Zeitschrift für Außen- und Sicherheitspolitik
https://doi.org/10.1007/s12399-024-00983-x

ESSAY

Von der Defensive zur Cyberoffensive? Aktive Cyberabwehr, *Hackbacks* und der Diskurs der Akteure in der deutschen Cybersicherheitspolitik

Janine Schmoldt

Eingegangen: 14. Juni 2023 / Angenommen: 13. Dezember 2023

Zusammenfassung Dieser Beitrag behandelt die deutsche Cybersicherheitsdebatte zur aktiven Cyberabwehr aus verfassungs- und völkerrechtlicher Sicht. Der Akteursdiskurs wird rekonstruiert, um zu ermitteln, wer im Falle eines Cyberangriffs unterhalb der Schwelle eines bewaffneten Konflikts ein Mandat zur aktiven Cyberabwehr erhalten sollte. Rechtliche Fragen und mögliche Risiken aktiver Cyberabwehrmaßnahmen werden adressiert und die Konsequenzen für die internationalen Beziehungen sowie die internationale Sicherheitspolitik erläutert.

Schlüsselwörter Cyber · Hackback · Aktive Cyberabwehr · Cybersicherheit · Völkerrecht

From Defence to Cyber Offensive? Active Cyber Defence, Hackbacks and Actors' Discourse in German Cyber Security Policy

Abstract This article examines the German cyber security policy debate on active cyber defence from a constitutional and international law perspective. The actors' discourse is reconstructed to determine who should receive an active cyber defence mandate in the case of a cyber-attack below the level of an armed conflict. Legal issues and possible risks concerning active cyber defence measures will be addressed to show the consequences for international relations and international security policy.

Keywords Cyber · Hackback · Active cyber defense · Cyber security · International law

✉ Janine Schmoldt
Universität Erfurt, Nordhäuser Str. 63, 99089 Erfurt, Deutschland
E-Mail: janine.schmoldt@uni-erfurt.de

Published online: 08 April 2024

1 Einleitung

Mit 136.865 erfassten Cyberkriminalitätsdelikten war die Zahl der Cyberangriffe in der Bundesrepublik Deutschland im Jahr 2023 auf einem ähnlich hohen Niveau wie in den beiden Vorjahren (BKA 2023a, S. 4). Doch nicht nur die Anzahl von Cyberangriffen ist hoch, auch die Qualität von Angriffen und Tätern steigt, wie auch die Anzahl von Sicherheitslücken, sodass sich die digitale Bedrohungslage in Deutschland insgesamt weiter zuspitzt. Nachdem das Bundesamt für Sicherheit in der Informationstechnik (BSI) noch vor drei Jahren schlussfolgerte, die digitale Bedrohungslage in Deutschland sei „angespannt bis kritisch" (BSI 2021, S. 9), so spezifiziert das BSI im Jahr 2023, die Bedrohung im Cyberraum sei „so hoch wie nie zuvor" (BSI 2023b, S. 11).

Der Ukrainekrieg hat diese Bedrohungslage dabei insgesamt weiter verschärft. Denn staatliche und nicht-staatliche Akteure und patriotische Hacker greifen nicht nur wechselseitig Ziele der jeweils anderen Kriegspartei an,[1] sondern es wurden auch Cyber-Aktivitäten gegen westliche Staaten beobachtet, „die vereinzelt auch Kritische Infrastrukturen in Deutschland betrafen" (BSI 2022, S. 46). So wurden beispielsweise Cyberangriffe gegen den Hamburger Windkraftanlagenbauer Nordex ausgeführt, der seine IT-Systeme daraufhin vorsorglich abgeschaltet hat (NDR 2022), gegen die Deutsche Windtechnik AG, welche die Kontrolle über knapp 2000 Windräder verlor (Knop 2022), und gegen Webseiten des Verteidigungsministeriums, des Bundestages und der Bundes- und Landespolizeibehörden, zu denen sich die russische Hackergruppe Killnet bekannte (Tagesschau 2022a).

Bereits zu Beginn des Ukrainekrieges[2] kam es zu einem Cyberangriff auf Uplink-Modems des europäischen Satelliten KA-Sat, mit dem Ziel, die Kommunikation des ukrainischen Militärs und der Polizei zu stören. Allerdings führte dieser Cyberangriff auch europaweit zu Kollateralschäden (Mäder 2022). In Deutschland konnten knapp 5800 Windenergieanlagen nicht mehr überwacht und gewartet werden (Brühl 2022), zudem waren „Geräte der Gefahrenabwehr eines Landkreises" (BSI 2022, S. 49) und Feuerwehren, welche die Satellitenverbindung für ihre Notfallkommunikation nutzen, betroffen (Mäder 2022). All diese Angriffe führten mit zu Warnungen vor russischen Cyberangriffen auf westliche kritische Infrastrukturen (CISA 2022) und bringen im Zuge dessen das Thema aktive Cyberabwehr zurück auf die Agenda.

Bundesinnenministerin Nancy Faeser zufolge sind Möglichkeiten erforderlich, um Cyberangriffe zu beenden oder neue zu verhindern. Hierfür müsse auch über

[1] Bereits im Januar 2022 wurden ukrainische Regierungswebseiten das Ziel von massiven Cyberangriffen. Hunderte von ukrainischen Rechnern sollen mit einer datenlöschenden Wiper-Schadsoftware infiziert worden sein. Zudem erklärte das Hackerkollektiv Anonymous Russlands Präsident Wladimir Putin am Tag der Invasion den Cyberkrieg. Aber auch die ukrainische Regierung rief dazu auf, sich an dem Krieg zu beteiligen und Teil einer IT-Army of Ukraine zu werden. Auf russischer Seite formierten sich ebenfalls Hacker und Hackergruppen, wie beispielsweise die Ransomwaregruppe Conti. Insgesamt gesehen sind viele verschiedene staatliche und nicht-staatliche Akteure wie etwa patriotische Hacker im Cyberraum aktiv und an dem bewaffneten Konflikt mit Cyberangriffen beteiligt.

[2] Insgesamt wurden seit Kriegsbeginn mehr als 700 Objekte der ukrainischen kritischen Infrastruktur, wie Umspannwerke oder Gaspipelines, zerstört. Seit Herbst 2022 werden zudem gezielt Anlagen der ukrainischen Energieversorgung attackiert, sodass das ukrainische Stromnetz stark beschädigt und die Bevölkerung teilweise von der Wärme- und Wasserversorgung abgeschnitten wurde (Tagesschau 2022b).

aktive Maßnahmen nachgedacht werden, welche über die Aufklärung eines Angriffs hinausgehen. Dafür ist laut Faeser auch eine Grundgesetzänderung nötig, um entsprechenden Akteuren die Befugnis zur aktiven Cyberabwehr zu geben (Quadbeck und Decker 2022). Gleichsam macht auch Außenministerin Annalena Baerbock im September 2022 klar: „Wenn wir wirksamer agieren wollen, müssen wir die Verantwortlichkeiten für die Cyberabwehr klar zuweisen, auch unterhalb der Schwelle militärischer Angriffe. Ich persönlich bin überzeugt, dass wir unsere Kräfte bündeln müssen – auch wenn das eine Verfassungsänderung braucht" (Auswärtiges Amt 2022).

Faeser und Baerbock knüpfen mit ihren Aussagen an eine lange Debatte um *Hackback*-Operationen an: Seit dem Jahr 2018 arbeitet das Bundesinnenministerium an einem Plan zur aktiven Cyberabwehr, damit die Bundesrepublik im Falle eines Cyberangriffs, der unterhalb der Schwelle eines bewaffneten Konfliktes liegt, agieren kann. Diese Überlegungen münden im Jahr 2023 schließlich auch in Deutschlands Nationaler Sicherheitsstrategie, in welcher die Bundesregierung darlegt, eine „Bundeskompetenz zur Gefahrenabwehr bei schwerwiegenden Cyberangriffen aus dem In- und Ausland durch Änderung des Grundgesetzes" (Auswärtiges Amt 2023, S. 62) anzustreben. Im Laufe der Jahre kam es dabei zu einem sogenannten *Diskurs der Akteure*: Denn unterschiedlichsten Sicherheitsakteuren wie dem Bundesnachrichtendienst, der Bundespolizei, der Bundeswehr oder dem BSI sollte das Mandat zur aktiven Cyberabwehr gegeben werden. Hintergrund dieser Überlegungen sind dabei nicht nur die Cyberangriffe im Zuge des Ukrainekrieges, sondern auch die Hackerangriffe auf den Deutschen Bundestag 2015, die Ransomware-Angriffe WannaCry und NotPetya aus dem Jahr 2017 sowie die Cyberoperationen im Zuge der US-Präsidentschaftswahlen 2016 und 2020.

