalb der Grenze des bewaffneten Konflikts", „Kompromittierung von Unternehmen im Rahmen strategischer Wirtschaftsspionage" beurteilt werden. Für die Zurechnung kommen Beurteilungen wie „eher ungewiss" und „sehr gewiss" infrage, die bereits von unterschiedlichen (deutschen) Behörden bei der Zurechnung von Cyberoperationen verwendet werden.

| Vorfall/Auswirkungen/ Schweregrad | Gewissheit der Zurechnung | Beantwortungsinstrumente (und Zuschreibung) |
|---|---|---|
| Demokratischer Prozess ist gestört, z. B. durch Kompromittierung von privaten Emailkonten und Veröffentlichung der dort vorgefundenen Kommunikation (Leaks)[125] | Sehr gewiss | Sanktionen<br>Strafrechtliche Ermittlungen<br>Diplomatische Maßnahmen<br>(Zuschreibung) |
| | Gewiss | Strafrechtliche Ermittlungen<br>Diplomatische Maßnahmen<br>(Zuschreibung) |
| | Eher ungewiss | Weitergabe von Informationen |
| | Ungewiss | Keine Maßnahme |
| Kritische Infrastruktur musste für kurze Zeit vom Netz genommen werden, da zum Beispiel eine Kompromittierung detektiert | ... | ... |
| Katastrophenfall wurde ausgerufen, zum Beispiel weil mehrere Krankenhäuser sich wegen einer Kompromittierung von der Notfallversorgung abmelden müssen | ... | ... |
| Auswirkungen von Cyberoperationen erreichen möglicherweise die Auswirkungen eines bewaffneten Konflikts, zum Beispiel Sabotage, die zum Ausfall von Teilen des Stromnetzes führt | ... | ... |
| Gezielte strategische Wirtschaftsspionage mittels Cyberoperationen gegen Unternehmen | ... | ... |
| Weiteres | ... | ... |

*Abb. 1: Beispiel für ein Stufensystem für Auswirkungen von Cyberoperationen.*

**Adressiert Herausforderungen:**
- (Cyber-)Strategielosigkeit
- Fehlender Prozess (Prozess braucht Schwellenwerte und Beurteilung)

## 4.6 Von der „Holschuld“ zur „Bringschuld“

Untersuchungen von Cybervorfällen sowie Analysen zu Urheberschaft dieser Vorfälle (Zurechnung) werden auf der operativen Ebene (unter anderem vom BSI und BfV) und in der Regel im Rahmen der Zusammenarbeit innerhalb des Cyber-AZ angefertigt. Es gibt hierbei jedoch keinen Automatismus, der die Ergebnisse – Vorfallsberichte und Zurechnungsberichte – strategisch mit der politischen Ebene verbindet. So werden die Berichte an die politische Ebene gegeben, wenn ein Vorfall als politisch signifikant ist oder so bewertet wird, bereits in den Medien diskutiert wird oder die zuständige Behörde den Vorfall für relevant erachtet. Neben den unter „Öffentliche Zuschreibung“ genannten Auswirkungen wird bei dieser Relevanz oft von Vorfällen mit „erheblichen Auswirkungen“[126] gesprochen, ohne dass diese klar definiert sind. Die Entscheidung darüber, was „erheblich“ ist und was nicht, sollte nicht auf der operativen Ebene, sondern auf der politischen Ebene getroffen werden. Aus diesem Grund sollten alle Berichte in den interministeriellen Jour fixe „Cybersicherheit“ gegeben werden, damit dort informiert diskutiert und entschieden werden kann. Damit wird das Berichtswesen von der „Holschuld“ (Ministerien müssen Berichte anfordern) zur „Bringschuld“ (alle Berichte müssen in den Jour fixe gegeben werden) umgewandelt. Dies würde weiterhin den beteiligten Ministerien ermöglichen, ein besseres Verständnis über die Cyberlage zu gewinnen.

**Adressiert Herausforderungen:**
- (Cyber-)Strategielosigkeit
- Fehlender Prozess
- Fragmentiertes Lagebild

98 Dmitri Alperovitch und Ian Ward (2021), How Should the U.S. Respond to the SolarWinds and Microsoft Exchange Hacks?, in: *Lawfare* (12.3.2021), online unter: https://www.lawfareblog.com/how-should-us-respond-solarwinds-and-microsoft-exchange-hacks (letzter Zugriff: 27.4.2021).

99 Rat der Europäischen Union (2020), Entschließung des Rates zur Verschlüsselung – Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung, online unter: https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/de/pdf (letzter Zugriff: 27.4.2021).

100 Siehe z. B. Max Smeets (2019), There Are Too Many Red Lines in Cyberspace, in: *Lawfare* (20.3.2019), online unter: https://www.lawfareblog.com/there-are-too-many-red-lines-cyberspace (letzter Zugriff: 27.04.2021) und Mark Pomerleau (2016), Cyber red lines: ambiguous by necessity?, in: *c4isr.com*, online unter: https://www.c4isrnet.com/2016/09/09/cyber-red-lines-ambiguous-by-necessity/ (letzter Zugriff: 27.4.2021).

101 Laura Bate, Phoebe Benich, Val Cofield, Karrie Jefferson, Ainsley Katz und Sang Lee (2020), Defending Forward by Defending Norms, in: *Lawfare* (11.3.2020), online unter: https://www.lawfareblog.com/defending-forward-defending-norms (letzter Zugriff: 27.4.2021) und James A. Lewis (2021), Toward a More Coercive Cyber Strategy, online unter: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210310_Lewis_Cyber_Strategy.pdf (letzter Zugriff: 27.4.2021).

102 Thomas Reinhold und Christian Reuter (2019), Arms Control and its Applicability to Cyberspace, in: Cristian Reuter (Hrsg.), Information Technology for Peace and Security. Wiesbaden, Springer, S. 207–231.

103 Ciaran Martin (2020), a. a. O.

104 Siehe z. B. Sven Herpig (2020c), Die „Unabhängigkeit" des Bundesamtes für Sicherheit in der Informationstechnik. Stiftung Neue Verantwortung, online unter: https://www.stiftung-nv.de/sites/default/files/snv-unabhaengigkeit_des_bsi_final.pdf (letzter Zugriff: 27.4.2021) und Sven Herpig (2020b), IT-Sicherheitsgesetz 2.0. Eine vertane Chance für die IT-Sicherheit in Deutschland, a. a. O.

105 Vgl. Max Smeets (2019), Cyber Command's Strategy Risks Friction With Allies, in: *Lawfare*, (28.5.2019), https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies (letzter Zugriff: 27.4.2021).

106 Stiftung Neue Verantwortung (2021), Deutschlands staatliche Cybersicherheitsarchitektur. Impulse, a. a. O. und Bundesministerium des Innern, für Bau und Heimat (2020), Online-Kompendium Cybersicherheit in Deutschland, a. a. O.

107 Nationales Zentrum für Cybersicherheit, Schweizerische Eidgenossenschaft (2021), Der Delegierte des Bundes für Cybersicherheit, online unter: https://www.ncsc.admin.ch/ncsc/de/home/ueber-ncsc/der-delegierte.html (letzter Zugriff: 27.4.2021).

108 Maggie Miller (2021), Cyber czar to draw on new powers from defense bill, in: *The Hill*, online unter: https://thehill.com/policy/cybersecurity/533457-cyber-czar-to-draw-on-new-powers-from-defense-bill (letzter Zugriff: 27.4.2021).

