Kerstin Zettl-Schabath und Sebastian Harnisch

Eine »operative digitale Zeitenwende«: Cybersicherheit im Rahmen der Nationalen Sicherheitsstrategie Deutschlands

Zusammenfassung: In der Cyber-Außen- und Sicherheitspolitik ist die Nationale Sicherheitsstrategie in eine Vielzahl nationaler und internationaler Strategiedokumente eingebettet. Seit Anfang der 2000er-Jahre versuchen die Bundesrepublik und ihre Verbündeten sich durch mehr Kooperation vor einer wachsenden Anzahl krimineller, bösartiger ökonomisch-, politisch- und militärisch-relevanter Cybervorfälle zu schützen. Der Beitrag untersucht zunächst, welche Ziele, Mittel und Instrumente die Nationale Sicherheitsstrategie aus diesen Dokumenten aufnimmt und weiterentwickelt. Sodann werden die internationale Cyberdiplomatie der Bundesregierung, ihr Attributionsverhalten sowie Maßnahmen zur »aktiven Cyberabwehr« daraufhin analysiert, ob und inwiefern die Ziele der Sicherheitsstrategie bereits umgesetzt worden sind. Der Beitrag kommt zu dem Ergebnis, dass die Umsetzung der Sicherheitsstrategie erkennbare Lücken aufweist. Wir empfehlen zum einen die verstärkte Nutzung europäischer Instrumente, gemeinsame Attribuierungen von Angriffen sowie die umfassendere Umsetzung von EU-Regulierung, insbesondere NIS-2. Zum anderen muss die deutsche Cyber-Außen- und Sicherheitspolitik institutionell gestärkt werden, etwa durch eine verfassungsrechtliche Befähigung des Bundeskriminalamtes (BKA) und eine verbesserte Ressortabstimmung bei der Umsetzung des KRITIS-Dachgesetzes.

Schlüsselwörter: Cybersicherheit, Attribution, Abschreckung, Resilienz, Normen, Sanktionen, Cyberkriminalität, Proxies, Cyberabwehr

Kerstin Zettl-Schabath and Sebastian Harnisch, A Digital »Zeitenwende«: Small and Operational. Cybersecurity in Germany`s National Security Strategy

Summary: In cyber foreign and security policy, the National Security Strategy is embedded in a large number of national and international strategy documents that have sought to protect Germany and its allies from a growing number of criminal malicious economic, political and militarily relevant cyber incidents since the early 2000s. The article first examines which goals, means and instruments the national security strategy takes from these documents and develops them further. It then analyses the German government's international cyber diplomacy, its attribution behavior and measures for ‘active cyber defence’ and whether and as to how far the explicit goals of the Security Strategy have been achieved. By naming specific instruments, in particular the increased attribution of attacks and constitutional authorization of the Federal Criminal Police Office (BKA) as well as the comprehensive implementation of EU regulation (NIS-2), there is justified hope that the Federal Republic's protection, which has been patchy to date, can be gradually

improved. However, this will require more efficient ministerial coordination, as the sluggish implementation of the KRITIS umbrella law shows, as well as more active involvement of business and civil society in the short and medium term, so that they can also take better responsibility for their own protection.

Keywords: cybersecurity, attribution, deterrence, resilience, norms, sanctions, cybercrime, proxies

Kerstin Zettl-Schabath, Dr., ist wissenschaftliche Mitarbeiterin an der Universität Heidelberg und forscht im Rahmen des Projekts »European Repository of Cyber Incidents« (EuRepoC) zu Cyberkonflikten.

Korrespondenzanschrift: kerstin.zettl@ipw.uni-heidelberg.de

Sebastian Harnisch, Prof. Dr., ist Professor für Internationale Beziehungen und Außenpolitikforschung an der Universität Heidelberg und lehrt und forscht unter anderem zu Cybersicherheit, Internet Governance und Netzpolitik.

Korrespondenzanschrift: sebastian.harnisch@ipw.uni-heidelberg.de

1 Einleitung

Die Nationale Sicherheitsstrategie von 2023 ist keine »strategische Zeitenwende« im digitalen Raum, denn die Bundesrepublik wird kriminelle und staatlich-unterstützte Cyberangriffe weiterhin gemeinsam mit internationalen Verbündeten sowie Wirtschaft und Gesellschaft abwehren. Sie kann aber als »operative Zeitenwende« betrachtet werden: So haben bundesdeutsche Akteure die Ukraine seit dem russischen Angriffskrieg aktiv befähigt, ihre digitale Selbstverteidigung weiter zu verbessern. Sodann haben das Bundeskriminalamt (BKA), das Bundesamt für Sicherheit in der Informationstechnik (BSI) als auch das Auswärtige Amt und weitere Institutionen aktiver von öffentlichen Attributionen, das heißt der Zuweisung von Verantwortlichkeiten für Cyberoperationen, Gebrauch gemacht. Und schließlich sind die rechtlichen Grundlagen für eine erweiterte Gefahrenabwehr durch das BKA von der scheidenden Bundesregierung noch auf den Weg gebracht worden. Daneben bleibt der Gestaltungsanspruch der Strategie in der Cybersicherheitspolitik bemerkenswert schwach: Auf europäischer Ebene wird die *Cyber Diplomacy Toolbox (CDT)* als gemeinsamer *EU*-Instrumentenkasten nicht erwähnt und im deutschen Attributionsverhalten wird die Normbildung auf globaler Ebene vernachlässigt.

