Stellungnahme von Dr. Sven Herpig[1], Leiter für Cybersicherheitspolitik und Resilienz bei der Stiftung Neue Verantwortung e. V. (SNV), für die öffentliche Anhörung des Ausschusses für Digitales des Deutschen Bundestags am 25. Januar 2023 zum Thema "Cybersicherheit - Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland".

Kontakt
Dr. Sven Herpig
Leiter für Cybersicherheitspolitik und Resilienz
Stiftung Neue Verantwortung e. V.
Email: sherpig@stiftung-nv.de
Twitter: @z_edian
Mastodon: @z_edian@infosec.exchange

[1] Stiftung Neue Verantwortung (2023): Dr. Sven Herpig

Zusammenfassung und Übersicht

Seit der Verabschiedung der „Cybersicherheitsstrategie für Deutschland“ im Jahr 2011 ist die deutsche Cybersicherheitsarchitektur zu einem hochkomplexen Gebilde herangewachsen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat einen massiven Personal-, Finanz- und Zuständigkeitsaufwuchs erfahren, auch andere Behörden haben neue Abteilungen und Organisationsbereiche geschaffen. Teils sind völlig neue Einrichtungen entstanden, wie zum Beispiel der Nationale Cyber-Sicherheitsrat (NCSR) und das Nationale Cyber-Abwehrzentrum (NCAZ), und es wurden zahlreiche Initiativen ins Leben gerufen.

Alles in allem umfasst die deutsche Cybersicherheitsarchitektur heute mehr als 80 Akteure, die wiederum mit einer Vielzahl von Akteuren auf Kommunal-, Länder-, EU- und NATO-Ebene in Verbindung stehen. Entsprechend groß ist die Gefahr, dass es zu Ineffizienz, Chaos und – in den Worten des IT-Sicherheitsexperten Manuel Atug – zu einer „Verantwortungsdiffusion“ kommt. Reformen und ein „struktureller Umbau der IT-Sicherheitsarchitektur“, wie ihn sich die Bundesregierung in ihrem Koalitionsvertrag vorgenommen hat, sind dringend geboten.

Dabei betreffen die strukturellen Probleme nicht nur das institutionelle Gefüge, sondern auch die zur Verfügung stehenden Instrumente. So ist in einigen Fällen – beispielhaft wäre hier die Debatte um Hackbacks und aktive Cyberabwehr zu nennen – unklar, warum die Bundesregierung erweiterte Befugnisse anstrebt; in anderen Fällen gibt es dringenden Verbesserungsbedarf, etwa beim Schwachstellenmanagement. Diese Instrumente gemeinsam mit Expert:innen und Praktiker:innen aus unterschiedlichen Sektoren auszuarbeiten und passgenauer zu machen, wäre ein wichtiger Schritt in Richtung einer klugen, nachhaltigen Cybersicherheitspolitik.

Die vorliegende Stellungnahme ist anlässlich der öffentlichen Anhörung des Ausschusses für Digitales des Deutschen Bundestags am 25. Januar 2023 zum Thema „Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland“ entstanden. Sie enthält exemplarisch konkrete Empfehlungen, wie eine Reform des institutionellen Gefüges aussehen und das zur Verfügung stehende Instrumentarium verbessert werden könnte. Bisher fehlte es den Bundesregierungen an Transparenz, proaktiver Kommunikation und Evaluations- und Reformwillen. Zudem gelingt es nicht, die Zivilgesellschaft in einem angemessenen Rahmen einzubeziehen. Letzteres wäre aber besonders wichtig, um Defizite zu erkennen und zu beseitigen.

Eine zentrale Empfehlung lautet deshalb, dass die Bundesregierung eine mit unabhängigen Expert:innen und Praktiker:innen besetzte Kommission zur Evaluierung der deutschen Cybersicherheitsarchitektur und Erarbeitung des entsprechenden Reformbedarfs einsetzt; diese Kommission sollte hinreichend mit Informationen ausgestattet werden, um effektiv arbeiten zu können. Die teils antagonistische Beziehung zwischen Regierung auf der einen und Vertreter:innen von Wirtschaft, Wissenschaft und Zivilgesellschaft auf der anderen Seite sollte dringend verbessert werden, um die deutsche Cybersicherheitspolitik bestmöglich aufzustellen und Deutschland im Cyberraum zu mehr Resilienz zu verhelfen.

1. Cybersicherheit – Zuständigkeiten in der Bundesrepublik Deutschland

Einleitung

Seit der Verabschiedung der Cyber-Sicherheitsstrategie für Deutschland (2011) ist die deutsche Cybersicherheitsarchitektur (vgl. Abbildung 1) stetig stark gewachsen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat einen massiven Personal-, Finanz-[2] und Zuständigkeitsaufwuchs[3] erfahren, Sicherheitsbehörden wie das Bundeskriminalamt (BKA) haben entsprechende Abteilungen[4] gegründet, bei der Bundeswehr (Bw) wurde ein neuer Organisationsbereich geschaffen[5] und viele komplett neue Akteure, etwa das Nationale Cyber-Abwehrzentrum (NCAZ)[6], wurden aufgebaut. Hinzu kommen zahlreiche Initiativen und Arbeitsgruppen. Nur ein geringer Teil dieser Akteure, mit Ausnahme des NCAZ und des Nationalen Cyber-Sicherheitsrats (NCSR), wurde jemals evaluiert oder gar grundlegend reformiert. Abgesehen von einigen Initiativen ist keine Institution bekannt, die in dieser Zeit komplett abgeschafft wurde.

Das führt dazu, dass es auf Bundesebene mittlerweile über 80 Akteure gibt[7], die jeweils für Teilbereiche der deutschen Cybersicherheit zuständig sind. Diese Teilzuständigkeiten können zum Beispiel das Formulieren von Strategien und Policies, Fortbildungen und Informationsaustausch sowie die operative Umsetzung umfassen. Hinzu kommen zahlreiche Verbindungen zu den Akteuren auf Kommunal-, Länder-, EU- und NATO-Ebene. Thomas Köhler, Lehrbeauftragter an der Hochschule der Polizei Brandenburg, beschreibt das Endresultat als “Zuständigkeitschaos”[8], Manuel Atug, namhafter IT-Sicherheitsexperte, als “Verantwortungsdiffusion”[9].

Ein weiteres Problem ist, dass es oft an öffentlich verfügbaren Informationen über all diese

[2] Bundesministerium der Finanzen (2023): Bundeshaushalt
[3] Bundesamt für Sicherheit in der Informationstechnik (2023): Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG)
[4] Bundeskriminalamt (2023): Die Geschichte des Bundeskriminalamtes
[5] Bundeswehr (2023): Auftrag des Organisationsbereichs CIR
[6] Bundeskriminalamt (2023): Das Nationale Cyber-Abwehrzentrum
[7] Stiftung Neue Verantwortung (2023): Deutschlands staatliche Cybersicherheitsarchitektur
[8] Thomas Köhler (2021), Cybersicherheit ohne Fachbereichsegoismen!
[9] Manuel Atug (2022): [Post auf Twitter zum ZDF Magazin Royale vom 7. Oktober 2022]

Akteure und ihre Tätigkeiten mangelt. Ein Beispiel dafür ist die rechtliche und organisatorische Kooperationsgrundlage der Behörden des NCAZ. Laut Koalitionsvertrag hat sich die Bundesregierung vorgenommen, einen "strukturellen Umbau der IT-Sicherheitsarchitektur" einzuleiten.[10] Auf die über 10 Jahre währende Aufbauphase soll eine Konsolidierungsphase folgen, damit die Effektivität der Cybersicherheitsarchitektur gewährleistet ist, vor allem im Krisenfall. Das ist erstmal begrüßenswert. Allerdings besteht die Gefahr, dass lediglich weitere Befugnisse geschaffen und weitere Ressourcen einem mangelhaften System zugeführt werden. Davor warnt im Kontext des Gematik-Umbaus auch Anke Domscheit-Berg mit den Worten: "Eine dysfunktionale Einrichtung mit noch mehr Ressourcen und Befugnissen auszustatten, halte ich ohne eine grundlegende Reform der [Einrichtung] für ein gefährliches Unterfangen".[11] Weiterhin sollten bei der Konsolidierung sowohl die vertikalen als auch die horizontalen Verbindungen mitgedacht werden. Ein Beispiel für vertikale Verbindungen ist die viel diskutierte Zentralstellenfunktion des BSI; horizontale Verbindungen finden sich unter anderem im Zusammenhang mit dem geplanten KRITIS-Dachgesetz.