109 Vgl. z. B. Allison Peters und Pierce MacConaghy (2021), Unpacking US Cyber Sanctions, in: *Third Way*, online unter: https://www.thirdway.org/memo/unpacking-us-cyber-sanctions (letzter Zugriff: 27.4.2021).

110 Stiftung Neue Verantwortung (2021), Deutschlands staatliche Cybersicherheitsarchitektur. Impulse, a. a. O. und Bundesministerium des Innern, für Bau und Heimat (2020), Online-Kompendium Cybersicherheit in Deutschland, a. a. O.

111 Das erinnert an die langjährige Debatte zur Schaffung eines Nationalen Sicherheitsrates. Siehe z. B. Sicherheitshalber (2019), #19: Wer macht deutsche Sicherheitspolitik? Bundeswehr in Afrika, online unter: https://www.youtube.com/watch?v=nppsBtQjhXQ (letzter Zugriff: 27.4.2021).

112 Eine solche Art Gremium wird in der Kabinettfassung zum Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 16.12.2020 in der Erläuterung zu Paragraf 9b BSIG-E Absatz 3 zur Entscheidung über die Untersagung des Einsatzes kritischer Komponenten vorgeschlagen, vgl. Bundesministerium des Innern, für Bau und Heimat (2020), Gesetzentwurf der Bundesregierung. Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme, online unter: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/it-sicherheitsgesetz.pdf (letzter Zugriff: 4.5.2021).

113 Um eine gewisse Flexibilität zu wahren und die Cybersicherheitsarchitektur Deutschlands nicht noch weiter zu verkomplizieren wäre dieser Modus operandi gegenüber anderen Arten der Institutionalisierung zu bevorzugen.

114 Siehe Bundesamt für Verfassungsschutz (2021), Cyberabwehr, a. a. O.; Deutsche Welle (2018), Germany warns Russia over cyberattacks, 5.10.2018, online unter: https://www.dw.com/en/germany-warns-russia-over-cyberattacks/a-45767953 (letzter Zugriff: 27.4.2021); Der Spiegel (2020), EU verhängt neue Sanktionen gegen Russland, 22.10.2020, online unter: https://www.spiegel.de/politik/ausland/eu-verhaengt-neue-sanktionen-gegen-russland-a-e869983a-979f-4c00-951e-37a5ff57fc91 (letzter Zugriff: 27.4.2021).

115 Siehe z. B. Cybersecurity & Infrastructure Security Agency (2021), Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA), online unter: https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure letzter Zugriff: 27.4.2021).

116 Siehe z. B. European Parliament (2018), Attribution of the NotPetya attack, online unter: https://www.europarl.europa.eu/doceo/document/E-8-2018-001005_EN.html letzter Zugriff: 27.4.2021).

117 Sven Herpig und Thomas Reinhold (2018), a. a. O.

118 Florian J. Egloff (2020b), Contested public attributions of cyber incidents and the role of academia, in: *Contemporary Security Policy*, Vol. 41, 2020, Iss. 1 S. 55–82, online unter: https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1677324 (letzter Zugriff: 27.4.2021).

119 Ders. (2020a), Public attribution of cyber intrusions, a. a. O.

120 Svilen Ivanov (2018), Was ist Cyber Threat Intelligence und wofür kann man es nutzen?, online unter: https://www.isaca.de/sites/default/files/isaca_fokus_bonn_cti_ivanov_2018-06-28.pdf (letzter Zugriff: 27.4.2021).

121 Siehe z. B. Florian J. Egloff und Max Smeets (2021), Publicly attributing cyber attacks: a framework, in: *Journal of Strategic Studies*, Ahead-Of-Print, S. 1–32, online unter: https://www.tandfonline.com/doi/epub/10.1080/01402390.2021.1895117 (letzter Zugriff: 27.4.2021).

122 Vgl. Johannes Wiggen (2020), Chancen und Grenzen europäischer Cybersicherheitspolitik, in: *ZEI Discussion Paper*, C 261/2020, Zentrum für Europäische Integrationsforschung, online unter: https://www.zei.uni-bonn.de/dateien/discussion-paper/dp-261-2020-wiggen.pdf (letzter Zugriff: 27.4.2021).

123 Siehe z. B. Zach Dorfman (2021), The risks and rewards of charging state-backed hackers , in: *axios.com*, online unter: https://www.axios.com/hackers-north-korea-charging-risks-rewards-381605c7-346e-410e-b9bf-8d35691bfe08.html (letzter Zugriff: 27.4.2021) und The Federal Government (2021), On the Application of International Law in Cyberspace, Position Paper* – March 2021, online unter: https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf (letzter Zugriff: 27.4.2021).

124 Rebecca Beigel und Julia Schuetze (2021), Cybersecurity Exercises for Policy Work: Exploring the Potential of Cybersecurity Exercises as an Instrument for Cybersecurity Policy Work. Stiftung Neue Verantwortung, online unter: https://www.stiftung-nv.de/sites/default/files/cybersecurity.exerises.policy.work___0.pdf (letzter Zugriff: 29.4.2021) und Robert S. Dewar (2018), CSS Cyber Defense Report: Cybersecurity and Cyberdefense Exercises, online unter: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-10-Cyber_Exercises.pdf (letzter Zugriff: 27.4.2021).

125 Sven Herpig, Julia Schuetze und Jonathan Jones (2018), a. a. O.

126 EUR-Lex (2020), Restriktive Maßnahmen der EU gegen Cyberangriffe, online unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=LEGISSUM:4399784 (letzter Zugriff: 27.4.2021).

# 5. Prozess für die Beantwortung von Cyberoperationen

Auf Basis der aktuellen Strukturen und unter Berücksichtigung der in diesem Papier getätigten Empfehlungen, lässt sich ein Sollprozess zur Beantwortung von Cyberoperationen skizzieren.

Folgender Prozess (vgl. Abb. 2) könnte als Diskursgrundlage genutzt werden:

1. Opfer von Cyberoperationen sollten direkt Polizei und/oder Verfassungsschutz unterrichten. In Bundesländern mit einer Organisationseinheit für Cybersicherheit (z. B. Hessen3C, bayerisches Landesamt für Sicherheit in der Informationstechnik) sollten auch diese Stellen darüber in Kenntnis gesetzt werden. Zusätzlich dazu werden die entsprechenden Aufsichtsbehörden und das BSI informiert, sofern das (rechtlich) notwendig ist – zum Beispiel bei Kritischen Infrastrukturen. Andersherum müssten diese Behörden Opfer von Cyberoperationen informieren, wenn sie davon Kenntnis erlangen.

2. Informationen über Vorfälle auf Kommunal- und Länderebene sollten entsprechend ihres Ursprungs in den Bundesbehörden (BSI, BfV und BKA) aggregiert werden. Wo möglich, könnten diese Informationen bereits auf der Landesebene durch das entsprechende „Landesamt für Sicherheit in der Informationstechnik“ aggregiert werden. Bereits an dieser Stelle sollten, wenn möglich und nötig, die technischen IoCs geteilt werden. Über den polizeilichen Weg geht der Vorgang dann möglicherweise an die entsprechende Staatsanwaltschaft.