Dieser Beitrag beleuchtet aus politik- und rechtswissenschaftlicher Perspektive die Debatte um *Hackback*-Operationen und untersucht damit die Transformation von einer eher defensiv ausgerichteten hin zu einer offensiveren deutschen Cybersicherheitspolitik. Dabei wird in drei Schritten vorgegangen: Erstens wird der Diskurs der Akteure vorgestellt, um aufzuzeigen, welchen deutschen Sicherheitsbehörden im Falle eines Cyberangriffs, der unterhalb der Schwelle eines bewaffneten Konfliktes liegt, das Mandat zur aktiven Cyberabwehr gegeben werden soll. Diese Mandatserweiterungen werden zweitens vor dem Hintergrund der bestehenden völkerrechtlichen und verfassungsrechtlichen Rahmenbedingungen beleuchtet. Drittens, und damit abschließend, wird dargelegt, welche Folgen und Risiken Maßnahmen der aktiven Cyberabwehr als Antwort auf Cyberangriffe, die unterhalb der Schwelle eines bewaffneten Konfliktes liegen, für die internationalen Beziehungen und die internationale Sicherheitspolitik haben können.

2 Der Diskurs der Akteure

Die Debatte um die offensive Verteidigung und Sicherung kritischer und digitaler Infrastrukturen ist unter vielen Begriffen bekannt. Seit dem Jahr 2017 beschreiben Termini wie „aktive Cyberabwehr", „digitaler Gegenangriff", „finaler digitaler Rettungsschuss", „digitaler Gegenschlag" oder *„Hackback"* „die Suche nach Maß-

nahmen für die aktive, zivile und militärische Gegenwehr in einem Szenario eines Cyberangriffs auf deutsche Systeme (kritischer, staatlicher oder privater Natur)“ (Deutscher Bundestag 2018, S. 1).

Im Jahr 2017[3] lud das Bundeskanzleramt zu einer Sitzung des geheimen Bundessicherheitsrates ein, in welcher diskutiert wurde, wie sich Deutschland im digitalen Zeitalter verteidigen könne, wenn Hacker wie bereits im Jahr 2015 in Systeme des Deutschen Bundestages eindringen, oder wenn die kritische Infrastruktur Deutschlands angegriffen werden würde. Ein breiter Konsens des Gremiums suggerierte, dass die Bundesrepublik Deutschland, ebenso wie beispielsweise die USA, die Fähigkeiten zum digitalen Gegenschlag als Ultima Ratio brauche (Mascolo 2017; Mascolo und Steinke 2018). Im Falle eines Cyberangriffs, der unterhalb der Schwelle eines bewaffneten Konfliktes liegt, solle die Bundesrepublik Deutschland künftig zurückhacken können.

Klaus Vitt, damaliger Staatssekretär des Bundesinnenministeriums und Beauftragter der Bundesregierung für Informationstechnik zufolge zeigt die Erfahrung, „dass eine rein defensive Cyberabwehr künftig nicht mehr reichen wird […]. Wir benötigen als letzten Schritt auch Möglichkeiten für eine aktive zivile Abwehr“ (Heide und Riedel 2019). Ebenso wie die derzeitige Bundesinnenministerin machte auch ihr Vorgänger Horst Seehofer klar, dass herkömmliche Abwehrmaßnahmen bei digitalen Katastrophen und Hackerangriffen auf kritische Infrastrukturen nicht mehr ausreichen könnten (Becker 2019). Von *Hackback* möchte die Bundesregierung allerdings nicht sprechen.[4] Im Jahr 2021 stellen die Regierungsparteien in ihrem Koalitionsvertrag klar, dass sie *Hackback*-Operationen als Mittel der Cyberabwehr grundsätzlich ablehnen (Bundesregierung 2021, S. 16–17). Dies wird im Jahr 2023 von der Bundesregierung in der Nationalen Sicherheitsstrategie Deutschlands nochmals iteriert (Auswärtiges Amt 2023, S. 62). Stattdessen wird der Begriff der aktiven Cyberabwehr verwendet, womit, so eine Definition der Stiftung Neue Verantwortung, „[e]ine aktive Gegenmaßnahme unterhalb der Schwelle des bewaffneten Konflikts [gemeint ist], die dazu ausgelegt ist einen Cyber-Angriff abzuwehren und/oder aufzuklären“ (Stiftung Neue Verantwortung 2018). Die Bundesregierung selbst bedient sich einer ähnlichen Erläuterung und definiert im Februar 2023 aktive Cyberabwehr als aktive Maßnahme, welche das Ziel verfolgt, „die zum Angriff genutzten informationstechnischen Systeme mit informationstechnischen Mitteln zu manipulieren oder zu stören“ (Deutscher Bundestag 2023, S. 3).

Im Gegensatz dazu unterliegen *Hackbacks*, so die Bundesregierung im Jahr 2023, keiner definitorischen Beschränkung – die gesamte IT-Infrastruktur eines (vermeintlichen) Angreifers kann somit als legitimes Ziel eines *Hackbacks* verstanden werden, wodurch auch Vergeltungsangriffe auf zivile Infrastrukturen vorstellbar sind (Deutscher Bundestag 2023, S. 4). Ebenfalls vorstellbar ist das Eindringen in Computernetzwerke, um Angriffe direkt auf dem eigenen System zu unterbinden, „indem etwa

[3] In den USA wurde die Debatte um aktive Cybermaßnahmen bzw. aktive Verteidigung (*active defense*) bereits im Jahr 2012 geführt. Siehe beispielsweise Nakashima (2012).

[4] So stellt die Bundesregierung in einer Antwort auf eine Bundestagsanfrage im November 2018 klar, dass der Terminus *Hackback* „von der Bundesregierung konzeptionell grundsätzlich nicht verwendet [wird], weder für Aktivitäten der Cyberabwehr noch der Cyberverteidigung“ (Deutscher Bundestag 2018, S. 2).

die angreifende Hard- und Software lahmgelegt oder gar zerstört werden“ (Reinhold und Schulze 2017, S. 3). Aufgrund dieser „fehlenden definitorischen Beschränkungen sind *Hackbacks* [daher] kein Mittel militärischer Operationsführung“ (Deutscher Bundestag 2023, S. 4) für die deutsche Bundesregierung.

Diese Differenzierung von einerseits aktiver Cyberabwehr als Gefahrenabwehr und andererseits *Hackback* als digitalen Vergeltungsangriff oder Vergeltungsschlag wird sowohl von Nancy Faeser, als auch von Wissenschaftlerinnen und Wissenschaftlern wie etwa Haya Shulman, Michael Waidner, Tanya Gärtner und Annika Selzer vorgenommen (BMI 2022c; Shulman und Waidner 2023; Gärtner und Selzer 2023). Von aktiver Cyberabwehr und *Hackback* ist als weiteres Mittel der gesamtstaatlichen Cybersicherheit Deutschlands die Cyberverteidigung abzugrenzen. Denn während sich Maßnahmen der aktiven Cyberabwehr auf Angriffe beziehen, die unterhalb der Schwelle zu bewaffneten Konflikten liegen (wie beispielsweise Delikte der Cyberkriminalität) richtet sich die Cyberverteidigung gegen Angriffe, die oberhalb der Schwelle zu bewaffneten Konflikten liegen und damit einen Kriegszustand auslösen. Insofern bezieht sich der Begriff der Cyberverteidigung auch auf „die aktive Verteidigung im Cyberraum“ (Deutscher Bundestag 2023, S. 3) durch die Streitkräfte bzw. die Bundeswehr.

Im Juni 2019 führte der damalige Generalleutnant Ludwig Leinhos, Inspekteur Cyber- und Informationsraum der Bundeswehr in einem Interview den Begriff des digitalen Verteidigungsfalls ein, unter welchem er „eine schlagwortartige Beschreibung einer Situation [versteht], bei der es in Deutschland zu massiven Störungen durch Cyber-Angriffe kommt. Diese können beispielsweise große wirtschaftliche Schäden hervorrufen, Einschränkungen bei der Versorgung der Bevölkerung auslösen oder Einschränkungen der staatlichen Handlungsfähigkeit bewirken. Dabei bleiben die Angriffe und Auswirkungen jedoch noch unterhalb der Schwelle, die einen klassischen Verteidigungsfall auslösen würde“ (Spartanat Redaktion 2020). Leinhos stellt dabei klar, dass der digitale Verteidigungsfall nicht mit dem in Artikel 115a Grundgesetz geregelten militärischen Verteidigungsfall gleichzusetzen ist und fordert die Nutzung und Koppelung von Fähigkeiten staatlicher Institutionen. Die Bundeswehr, so Leinhos, könnte in einem digitalen Verteidigungsfall „beispielsweise im Rahmen der Amtshilfe mit Cyberabwehrexperten“ (Spartanat Redaktion 2020) unterstützen. Die deutsche Bundesregierung selbst verwendet den Terminus digitaler Verteidigungsfall nicht (Deutscher Bundestag 2019, S. 2).

Wenngleich politische Akteure die Begriffe aktive Cyberabwehr, *Hackback* und Cyberverteidigung trennen und abgrenzen, gibt es auch kritische Stimmen, die argumentieren, dass aktive Cyberabwehrmaßnahmen oder Gefahrenabwehr im Cyberraum im wesentlichen *Hackbacks* sind (Herpig 2023). Die Grenzen, so ein Kritikpunkt, zwischen offensiver und defensiver Cyberabwehr verschwimmen (Rundfeldt 2023), wenn das vierstufige Vorgehen,[5] welches bei einem Cyberangriff aus dem Ausland greifen soll, betrachtet wird:[6] Die ersten beiden Stufen sollen Datenverkehre umlenken oder blockieren, sodass noch nicht von aktiven Cyberabwehrmaßnah-

[5] Dieses wurde im Jahr 2019 durch den Bayerischen Rundfunk in Teilen öffentlich zugänglich gemacht.