Es wird daher angeregt, dass die Bundesregierung eine mit unabhängigen Expert:innen und Praktiker:innen besetzte Kommission zur Evaluierung der deutschen Cybersicherheitsarchitektur und Erarbeitung des entsprechenden Reformbedarfs einsetzt.

Damit die Kommission ihre Arbeit vollumfänglich erledigen kann, braucht es jedoch mehr Transparenz. Nur so können bestehende Strukturen evaluiert, Defizite identifiziert und Deutschlands Cybersicherheitsarchitektur reformiert werden. Die Bundesregierung muss proaktiver kommunizieren und darf nicht darauf warten, dass Medien, Zivilgesellschaft und Wissenschaft Anfragen gemäß Informationsfreiheitsgesetz (IFG) stellen.[12] **Nur weil etwas bis zu einer IFG-Anfrage zurückgehalten werden kann, heißt das nicht, dass dies auch geschehen sollte.**

Im Folgenden werden auf Basis öffentlich verfügbarer Informationen für ausgewählte, zentrale Akteure der deutschen Cybersicherheitsarchitektur exemplarisch Reformideen vorgestellt. Es besteht kein Anspruch auf Vollständigkeit.

[10] Sozialdemokratische Partei Deutschlands (SPD), BÜNDNIS 90/DIE GRÜNEN und Freie Demokratische Partei (FDP) (2021): MEHR FORTSCHRITT WAGEN
[11] Marie Zahout (2022): KONNEKTOREN Ministerium besteht auf Austausch
[12] FragDenStaat (2016): Anhang „Cyber-AZ-AuftragundArbeitsweise_final_geschwrzt.pdf"

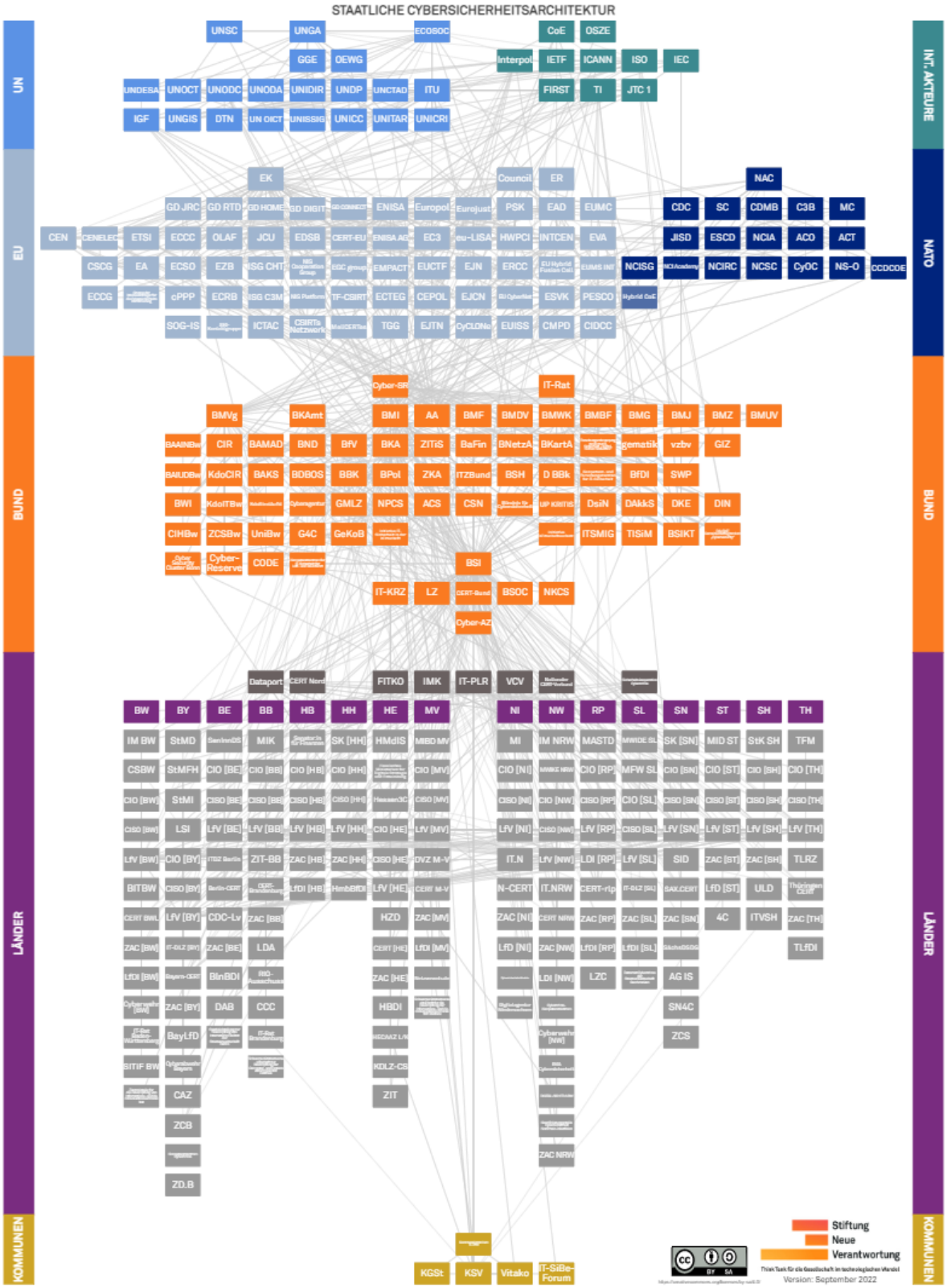

Abbildung 1: Deutschlands staatliche Cybersicherheitsarchitektur[13], CC BY-SA 4.0 Stiftung Neue Verantwortung e. V.