3. Die Informationen werden von den Behörden im Nationalen Cyber-Abwehrzentrum zusammengetragen, durch Informationen weiterer Behörden (z. B. BND und Bw) und ausländischer Partnerorganisationen (Nachrichtendienste, CERTs u. Ä.) angereichert und analysiert. Während die deutschen Nach-

richtendienste im Rahmen ihrer Befugnisse weitere Informationen zu dem Vorfall einholen, kann das BSI sowohl (technische) Informationen einholen als auch weitergeben und andere (in- und ausländische) Akteure warnen. Eine Informationsweitergabe im Rahmen der technischen Reaktion (vgl. „Reaktion“) kann auch bereits nach Subsidiaritätsprinzip vorher erfolgen.

4. Parallel dazu werden entsprechende Produkte (Vorfallsberichte und Zurechnungsberichte) in den zuständigen Behörden angefertigt.

5. Auf Basis der individuellen behördlichen Produkte und weiterführenden Informationen stimmen die Behörden im Cyber-AZ einen Vorfallsbericht und einen Zurechnungsbericht ab. Diese abgestimmten Berichte sowie bei unterschiedlicher Auffassung zusätzlich abweichende Berichte/Stellungnahmen einzelner Behörden, gehen unaufgefordert an den interministeriellen Jour fixe „Cybersicherheit“.

6. Die im interministeriellen Jour fixe vertretenen Akteure diskutieren unter Vorsitz der bzw. des Beauftragten auf Grundlage der strategischen Vorgaben aus der Cybersicherheitspolitikstrategie und den abgestimmten Vorfalls- und Zurechnungsberichten (ggf. individuelle Cyberoperationen zusammengefasst zu -kampagnen) – in enger Abstimmung mit ihren jeweiligen Häusern – den Einsatz von Instrumenten.

7. Die abgestimmten Instrumente werden nach Vorlage beim und Zustimmung durch das Bundeskabinett von den jeweils federführenden Behörden implementiert und der interministerielle Jour fixe über die Entwicklungen unterrichtet. Die bzw. der Beauftragte beaufsichtigt die Implementierung und Folgen des Instrumenteneinsatzes.

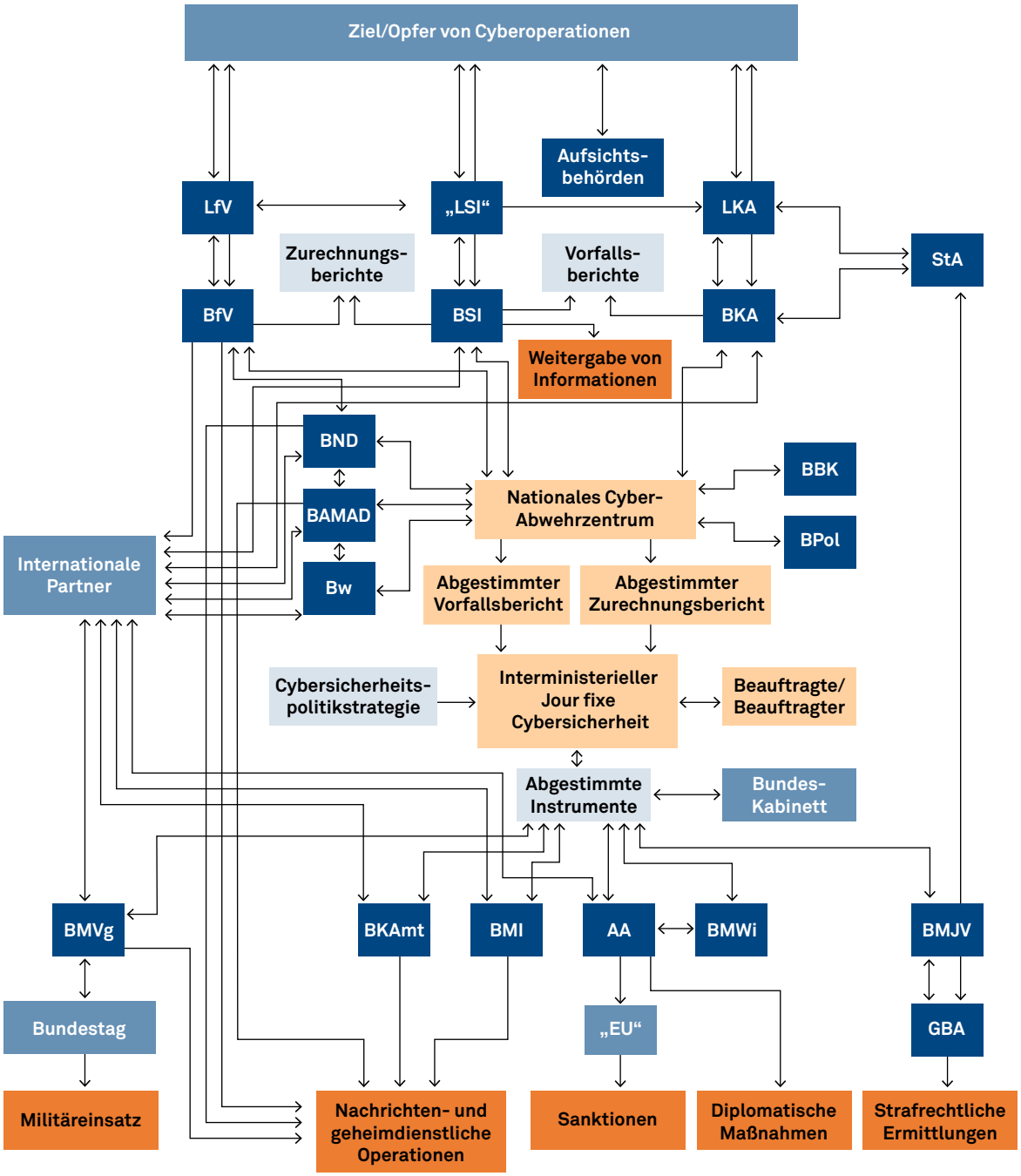



*Abb. 2: Möglicher Sollzustand der Beantwortung von Cyberoperationen mit nationalem Fokus.*

# 6. Fazit

Der ehemalige US-amerikanische Verteidigungsminister Robert Gates wird im Zusammenhang mit strategischen Fragestellungen zu Cybersicherheitspolitik mit den Worten „we're wandering in dark territory" zitiert.[127] Basis dafür war, dass Policyüberlegungen nicht gemacht und/oder nicht umgesetzt worden waren. Seit dieser Zeit hat sich die Policywelt allerdings weiterentwickelt. Auf der einen Seite wird nun zusätzlich zu IT-Sicherheit auch von Resilienz und Assume Breach[128] gesprochen und auf der anderen Seite bei der Beantwortung von Cyberoperationen auch von Persistent Engagement[129], Strafverfahren und Sanktionen.

Während Deutschland im Bereich der Cybersicherheitspolitik für viele Jahre, zuletzt mit den Regulierungen aus dem IT-Sicherheitsgesetz 2015, durchaus führend war, hat es im Policybereich in den letzten Jahren den Anschluss verloren. Dazu haben unter anderem die Schaffung einer fehleranfälligen Cybersicherheitsarchitektur[130] und eine inadäquate Adressierung des Zielkonflikts zwischen Strafverfolgung im Cyberraum und IT-Sicherheit[131] beigetragen. Damit Deutschland wieder eine Vorreiterrolle in der Cybersicherheitspolitik einnehmen kann, muss es sich mit den aktuellen Policyherausforderungen beschäftigen und mutige Reformen anstoßen. Grundlage hierfür sollte eine Cybersicherheitspolitikstrategie bilden, die positiv definiert, welche langfristigen Ziele Deutschland in diesem Bereich verfolgt.