[6] „Obwohl in einer öffentlichen Bundestagsanhörung auch über das Stufenmodell gesprochen wurde, ist es bisher nicht öffentlich. Das Bundeskriminalamt hat es entwickelt, aber mit der Geheimhaltungsstufe

men gesprochen werden kann. Innerhalb der dritten Stufe sollen Sicherheitsbehörden allerdings fremde Netzwerke hacken, infiltrieren, Daten löschen oder verändern dürfen und innerhalb der vierten Stufe in Systeme eindringen und diese herunterfahren können (Tanriverdi 2019; Kipker 2023, 2019; Stiftung Neue Verantwortung 2018; Herpig 2019). Eine Befürchtung ist hierbei, dass dieses Stufenmodell in den nachfolgenden Jahren sukzessive auf offensive Maßnahmen erweitert wird, die bereits vorgezeichnet sind (Rundfeldt 2023). So zählt Johannes Rundfeldt zufolge die Ausführung von fremdem Quellcode auf einem Zielsystem (eine Maßnahme der vierten Stufe) zu offensiven Maßnahmen, ebenso wie die Verwendung eines Netzwerkscanner-Werkzeugs in den Stufen eins oder zwei (Rundfeldt 2023). Zusammengenommen bedeutet dies laut Rundfeldt, dass aktive Cyberabwehr im Grunde offensive *Hackbacks* sind (Rundfeldt 2023).

Neben verschiedenen verfassungs- und völkerrechtlichen Fragen stellt sich in Deutschland die Kompetenz-, Verantwortungs- und Zuständigkeitsfrage: Welche Sicherheitsbehörde oder welche Einheit soll das Mandat zur aktiven Cyberabwehr erhalten? In der Diskussion sind drei Akteure,[7] wie im Folgenden dargelegt wird: 1) der Bundesnachrichtendienst, 2) das Bundeskriminalamt und 3) das Bundesamt für Sicherheit in der Informationstechnik.

2.1 Der Bundesnachrichtendienst

Zuständig für digitale Gegenschläge soll, so der damalige Bundesinnenminister Horst Seehofer, der Bundesnachrichtendienst (BND) sein (Heide und Riedel 2019), der als Auslandsgeheimdienst der Bundesrepublik Deutschland sicherheitsrelevante

„Nur für den Dienstgebrauch“ versehen. Es ist nicht öffentlich bekannt, ob dieses Modell noch die aktuelle Referenz des Innenministeriums ist oder ob es mittlerweile aktualisiert wurde“ (Herpig 2019).

[7] Auch Deutschlands Inlandsgeheimdienst, das Bundesamt für Verfassungsschutz, forderte im Jahr 2017 die Befugnis zum digitalen Gegenschlag. So vertrat der damalige Präsident des Bundesamtes für Verfassungsschutz Hans-Georg Maaßen die Meinung, dass die deutsche Spionageabwehr die Möglichkeit zu Cyber-Gegenmaßnahmen erhalten müsse: „Wir halten es für notwendig, dass wir nicht nur rein defensiv tätig sind […]. Sondern wir müssen auch in der Lage sein, den Gegner anzugreifen, damit er aufhört, uns weiter zu attackieren“ (Spiegel 2017). Maaßen denkt dabei an das Löschen von Daten, „die auf einen fremden Server abgeflossen sind“ (Reuters 2017) und an das Ausspähen von Angreifern im Cyberraum (Reuters 2017; Diehl und Reinbold 2017) und spezifiziert: „Wenn wir als Inlandsnachrichtendienst erkennen, dass […] der Bundestagsserver gehackt ist und die Daten abfließen auf einen ausländischen Server, muss es im Sinn einer Nacheile möglich sein, diese Daten löschen zu können, bevor sie weiterverbreitet werden“ (Reuters 2017). Zudem solle der Verfassungsschutz zur Informationsgewinnung Angriffsserver auch selbst mit Schadsoftware infizieren dürfen: „Das wäre, wie wenn man in der Realwelt einen ausländischen Agenten umdreht und zu einem Counter-Man macht, dass also dieser ausländische Agent dann für uns arbeitet“ (Reuters 2017). Da der derzeitige Verfassungsschutz-Präsident Thomas Haldenwang allerdings betonte, dass aktive Cyberabwehrmaßnahmen für den Verfassungsschutz aufgrund fehlender Exekutivbefugnisse und aufgrund der primären Aufgabe der Attribution von ausländischen Cyberangriffen „wesensfremd“ (Sehl 2019) seien, wird das Bundesamt für Verfassungsschutz in diesem Beitrag nicht als Akteur für aktive Cyberabwehr angeführt. Allerdings wird darauf verwiesen, dass der Verfassungsschutz bereits das technische Wissen und die entsprechenden Fähigkeiten hat, wie die Cyberabwehr des Verfassungsschutzes, welche Cyberangriffe beobachtet, analysiert, attribuiert und sensibilisiert, verdeutlicht (Bundesamt für Verfassungsschutz 2022). In der neuen Cybersicherheitsagenda der Bundesregierung aus dem Jahr 2022 wurden zudem als Maßnahme und Ziel in der 20. Legislaturperiode auch die „Modernisierung der IT-Infrastruktur im BfV [und die] Fortentwicklung der Cyberfähigkeiten des BfV“ (BMI 2022a) festgeschrieben.

Nachrichten aus dem Ausland bewertet und beschafft[8] und neben dem Bundesamt für Verfassungsschutz (BfV) und dem Militärischen Abschirmdienst (MAD) eine von drei Sicherheitsbehörden Deutschlands ist,[9] die sich ausschließlich mit der Beschaffung und Auswertung von Informationen befassen.[10] Darüber hinaus unterstützt der BND die Bundeswehr mit Lagebildern bei der Sicherung von Auslandseinsätzen. Der BND ist auch bei Cyberangriffen aus dem Ausland gefordert, wobei ihm eine besondere Rolle zukommt: „Er hat die Befugnis und die technischen Möglichkeiten zur strategischen Erfassung internationaler Datenverkehre“ (BND 2021). Das bereits erwähnte interne Konzeptpapier der Bundesregierung plädiert ebenfalls dafür, dass der BND offensive Cyberoperationen ausführen solle (Tanriverdi 2019). Aufgrund der Tatsache, dass der BND bereits konstant Informationen über Cyberangreifer, ihr Vorgehen sowie ihre Infrastrukturen sammelt, sei der BND der geeignete Kandidat. Im Konzeptpapier zum Ausbau der Abwehrfähigkeit des Bundes wird daher argumentiert: „Die Befugnis zur Umsetzung [...] beim BND anzusiedeln, ist aus fachlicher Sicht sinnvoll“ (Tagesschau 2019, ab Minute 1:25). Damit würden dem BND erstmals[11] Exekutivbefugnisse zugestanden werden. Georg Mascolo und Ronen Steinke schlussfolgern daher: „Viel deutet darauf hin, dass der BND bald erstmals in seiner mehr als 60-jährigen Geschichte die Lizenz zum Schießen bekommt. Zwar nur im virtuellen Raum, nicht mit Pistolen, sondern nur mit deren digitalem Äquivalent, mit Cyberwaffen“ (Mascolo und Steinke 2018). Argumentiert wird, dass die im Jahr 2013 gegründete BND-Unterabteilung T4 bereits in fremde Netze, Computersysteme und Handys eindringen könne und damit das technische Wissen im BND vorhanden sei. Zudem könne der BND als Auslandsgeheimdienst auch aus dem Ausland operieren. Dass der BND folglich für *Hackback*-Operationen geeignet ist, bestätigt BND-Präsident Bruno Kahl deutlich: „Der Nachrichtendienst stünde zur Verfügung [...]. Technisch möglich ist es. Die Fähigkeiten sind auch schon da im BND“ (Mascolo und Steinke 2018). Auch sein Vorgänger, Gerhard Schindler, macht klar: „Es gibt keine vernünftige Alternative zum BND“ (Mascolo und Steinke 2018).

2.2 Die Bundespolizei und das Bundeskriminalamt

Neben Deutschlands Auslandsgeheimdienst soll ebenso eine Polizeibehörde für die aktive Cyberabwehr zuständig sein, wenn dabei der BND „zwingend mit einbezogen“ (Tanriverdi 2019) wird. Im Jahr 2020 wollte das Bundesinnenministerium daher

[8] Für weiterführende Informationen zur Historie des BND siehe Krieger (2021), Erxleben (2015), Wolf (2018).

[9] Dabei ist der MAD für die Sicherung der Einsatzbereitschaft der deutschen Bundeswehr zuständig, während das BfV als Inlandsgeheimdienst gemeinsam mit den Landesämtern für Verfassungsschutz extremistische und verfassungsfeindliche Bestrebungen beobachtet.

[10] Die Gewährleistung von innerer Sicherheit ist nicht nur eine wichtige Voraussetzung, um individuelle Freiheitsrechte zu wahren, sondern auch die Grundlage für sozialen und wirtschaftlichen Wohlstand. Aus diesem Grund hält die Bundesrepublik Deutschland „polizeiliche, militärische und nachrichtendienstliche Mittel vor, um potentielle Gefahren und tatsächliche Bedrohungen aus dem In- und Ausland aufzuklären und ihnen entgegenzuwirken“ (Erxleben 2015, S. 15).