[13] Stiftung Neue Verantwortung (2023): Deutschlands staatliche Cybersicherheitsarchitektur

Reform der Cybersicherheitsarchitektur

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Seit vielen Jahren wird diskutiert, wie sich die (fachliche) Unabhängigkeit des BSI vom Bundesministerium des Innern und für Heimat (BMI) vergrößern ließe. Reformvorschläge[14] wurden begleitet von einer ersten, noch recht zaghaften Gesetzesänderung – in Gestalt des "Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme"[15]. In § 1 des BSI-Gesetzes heißt es seitdem: "Aufgaben gegenüber den Bundesministerien führt das Bundesamt auf Grundlage wissenschaftlich-technischer Erkenntnisse durch". Die Änderung wurde weder durch Expert:innen noch die Bundesregierung als ausreichend bewertet, weshalb es im Koalitionsvertrag folgerichtig heißt: "Wir [...] stellen das Bundesamt für Sicherheit in der Informationstechnik (BSI) unabhängiger auf [...]".[16]

Für jedwede Reform des BSI sollte eine nicht verhandelbare Grundlage, **die Conditio sine qua non, die Integrität des BSI** sein. Jede Disruption der internen Wertschöpfungskette kann die Effektivität der Behörde stark beeinträchtigen. Die operative IT-Sicherheit und technischen Erkenntnisse, vor allem der Organisationsbereiche Operative Cyber-Sicherheit (OC) und Technik-Kompetenzzentren (TK) und Krypto-Technik und IT-Management (KM), bilden die Grundlage für Aufgaben des BSI, etwa für den Schutz Kritischer Infrastrukturen oder den Verbraucherschutz. Das BMI dürfte aufgrund der operativen Aufgaben gerade in den Bereichen OC, TK und KM größtes Interesse an einer fachlichen Aufsicht haben.

Sollte die Bundesregierung das BSI im Ressort des BMI belassen wollen, könnten folgende Reformen zu einer größeren Unabhängigkeit des BSI beitragen:

1. Es sollte **dem BMI untersagt werden, dem BSI Ergebnisweisungen** zu erteilen. So kann besser sichergestellt werden, dass die Behörde rein auf Grundlage wissenschaftlich-technischer Erkenntnisse entscheidet. Um seiner Aufsichtsfunktion nachzukommen, sollte **das BMI die Arbeit des BSI über breitere Arbeitsprogramme steuern oder sogar nur im Rahmen einer Ex-Post-Aufsicht prüfen**.

[14] Sven Herpig (2020): Die „Unabhängigkeit" des Bundesamtes für Sicherheit in der Informationstechnik und Sven Herpig (2021): Wie kann das BSI unabhängiger werden?
[15] Bundesgesetzblatt (2021): Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme
[16] Sozialdemokratische Partei Deutschlands (SPD), BÜNDNIS 90/DIE GRÜNEN und Freie Demokratische Partei (FDP) (2021): MEHR FORTSCHRITT WAGEN

2. Alle **fachlichen Weisungen des BMI an das BSI werden in einem Register hinterlegt**, das von den Abgeordneten des Deutschen Bundestags eingesehen werden kann. Dies hilft bei der Evaluierung der Abhängigkeit des BSI vom BMI.
3. Die **unbegründete Sonderregelung für das BSI in §26 GGO sollte abgeschafft werden**.[17] Nur so kann das BSI vollumfänglich seiner Querschnittsfunktion für Digitalisierungsprojekte der gesamten Bundesregierung nachkommen.
4. Das **BSI sollte weiterhin von einem:r Beamten:in und keinem:r politischen Beamten:in geführt werden**. Dies würde die fachliche Ausrichtung der Behörde unterstreichen. Auch wenn diese Maßnahme eine direkte Einflussnahme des:r Ministers:in auf die Position nicht notwendigerweise verhindert, erschwert sie sie zumindest.[18]
5. **Der:die Präsident:in des BSI wird gleichzeitig zum Chief Information Security Officer Bund** (CISO Bund) ernannt und bekommt direktes **Vortragsrecht bei dem:der Innenminister:in**. So kann zumindest rudimentär die in der IT-Sicherheitsmanagementliteratur befürwortete Trennung zwischen Chief Information Officer (CIO) und CISO auf Bundesebene gewährleistet werden.
6. Die **Fachaufsicht des BSI sollte innerhalb des BMI stärker von der Fachaufsicht der Cyberfähigkeiten der Sicherheitsbehörden getrennt werden**. Hierzu sollte die Fachaufsicht des BSI von der Abteilung Cyber- und Informationssicherheit (CI) in eine andere Abteilung, zum Beispiel Digitale Gesellschaft; Informationstechnik (DG) übertragen werden.

Nationales Cyberabwehrzentrum (NCAZ)

Nach Gründung des NCAZ im Jahr 2011[19] wurde dieses mehrfach reformiert. So wurde zum Beispiel das BSI als alleiniger Koordinator abgelöst und 2020 ein Weiterentwicklungsprozess gestartet, der 2021 in der Aufnahme von Ländern und Judikative im NCAZ mündete.[20] Während die Reformen auf den ersten Blick nachvollziehbar erscheinen, ist die angedachte Rolle des NCAZ in der deutschen Cybersicherheitsarchitektur weiterhin unklar. Das liegt vor allem daran, dass die Grundlage der Zusammenarbeit, Kooperationsabkommen oder andere Dokumente zwischen den Behörden, nicht öffentlich einsehbar sind. In der Vergangenheit

[17] Die Bundesregierung (2020): Gemeinsame Geschäftsordnung der Bundesministerien - GGO
[18] Nikolaus Doll (2023): Meuterei gegen Innenministerin Faeser
[19] Bundeskriminalamt (2023): Das Nationale Cyber-Abwehrzentrum
[20] Bundeskriminalamt (2023): Das Nationale Cyber-Abwehrzentrum

mussten sie per IFG angefragt werden.[21] Weiterhin ist der Name des NCAZ irreführend, da es nicht für die (operative) Cyberabwehr[22] zuständig ist, sondern lediglich eine Plattform für den schnellen Austausch von Informationen und zur Koordinierung von Schutzmaßnahmen (Wortlaut gem. Eigendarstellung).[23] Es gibt daher zwei grundsätzliche Überlegungen: das NCAZ in seiner aktuellen Funktion zu belassen oder seine Rolle weiter auszubauen. Für beides sind weitere Reformen notwendig:

1. Sollte das NCAZ keine Befugnisse erhalten, also zum Beispiel nicht eigenständig Maßnahmen zur Cyberabwehr anordnen können, ist **die Rechtsgrundlage vermutlich ausreichend**. Um dies abschließend beurteilen zu können, **sollten – so weit wie möglich – alle die Struktur und Zusammenarbeit des NCAZ betreffenden Dokumente öffentlich verfügbar gemacht werden**. Relevante Aspekte sind unter anderem die **operative Umsetzung des Trennungsgebots**[24]. Weiterhin sollte **der Namen des NCAZ angepasst werden**, um die Rolle als Austausch- und Koordinierungsplattform besser zu reflektieren. Zusätzlich sollte darüber nachgedacht werden, **Informationspflichten für die Behörden** einzuführen, damit diese alle Informationen, die sie zu einem diskutierten Vorfall haben, einbringen müssen und dies nicht nur auf freiwilliger oder selektiver Basis stattfindet. In Ergänzung dazu sollte geprüft werden, ob das **NCAZ geeignet wäre, das bisher fragmentierte Lagebild**[25] **in ein Gesamtlagebild (horizontal und vertikal) zusammenzuführen**.
   Weiterhin sollte geprüft werden, ob eine **Einbeziehung aller Länder**, wie im Rahmen der 218. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder[26] angedacht, zielführend wäre, und **ob die bestehende Rechtsgrundlage für einen Informationsaustausch zwischen Bund und Ländern überhaupt ausreicht.**
2. Sollte das NCAZ Befugnisse erhalten und/oder zur Anlaufstelle für IT-Sicherheitsvorfälle und zur zentralen Stelle für Cyberabwehr werden, **bedarf es einer**