Ein gemeinsames, strategisches Denken von Innen-, Außen- und Verteidigungspolitik sowie weiteren Politikfeldern als Cybersicherheitspolitik ist dringend notwendig, um mit den aktuellen Herausforderungen Schritt halten zu können. In dem vorliegenden Papier wurden exemplarisch für den Bereich der Beantwortung von Cyberoperationen Herausforderungen der aktuellen deutschen Cybersicherheitspolitik aufgezeigt und erste Handlungsempfehlungen entwickelt.

Deutschland braucht eine klare Vision für mehr Sicherheit und Stabilität im Cyberraum, die mit Partnerstaaten gemeinsam vorangetrieben wird – und als Grundlage dafür ist eine Reform der deutschen Cybersicherheitspolitik geboten.

127 Fred Kaplan (2016), a. a. O.

128 Siehe z. B. Ray Pompon (2017), a. a. O.

129 Siehe z. B. Jacquelyn G. Schneider (2019), Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy, in: *Lawfare* (10.5.19), online unter: https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy (letzter Zugriff: 27.4.2021).

130 Stiftung Neue Verantwortung (2021), Deutschlands staatliche Cybersicherheitsarchitektur. Impulse, a. a. O. und Bundesministerium des Innern, für Bau und Heimat (2020), Online-Kompendium Cybersicherheit in Deutschland, a. a. O.

131 Sven Herpig (2019), Entwurf für neues IT-Sicherheitsgesetz: Warum sollte die Polizei Instagram-Passwörter bekommen?, in: *Spiegel.de*, online unter: https://www.spiegel.de/netzwelt/netzpolitik/it-sicherheitsgesetz-bundesinnenministerium-will-neue-polizei-befugnisse-a-1262339.html (letzter Zugriff: 27.4.2021).

# Quellen- und Literaturverzeichnis


A

**Ackerman, Spencer/MacAskill, Ewen/Ross, Alice: Junaid Hussain:** British hacker for Isis believed killed in US air strike. In: *The Guardian*, 27.8.2015, https://www.theguardian.com/world/2015/aug/27/junaid-hussain-british-hacker-for-isis-believed-killed-in-us-air-strike (letzter Zugriff: 27.4.2021).

**Alperovitch, Dimitri/Ward, Ian:** How Should the U.S. Respond to the SolarWinds and Microsoft Exchange Hacks? In: *Lawfare*, 11.3.2021, https://www.lawfareblog.com/how-should-us-respond-solarwinds-and-microsoft-exchange-hacks (letzter Zugriff 27.4.2021).

**Auswärtiges Amt:** *Auswärtiges Amt zum Hackerangriff auf den Deutschen Bundestag*, Pressemitteilung vom 28.5.2020, https://www.auswaertiges-amt.de/de/newsroom/hackerangriff-bundestag/2345542 (letzter Zugriff: 27.4.2021).

B

**Baram, Gil:** Indicting Russia's Most Destructive Cyberwar Unit: The Implications of Public Attribution. In *Council on Foreign Relations* (23.11.2020), https://www.cfr.org/blog/indicting-russias-most-destructive-cyberwar-unit-implications-public-attribution (letzter Zugriff: 27.4.2021).

**Bate, Laura/Benich, Phoebe/Cofield, Val/Jefferson, Karrie/Katz, Ainsley/Lee, Sang:** Defending Forward by Defending Norms. In: *Lawfare*, 11.3.2020, https://www.lawfareblog.com/defending-forward-defending-norms (letzter Zugriff: 27.4.2021).

**Baumgärtner, Maik/Röbel, Sven:** Hacker-Angriff auf den Bundestag: Generalbundesanwalt übernimmt Ermittlungen. In: *Der Spiegel*, 20.1.2016, https://www.spiegel.de/politik/deutschland/hacker-angriff-auf-bundestag-generalbundesanwalt-uebernimmt-ermittlungen-a-1073041.html (letzter Zugriff: 27.4.2021).

**Beigel, Rebecca/Schuetze, Julia:** Cybersecurity Exercises for Policy Work: Exploring the Potential of Cybersecurity Exercises as an Instrument for Cybersecurity Policy Work, *Stiftung Neue Verantwortung* (Hrsg.), April 2021, https://www.stiftung-nv.de/sites/default/files/cybersecurity.exerises.policy.work___0.pdf (letzter Zugriff: 29.4.2021).

**Bundesamt für Justiz:** *Internationale Rechtshilfe in Strafsachen*, 2021, https://www.bundesjustizamt.de/DE/Themen/Gerichte_Behoerden/IRS/Rechtshilfe_node.html (letzter Zugriff: 27.4.2021).

**Bundesamt für Sicherheit in der Informationstechnik:** *Cyber-Sicherheit: Warn- und Informationsdienst (WID)*, 2021, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Technische-Sicherheitshinweise-und-Warnungen/Technische-Sicherheitshinweise/technische-sicherheitshinweise.html (letzter Zugriff: 27.4.2021).

**Bundesamt für Sicherheit in der Informationstechnik:** *Das Nationale Cyber-Abwehrzentrum*, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/Nationales-IT-Lagezentrum/Nationales-Cyber-Abwehrzentrum/nationales-cyber-abwehrzentrum_node.html (letzter Zugriff: 27.4.2021).

**Bundesamt für Sicherheit in der Informationstechnik:** *Die Lage der IT-Sicherheit in Deutschland 2019*, 17.10.2019, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf (letzter Zugriff: 27.4.2021).

**Bundesamt für Sicherheit in der Informationstechnik:** *Die Lage der IT-Sicherheit in Deutschland 2020*, 20.10.2020, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf (letzter Zugriff: 27.4.2021).

**Bundesamt für Sicherheit in der Informationstechnik:** *Die Lage der IT-Sicherheit in Deutschland,* 2021, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Jahreslageberichte/jahreslageberichte_node.html (letzter Zugriff: 27.4.2021).

**Bundesamt für Sicherheit in der Informationstechnik:** *Glossar der Cyber-Sicherheit*, 2021, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html;jsessionid=0E6EA6061B01579E0B665831030639F5.internet461?nn=522504&cms_lv2=132764 (letzter Zugriff: 27.4.2021).

**Bundesamt für Verfassungsschutz:** *BfV Cyber-Brief Nr. 01/2019*, 6.12.2019, https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/2019/bfv-cyber-brief-2019-1.pdf;jsessionid=F92035623869FAE61FECBA2EE7CC1AD0.intranet231?__blob=publicationFile&v=5 (letzter Zugriff: 27.4.2021).

**Bundesamt für Verfassungsschutz:** *Cyberabwehr*, 2021, https://web.archive.org/web/20210118163638/https:/www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/pb-cyberabwehr (letzter Zugriff: 27.4.2021).

**Bundesamt für Verfassungsschutz:** *Publikationen*, 2021, https://www.verfassungsschutz.de/SiteGlobals/Forms/Suche/Publikationensuche_Formular.html?cl2Taxonomies_Themen_fq=themen+verfassungsschutz (letzter Zugriff: 4.5.2021).

**Bundeskriminalamt:** *Bundeslagebild Cybercrime 2019*, 30.9.2020, https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2019.pdf (letzter Zugriff: 27.4.2021).