[11] Seit Operation Rusty und Operation Gehlen.

weitgehende Befugnisse im Bundespolizeigesetz verankern. Einem Entwurf für ein neues Bundespolizeigesetz ist zu entnehmen, dass die Bundespolizei „Cyberangriffe auswerten, umlenken, zurückverfolgen und Maßnahmen zur Früherkennung von Cyberangriffen einleiten“ (Biselli 2020) und „zur Abwehr einer gegenwärtigen Gefahr eines Cyberangriffs mit technischen Mitteln in informationstechnische Systeme, von denen der Cyberangriff ausgeht, 1. eingreifen, und 2. aus ihnen Daten erheben, übernehmen, löschen und verändern“(Biselli 2020) könne. In bestimmten Fällen dürfe die Bundespolizei zudem „Maßnahmen vornehmen, die zu einer Überlastung, Nichtverfügbarkeit oder sonstigen Störung der Funktion der für den Cyberangriff genutzten informationstechnischen Infrastruktur führen“ (Biselli 2020), wobei diese Maßnahmen auch eingeleitet werden können, ohne dass betroffene Personen davon Kenntnis haben. Somit finden sich alle Stufen der aktiven Cyberabwehr in dem Gesetzesentwurf wieder (Biselli 2020). Zwar wurden diese Vorschläge und Passagen schlussendlich nicht übernommen,[12] doch „[d]ie Formulierungen im Bundespolizeigesetz-Entwurf waren der deutlichste Schritt in Richtung *Hackback*, der sich bisher in einem Gesetzentwurf fand“ (Biselli 2020).

Sollten diese Überlegungen weitergeführt werden und der Bundespolizei die Aufgabe der aktiven Cyberabwehr übertragen werden, müsste dies auch in den Polizeigesetzen der Bundesländer verankert werden. Mehrere Bundesländer sollen allerdings signalisiert haben, „dass sie die Kompetenz der Cyberabwehr lieber beim Bund sähen, also beim Bundeskriminalamt (BKA) unter dessen Präsidenten Holger Münch“ (Baumgärtner et al. 2017). Daher hat Nancy Faeser bereits im Juli 2022 verkündet, dass der Bund „vor allem dem Bundeskriminalamt (BKA) – gegebenenfalls auch mehreren Behörden – einschlägige Zuständigkeiten geben“ (Krempl 2022) müsse. Im April 2023 wird Faeser konkreter und möchte dem BKA „eine Kompetenz zur Gefahrenabwehr bei Cyberangriffen einräumen“ (Rath 2023), damit dieses „Angreifer und Angreiferinnen identifizieren, Attacken stoppen oder zumindest abmildern“ (Rath 2023) kann.

2.3 Das Bundesamt für Sicherheit in der Informationstechnik

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist als Akteur für das Mandat zur aktiven Cyberabwehr im Gespräch. Zu den Aufgaben des BSI gehören bereits unter anderem die Abwehr von Cyberangriffen bzw. der Schutz der Regierungsnetze und der Bundesverwaltung durch eine kontinuierliche Beobachtung der Cybersicherheitslage, durch die Bewertung und Analyse von Sicherheitsrisiken und Schwachstellen und durch eine Einschätzung von Auswirkungen neuer Trends und Entwicklungen im Cybersicherheitskontext. Zudem fungiert das BSI mit seinem Lagezentrum bundesweit als zentrale Meldestelle für Cyberangriffe und -vorfälle (BSI 2023c) und leistet durch sein Computer Emergency Response Team (CERT-Bund) Unterstützung bei Cybersicherheitsvorfällen (BSI 2023a). Dieses weite Aufgabenspektrum führte mit zu der Forderung, dass das BSI nicht mehr

[12] Der entsprechende § 74 Abwehr von Cyberangriffen entstamme „aus einem früheren Referentenentwurf, den das Innenressort noch einmal angepasst hat, um zunächst andere Überwachungsbefugnisse für die Bundespolizei durchzubringen“ (Krempl 2020).

rein defensiv tätig sein soll, „sondern offensiv in IT-Systeme eindringen“ (Meister und Biselli 2019) und damit aktive Cyberabwehr beitreiben soll. Sowohl Arne Schönbohm in seiner damaligen Funktion als BSI-Präsident als auch die derzeitige BSI-Präsidentin Claudia Plattner befürworten aktive Cyberabwehrmaßnahmen. Während Schönbohm im Jahr 2022 klarmachte, dass aktive Cyberabwehr hilfreich sei, um den Zugriff von Angreifern auf Datenströme sowie den Abfluss von Datensätzen zu unterbinden (Tremmel 2022) stellt Plattner im Jahr 2023 heraus: „Man kann nicht immer nur abwehren, sondern man muss im Zweifelsfall auch mal dafür sorgen, dass man aus der Schusslinie kommt, oder dafür sorgen, dass Angriffe nicht mehr stattfinden“ (Greis 2023).

Nach der Vorstellung des Diskurses der Akteure beleuchtet Kapitel 3 eine mögliche Mandatserweiterung der vorgestellten deutschen Sicherheitsbehörden vor dem Hintergrund bestehender völkerrechtlicher und verfassungsrechtlicher Rahmenbedingungen, um zu prüfen, ob und inwieweit eine Mandatserweiterung der vorgestellten Akteure verfassungs- und völkerrechtlich zulässig wäre.

3 Verfassungs- und völkerrechtliche Rahmenbedingungen

Alle Maßnahmen der aktiven Cyberabwehr, so macht die Bundesregierung im Jahr 2018 und auch im Jahr 2023 klar, müssen sich im Rahmen des geltenden Verfassungs- und Völkerrechts bewegen (Deutscher Bundestag 2018, S. 2; Auswärtiges Amt 2023, S. 62). Ob und inwieweit Polizei und Nachrichtendienste in der aktiven Cyberabwehr tätig werden und zusammenwirken können, ist allerdings fraglich, denn das Trennungsgebot zwischen Polizei und Geheimdiensten steht solch einem „Zusammenwirken“ entgegen und beschränkt Exekutivkompetenzen auf Polizeidienste. Dies findet sich auch in § 1 Absatz 1 Satz 3 BND-Gesetz,[13] welches den BND als Bundesoberbehörde im Geschäftsbereich des Bundeskanzleramtes definiert, der keiner polizeilichen Dienststelle angegliedert werden darf. Ein Absatz später wird darauf verwiesen, dass der BND vornehmlich die Aufgabe hat, Informationen über das Ausland zu sammeln, die außen- und sicherheitspolitisch von Bedeutung für die Bundesrepublik sind. Diese Berichtspflicht ist auch in § 33 BND-Gesetz niedergelegt. Um Informationen zu akquirieren, ist der BND legitimiert, nachrichtendienstliche Mittel wie klassische Informanten (HUMINT), die Auswertung von Satelliten- und Luftbildaufnahmen (IMINT), elektronischer Kommunikation (SIGNINT) oder öffentlich zugängliche Quellen (OSINT) einzusetzen. Angewandt auf den Cyberbereich bedeutet dies, so Dennis-Kenji Kipker, „dass der BND[14] zwar umfassende Informationen über relevante Daten sammeln, aber nicht

[13] Am 20. Dezember 1990 verabschiedet der Deutsche Bundestag ein Gesetz über den Bundesnachrichtendienst, welches die Aufgaben und Befugnisse des BND festlegt.

[14] Selbige Schlussfolgerung kann auch für den Verfassungsschutz gezogen werden, heißt es doch in § 3 Absatz 1 des Bundesverfassungsschutzgesetzes, dass dieser Informationen über „Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziele haben“, sammelt.

selber aktive Cyber-Angriffe durchführen darf, was beim ‚Hackback' aber der Fall wäre" (Kipker 2019).

Alles in allem konstatieren die Wissenschaftlichen Dienste des Deutschen Bundestages: „Nach derzeitiger Rechtslage haben die Nachrichtendienste [...] grundsätzlich keine klassischen Eingriffsbefugnisse. Ihr Zuständigkeitsbereich beschränkt sich auf Aufklärungsmaßnahmen" (Wissenschaftliche Dienste des Deutschen Bundestages 2018). Auch das BKA ist nach derzeitiger Rechtslage nicht legitimiert, Cyberangriffe im Ausland auszuführen, sondern ermittelt im Auftrag des Generalbundesanwaltes in „besonders schweren Fällen von Computersabotage" (BKA 2023b). Die Ausführung von offensiven Cyberangriffen auf ausländische Institutionen oder Einrichtungen fallen ebenso wenig in die Zuständigkeit des BSI. Zwar ist dieses gemäß § 3 BSI-Gesetz für die „Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes"[15] zuständig, offensive Angriffe mandatiert das BSI-Gesetz derzeit allerdings nicht.