[21] Sven Herpig und Clara Bredenbrock (2019): Cybersicherheitspolitik in Deutschland
[22] Definition laut Bundesministerium des Innern, für Bau und Heimat (2021): Cybersicherheitsstrategie für Deutschland 2021: “Cyberabwehr umfasst alle Maßnahmen mit dem Ziel, den Erfolg von tatsächlichen oder geplanten Cyberangriffen zu verhindern oder abzuschwächen”. Vergleiche Sven Herpig (2021): Active Cyber Defense Operations. Assessment and Safeguards.
[23] Bundeskriminalamt (2023): Das Nationale Cyber-Abwehrzentrum
[24] Siehe unter anderem Deutscher Bundestag, Wissenschaftliche Dienste (2018): Gemeinsames Terrorismusabwehrzentrum (GTAZ) Rechtsgrundlagen und Vergleichbarkeit mit anderen Kooperationsplattformen
[25] Sven Herpig (2021): Die Beantwortung von staatlich verantworteten Cyberoperationen
[26] Innenministerkonferenz 2022 in Bayern (2022): Sammlung der zur Veröffentlichung freigegebenen Beschlüsse der 218. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder

grundlegenden Reform der Plattform. Das NCAZ müsste im Rahmen eines **Errichtungsgesetzes** auf eine solide Rechtsgrundlage gestellt werden, die **Rechte und Pflichten** für die dort vertretenen Behörden und Akteure beinhaltet. In diesem Fall wäre dann vor allem die **Abgrenzung zum BSI** – unter anderem zum IT-Lagezentrum und IT-Krisenreaktionszentrum (Bund) und zu Befugnissen wie §7b[27] oder §7c[28] – zu klären.

Nationaler Cybersicherheitsrat (NCSR)

Der NCSR wurde 2011 gegründet und unter anderem mit der Cybersicherheitsstrategie 2016[29] reformiert. Er soll "die Zusammenarbeit im Bereich Cyber-Sicherheit innerhalb der Bundesregierung sowie zwischen Staat und Wirtschaft" organisieren und wird "durch die Expertise einer ständigen wissenschaftlichen Arbeitsgruppe unterstützt".[30] Abgesehen von einem Input zum Entwurf der Cybersicherheitsstrategie 2021[31] ist nichts über die Einbeziehung der Zivilgesellschaft bekannt.

Gemäß Cybersicherheitsarchitektur ist der NCSR in der Theorie der zentrale Akteur auf strategischer Ebene, der unter anderem die gesamte Bundesregierung zusammenbringt. Außerhalb der technischen Impulspapiere der Wissenschaftlichen Arbeitsgruppe[32] ist öffentlich wenig über die Arbeit des NCSR bekannt. Eine zentrale strategische Rolle bei der Weiterentwicklung der deutschen Cybersicherheitspolitik ist nicht erkennbar.[33] **Der NCSR sollte daher dringend reformiert, ersetzt oder abgeschafft werden**.

1. Eine **Reform des NCSR** muss das Gremium zwingend inklusiver gestalten und neben der Einbindungen von **Vertreter:innen aus der Wissenschaft** (abseits der

[27] Bundesministerium der Justiz (2023): Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) § 7b Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden
[28] Bundesministerium der Justiz (2023): Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) § 7c Anordnungen des Bundesamtes gegenüber Diensteanbietern
[29] Bundesministerium des Innern, für Bau und Heimat (2023): Cyber-Sicherheitsstrategie für Deutschland 2016
[30] Der Beauftragte der Bundesregierung für Informationstechnik (2023): Der Nationale Cyber-Sicherheitsrat (NCSR)
[31] Sven Herpig (2021): Mündliche Stellungnahme [...] zur Cybersicherheitsstrategie 2021 im Nationalen Cyber-Sicherheitsrat am 15.06.2021
[32] Fraunhofer SIT (2023): Beratung aus der Forschung. Wissenschaftliche Arbeitsgemeinschaft Nationale Cyber-Sicherheit
[33] Sven Herpig (2021): Thread [auf Twitter] zum Nationalen Cyber-Sicherheitsrat und wie er seine Rolle in der deutschen Cybersicherheitsarchitektur (nicht) wahrnimmt.

existierenden Arbeitsgruppe) auch die **Zivilgesellschaft einbinden**. Weiterhin sollte eine **ressortübergreifende Geschäftsstelle** geschaffen werden, die operative Arbeit übernehmen kann und nicht nur administrativ die Sitzungen organisiert. Im Moment bestehen die Sitzungen aus aneinandergereihten Vorträgen. Viel wichtiger wäre, dass der **NCSR konkret an der strategischen Ausrichtung Deutschlands arbeitet**. Zu den drängenden Themen gehören das **Formulieren und Evaluieren von Policies, die Reform der Cybersicherheitsarchitektur und die ressortübergreifende Koordination von Strategien**. Der NCSR müsste sich speziell mit der Erarbeitung der Cybersicherheitsstrategie befassen und mit der Frage, wie die Umsetzung beaufsichtigt werden könnte, aber auch mit **Prozessen wie dem Schwachstellenmanagement oder Attributionsverfahren**.

2. Aufgrund der weiterhin steigenden Relevanz des Themas Cybersicherheit für die Sicherheitspolitik Deutschlands sollte die **Ernennung eines:r ressortübergreifenden Cybersicherheitspolitikbeauftragten**[34] geprüft werden. Diese:r könnte den **NCSR ersetzen oder ihm vorstehen**. Auch in diesem Fall bedarf es einer entsprechend ausgestatteten Geschäftsstelle und eines interministeriellen Jour Fixes, um die genannten Aufgaben anzugehen[35].
3. Sollte es keinen konstruktiven Konsens für eine Reform oder ein Ersetzen des NCSR geben, **sollte das Gremium im Zuge der Konsolidierung der Cybersicherheitsarchitektur ersatzlos gestrichen werden.** Es hat in seiner aktuellen Verfasstheit keine Bedeutung für die Cybersicherheitspolitik und -architektur Deutschlands.

Chief Information Security Officers für den Bund (CISO BUND)

Um zusätzlich zu der Bündelung der IT-Vorhaben des Bundes beim Chief Information Officer (CIO BUND) auch die IT-Sicherheitsvorhaben in ähnlicher Weise zu bündeln, plant das BMI laut seiner Cybersicherheitsagenda[36] die Einführung eines:r Chief Information Security Officers für den Bund (CISO BUND). Dieses Vorhaben ist unterstützenswert, wenn folgende Aspekte berücksichtigt werden:

1. Das **Abhängigkeitsverhältnis des:der CISO BUND vom CIO BUND sollte so**

[34] Sven Herpig (2021): Die Beantwortung von staatlich verantworteten Cyberoperationen
[35] Sven Herpig (2021): Die Beantwortung von staatlich verantworteten Cyberoperationen
[36] Bundesministerium des Innern und für Heimat (2022): Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat

gering wie möglich sein. Dieser Umstand ergibt sich aus den Best Practices im IT-Sicherheitsmanagement.[37] Der:die CISO BUND sollte möglichst **weisungsunabhängig** vom CIO BUND agieren können. Da der CIO BUND derzeit auf Staatssekretärsebene im BMI angesiedelt ist, sollte der:die CISO BUND zumindest ein **direktes Vortragsrecht bei der Innenministerin** haben.