**Bundeskriminalamt:** *Bundeslagebilder Cybercrime*, 2021, https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html (letzter Zugriff: 27.4.2021).

**Bundesministerium der Verteidigung:** *FAQ: Cyber-Abwehr*, 2021, https://www.bmvg.de/de/themen/cybersicherheit/cyber-verteidigung/cyber-abwehr (letzter Zugriff: 27.4.2021).

**Bundesministerium des Innern, für Bau und Heimat:** *Online-Kompendium Cybersicherheit in Deutschland*, 26.2.2021, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/it-digitalpolitik/online-kompendium-nationaler-pakt-cybersicherheit.pdf (letzter Zugriff: 27.4.2021).

**Bundesministeriums des Innern, für Bau und Heimat:** *Gesetzentwurf der Bundesregierung. Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme*, 16.12.2020, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/it-sicherheitsgesetz.pdf (letzter Zugriff: 27.4.2021).

**Bundesnachrichtendienst:** *Cybersicherheit*, 2021, https://www.bnd.bund.de/DE/Die_Themen/Cybersicherheit/cybersicherheit_node.html (letzter Zugriff: 27.4.2021).

C **Cavelty, Myriam Dunn/Egloff, Florian J.:** The Politics of Cybersecurity: Balancing Different Roles of the State. In: *St Antony's International Review* 15, Vol. 15, 2019, No.1, S. 37–57, https://www.researchgate.net/publication/338572624_The_Politics_of_Cybersecurity_Balancing_Different_Roles_of_the_State (letzter Zugriff: 27.4.2021).

**Cimpanu, Catalin:** US sues to recover cryptocurrency funds stolen by North Korean hackers. In: *ZDNet*, 27.8.2020, https://www.zdnet.com/article/us-sues-to-recover-cryptocurrency-funds-stolen-by-north-korean-hackers/ (letzter Zugriff: 27.4.2021).

**Cimpanu, Catalin:** EU sanctions Russia over 2015 German Parliament hack. In: *ZDNet*, 22.10.2020, https://www.zdnet.com/article/eu-sanctions-russia-over-2015-german-parliament-hack/ (letzter Zugriff: 27.4.2021).

**Cybersecurity & Infrastructure Security Agency:** *Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA)*, 5.1.2021, https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure (letzter Zugriff: 27.4.2021).

D **Der Spiegel:** *EU verhängt neue Sanktionen gegen Russland*, 22.10.2020, https://www.spiegel.de/ausland/eu-verhaengt-neue-sanktionen-gegen-russland-a-e869983a-979f-4c00-951e-37a5ff57fc91 (letzter Zugriff: 27.4.2021).

**Der Spiegel:** *Hackerangriff auf Regierungsnetz läuft noch*, 1.3.2018, https://www.spiegel.de/netzwelt/netzpolitik/hackerangriff-auf-regierungsnetz-unter-kontrolle-aber-laeuft-noch-a-1196039.html (letzter Zugriff: 27.4.2021).

**Deutsche Welle:** *Germany warns Russia over cyberattacks*, 5.10.2018, https://www.dw.com/en/germany-warns-russia-over-cyberattacks/a-45767953 (letzter Zugriff: 27.4.2021).

**Deutscher Bundestag:** *Im Cyberraum verschwimmen die Grenzen zwischen Angriff und Verteidigung*, 15.3.2021, https://www.bundestag.de/dokumente/textarchiv/2021/kw11-pa-verteidigung-806470 (letzter Zugriff: 27.4.2021).

**Dewar, Robert S.:** CSS Cyber Defense Report: Cybersecurity and Cyberdefense Exercises, *Center for Security Studies ETH Zürich* (Hrsg.), Zürich, September 2018, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-10-Cyber_Exercises.pdf (letzter Zugriff: 29.04.2021).

**Die Bundesregierung:** *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz, Agnieszka Brugger, Tabea Rößner, weiterer Abgeordneter und der Fraktion Bündnis 90 / Die Grünen – Drucksache 19/11755 – IT-Sicherheit durch mehr Transparenz und Standardisierung bei Zählweisen und Klassifizierungen von Angriffen*. In: Deutscher Bundestag, 12.8.2019, https://dip21.bundestag.de/dip21/btd/19/122/1912280.pdf (letzter Zugriff: 27.4.2021).

**Die Bundesregierung:** *Weissbuch 2016 zur Sicherheitspolitik und Zukunft der Bundeswehr*, 2016, https://www.bundesregierung.de/resource/blob/975292/736102/64781348c12e4a80948ab1bdf25cf057/weissbuch-zur-sicherheitspolitik-2016-download-data.pdf (letzter Zugriff: 27.4.2021).

**Dorfman, Zach:** The risks and rewards of charging state-backed hackers. In: *Axios.com*, 24.2.2021, https://www.axios.com/hackers-north-korea-charging-risks-rewards-381605c7-346e-410e-b9bf-8d35691bfe08.html (letzter Zugriff: 27.4.2021).

E

**Egloff, Florian J./Smeets, Max:** Publicly attributing cyber attacks: a framework. In: *Journal of Strategic Studies*, 2021, Ahead-Of-Print, S. 1–32, https://www.tandfonline.com/doi/epub/10.1080/01402390.2021.1895117 (letzter Zugriff: 27.4.2021).

**Egloff, Florian J.:** Contested public attributions of cyber incidents and the role of academia. In: *Contemporary Security Policy*, Vol. 41, 2020, Iss. 1, S. 55–82, https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1677324 (letzter Zugriff: 27.4.2021).

**Egloff, Florian J.:** Public attribution of cyber intrusions. In: *Journal of Cybersecurity*, Vol. 6, 2020, Iss. 1, 14.9.2020, https://academic.oup.com/cybersecurity/article/6/1/tyaa012/5905454 (letzter Zugriff: 27.4.2021).

**EUR-Lex:** *Restriktive Maßnahmen der EU gegen Cyberangriffe*, 20.1.2020, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=LEGISSUM:4399784 (letzter Zugriff 27.4.2021).

**European Commission:** *Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148*, 16.12.2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0823 (letzter Zugriff: 29.4.2021).

**European Government CERTs group:** *European Government CERTs group*, 2020, http://www.egc-group.org/ (letzter Zugriff: 27.4.2021).

**European Parliament:** *Attribution of the NotPetya attack*, 19.2.2018, https://www.europarl.europa.eu/doceo/document/E-8-2018-001005_EN.html (letzter Zugriff: 27.4.2021).

**European Union Agency for Cybersecurity:** *CSIRTs Network*, 2021, https://csirtsnetwork.eu/ (letzter Zugriff: 27.4.2021).

F **Flade, Florian/Mascolo, Georg:** Bärenjagd. In: *Süddeutsche Zeitung*, 5.5.2020, https://www.sueddeutsche.de/politik/hack-bundestag-angriff-russland-1.4891668 (letzter Zugriff: 27.4.2021).

G **General Secretariat of the Council of the European Union:** *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities – approval of the final text*, 9.10.2017, https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf (letzter Zugriff: 27.4.2021).

**Gierow, Hauke:** Die erste Ransomware: Der Virus des wunderlichen Dr. Popp. In: *golem.de*, 7.7.2016, https://www.golem.de/news/die-erste-ransomware-der-virus-des-wunderlichen-dr-popp-1607-121809.html (letzter Zugriff: 27.4.2021).