Darüber hinaus verbietet das Grundgesetz (GG) in Artikel 26 Handlungen, die das friedliche Zusammenleben der Völker stören. Offensive Cybermaßnahmen würden also nicht nur gegen Paragrafen des BND-, BKA-, und BSI-Gesetzes verstoßen, sondern wären auch verfassungswidrig. Allerdings beschränkt sich der Anwendungsbereich des Artikel 26 GG nicht auf Handlungen der Bundeswehr. Diese hat bereits in ihrem „Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr 2016" eine Strategie entwickelt, die ein Tätigwerden im Cyberraum beschreibt. Im Jahr 2017 wurde dann das Kommando Cyber- und Informationsraum aufgestellt, welches mit dem Zentrum Cyberoperationen in der Lage ist, offensive Cyberoperationen durchzuführen. Um allerdings tätig werden zu können, müsste gemäß Artikel 115a GG ein Verteidigungsfall vorliegen. Nur dann ist die Bundeswehr mandatiert, Gewalt anzuwenden oder aktive Cyberabwehrmaßnahmen durchzuführen. Die Bundesregierung selbst erläutert dazu: „Ein Cyberangriff kann unter bestimmten Bedingungen einen bewaffneten Angriff im Sinne von Artikel 51 der UN-Charta darstellen. In diesem Fall steht der Bundesrepublik Deutschland das Recht auf Selbstverteidigung zu und sie könnte auf diesen bewaffneten Angriff mit allen zulässigen militärischen Mitteln reagieren" (Deutscher Bundestag 2018, S. 6). Allerdings sind Maßnahmen der aktiven Cyberabwehr als Antwort auf Cyberangriffe gedacht, die unterhalb der Schwelle eines bewaffneten Konfliktes liegen. Würde die Bundeswehr oder eine andere Sicherheitsbehörde also eben jene Maßnahmen durchführen, so würde sie gegen das völkerrechtliche Gewaltverbot, niedergelegt in Artikel 2 Ziffer 4 der UN-Charta, verstoßen.

Mit dem „Recht auf Gegenmaßnahmen" gibt es völkerrechtlich gesehen allerdings sehr wohl Möglichkeiten, auf Cyberoperationen, die unterhalb der Schwelle eines bewaffneten Konfliktes liegen, zu reagieren. Niedergelegt in den „Draft articles on Responsibility of States for internationally wrongful acts" stellen diese Normen zwar keinen völkerrechtlichen Vertrag dar, allerdings wurden die Artikelentwürfe von der Generalversammlung der Vereinten Nationen als Resolution verabschiedet und spiegeln in weiten Teilen den Stand der Entwicklung des Völkergewohnheitsrechts wider. Wenn eine Cyberoperation eine Primärnorm, beispielsweise die Souveränität

[15] § 3 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik.

Deutschlands, verletzt, dann kommen mit Artikel 52 sogenannte Sekundärnormen zur Anwendung und der angegriffene Staat kann „solche dringenden Gegenmaßnahmen ergreifen, die zur Sicherung seiner Rechte notwendig sind“. In diesem Sinne sind Gegenmaßnahmen gerechtfertigte, völkerrechtswidrige Akte, die als Antwort auf einen vorangegangenen Völkerrechtsbruch zu verstehen sind. Wie die meisten Rechtsnormen, unterliegt auch das Recht auf Gegenmaßnahmen bestimmten Voraussetzungen: So muss eine Cyberoperation beispielsweise zurechenbar sein und der angegriffene Staat hat den angreifenden Staat aufzufordern, den Rechtsbruch zu beenden. Darüber hinaus muss dem angreifenden Staat die Ergreifung von Gegenmaßnahmen mitgeteilt werden. Die Gegenmaßnahmen selbst müssen verhältnismäßig sein und dürfen nicht die Verpflichtung zur Unterlassung der Androhung oder Anwendung von Gewalt beeinflussen.

Die derzeitige Rechtslage lässt zwar aktuell keine offensiven Cybermaßnahmen zu, wie gezeigt wurde, doch entsprechend sind Gesetzes-Änderungen im Gespräch und gefordert. Fraglich ist allerdings, was solch eine Zeitenwende in Form von Mandatserweiterungen in der Cybersicherheitspolitik für Risiken mit sich bringen könnte.

4 Mögliche Folgen und Risiken aktiver Cyberabwehr

Angesichts der hohen, hybriden und anfangs dargestellten Bedrohungslage im Cyberraum sind Staat, Wirtschaft und Gesellschaft gefordert, entsprechende Cybersicherheitskompetenzen aufzubauen, um digital souverän agieren zu können. „Denn die Bedrohungslage im Cyberraum“, so Bundesinnenministerin Faeser, „wächst jeden Tag. Die Zeitenwende, die wir angesichts des russischen Angriffskriegs gegen die Ukraine erleben, erfordert eine strategische Neuaufstellung und deutliche Investitionen in unsere Cybersicherheit. Bund und Länder müssen Cybergefahren koordiniert entgegentreten und ihre Fähigkeiten permanent weiterentwickeln“ (BMI 2022b). Daher wird eine Grundgesetzänderung gefordert, um neue Befugnisse für die deutschen Sicherheitsbehörden zu schaffen. So sind der BND, das BKA und das BSI im Gespräch, das Mandat der aktiven Cyberabwehr zu erhalten, um „schwerwiegende Cyberangriffe verhindern, stoppen oder zumindest abschwächen“ (BMI 2022b) zu können.

Der vorherige Abschnitt hat gezeigt, dass die derzeitigen verfassungs- und völkerrechtlichen Rahmenbedingungen einer Mandatserweiterung hin zur aktiven Cyberabwehr allerdings entgegenstehen und Maßnahmen der aktiven Cyberabwehr insbesondere gegen das völkerrechtliche Gewaltverbot verstoßen. Dies führt unweigerlich zu der Frage, ob im Falle einer Grundgesetzänderung und einer Mandatserweiterung einer deutschen Sicherheitsbehörde Maßnahmen der aktiven Cyberabwehr nicht das Risiko eines Verstoßes gegen das Gewaltverbot und damit einen Völkerrechtsbruch mit sich bringen würden. Denn dem sogenannten *Target-based* Ansatz[16] zufolge können Cyberoperationen, die gegen kritische Infrastrukturen gerichtet sind, als Ge-

[16] Neben dem *Instrument-based* und dem *Effect-based*-Ansatz ist der *Target-based*-Ansatz einer der Ansätze, die erklären, inwieweit Cyberoperationen Gewaltanwendungen darstellen. Folgt man dem *Instru-*

waltanwendung eingestuft werden, da „humanitäre Notlagen entstehen [könnten], die [wiederum] Tod und Zerstörung in weitem Umfang heraufbeschwören [könnten]“ (Dornbusch 2018, S. 101). Bezogen auf Maßnahmen der aktiven Cyberabwehr kann folglich konstatiert werden, dass diese als Gewaltanwendung verstanden werden können, wenn etwa fremde Netzwerke infiltriert bzw. gehackt werden und so ein weitreichender und langanhaltender Funktionsverlust kritischer Infrastrukturen die Folge ist. Denn auch wenn kritische Infrastrukturen nicht das primäre Ziel aktiver Cyberabwehr sind, so spielt die Vernetzung von Systemen eine große Rolle. Wird beispielsweise ein System in der Russischen Föderation durch aktive Cyberabwehr infiltriert, könnte dies „eine Kettenreaktion von Ausfällen [auch in Bereichen der kritischen Infrastrukturen] auslösen, deren Folgen niemand absehen kann“ (Klaus 2023). Damit kann das Risiko, mit Maßnahmen der aktiven Cyberabwehr Gewalt anzuwenden und damit gegen das völkerrechtliche Gewaltverbot zu verstoßen, als hoch eingestuft werden.

Ein weiteres Risiko von aktiver Cyberabwehr ist das sogenannte Sicherheitsdilemma, in welches Staaten geraten könnten, etwa wenn dem Aufbau von offensiven Cyberfähigkeiten mit dem Aufbau von Gegenfähigkeiten begegnet wird, um ein Mächtegleichgewicht herzustellen. In der derzeitigen Staatenpraxis könnte es zumindest theoretisch zu einem digitalen Wettrüsten kommen, betrachtet man die Cyberfähigkeiten einzelner Staaten: So hat die USA mit ihrer im Jahr 2018 veröffentlichten Cyberstrategie beispielsweise deutlich gemacht, dass ihre Cyber Command Forces zurückhacken, selbst wenn eine erfolgte Cyberoperation unterhalb der Schwelle eines bewaffneten Konfliktes liegt: „We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict“ (Department of Defense 2018). Auch das Vereinigte Königreich verfügt bereits über offensive Cyberkapazitäten, um sowohl Gegenangriffe als auch Hackerangriffe durchzuführen (Sabbagh 2020). In Estland soll sogar eine Art Cyber-Wehrpflicht für offensive Cyberoperationen eingeführt werden (Conrad und Werkhäuser 2019).