2. In der aktuellen Cybersicherheitsarchitektur wäre **der:die Präsident:in des BSI prädestiniert für die Rolle des:der CISO BUND** – vorausgesetzt, das BSI fände wie gefordert zu einer stärkeren Unabhängigkeit vom BMI.[38]

Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)

ZITiS, das sich selbst "die Cyber-Behörde 4.0"[39] nennt, wurde 2017 mit einem Errichtungserlass aus dem damaligen Bundesministerium des Innern, für Bau und Heimat geschaffen. ZITiS unterstützt in zentraler Funktion Sicherheitsbehörden mit Werkzeugen und Lösungen, die diese für ihre Aufgabenerfüllung benötigen (Wortlaut gem. Eigendarstellung)[40]. Es arbeitet in den Bereichen digitale Forensik, Telekommunikationsüberwachung, Kryptoanalyse und Big Data Analyse.[41] ZITiS ermöglicht es den Sicherheitsbehörden, die in ihren Befugnissen vorgesehenen Grundrechtseingriffe durchzuführen. Während damit rechtlich gesehen kein Errichtungsgesetz notwendig war um ZITiS zu gründen, wäre es aufgrund der unterstützenden Rolle bei Grundrechtseingriffen normativ sinnvoll, ein solides Rechtsfundament für ihre Arbeit zu schaffen. Dies gilt vor allem dann, wenn ZITiS Teil des geforderten Schwachstellenmanagement-Prozesses wird.

Die Bundesregierung sollte ein Errichtungsgesetz für ZITiS verabschieden und damit alle Aufgaben, Rechte und Pflichten transparent und nachhaltig festsetzen. Damit ZITiS zu einer besseren IT- und Cybersicherheit in Deutschland beitragen kann, **sollte die Behörde außerdem dazu verpflichtet werden, gefundene Schwachstellen im Rahmen eines noch zu etablierenden Schwachstellenmanagements an das BSI zu melden**.

[37] Bundesamt für Sicherheit in der Informationstechnik (2017): BSI-Standard 200-2 und ISACA Germany Chapter (2016): Implementierungsleitfaden ISO/IEC 27001:2013 und Bundesanstalt für Finanzdienstleistungsaufsicht (2018): IT-Sicherheit: Aufsicht konkretisiert Anforderungen an die Kreditwirtschaft
[38] Sven Herpig (2020): Die „Unabhängigkeit" des Bundesamtes für Sicherheit in der Informationstechnik
[39] Zentrale Stelle für Informationstechnik im Sicherheitsbereich (2023): Die Cyber-Behörde 4.0
[40] Zentrale Stelle für Informationstechnik im Sicherheitsbereich (2023): Wer wir sind
[41] Zentrale Stelle für Informationstechnik im Sicherheitsbereich (2023): Wer wir sind

Agentur für Innovation in der Cybersicherheit (Cyberagentur)

Die im Jahr 2020 gegründete Cyberagentur musste bereits zahlreiche Rückschläge verkraften. Die GmbH musste Wechsel an ihrer Spitze, Belastungen durch den Fachkräftemangel[42] und Kürzungen ihres Budgets[43] hinnehmen. Letzteres deutet im besten Fall darauf hin, dass die Bundesregierung bei der Cyberagentur keine Priorität sieht. Im schlimmsten Fall deutet es auf Unzufriedenheit mit ihrer Arbeit hin. Dafür würde sprechen, dass die Cyberagentur bisher erst zwei Vergabeverfahren abgeschlossen hat.[44] Vergabeverfahren sind aber die Kernaufgabe und Raison d'Être der GmbH. Bei diesen Herausforderungen ist es wenig vertrauenerweckend, dass sich der aktuelle "Cyberagentur-Chef" offenbar weniger Kontrolle wünscht.[45]

Weil ohnehin Fachkräfte fehlen und weil es bei so vielen ähnlich ausgerichteten Institutionen und Stellen[46] zwangsläufig zu Redundanzen und Effizienzverlusten kommt, **sollte eine Reform der deutschen Cybersicherheitsarchitektur auf eine Verschlankung und Verringerung dieser Akteure abzielen.**

Cybersicherheitsinitiativen

Die deutsche Cybersicherheitsarchitektur ist durchzogen von einer Anzahl an Cybersicherheitsinitiativen, die auf das BMI oder das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) zurückgehen.[47] Dazu gehören unter anderem der Nationale Pakt Cybersicherheit (NPCS)[48], das Bündnis für Cybersicherheit[49], Deutschland sicher im Netz (DsiN)[50], die Initiative Wirtschaftsschutz[51] und die Initiative IT-Sicherheit in der Wirtschaft[52] –

[42] Stern (2023): Fachkräftemangel. Cyberagentur sucht weiter Mitarbeiter
[43] Paul Dalg (2022): Haushaltspolitik. Cybersicherheit im Bundeshaushalt und Paul Dalg (2022): Cyberagentur. „Natürlich würden wir uns manchmal weniger Kontrolle wünschen"
[44] Cyberagentur (2023): Ausschreibungen
[45] Paul Dalg (2022): Cyberagentur. „Natürlich würden wir uns manchmal weniger Kontrolle wünschen"
[46] Unter anderem mit der Bundesagentur für Sprunginnovationen (SprinD), dem Forschungsinstitut Cyber Defence der Bundeswehr (CODE) und mit ZITiS gibt es in Deutschland eine ganze Reihe ähnlicher Institutionen wie die Cyberagentur. In eine ähnliche Richtung gehend, aber gänzlich anders gelagert, sind unter anderem das Zentrum für Digitale Souveränität der öffentlichen Verwaltung (ZenDIS) und das Cyber Innovation Hub der Bundeswehr (CIHBw).
[47] Stiftung Neue Verantwortung (2023): Deutschlands staatliche Cybersicherheitsarchitektur
[48] Bundesministerium des Innern und für Heimat (2023): Nationaler Pakt Cybersicherheit
[49] Bundesministerium des Innern und für Heimat (2018): Industrie und BMI etablieren Bündnis für Cybersicherheit
[50] Deutschland sicher im Netz (2023): Deutschland sicher im Netz
[51] Initiative Wirtschaftsschutz (2023): Initiative Wirtschaftsschutz
[52] Bundesministerium für Wirtschaft und Klimaschutz (2023): IT-Sicherheit in der Wirtschaft

zu denen es teils auch noch Unterinitiativen gibt[53].

Im Zuge einer Reform der deutschen Cybersicherheitsarchitektur **sollte aus Effizienz- und Effektivitätsgründen eine Konsolidierung dieser Initiativen eingehend geprüft werden**. Weiterhin wird angeregt, die übriggebliebenen Initiativen **unter einem gemeinsamen Dach zu bündeln, zum Beispiel unter einem reformierten NCSR**.

[53] Bundesministerium für Wirtschaft und Klimaschutz (2016): Die Transferstelle IT-Sicherheit im Mittelstand (TISiM) bietet Informationen aus einer Hand

2. Cybersicherheit – Instrumente in der Bundesrepublik Deutschland

Aktive Cyberabwehr und Hackback

Im Koalitionsvertrag heißt es: “Hackbacks lehnen wir als Mittel der Cyberabwehr grundsätzlich ab”. Aktive Cyberabwehr wird nicht angesprochen. Im politischen Raum hingegen werden beide Themen seit vielen Jahren diskutiert.[54]

Die SNV definiert Aktive Cyberabwehr als ”eine oder mehrere technische Maßnahmen, die von einem einzelnen Staat oder kollektiv durchgeführt oder von einer staatlichen Stelle angeordnet werden, mit dem Ziel, die Auswirkungen einer bestimmten laufenden böswilligen Cyber-Operation oder -Kampagne zu neutralisieren und/oder abzuschwächen und/oder sie technisch zuzuordnen”[55]. Cyberabwehr wird von der Bundesregierung definiert als “alle Maßnahmen mit dem Ziel, den Erfolg von tatsächlichen oder geplanten Cyberangriffen zu verhindern oder abzuschwächen”[56].