**Greenberg, Andy:** Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. New York: Doubleday, 2019.

**Gross, Michael Joseph:** Enter the Cyber-Dragon. In: *Vanity Fair* 2.8.2011, https://www.vanityfair.com/news/2011/09/chinese-hacking-201109 (letzter Zugriff: 27.4.2021).

H **Handelsblatt:** *Cyber-Attacke: EU sanktioniert Russen für Hackerangriff auf Bundestag*, 22.10.2020, https://www.handelsblatt.com/politik/international/cyber-attacke-eu-sanktioniert-russen-fuer-hackerangriff-auf-bundestag/26300620.html (letzter Zugriff: 27.4.2021).

**Healey, Jason:** Beyond Attribution: Seeking National Responsibility for Cyber Attacks, *Atlantic Council* (Hrsg.), 2011, https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF (letzter Zugriff: 27.4.2021).

**Herpig, Sven/Bredenbrock, Clara:** Cybersicherheitspolitik in Deutschland. Akteure, Aufgaben und Zuständigkeiten. Im Fokus: Das Cyber-Abwehrzentrum, *Stiftung Neue Verantwortung (Hrsg.)*, April 2019, https://www.stiftung-nv.de/sites/default/files/cybersicherheitspolitik_in_deutschland.pdf (letzter Zugriff: 4.5.2021).

**Herpig, Sven/Reinhold, Thomas:** Spotting the bear: credible attribution and Russian operations in cyberspace. In: Popescu, Nicu/Secrieru, Stanislav (Hrsg.): *Hacks, Leaks and Disruptions. Russian Cyber Strategies*, in: Chaillot Papers No. 148, European Union Institute for Security Studies (Hrsg.), 2018, S. 33–43, https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf (letzter Zugriff: 27.4.2021).

**Herpig, Sven/Schuetze, Julia/Jones, Jonathan:** Der Schutz von Wahlen in vernetzten Gesellschaften: Wie sich die Sicherheit datenintensiver Wahlen erhöhen lässt, *Stiftung Neue Verantwortung* (Hrsg.), Oktober 2018, https://www.stiftung-nv.de/sites/default/files/der_schutz_von_wahlen_in_vernetzten_gesellschaften.pdf (letzter Zugriff: 27.4.2021).

**Herpig, Sven:** Aktive Cyber-Abwehr/Hackback. In: Stiftung Neue Verantwortung, online unter: https://www.stiftung-nv.de/de/publikation/hackback-ist-nicht-gleich-hackback (letzter Zugriff: 27.4.2021).

**Herpig, Sven:** *Anti-War and the Cyber Triangle – Strategic Implications of Cyber Operations and Cyber Security for the State*, Januar 2016, https://www.stiftung-nv.de/sites/default/files/antiwar_cybertriangle-herpig.pdf (letzter Zugriff: 27.4.2021).

**Herpig, Sven:** Cyber Operations: Defending Political IT-Infrastructures, *Stiftung Neue Verantwortung* (Hrsg.), June 2017, https://www.stiftung-nv.de/sites/default/files/tcf-defending_political_lt-infrastructures-problem_analysis.pdf (letzter Zugriff: 27.4.2021).

**Herpig, Sven:** Die „Unabhängigkeit“ des Bundesamtes für Sicherheit in der Informationstechnik, *Stiftung Neue Verantwortung* (Hrsg.), September 2020, https://www.stiftung-nv.de/sites/default/files/snv-unabhaengigkeit_des_bsi_final.pdf (letzter Zugriff: 27.4.2021).

**Herpig, Sven:** Entwurf für neues IT-Sicherheitsgesetz: Warum sollte die Polizei Instagram-Passwörter bekommen? In: *Spiegel.de*, 15.4.2019, https://www.spiegel.de/netzwelt/netzpolitik/it-sicherheitsgesetz-bundesinnenministerium-will-neue-polizeibefugnisse-a-1262339.html (letzter Zugriff: 27.4.2019).

**Herpig, Sven:** IT-Sicherheitsgesetz 2.0. Eine vertane Chance für die IT-Sicherheit in Deutschland. In: netzpolitik.org, 20.6.2020, https://netzpolitik.org/2020/eine-vertane-chance-fuer-die-it-sicherheit-in-deutschland/ (letzter Zugriff: 27.4.2021).

**Herpig, Sven:** Staatliches Hacken in Deutschland: Öffentliche Sicherheit kontra IT-Sicherheit, In: *Security Insider*, 6.11.2017, https://www.security-insider.de/oeffentliche-sicherheit-kontra-it-sicherheit-a-658471/ (letzter Zugriff: 27.4.2021).

**Herpig, Sven:** Strategielos im Cyber- und Informationsraum? In: *Tagesspiegel*, 6.8.2019, https://background.tagesspiegel.de/digitalisierung/strategielos-im-cyber-und-informationsraum (letzter Zugriff: 27.4.2021).

**Herpig, Sven:** When does a cyber attack/operation become a (cyber) campaign? – *Twitter Thread*, 19.11.2020, https://twitter.com/z_edian/status/1329425489275056132 (letzter Zugriff: 27.4.2021).

**Hollis, David:** Cyberwar Case Study: Georgia 2008, *Small Wars Journal* (Hrsg.), 6.1.2011, https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf (letzter Zugriff: 27.4.2021).

I

**IBM Security:** *Cost of a Data Breach Report 2020*, 2020, https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/de (letzter Zugriff: 27.4.2021).

**International Cyber Law in Practice:** *Israeli attack against Hamas cyber headquarters in Gaza* (2019), 7.1.2021, https://cyberlaw.ccdcoe.org/wiki/Israeli_attack_against_Hamas_cyber_headquarters_in_Gaza_(2019) (letzter Zugriff: 27.4.2021).

**Ivanov, Svilen:** *Was ist Cyber Threat Intelligence und wofür kann man es nutzen?*, ISACA Fokus Event Meet & Explore, 28.06.2018, Bonn, https://www.isaca.de/sites/default/files/isaca_fokus_bonn_cti_ivanov_2018-06-28.pdf (letzter Zugriff 27.4.2021).

J

**Johnson, Blake/Caban, Dan/Krotofil, Marina/Scali, Dan/Brubaker, Nathan/Glyer, Christopher:** Attackers Deploy New ICS Attack Framework „TRITON“ and Cause Operational Disruption to Critical Infrastructure. In: *Fire Eye*, 14.12.2017, https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html (letzter Zugriff: 27.4.2021).

K

**Kaplan, Fred:** *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster, 2016.

**Keitner, Chimène I:** Attribution by Indictment. In: *American Journal of International Law*, Vol. 113, 2019, Iss. 2, S. 207–212, https://www.cambridge.org/core/journals/american-journal-of-international-law/article/attribution-by-indictment/F7FBB757CF9F597A7818FEEB6015DBD6 (letzter Zugriff: 27.4.2021).

**Kettemann, Matthias C./Paulus, Alexandra:** Ein Update für das Internet: Reform der globalen digitalen Zusammenarbeit 2021, *Stiftung Entwicklung und Frieden* (Hrsg.), Dezember 2020, https://www.sef-bonn.org/de/publikationen/global-governance-spotlight/42020/ (letzter Zugriff: 27.4.2021).

**Kwang, Kevin:** *Singapore health system hit by ‚most serious breach of personal data' in cyberattack; PM Lee's data targeted*. In: *Channel News Asia*, 20.7.2018, https://www.channelnewsasia.com/news/singapore/singhealth-health-system-hit-serious-cyberattack-pm-lee-target-10548318 (letzter Zugriff: 27.4.2021).