Diese Fähigkeiten und Maßnahmen könnten die Bedrohungslage verschärfen, zum Beispiel wenn die Attribution bzw. Zuordnung eines zu stoppenden Angriffs auf einen bestimmten Angreifer nicht klar ist. Denn IP-Adressen und Identitäten können verschleiert und anonymisiert werden, indem beispielsweise Cyberangriffe über Botnetze, kompromittierte und hintereinander gereihte Rechner, ausgeführt werden, so dass die IP-Adresse oder Identität des unbeteiligten Dritten Botrechners sichtbar, die des Angreifers allerdings verschleiert ist (Reinhold und Schulze 2017, S. 9; Riemann 2020, S. 144). Und selbst wenn durch technische Attribution der Ursprungsort oder die Urheber-IP-Adresse identifiziert werden kann, so „bleibt

ment-based-Ansatz, so sind die eingesetzten Mittel ausschlaggebend, wobei bei einer weiten Auslegung physischer, militärischer Zwang und bei einer engen Auslegung Waffen im weiteren Sinne entscheidend sind. Da bei Cyberoperationen das Kriterium des physischen, militärischen Zwangs nicht unmittelbar gegeben ist und der Begriff der Waffe völkerrechtlich nicht allgemein anerkannt definiert ist, ist dieser Ansatz nur bedingt hilfreich. Der *Effect-based* Ansatz hingegen zielt auf die Effekte und Auswirkungen von Cyberangriffen ab und definiert diese als Gewaltanwendungen, wenn physische Schäden die mittelbaren Folgen sind. In den meisten Fällen können solche Schäden allerdings erst ex-post bestimmt werden. Für weitere Informationen siehe Dornbusch (2018, S. 71), Kreß (2019), Petersen (2020).

nach wie vor unklar, wer der Urheber eines Angriffs war, oder anders ausgedrückt, *welche Person* sich *in welcher Funktion* zum Angriffszeitpunkt *hinter der Maschine* [dem Computersystem] verbarg“ (Schulze 2015, S. 47; Harrison Dinniss 2014, S. 145–146). Insofern muss klargestellt werden, gegen wen sich Maßnahmen der aktiven Cyberabwehr richten sollen. Denn ohne eine zweifelsfreie Attribution ist politisches Handeln und auch das Recht auf Gegenmaßnahmen nicht anwendbar und möglich. Je weniger Zeit allerdings für eine zielgenaue Attribution aufgrund von Krisenreaktionen zur Verfügung steht, desto unwahrscheinlicher ist es, dass Attribution gelingt und Gegenmaßnahmen, wie in Artikel 52 der „Draft articles on Responsibility of States for internationally wrongful acts“ beispielsweise dargelegt, vollzogen werden können. Dies hängt auch mit den Effekten von Cyberangriffen zusammen: Nicht jeder Cyberangriff wird sofort als solcher erkannt. Meist ist es nicht unmittelbar ersichtlich, ob es sich bei einem Vorfall oder Krisenfall um einen Unfall, einen Bug oder einen Cyberangriff handelt (Reinhold und Schulze 2017, S. 9). So hielten die iranischen Atomwissenschaftler den Ausfall der Gaszentrifugen durch Überdruck und Überdrehzahl der Rotorgeschwindigkeit in der Urananreicherungsanlage in Natanz lange Zeit für einen Unfall statt für einen Angriff, der durch einen Computerwurm (Stuxnet) herbeigeführt wurde (Langner 2017). Da durch das Völkerrecht legitimierte Gegenmaßnahmen allerdings eine unmittelbare Reaktion erfordern, könnte ein Gegenschlag, der Monate später stattfindet, „als eigenständiger aggressiver Akt und nicht als legitime Selbstverteidigung interpretiert werden“ (Reinhold und Schulze 2017, S. 10). Dies führt unweigerlich zu einem Risiko der Eskalation.

Dieses Risiko der Eskalation wird durch *False-Flag*-Operationen weiter erhöht. Denn wenn Angreifer bewusst falsche Fährten legen, steigt das Risiko, bei aktiven Cybermaßnahmen Unbeteiligte zu treffen (Kuhn 2023). Ein anschauliches Beispiel findet sich im April 2015, als der französische Fernsehsender TV5 Monde Ziel eines Cyberangriffs wurde. Zunächst wurde der Islamische Staat als Angreifer aufgrund der damaligen Terroranschläge in Frankreich identifiziert (Ehrenberg 2015; Zeit Online 2015; Deutschlandfunk 2015), später stellte sich jedoch heraus, dass russische Hacker für den Cyberangriff verantwortlich waren (Frankfurter Allgemeine Zeitung 2015; Süddeutsche Zeitung 2015).

Betrachtet man all diese möglichen Risiken und Folgen, so kann abschließend folgendes festgehalten werden: Aktive Cyberabwehr in Form von digitalen Vergeltungs- oder Gegenangriffen kann aufgrund des völkerrechtlichen Gewaltverbotes, dem Risiko des Sicherheitsdilemmas und aufgrund des im Cyberraum vorherrschenden Attributionsproblems risikoreich sein. Rechtlich sind solche Formen von aktiver Cyberabwehr unter bestimmten Voraussetzungen der Bundeswehr und insbesondere dem Kommando Cyber- und Informationsraum vorbehalten. Wird der Terminus „aktive Cyberabwehr“ allerdings als Verfolgung und Vereitelung von Straftaten verstanden, so sollte eine Mandatserweiterung nicht bei der Bundeswehr, den Nachrichtendiensten oder dem BSI, sondern bei den Strafverfolgungsbehörden angesiedelt werden. Ein möglicher Akteur hierfür könnte das BKA sein, welches auch bereits aktiv in der aktiven Cyberabwehr tätig war. So hat das BKA im Jahr 2021 gemeinsam mit anderen „Strafverfolgungsbehörden aus den Niederlanden, der Ukraine, Litauen, Frankreich sowie England, Kanada und den USA die Infrastruktur der

Schadsoftware Emotet mit Unterstützung von Europol und Eurojust übernommen und zerschlagen“ (BKA 2021).

Funding Open Access funding enabled and organized by Projekt DEAL.

Literatur

Auswärtiges Amt (2022). Rede von Außenministerin Annalena Baerbock auf der Konferenz „Shaping Cyber Security“ in Potsdam. https://www.auswaertiges-amt.de/de/newsroom/cyber-sicherheit/2554640. Zugegriffen: 22. Nov. 2023.

Auswärtiges Amt (2023). Wehrhaft. Resilient. Nachhaltig. Integrierte Sicherheit für Deutschland. Nationale Sicherheitsstrategie. https://www.nationalesicherheitsstrategie.de/Sicherheitsstrategie-DE.pdf. Zugegriffen: 10. Dez. 2023.

Baumgärtner, M., Gebauer, M., Knobbe, M., Rosenbach, M., & Wiedmann-Schmidt, W. (2017, 24. Nov.). So rüstet sich Deutschlands geheime Cyberarmee. Spiegel. https://www.spiegel.de/spiegel/deutschland-ruestet-im-cyberkrieg-auf-a-1179975.html. Zugegriffen: 5. Okt. 2023.

Becker, M. (2019, 16. Okt). Der geheime Krieg im Netz. Deutschlandfunk. https://www.deutschlandfunk.de/aktive-cyber-abwehr-fuer-deutschland-der-geheime-krieg-im-100.html. Zugegriffen: 19. Feb. 2024.

Biselli, A. (2020, 29. Jan.). Hackback im Bundespolizeigesetz: Seehofer wollte den digitalen Gegenangriff starten (Update). Netzpolitik.org. https://netzpolitik.org/2020/hackback-bundespolizei-seehofer-will-den-digitalen-gegenangriff-starten/#netzpolitik-pw. Zugegriffen: 4. Okt. 2023.

BKA (2023a). Cybercrime Bundeslagebild 2022. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2022.pdf?__blob=publicationFile&v=4. Zugegriffen: 3. Okt. 2023.

BKA (2023b). Ermittlungen. https://www.bka.de/DE/UnsereAufgaben/Aufgabenbereiche/Ermittlungen/ermittlungen_node.html. Zugegriffen: 7. Sep. 2023.

BMI (2022b). Pressemitteilung: Bundesinnenministerin stellt ihre Cybersicherheitsagenda vor. https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2022/07/cybersicherheitsagenda.html. Zugegriffen: 5. Sep. 2023.

BMI (2022c, 8. Juni). re:publica 2022. Rede der Bundesministerin des Innern und für Heimat Nancy Faeser. Der resiliente Staat: Die Folgen des Ukraine-Krieges für das digitale Deutschland. https://www.bmi.bund.de/SharedDocs/reden/DE/2022/faeser-20220609-republica.html. Zugegriffen: 23. Nov. 2023.

BMI – Bundesministerium des Innern und für Heimat (2022a). Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat. Ziele und Maßnahmen für die 20. Legislaturperiode. https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.pdf;jsessionid=7688B1AC334003C4445031A1CFDCC6E1.1_cid295?__blob=publicationFile&v=4. Zugegriffen: 19. Okt. 2023.

Brühl, J. (2022, 4. Apr.). Krieg in der Ukraine: Angriff auf „Ka-Sat 9A“. Süddeutsche Zeitung. https://www.sueddeutsche.de/wirtschaft/hack-gegen-satellitennetzwerk-angriff-auf-ka-sat-9a-1.5560370. Zugegriffen: 22. Nov. 2023.

BSI (2022). Die Lage der IT-Sicherheit in Deutschland 2022. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=6. Zugegriffen: 11. Dez. 2023.

BSI (2023a). CERT-Bund. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html. Zugegriffen: 1. Okt. 2023.

BSI (2023b). Die Lage der IT-Sicherheit in Deutschland 2023. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?__blob=publicationFile&v=7. Zugegriffen: 11. Dez. 2023.

BSI (2023c). Unser Leitbild. https://www.bsi.bund.de/DE/Das-BSI/Leitbild/leitbild_node.html. Zugegriffen: 1. Sep. 2023.