Als Hackback lässt sich folgende Teilmenge von Maßnahmen unter der SNV-Definition von Aktiver Cyberabwehr feststellen: “Technische, intrusive [i.S.v. Einwirkung auf Vertraulichkeit, Integrität und Verfügbarkeit] Maßnahmen im Rahmen von defensiven [i.S.d. Reactio, nicht der Actio] Operationen im In- und/oder Ausland zum Neutralisieren, Abschwächen und/oder Zurechnen von kriminellen, nachrichtendienstlichen und/oder militärischen Aktivitäten gegen die in der Sicherheitsverantwortung liegenden [i.S.v. z.B. beim Staat: Behörden, KRITIS, UBI, ...] IT-Infrastrukturen”.[57] Dies ist gegebenenfalls deckungsgleich mit Operationen, die die Bundesregierung als “Computer Netzwerk Interventionen” (CNI) oder Aktive Cyberabwehrmaßnahmen ab der Stufe 3 bezeichnet. Der Begriff Hackback wird von der Bundesregierung "konzeptionell grundsätzlich nicht verwendet"[58].

Es bestehen bereits rechtliche Grundlagen für Befugnisse, die gemäß den Definitionen der

[54] Sven Herpig et al. (2020): Aktive Cyberabwehr/ Hackback in Deutschland
[55] Sven Herpig (2021): Active Cyber Defense Operations. Assessment and Safeguards, Übersetzung durch Autor.
[56] Bundesministerium des Innern, für Bau und Heimat (2021): Cybersicherheitsstrategie für Deutschland 2021
[57] Sven Herpig (2022): [Thread auf Twitter zur Definition von Hackback]
[58] Eva Wolfangel (2022): Was heißt hier Hackback?

SNV und der Bundesregierung unter (aktive) Cyberabwehr fallen. Diese beinhalten, aber beschränken sich nicht auf:

- BSIG §7b[59]: Einsatz von „Honeypots“
- BSIG §7c[60]: Anordnung zur Umleitung und Analyse des Datenverkehrs (ggü. TK-Diensteanbieter)
- BSIG §7c[61]: Anordnung zur technischen Bereinigung (ggü. TK-Diensteanbieter)
- BNDG §34[62]: Eingriff in informationstechnische Systeme von Ausländern im Ausland („Gefahrenfrüherkennung“)
- BNDG §19[63]: Strategische Ausland-Fernmeldeaufklärung („Gefahrenfrüherkennung“)

Es ist auf Grundlage der öffentlich zur Verfügung stehenden Informationen nicht ersichtlich, welche Befugnisse den Sicherheitsbehörden im Bereich der (aktiven) Cyberabwehr fehlen.

Die Bundesregierung diskutiert als Grundlage für (aktive) Cyberabwehr eine Verfassungsänderung, vor allem um die Zuständigkeiten auf Bundesebene zu bündeln.[64] Jedoch ist trotz langjähriger Debatte unklar, welche spezifischen Befugnisse die Bundesregierung zur (aktiven) Cyberabwehr vermisst. Weder strategische Konzepte, noch Rechtsetzungsbedarf oder konkrete operative Fallbeispiele zur Illustration der Notwendigkeit wurden vom federführenden Bundesministeriums des Innern und für Heimat öffentlich[65] angeführt. Eine Verfassungsänderung anzustreben, ohne konkreten Handlungsbedarf demonstrieren zu können, ist aus demokratietheoretischer Sicht höchst problematisch.

[59] Bundesministerium der Justiz (2023): Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) § 7b Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden
[60] Bundesministerium der Justiz (2023): Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) § 7c Anordnungen des Bundesamtes gegenüber Diensteanbietern
[61] Bundesministerium der Justiz (2023): Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) § 7c Anordnungen des Bundesamtes gegenüber Diensteanbietern
[62] Bundesministerium der Justiz (2023): Gesetz über den Bundesnachrichtendienst (BND-Gesetz - BNDG) § 34 Eingriff in informationstechnische Systeme von Ausländern im Ausland
[63] Bundesministerium der Justiz (2023): Gesetz über den Bundesnachrichtendienst (BND-Gesetz - BNDG) § 19 Strategische Ausland-Fernmeldeaufklärung
[64] Johannes Leithäuser (2022): Die Cyber-Abwehr zieht die Lehren aus dem Ukrainekrieg
[65] Hakan Tanriverdi (2019): Die Hackback-Pläne der Bundesregierung

Die Bundesregierung sollte das Bundesministerium des Innern und für Heimat auffordern, den konkreten Vorschlag für ein Konzept zur Aktiven Cyberabwehr sowie Fallbeispiele, wie diese Maßnahmen die IT-Sicherheit Deutschlands verbessern würden, öffentlich vorzulegen und mit Sachverständigen im entsprechenden Ausschuss zu debattieren. Der von der SNV im Rahmen ihres Transatlantischen Cyber Forums mit Vertreter:innen aus Wirtschaft, Wissenschaft und Zivilgesellschaft entwickelte Analyserahmen "Active Cyber Defense Operations. Assessment and Safeguards"[66] kann bei der Beurteilung des Konzepts hilfreich sein. Die SNV wird ihre Arbeit hierzu im Laufe des Jahres fortsetzen.[67]

Zusätzlich sollte die Bundesregierung den von ihr im Koalitionsvertrag genutzten Begriff des Hackbacks definieren, um mehr Klarheit zu schaffen.[68]

Um aktive Maßnahmen für die Gewährleistung der IT-Sicherheit zu fördern, sollte die Bundesregierung darüber hinaus die rechtlichen Rahmenbedingungen für staatlich koordiniertes oder unterstütztes Threat Hunting, vor allem für Kritische Infrastrukturen, prüfen und gegebenenfalls anpassen.[69]

Schwachstellenmanagement

Im Koalitionsvertrag heißt es: "Wir führen[...] ein wirksames Schwachstellenmanagement, mit dem Ziel Sicherheitslücken zu schließen, [...] ein".

Die Bundesregierung arbeitet unter Federführung des Bundesministeriums des Innern und für Heimat seit mehreren Jahren an der Einführung des Schwachstellenmanagement-Prozesses ("Government Disclosure Decision Process" (GDDP)/ "Vulnerability Equities Process" (VEP)[70]). Hierzu hat die SNV ein Modell vorgelegt.[71] Es sieht vor, dass alle Behörden sämtliche Schwachstellen diesem Prozess zuführen, also auch jene in erworbenen oder von internationalen Partnern mit deutschen Stellen geteilten Dienstleistungen und Produkten. Das Modell ist nur dann wirksam, wenn es so wie beschrieben umgesetzt wird. Sollte die Bundesregierung dieses Modell nicht oder nur teilweise umsetzen können, sollte stattdessen

[66] Sven Herpig (2021): Active Cyber Defense Operations. Assessment and Safeguards
[67] Stiftung Neue Verantwortung (2023): Transatlantic Cyber Forum
[68] Sven Herpig (2022): Aktive Cyberabwehr statt Hackback?
[69] Sven Herpig (2022): Cybersicherheitspolitik: Deutsche Ideenlosigkeit?
[70] Sven Herpig and Ari Schwartz (2019): The Future of Vulnerabilities Equities Processes Around the World
[71] Sven Herpig (2018): Schwachstellen-Management für mehr Sicherheit

rechtlich festgelegt werden, dass alle Behörden Schwachstellen bei Bekanntwerden umgehend über das Bundesamt für Sicherheit in der Informationstechnik in einen Coordinated Vulnerability Disclosure (CVD) Prozess[72] geben müssen.