L

**Lewis, James A.:** Toward a More Coercive Cyber Strategy, *Center for Strategic & International Studies* (Hrsg.), March 2021, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210310_Lewis_Cyber_Strategy.pdf (letzter Zugriff: 27.7.2021).

**Lohmann, Sascha:** Sanktionen in den internationalen Beziehungen. Bundeszentrale für politische Bildung. In: *Bundeszentrale für politische Bildung*, 31.8.2018, https://www.bpb.de/apuz/275108/sanktionen-in-den-internationalen-beziehungen (letzter Zugriff: 27.4.2021).

**Luber, Stefan/Schmitz, Peter:** Definition Zero Trust – Was ist ein Zero-Trust-Modell? In: *Security Insider*, 4.10.2018, https://www.security-insider.de/was-ist-ein-zero-trust-modell-a-752389/ (letzter Zugriff: 27.4.2021).

**Luber, Stefan/Schmitz, Peter:** Was ist ein Honeypot? In: *Security-Insider* (18.4.2018), https://www.security-insider.de/was-ist-ein-honeypot-a-703883/ (letzter Zugriff: 27.4.2021).

**Lyngaas, Sean:** German intelligence agencies warn of Russian hacking threats to critical infrastructure. In: *Cyberscoop*, 26.5.2020, https://www.cyberscoop.com/german-intelligence-memo-berserk-bear-critical-infrastructure/ (letzter Zugriff: 27.4.2021).

M

**Martin, Ciaran:** Cyber weapons are called viruses for a reason: statecraft, security and safety in the digital age. In: *The Strand Group*, 10.11.2020, https://thestrandgroup.kcl.ac.uk/event/ciaran-martin-cyber-weapons-are-called-viruses-for-a-reason-statecraft-security-and-safety-in-the-digital-age/ (letzter Zugriff: 27.4.2021).

**Matchett, Leah/Sukin, Lauren/Hedgecock, Kathryn:** American Public Reticent to Retaliate Against SolarWinds Hack. In: *The National Interest*, 2021, https://nationalinterest.org/feature/american-public-reticent-retaliate-against-solarwinds-hack-176459 (letzter Zugriff: 27.4.2021).

**Miller, Maggie:** Cyber czar to draw on new powers from defense bill. In: *The Hill*, 9.1.2021, https://thehill.com/policy/cybersecurity/533457-cyber-czar-to-draw-on-new-powers-from-defense-bill (letzter Zugriff: 27.4.2021).

**MISP:** *MISP – Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing*, 2021, https://www.misp-project.org/index.html (letzter Zugriff: 27.4.2021).

**Modderkolk, Huik:** *Dutch agencies provide crucial intel about Russia's interference in US-elections*. In: *de Volkskrant*, 2018, https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/ (letzter Zugriff: 27.4.2021).

N

**National Institute of Standards and Technology:** *Tactics, Techniques, and Procedures (TTPs)*, 2021, https://csrc.nist.gov/glossary/term/Tactics_Techniques_and_Procedures (letzter Zugriff: 27.4.2021).

**National Security Agency:** *Russian State-Sponsored Actors Exploiting Vulnerability in VMware Workspace ONE Access Using Compromised Credentials*, December 2020, https://media.defense.gov/2020/Dec/07/2002547071/-1/-1/0/CSA_VMWARE%20ACCESS_U_OO_195076_20.PDF (letzter Zugriff: 27.4.2021).

**Nationales Zentrum für Cybersicherheit, Schweizerische Eidgenossenschaft:** *Der Delegierte des Bundes für Cybersicherheit*, 12.1.2021, https://www.ncsc.admin.ch/ncsc/de/home/ueber-ncsc/der-delegierte.html (letzter Zugriff: 27.4.2021).

P

**Paulus, Alexandra/Herpig, Sven:** Covid-19: Why states now need to consider self-restraint in the cyber domain. In: *About Intel*, 9.4.2020, https://aboutintel.eu/covid-cyber-china/ (letzter Zugriff: 27.4.2021).

**Peters, Allison/MacConaghy, Pierce:** Unpacking US Cyber Sanctions. In *Third Way*, 29.1.2021, https://www.thirdway.org/memo/unpacking-us-cyber-sanctions (letzter Zugriff: 27.4.2021).

**Pomerleau, Mark:** Cyber red lines: ambiguous by necessity? In: *c4isr.com*, 8.9.2016, https://www.c4isrnet.com/2016/09/09/cyber-red-lines-ambiguous-by-necessity/ (letzter Zugriff: 27.4.2021).

**Pompon, Ray:** Living in an Assume Breach world. In: *Helpnet Security*, 24.8.2017, https://www.helpnetsecurity.com/2017/08/24/assume-breach-world/ (letzter Zugriff: 27.4.2021).

R

**Rat der Europäischen Union:** *Entschließung des Rates zur Verschlüsselung – Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung*, 24.11.2020, https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/de/pdf (letzter Zugriff: 27.4.2021).

**Reinhold, Thomas/Reuter, Christian:** Arms Control and its Applicability to Cyberspace. In: Reuter, Christian (Hrsg.): *Information Technology for Peace and Security*. Wiesbaden: Springer, 2019, S. 207–231.

**Rovner, Joshua:** Warfighting in Cyberspace. In: *War on the Rocks*, 17.3.2021, https://warontherocks.com/2021/03/warfighting-in-cyberspace/ (letzter Zugriff: 27.4.2021).

S

**Schneider, Jacquelyn G.:** Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy. In: *Lawfare*, 10.5.2019, https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy (letzter Zugriff: 27.4.2021).

**Schuetze, Julia:** EU-US Cybersecurity Policy Coming Together: Recommendations for instruments to accomplish joint strategic goals. In: *EU Cyber Direct*, November 2020, https://eucyberdirect.eu/wp-content/uploads/2020/11/rif_eu-us-cybersecurity-final.pdf (letzter Zugriff: 29.4.2021).

**Schulze, Matthias/Herpig, Sven:** Germany Develops Offensive Cyber Capabilities Without A Coherent Strategy of What to Do With Them. In: *Council on Foreign Relations*, 3.12.2018, https://www.cfr.org/blog/germany-develops-offensive-cyber-capabilities-without-coherent-strategy-what-do-them (letzter Zugriff: 27.4.2021).

**Shandler, Ryan/Gross, Michael L./Canetti, Daphna:** A fragile public preference for cyber strikes: Evidence from survey experiments in the United States, United Kingdom, and Israel. In: *Contemporary Security Policy*, Jahrgang 42, 2021, Nr. 2, online unter: https://www.tandfonline.com/doi/abs/10.1080/13523260.2020.1868836 (letzter Zugriff: 27.4.2021).

**Sicherheitshalber:** #19: *Wer macht deutsche Sicherheitspolitik?* | *Bundeswehr in Afrika*, 2.11.2019, https://www.youtube.com/watch?v=nppsBtQjhXQ (letzter Zugriff: 27.4.2021).

**SingCERT:** *Revil Unravelled*, 01.9.2020, https://www.csa.gov.sg/singcert/publications/revil-unravelled (letzter Zugriff: 27.4.2021).

**Smeets, Max:** Cyber Command's Strategy Risks Friction With Allies. In: *Lawfare*, 28.5.2019, https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies (letzter Zugriff: 27.4.2021).