BSI – Bundesamt für Sicherheit in der Informationstechnik (2021). Die Lage der IT-Sicherheit in Deutschland 2021. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf;jsessionid=F0664AB63E495A4351D16F72E2E0C75D.internet471?__blob=publicationFile&v=3. Zugegriffen: 13. Sep. 2023.

Bundesamt für Verfassungsschutz (2022). Cyberabwehr, Begriff und Auftrag. https://www.verfassungsschutz.de/DE/themen/cyberabwehr/begriff-und-auftrag/begriff-und-auftrag_artikel.html. Zugegriffen: 26. Nov. 2023.

BKA – Bundeskriminalamt (2021, 27. Jan). Infrastruktur der Emotet-Schadsoftware zerschlagen. Pressemitteilung der Generalstaatsanwaltschaft Frankfurt am Main -ZIT- und des Bundeskriminalamtes. https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html. Zugegriffen: 13. Okt. 2023.

BND – Bundesnachrichtendienst (2021). Cybersicherheit. https://www.bnd.bund.de/DE/Die_Themen/Cybersicherheit/cybersicherheit_node.html. Zugegriffen: 7. Okt. 2023.

Bundesregierung (2021). Mehr Fortschritt wagen – Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit. Koalitionsvertrag 2021 – 2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), BÜNDNIS 90 / DIE GRÜNEN und den Freien Demokraten (FDP). https://www.bundesregierung.de/resource/blob/974430/1990812/93bd8d9b17717c351633635f9d7fba09/2021-12-10-koav2021-data.pdf?download=1. Zugegriffen: 3. Dez. 2023.

Conrad, N., & Werkhäuser, N. (2019). Lizenz zum Hacken: Wie schlägt Deutschland bei Cyberattacken zurück?. Deutsche Welle. https://www.dw.com/de/lizenz-zum-hacken-wie-schl%C3%A4gt-deutschland-bei-cyberattacken-zur%C3%BCck/a-49444484. Zugegriffen: 30. Nov. 2023.

CISA – Cyber Security and Information Security Agency (2022). Russian state-sponsored and criminal cyber threats to critical infrastructure. https://www.cisa.gov/uscert/ncas/alerts/aa22-110a. Zugegriffen: 22. Nov. 2023.

Department of Defense (2018). Cyber Strategy 2018. Summary. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF. Zugegriffen: 22. Nov. 2023.

Deutscher Bundestag (2018). Drucksache 19/5076. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Manuel Höferlin, Stephan Thomae, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP. Hackbacks als aktive digitale Gegenwehr. https://dip21.bundestag.de/dip21/btd/19/054/1905472.pdf. Zugegriffen: 2. Dez. 2023.

Deutscher Bundestag (2019). Drucksache 19/12235. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Alexander Graf Lambsdorff, Grigorios Aggelidis, Renata Alt, weiterer Abgeordneter und der Fraktion der FDP. Digitaler Verteidigungsfall. https://dserver.bundestag.de/btd/19/122/1912235.pdf. Zugegriffen: 15. Nov. 2023.

Deutscher Bundestag (2023). Drucksache 20/5597. Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der CDU/CSU. Verteidigung im Cyberraum – EU-Kooperation und aktive Cyberverteidigung. https://dserver.bundestag.de/btd/20/055/2005597.pdf. Zugegriffen: 8. Dez. 2023.

Deutschlandfunk (2015, 10. Apr.). Cyber-Attacke auf TV5 Monde. Für einen Koffer voller Bargeld. https://www.deutschlandfunk.de/cyber-attacke-auf-tv5-monde-fuer-einen-koffer-voller-bargeld-100.html. Zugegriffen: 4. Nov. 2023.

Diehl, J., & Reinbold, F. (2017, 10. Dez.). Wenn der Staat zum Hacker wird. Spiegel. https://www.spiegel.de/netzwelt/netzpolitik/hackback-wenn-der-staat-zum-hacker-werden-will-a-1179423.html. Zugegriffen: 26. Nov. 2023.

Harrison Dinniss, H. (2014). *Cyber warfare and the laws of war.* Cambridge: Cambridge University Press.

Dornbusch, J. (2018). *Das Kampfführungsrecht im internationalen Cyberkrieg.* Dissertation. Baden-Baden: Nomos.

Ehrenberg, M. (2015, 9. Apr.). Cyberterror. Nach dem Hacker-Angriff bei TV5 Monde: Wie sicher sind ARD & ZDF? Tagesspiegel. https://www.tagesspiegel.de/gesellschaft/medien/nach-dem-hacker-angriff-bei-tv5-monde-wie-sicher-sind-ard-zdf-5779327.html. Zugegriffen: 7. Sep. 2023.

Erxleben, S. (2015). *Agenten zwischen den Fronten. Der Bundesnachrichtendienst zwischen Auftrag, Rechtslage und Historie.* München: Herbert Utz Verlag.

Frankfurter Allgemeine Zeitung (2015, 9. Juni). Cyber-Angriff auf TV5 Monde. Ermittler verfolgen Spur nach Russland. https://www.faz.net/aktuell/politik/ausland/russen-sollen-hinter-cyber-attacke-auf-tv5-monde-stehen-13638777.html. Zugegriffen: 18. Okt. 2023.

Gärtner, T., & Selzer, A. (2023, 15. Aug.). Begriffsverwirrung verhindern: Was Maßnahmen Aktiver Cyberabwehr sind – und was nicht. Tagesspiegel Background. https://background.tagesspiegel.de/cybersecurity/begriffsverwirrung-verhindern-was-massnahmen-aktiver-cyberabwehr-sind-und-was-nicht. Zugegriffen: 9. Dez. 2023.

Greis, F. (2023, 7. Juli). Plattner fordert Gegenwehr bei Cyberangriffen. golem.de. https://www.golem.de/news/neue-bsi-praesidentin-plattner-will-gegenwehr-bei-cyberangriffen-2307-175669.html. Zugegriffen: 9. Dez. 2023.

Heide, D., & Riedel, D. (2019, 6. Juni). Seehofer will digitalen Gegenangriff gegen Hacker. Handelsblatt. https://www.handelsblatt.com/politik/deutschland/it-sicherheit-seehofer-will-digitalen-gegenangriff-gegen-hacker/24429802.html?ticket=ST-2211477-CkPvRB0zCIheFqu2OTaj-ap2. Zugegriffen: 30. Nov. 2023.

Herpig, S. (2019, 24. Apr.). Innenminister schaltet bei IT-Sicherheit schrittweise von Verteidigung auf Angriff. Netzpolitik.org. https://netzpolitik.org/2019/aktive-cyber-abwehr-innenminister-schaltet-bei-it-sicherheit-schrittweise-von-verteidigung-auf-angriff/. Zugegriffen: 5. Nov. 2023.

Herpig, S. (2023, 17. Aug.). Warum das Bundesinnenministerium den Begriff „Hackback" umdefiniert. Tagesspiegel Background. https://background.tagesspiegel.de/cybersecurity/warum-das-bundesinnenministerium-den-begriff-hackback-umdefiniert. Zugegriffen: 4. Dez. 2023.

Kipker, D.-K. (2019, 3. Juni). Hackback in Deutschland: Wer, was, wie und warum? Verfassungsblog. https://verfassungsblog.de/hackback-in-deutschland-wer-was-wie-und-warum/. Zugegriffen: 18. Okt. 2023.

Kipker, D.-K. (2023). Schriftliche Stellungnahme „Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland". Ausschussdrucksache 20(23)116 Deutscher Bundestag, Ausschuss für Digitales. https://www.bundestag.de/resource/blob/929758/9725e00cad76feaa54527f0130050b14/Stellungnahme-Kipker-data.pdf. Zugegriffen: 4. Dez. 2023.

Klaus, J. (2023, 31. März). Wie gefährlich sind Faesers Hacking-Pläne? zdfheute. https://www.zdf.de/nachrichten/digitales/vulkan-files-faeser-hackback-bka-kritik-100.html. Zugegriffen: 13. Sep. 2023.

Knop, D. (2022, 27. Apr.). Cyber-Angriff: Fernüberwachung von Windkraftanlagen lahmgelegt. Heise online. https://www.heise.de/news/Cyber-Angriff-legte-offenbar-Windturbinen-lahm-7066606.html. Zugegriffen: 22. Sep. 2023.

Krempl, S. (2020, 29. Jan.). Hackbacks: Bundespolizei sollte digitalen Gegenschlag führen dürfen. Heise online. https://www.heise.de/newsticker/meldung/Hackbacks-Bundespolizei-soll-digitalen-Gegenschlag-fuehren-duerfen-4648682.html. Zugegriffen: 4. Nov. 2023.

Krempl, S. (2022, 12. Juli). Cybersicherheitsagenda: BKA & Co. sollen Angriffsserver runterfahren können. Heise online. https://www.heise.de/news/Cybersicherheitsagenda-BKA-Co-sollen-Angriffsserver-runterfahren-koennen-7170649.html. Zugegriffen: 5. Nov. 2023.

Kreß, C. (2019). Zur Lage des völkerrechtlichen Gewaltverbots. *Zeitschrift für Außen- und Sicherheitspolitik, 12*(4), 453–476.

Krieger, W. (2021). *Die deutschen Geheimdienste. Vom Wiener Kongress bis zum Cyber War.* München: C.H. Beck.