Beide Optionen, die Umsetzung des SNV-Vorschlags[73] und die rechtliche Verankerung der ausnahmslosen Eingabe von Schwachstellen in einen CVD-Prozess, sind dem Status Quo[74] und jeder anderen Form eines Schwachstellenmanagement-Prozesses in jedem Fall vorzuziehen.

Die Bundesregierung sollte den von der SNV vorgeschlagenen Prozess zum Schwachstellenmanagement ohne Ausnahme umsetzen oder alternativ eine CVD-Pflicht für alle Bundesbehörden einführen. Nur so kann die IT-Sicherheit gestärkt und der Status Quo verbessert werden.

Recht auf Verschlüsselung

Im Koalitionsvertrag heißt es: “Wir führen ein Recht auf Verschlüsselung [...] ein.” Die deutsche Debatte um den richtigen Kurs bei der Verschlüsselungspolitik reicht Jahrzehnte und bis zur Gründung des BSI zurück. Sie ist damit vermutlich eine der Ältesten der deutschen Cybersicherheitspolitik.[75] Die Debatte beinhaltet Aspekte wie den Einsatz von Überwachungssoftware durch Polizeien und Nachrichtendienste (unter anderem bei Online-Durchsuchungen und Quellen-Telekommunikationsüberwachung) sowie Standardisierungsbemühungen für Abhörschnittstellen (im Rahmen von Lawful Interception).[76]

Eines der bis heute prägendsten Policy-Dokumente der deutschen Verschlüsselungspolitik ist

[72]Grundlagen zum Coordinated Vulnerability Disclosure (CVD) Prozess, siehe zum Beispiel: Tassilo Thieme (2021): Heureka! Von der Schwachstellenfindung bis zur Veröffentlichung: Entwicklung eines Coordinated Vulnerability Disclosure Prozesses für kleine und mittelständische IT-Unternehmen
[73]Basis für eine Präferenz des vorgelegten Modells über eine ausnahmslose CVD-Verpflichtung ist unter anderem die Regelung des Umgangs mit Grenzfällen (*Edge Cases*) wie Schwachstellen in Schadsoftware, siehe unter anderem Malvuln (2023): Finding and exploiting vulnerable Malware, und in entsprechend genutzten Tools, siehe unter anderem Gal Kristal (2021): Hotcobalt – New Cobalt Strike DoS Vulnerability That Lets You Halt Operations, sowie in maliziös-verwendeter Software, siehe unter anderem Lorenzo Franceschi-Bicchierai (2022): Russia Released a Ukrainian App for Hacking Russia That Was Actually Malware.
[74]Sven Herpig (2021): Schwachstellen im Koalitionsvertrag
[75]Zur gesamten Historie, siehe Sven Herpig und Stefan Heumann (2019): The Encryption Debate in Germany und Sven Herpig und Julia Schuetze (2021): The Encryption Debate in Germany: 2021 Update
[76]Sven Herpig (2022): Recht auf Verschlüsselung – nur mit Abhörschnittstelle?

der Kabinettsbeschluss der Deutschen Bundesregierung zu den „Eckpunkte[n] der deutschen Kryptopolitik“ vom 2. Juni 1999. Darin heißt es unter anderem: „Die Bundesregierung wird [...] die Verbreitung sicherer Verschlüsselung in Deutschland aktiv unterstützen“. Gleichzeitig wird jedoch auch die Handlungsfähigkeit der Sicherheitsbehörden adressiert, weshalb es weiter heißt: „Durch die Verbreitung starker Verschlüsselungsverfahren dürfen die gesetzlichen Befugnisse der Strafverfolgungs- und Sicherheitsbehörden zur Telekommunikationsüberwachung nicht ausgehöhlt werden“. Verkürzt wird die Kernidee dieser Eckpunkte oft mit „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ wiedergegeben. Auf die Eckpunkte folgten Absichtserklärungen wie die Digitale Agenda 2014-2017 und die Krypto-Charta 2015.[77]

So wurde es zum Standardvorgehen, Regulierung beim Einsatz von Ende-zu-Ende-Verschlüsselung bei gleichzeitigem Einsatz von Überwachungssoftware durch deutsche Sicherheitsbehörden im Rahmen von Quellen-Telekommunikationsüberwachung und Online-Durchsuchungen zu vermeiden. Dieser Grundsatz geriet 2019 auf der Innenminister(:innen)konferenz ins Wanken. Dort wurde die Möglichkeit eines “rechtmäßigen Zugangs”, Lawful Interception, diskutiert.[78] Diesem Vorhaben stellte sich in Form eines offenen Briefes ein breites Bündnis aus Politik, Wirtschaft, Wissenschaft und Zivilgesellschaft entgegen.[79] Das hielt die Bundesregierung jedoch nicht davon ab, das Thema auf EU-Ebene zu adressieren und ihre Ratspräsidentschaft zu nutzen, um einen entsprechenden Entschluss voranzutreiben.[80] Unterstrichen wurde die Bereitschaft der Bundesregierung zur Unterminierung von sicher implementierter, starker Ende-zu-Ende Verschlüsselung durch einen Passus der Cybersicherheitsstrategie 2021[81], in dem es heißt: „Technische und operative Lösungen für den rechtmäßigen Zugang zu Inhalten aus verschlüsselter Kommunikation sind in enger Abstimmung mit allen betroffenen Unternehmen, Interessenträgern und zuständigen Behörden auf europäischer Ebene entwickelt“. Wie die Umsetzung konkret aussehen soll, hat der Branchenverband der deutschen Informations- und Telekommunikationsbranche (Bitkom) in einem Positionspapier 2020[82] beschrieben: „Der

[77] Ausführlicher siehe Sven Herpig (2022): Recht auf Verschlüsselung – nur mit Abhörschnittstelle?
[78] Jörg Diehl, Martin Knobbe, Marcel Rosenbach und Wolf Wiedmann-Schmidt (2019): Seehofer greift WhatsApp an
[79] Offener Brief an das Bundesministerium des Innern, für Bau und Heimat (2019): Geplanter Eingriff in Verschlüsselung von Messenger-Diensten hätte fatale Konsequenzen
[80] Rat der Europäischen Union (2020): Entschließung des Rates zur Verschlüsselung – Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung
[81] Bundesministerium des Innern, für Bau und Heimat (2021): Cybersicherheitsstrategie für Deutschland 2021
[82] Bitkom (2020): Starke Verschlüsselung für mehr Sicherheit. Cyber-Sicherheit und Wirtschaftsschutz mit Verschlüsselung. Strafverfolgung und Gefahrenabwehr trotz Verschlüsselung

Blick muss also in Richtung des standardisierten Schnittstellenmanagements gehen. [...] Der Staat ist aufgerufen, sich neben den bereits eingebundenen Netzbetreibern und Systemlieferanten noch aktiver in den Standardisierungsgremien einzubringen, um benötigte sichere Schnittstellen-Definitionen mitzugestalten“.