**Smeets, Max:** There Are Too Many Red Lines in Cyberspace. In: *Lawfare*, 20.3.2019, https://www.lawfareblog.com/there-are-too-many-red-lines-cyberspace (letzter Zugriff 27.4.2021).

**Spiegel.de:** *Hackerangriff auf Regierungsnetz läuft noch*, 1.3.2018, https://www.spiegel.de/netzwelt/netzpolitik/hackerangriff-auf-regierungsnetz-unter-kontrolle-aber-laeuft-noch-a-1196039.html (letzter Zugriff: 27.4.2021).

**Steffens, Timo:** *Auf der Spur der Hacker: Wie man die Täter hinter der Computer-Spionage enttarnt*. Wiesbaden: Springer, 2018.

**Steffens, Timo:** Auf Tätersuche: Herausforderungen bei der Analyse von Cyber-Angriffen. In: *Heise online*, 8.2.2021, https://www.heise.de/hintergrund/Auf-Taetersuche-Herausforderungen-bei-der-Analyse-von-Cyber-Angriffen-5043620.html (letzter Zugriff: 27.4.2021).

**Steffens, Timo:** Threat Intelligence: IT-Sicherheit zum Selbermachen? In: *Heise online*, 7.11.2016 https://www.heise.de/security/artikel/Threat-Intelligence-IT-Sicherheit-zum-Selbermachen-3453595.html (letzter Zugriff: 27.4.2021).

**Stiftung Neue Verantwortung:** *Aktive Cyber-Abwehr/Hackback.* Leseliste 2017–2020 – Version 3.0 | Stand: 06.03.2020. Kuratiert von Sven Herpig et al. (AC/BC), https://www.stiftung-nv.de/sites/default/files/leseliste-cyberabwehrhackback_in_deutschland.pdf (letzter Zugriff 27.4.2021).

**Stiftung Neue Verantwortung:** Deutschlands staatliche Cybersicherheitsarchitektur. Impulse, 2021, online unter: https://www.stiftung-nv.de/de/publikation/akteure-und-zustaendigkeiten-der-deutschen-cybersicherheitspolitik (letzter Zugriff: 4.5.2021).

T **Tagesschau:** *Hackerangriff auf den Bundestag: Russischer Botschafter muss ins Auswärtige Amt*, 28.5.2020, https://www.tagesschau.de/inland/russische-hacker-101.html (letzter Zugriff: 27.4.2021).

**Tanriverdi, Hakan/Eckert, Svea/Strozyk, Jan/Zierer, Maximilian/Ciesielski, Rebecca:** Angriff auf das Herz der deutschen Industrie. In: *Bayrischer Rundfunk*, 24.7.2019, https://web.br.de/interaktiv/winnti/ (letzter Zugriff: 27.4.2021).

**Tanriverdi, Hakan:** Behörden warnen vor Angriffen: Russische Bären unter Hackerverdacht. In: *Tagesschau.de*, 27.5.2020, https://www.tagesschau.de/investigativ/br-recherche/hacker-angriff-infrastruktur-101.html (letzter Zugriff: 27.4.2021).

**The Federal Government:** *On the Application of International Law in Cyberspace*, Position Paper* – March 2021, https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf (letzter Zugriff: 27.4.2021).

**The SecDevGroup/Munk Centre for International Studies:** *Tracking GhostNet: Investigating a Cyber Espionage Network*, 29.3.2009, http://www.nartv.org/mirror/ghostnet.pdf (letzter Zugriff: 27.4.2021).

**Thinkst Canary:** Canarytokens, 2021, https://canary.tools/help/canarytokens (letzter Zugriff: 27.4.2021).

U

**United Nations Regional Information Centre for Western Europe:** *Charta der Vereinten Nationen und Statut des Internationalen Gerichtshofs*, Art. 2 Abs. 4 und 51, 1973, https://unric.org/de/wp-content/uploads/sites/4/2020/01/charta-1.pdf (letzter Zugriff: 27.4.2021).

**United States Department of Justice:** *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*, 19.11.2020, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and (letzter Zugriff: 27.4.2021).

**United States of America Office of the Director of National Intelligence:** *Background to „Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, 6.1.2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf (letzter Zugriff: 27.4.2021).

V

**Vavra, Shannon:** How the Pentagon is trolling Russian, Chinese hackers with cartoons. In: *Cyberscoop*, 12.11.2020, https://www.cyberscoop.com/pentagon-cyber-command-trolling-russian-chinese-hackers-cartoons/ (letzter Zugriff: 27.4.2021).

**Verteidigungsausschuss des Deutschen Bundestages:** *Protokoll der öffentlichen Anhörung zum Thema „Verfassungs- und völkerrechtliche Fragen im militärischen Cyber- und Informationsraum unter besonderer Berücksichtigung des Parlamentsvorbehaltes, der Zurechenbarkeit von Cyberangriffen sowie einer möglichen Anpassung nationaler und internationaler Normen"*, 15.3.2021, https://www.bundestag.de/resource/blob/828966/e4383b79a21f05de18f0495c453022d3/protokoll-data.pdf (letzter Zugriff: 27.4.2021).

W **Wiggen, Johannes:** Chancen und Grenzen europäischer Cybersicherheitspolitik. In: *ZEI Discussion Paper C 261 / 2020*, Zentrum für Europäische Integrationsforschung (Hrsg.), https://www.zei.uni-bonn.de/aktuelles/2020/zei-discussion-paper-c-261-2020 (letzter Zugriff: 27.4.2021).

Z **Zetter, Kim:** *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown, 2014.

# Autor

**Dr. Sven Herpig** ist Leiter für Internationale Cybersicherheitspolitik bei der Stiftung Neue Verantwortung e. V. (SNV). Bevor er zur SNV kam, arbeitete Dr. Herpig mehrere Jahre bei deutschen Bundesbehörden im Bereich IT-Sicherheit. Auf Einladung des Bundestags nahm er als Sachverständiger für IT-Sicherheit im Innenausschuss, als Sachverständiger für den militärischen Cyber- und Informationsraum im Verteidigungsausschuss und als Sachverständiger für Digitale Souveränität im Ausschuss Digitale Agenda teil. Weiterhin war er einer der deutschen Expertinnen und Experten in der EU DG for Internal Policies Studie zu staatlichem Hacken und briefte unter anderem den US Congressional Cybersecurity Caucus.

Spätestens 2015 mit dem Bekanntwerden des sogenannten Bundestags-Hack ist die Bedeutung von Cybersicherheit in Deutschland in den Fokus der Sicherheitspolitik geraten. Seitdem vergeht kaum ein Monat, ohne dass irgendwo auf der Welt eine neue staatlich verantwortete Cyberoperation bekannt wird – und mit ihr die Notwendigkeit, darauf zu reagieren. In Deutschland mangelt es bisher an einem umfassenden strategischen Ansatz sowie einem Prozess, um entschieden und zeitnah Cyberoperationen zu beantworten.

Was kann Deutschland mit der Beantwortung von staatlich verantworteten Cyberoperationen bezwecken? Welche Maßnahmen stehen der Bundesregierung hierfür zur Verfügung? Vor welchen Herausforderungen steht Deutschland bei ihrer Umsetzung? Was braucht es für eine strategische Beantwortung von staatlich verantworteten Cyberoperationen und wie könnte ein solcher Prozess aussehen? Dr. Sven Herpig widmet sich diesen Fragen und gibt erste Handlungsempfehlungen.