Kuhn, T. (2023). Smarte Schläge statt plumper Hackbacks. WiWo. https://www.wiwo.de/technologie/digitale-welt/cybersecurity-smarte-schlaege-statt-plumper-hackbacks/29147622.html. Zugegriffen: 10. Dez. 2023.

Langner, R. (2017). Stuxnet und die Folgen. Was die Schöpfer von Stuxnet erreichen wollten, was sie erreicht haben, und was das für uns alle bedeutet. https://www.langner.com/wp-content/uploads/2017/08/Stuxnet-und-die-Folgen.pdf. Zugegriffen: 15. Nov. 2023.

Mäder, L. (2022, 21. März). Ein Cyberangriff legte zu Beginn der Invasion die Kommunikation der Ukraine lahm. Er verursacht Kollateralschäden in ganz Europa. Neue Züricher Zeitung. https://www.nzz.ch/technologie/ein-cyberangriff-legte-zu-beginn-der-invasion-die-kommunikation-der-ukraine-lahmer-verursacht-kollateralschaeden-in-ganz-europa-ld.1675044. Zugegriffen: 22. Nov. 2023.

Mascolo, G. (2017, 19. Apr.). Deutschland plant Cyber-Gegenschläge. Süddeutsche Zeitung. https://www.sueddeutsche.de/digital/hacking-deutschland-plant-cyber-gegenschlaege-1.3469443. Zugegriffen: 2. Dez. 2023.

Mascolo, G., & Steinke, R. (2018, 5. Sep.). BND könnte Lizenz zum „Hack back" bekommen. Süddeutsche Zeitung. https://www.sueddeutsche.de/digital/cybersicherheit-bnd-koennte-lizenz-zum-hack-back-bekommen-1.4115365. Zugegriffen: 24. Nov. 2023.

Meister, A., & Biselli, A. (2019, 3. Apr.). IT-Sicherheitsgesetz 2.0. Wir veröffentlichen den Entwurf, der das BSI zur Hackerbehörde machen soll. Netzpolitik.org. https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/. Zugegriffen: 21. Nov. 2023.

Nakashima, E. (2012, 27. Feb.). When is a cyberattack a matter of defense? The Washington Post. https://www.washingtonpost.com/blogs/checkpoint-washington/post/active-defense-at-center-of-debate-on-cyberattacks/2012/02/27/gIQACFoKeR_blog.html?-utm_term=.f299848fff64. Zugegriffen: 21. Nov. 2023.

NDR (2022, 4. Apr.). Hackerangriff bei Windturbinenhersteller Nordex. https://www.ndr.de/nachrichten/mecklenburg-vorpommern/Hackerangriff-bei-Windturbinenhersteller-Nordex,nordex204.html. Zugegriffen: 22. Nov. 2023.

Petersen, L. A. (2020). Cyberangriffe – Definition, Regulierung, Pönalisierung. *Göttinger Rechtszeitschrift, 3*(4), 25–36.

Quadbeck, E., & Decker, M. (2022, 2. Apr.). Innenministerin Faeser zu Cybersicherheit: „Wir wollen die Abwehr stärken". RND. https://www.rnd.de/politik/abwehr-von-cyberattacken-zentrale-rolle-des-bundes-wichtig-GDIKMPPEQVEQBINNLUWMFI2VME.html. Zugegriffen: 22. Nov. 2023.

Rath, C. (2023, 3. Apr.). Faeser für aktive Cyberabwehr im Grundgesetz. RND. https://www.rnd.de/politik/hackbacks-durch-bka-nancy-faeser-will-aktive-cyberabwehr-im-grundgesetz-M53ZE4MU3VEZBB3VEVQZSEF44A.html. Zugegriffen: 1. Dez. 2023.

Reinhold, T., & Schulze, M. (2017). Digitale Gegenangriffe – Eine Analyse der technischen und politischen Implikationen von „hack backs". Forschungsgruppe Sicherheitspolitik, Stiftung Wissenschaft und Politik. https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/AP_Schulze_Hackback_08_2017.pdf. Zugegriffen: 24. Nov. 2023.

Reuters (2017, 5. Okt.). Verfassungsschutz will Befugnis für Cyber-Gegenangriffe. https://www.reuters.com/article/deutschland-verfassungsschutz-cyberangri-idDEKBN1CA1IH. Zugegriffen: 26. Nov. 2023.

Riemann, M. (2020). *Der Krieg im 20. und 21. Jahrhundert. Entwicklungen und Strategien.* Stuttgart: W. Kohlhammer.

Rundfeldt, J. (2023, 31. Jan.). Kommentar: Aktive Abwehr defensiver Offensive ist Cybersicherheitsfantasie. Heise online. https://www.heise.de/meinung/Kommentar-Aktive-Abwehr-defensiver-Offensive-ist-Cybersicherheitsfantasie-7474597.html. Zugegriffen: 10. Dez. 2023.

Sabbagh, D. (2020, 25. Sep.). Britain has offensive cyberwar capability, top general admits. The Guardian. https://www.theguardian.com/technology/2020/sep/25/britain-has-offensive-cyberwar-capability-top-general-admits. Zugegriffen: 23. Nov. 2023.

Schulze, S.-H. (2015). *Cyber-„War" – Testfall der Staatenverantwortlichkeit.* Dissertation, Universität Trier. Tübingen: Mohr Siebeck.

Sehl, M. (2019, 30. Okt.). Das Grundgesetz ändern für den Hack-back? Legal Tribune Online. https://www.lto.de/recht/nachrichten/n/hackback-cyber-gegen-angriff-abwehr-bnd-bfv-mad-geheimdienste-bundeswehr/. Zugegriffen: 9. Dez. 2023.

Shulman, H., & Waidner, M. (2023). Aktive Cyberabwehr. Klassifikation und Einschätzung der technischen Möglichkeiten zur aktiven Abwehr von Angriffen. *Datenschutz und Datensicherheit, 47*(8), 497–502.

Spartanat (2020, 29. Jun.). CYBERWAR (1): „Der digitale Verteidigungsfall gelingt nur bedingt". Spartanat. https://www.spartanat.com/2020/06/cyberwar-1-der-digitale-verteidigungsfall-gelingt-nur-bedingt/. Zugegriffen: 10. Okt. 2023.

Spiegel (2017, 10. Jan). Verfassungsschutz will Cybergegenangriffe starten. Spiegel. https://www.spiegel.de/netzwelt/netzpolitik/bundesamt-fuer-verfassungsschutz-plant-cyber-gegenangriffe-a-1129273.html. Zugegriffen: 26. Nov. 2023.

Stiftung Neue Verantwortung (2018, 24. Juli). Aktive Cyber-Abwehr / Hackback. Impulse. https://www.stiftung-nv.de/de/publikation/hackback-ist-nicht-gleich-hackback#collapse-newsletter_banner_bottom. Zugegriffen: 23. Nov. 2023.

Süddeutsche Zeitung (2015, 10. Juni). Ermittlungen gegen russische Hacker wegen Angriff auf TV 5 Monde. Süddeutsche Zeitung https://www.sueddeutsche.de/digital/cyberkriminalitaet-ermittlungen-gegen-russische-hacker-wegen-angriff-auf-tv-5-monde-1.2513970. Zugegriffen: 11. Okt. 2023.
Tagesschau (2019). Seehofer will digitalen Gegenschlag ermöglichen. https://www.youtube.com/watch?v=ULAKnjIX-yY. Zugegriffen: 15. Feb. 2024.
Tagesschau (2022a). Bundesregierung bestätigt Hacker-Angriffe. https://www.tagesschau.de/inland/cyberattacke-bundesregierung-ddos-101.html. Zugegriffen: 17. Feb. 2024.
Tagesschau (2022b). Zehntausende in Kiew weiter ohne Strom. https://www.tagesschau.de/ausland/ukraine-kiew-strom-101.html. Zugegriffen: 19. Feb. 2024.
Tanriverdi, H. (2019). Die Hackback-Pläne der Bundesregierung. Tagesschau. https://cyber-peace.org/wp-content/uploads/2019/05/Internes-Papier_-Die-Hackback-Pl%C3%A4ne-der-Bundesregierung-_-tagesschau.de_.pdf. Zugegriffen: 19. Feb. 2024.
Tremmel, M. (2022, 25. Apr.). BSI-Präsident spricht sich für Hackbacks aus. golem.de. https://www.golem.de/news/it-sicherheit-bsi-praesident-spricht-sich-fuer-hackbacks-aus-2204-164827.html. Zugegriffen: 9. Dez. 2023.
Wissenschaftliche Dienste des Deutschen Bundestages (2018). „Hackbacks“ im Ausland sind verfassungswidrig. Netzpolitik.org. https://netzpolitik.org/2018/wissenschaftliche-dienste-hackbacks-im-ausland-sind-verfassungswidrig/. Zugegriffen: 25. Nov. 2023
Wolf, T. (2018). *Die Entstehung des BND. Aufbau, Finanzierung, Kontrolle.* Berlin: Ch. Links Verlag.
Zeit Online (2015, 9. Apr.). IS-Hacker legen französischen TV-Sender lahm. Zeit Online. https://www.zeit.de/digital/2015-04/cyberangriff-is-sender. Zugegriffen: 11. Dez. 2023.