Zu den zahlreichen Nachteilen, die sich aus diesem Vorhaben ergeben, gehört die unnötige Gefährdung der IT- und Cybersicherheit der entsprechenden Lösungen und Dienstleistungen durch gesteigerte Komplexität und Organisationsanforderungen, sowie der vereinfachte Zugriff auf Daten von Menschenrechtsaktivist:innen, Journalist:innen, Rechtsanwält:innen und Oppositionellen durch autoritäre Staaten. Denn es ist ein Trugschluss, dass bei Verschlüsselung mit eingebauten Abhörschnittstellen nur die „guten, demokratischen Staaten“ mit starkem Rechtssystem Zugriff auf entsprechende Daten erlangen. Und selbst in diesen Staaten können Sicherheitsbehörden ihren Zugriff missbrauchen.[83]

Eine verschlüsselungsfördernde Policy ist in diesem Bereich wichtig, denn nur mit sicher implementierter, starker Ende-zu-Ende Verschlüsselung können Menschenrechte gewahrt und sensible Unternehmensdaten geschützt werden. Dabei geht es insbesondere darum, Inhalte vertraulich zu halten und Geschäftsgeheimnisse und persönliche Daten zu schützen. Es geht aber auch um die Verifizierung von Absendern, um Betrugsversuche zu unterbinden.

Die Bundesregierung sollte daher eine Stellungnahme des Bundesamtes für Sicherheit in der Informationstechnik anfordern. In der Stellungnahme sollte das BSI auf Basis wissenschaftlich-technischer Erkenntnisse (vgl. BSIG § 1) die Auswirkungen von entsprechenden Schnittstellen für den rechtmäßigen Zugang zu den Inhalten Ende-zu-Ende verschlüsselter Kommunikation auf die Cyber- und IT-Sicherheit für Staat, Wirtschaft und Gesellschaft beurteilen.

Zusätzlich sollte die Bundesregierung die Notwendigkeit für die sichere Implementierung starker Verschlüsselung ohne rechtmäßigen Zugang durch Abhörschnittstellen für Sicherheitsbehörden bei Ende-zu-Ende verschlüsselter Kommunikation in nationaler Gesetzgebung verankern. Dies könnte zum Beispiel in dem “Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien” (TTDSG) geschehen.

Die Exekutive sollte zusätzlich angehalten werden, das Recht auf Verschlüsselung, im

[83]Siehe zum Beispiel beck-aktuell (2022): Rechtswidrige Polizeiermittlungen mit Daten aus der Luca-App

Sinne von sicher implementierter starker Ende-zu-Ende Verschlüsselung, auch auf der EU-Ebene durchzusetzen und nicht durch Verordnungen, wie zum Beispiel zur Chatkontrolle[84], zu unterminieren. Als ersten Schritt sollte die Bundesregierung ihre Betrachtung der Resolution des Europäisches Rates zu "Encryption Security through encryption and security despite encryption"[85] öffentlich klarstellen.

Weitere Instrumente

Ausnutzung von Software-Schwachstellen

Für den Bereich Ausnutzung von Software-Schwachstellen für Strafermittlung hat die SNV im Oktober 2018 unter dem Namen **"A Framework for Government Hacking in Criminal Investigations"** eine Analyse vorgelegt, deren **Policy-Empfehlungen bis heute Bestand** haben.[86] Diese beinhalten:

1. Schaffen eines verbindlichen Rechtsrahmens für staatliches Hacken
2. Staatliche Unterstützung von Forschung zu Verschlüsselung und alternativen Beschaffungsmethoden digitaler Beweismittel
3. Einrichtung eines Fähigkeitenaufbauprogramms (unter anderem für die Judikative)
4. Implementierung von Richtlinien zum Umgang mit digitalen Beweismitteln (dazu gehören die sichere Übermittlung und digitale Signaturen)
5. Aufbau eines behördenübergreifenden Dialogs (in Kooperation mit der Landesebene)
6. Begrenzung von staatlichem Hacken auf "schwere Straftaten"
7. Veröffentlichung von Transparenzberichten
8. Verabschiedung von klaren Richtlinien für die Anbieter von Hacking-Werkzeugen und -Dienstleistungen
9. Schaffung eines staatlichen Schwachstellenmanagement-Verfahrens

Die Empfehlung "**Staatliche Unterstützung von Forschung zu Verschlüsselung und alternativen Beschaffungsmethoden digitaler Beweismittel**" adressiert die Relevanz der Ausnutzung von Software-Schwachstellen für Strafermittlungen von Sicherheitsbehörden. Die

[84] Digitale Gesellschaft, Chaos Computer Club und Digitalcourage (2023): Chatkontrolle STOPPEN! und Global Encryption Coalition (2022): Breaking encryption myths. What the European Commission's leaked report got wrong about online security
[85] Rat der Europäischen Union (2020): Entschließung des Rates zur Verschlüsselung – Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung
[86] Sven Herpig (2018): A Framework for Government Hacking in Criminal Investigations

im Koalitionsvertrag festgehaltene **Überwachungsgesamtrechnung kann dafür ein erster Schritt sein, wenn sie beinhaltet, unter welchen Umständen die Sicherheitsbehörden bereits Zugriff auf welche Arten von Daten und Informationen haben können**.

Maschinelles Lernen

Für den Bereich Cybersicherheit von Künstlicher Intelligenz (lies: IT-Sicherheit von Maschinellem Lernen) hat die SNV im Oktober 2020 unter dem Namen **"Understanding the Security Implications of the Machine-Learning Supply Chain"** eine Analyse vorgelegt, deren **Policy-Empfehlungen bis heute Bestand** haben.[87] Diese beinhalten:

1. Entwicklung eines Sicherheitsansatzes, der auf der konventionellen Informationssicherheit beruht
2. Erhöhung der Transparenz, Rückverfolgbarkeit, Validierung und Verifizierung
3. Identifizierung, Übernahme und Anwendung bewährter Verfahren
4. Ausfallsicherheits- und Resilienzmaßnahmen vorschreiben
5. Schaffung eines Ökosystems für IT-Sicherheit bei maschinellem Lernen
6. Einrichtung einer permanenten Plattform für den Austausch von Bedrohungen
7. Entwicklung eines Katalogs von Konformitätskriterien für Dienstanbieter
8. Förderung der Kompetenz im Bereich des maschinellen Lernens

Freie Software

Für den Bereich Cybersicherheit und Freie Software erarbeitet die Stiftung Neue Verantwortung derzeit im Rahmen ihres Transatlantischen Cyber Forums zusammen mit Vertreter:innen aus Wirtschaft, Wissenschaft und Zivilgesellschaft Policy-Empfehlungen für die **"staatliche Rolle bei der Verbesserung von IT-Sicherheit Freier Software"**.[88]

[87] Sven Herpig (2020): Understanding the Security Implications of the Machine-Learning Supply Chain
[88] Stiftung Neue Verantwortung (2023): Transatlantic Cyber Forum

3. Schlusswort

Über alle genannten Bereiche hinweg bleibt festzuhalten, dass es der Bundesregierung bei der deutschen Cybersicherheitspolitik massiv an a) Transparenz und proaktiver Kommunikation, b) konstruktiver Einbeziehung der Zivilgesellschaft, sowie c) Evaluations- und Reformwillen mangelt. Die teils antagonistische Beziehung zwischen Regierung auf der einen Seite und Vertreter:innen von Wirtschaft und Wissenschaft, aber vor allem Zivilgesellschaft auf der anderen Seite ist großteils auf diese Mängel zurückzuführen. Gemeinsam könnte die deutsche Cybersicherheitspolitik besser gestaltet werden.

Der Sachverständige bedankt sich bei den zahllosen deutschen und internationalen Vertreter:innen aus Verwaltung, Wirtschaft, Wissenschaft und Zivilgesellschaft für den Informationsaustausch, der maßgeblich als Basis für die hier referenzierten Analysen und demnach dieser Stellungnahme diente.