Mit der Nationalen Sicherheitsstrategie wurde erstmals ein Dokument vorgelegt, das im Bereich der Cyber-Außen- und Sicherheitspolitik und weiteren Politikfeldern Strategiedokumente wie das Weißbuch zur Sicherheitspolitik und das Weißbuch Multilatera-

lismus[1] ergänzt und bündelt. Den beteiligten Ministerien kam dabei der Auftrag zu, die bisherigen Cyberstrategien von 2011, 2016, und 2021 weiterzuentwickeln und die Rolle Deutschlands als Cyberakteur gegenüber der analogen und digitalen Umwelt zu definieren. Die Strategie sollte konkrete Ziele benennen sowie Strategien und Instrumente zu deren Umsetzung festlegen sowie notwendige rechtliche Anpassungen identifizieren.[2]

All dies ist vor dem Hintergrund eines sicherheitspolitischen Umfelds zu sehen, das sich angesichts des russischen Angriffskriegs gegen die Ukraine und zunehmender Übergriffe Chinas gegenüber Taiwan und im Südchinesischen Meer zusehends verschlechterte. In der Cybersicherheitspolitik zeigte sich dies etwa anhand vermehrter Angriffe russischer Cyberakteure gegen die Ukraine und ihre Unterstützerstaaten, adressiert unter anderem durch den Aufbau der *NATO Virtual Cyber Incident Support Capability* (VCISC) und des *EU Cybersecurity Emergency Mechanism* 2023.[3]

Der Beitrag untersucht zunächst, welche Ziele und Strategien die Nationale Sicherheitsstrategie aus früheren Strategiedokumenten übernommen und wie sich die Veränderung des sicherheitspolitischen Umfeldes auf diese ausgewirkt hat. Im dritten Abschnitt werden die Kernelemente der Strategie mit Bezug zum Thema Cybersicherheit vorgestellt und im Lichte der Cyberkonfliktforschung diskutiert. Abschnitt 4 analysiert Deutschlands bisherige Cybersicherheitspolitik, auf diplomatischer und operativer Ebene. Hierbei stehen die Formalisierung des nationalen Attributionsprozesses, die Nutzung der *CDT*, als auch operative Strafverfolgungsmaßnahmen gegen *Ransomware*-Gruppierungen im Rahmen einer aktiven Cyberabwehr im Fokus. Abschließend werden die Befunde erörtert und konkrete Handlungsempfehlungen ausgesprochen, die mehr europäische Zusammenarbeit sowie eine Stärkung des innerstaatlichen Politikprozesses vorsehen.

2 Deutschlands Cybersicherheitsstrategien vor 2023: Was bisher geschah

In diesem Abschnitt werden die bislang in Deutschland verabschiedeten Cybersicherheitsstrategien behandelt, die cyberdomänenspezifisch der nationalen Sicherheitsstrategie 2023 den Weg ebneten. Neben stetig steigendem institutionellem Aufwuchs auf nationaler Ebene stehen zudem die EU und NATO als Koordinationsrahmen deutscher Cybersicherheitspolitik im Fokus.

Die Sicherheitsstrategie von 2023 greift die wichtigsten Elemente der bisherigen Cyberstrategien auf und entwickelt diese erkennbar fort. Während die Bekämpfung von Computerkriminalität und der Schutz kritischer Infrastrukturen bereits in den 1980er- und 1990er-Jahren Aufmerksamkeit erlangten, führte die Bundesregierung, nach der

1 Bundesministerium der Verteidigung, *Weißbuch 2016. Zur Sicherheitspolitik und zur Zukunft der Bundeswehr* 2016; Auswärtiges Amt, *Weißbuch Multilateralismus der Bundesregierung – Gemeinsam für die Menschen. Drucksache 19/30294* 2021.

2 Münchner Sicherheitskonferenz (Hg.), *Zeitenwende | Wendezeiten – Sonderausgabe des MSR zur deutschen Außen- und Sicherheitspolitik | Münchner Sicherheitskonferenz* 2020, S. 151ff.

3 Eugenia Lostri, *What Will Mechanisms for Cybersecurity Aid Look Like?,* https://www.lawfaremedia.org/article/what-will-mechanisms-for-cybersecurity-aid-look-like, (Zugriff am 27.08.2024).

Gründung des BSI 1991, im Jahr 2011 eine erste Cybersicherheitsstrategie für Deutschland ein. Diese Strategie reagierte, ebenso wie Strategiedokumente in anderen westlichen (*EU*-)Staaten (u.a. Großbritannien, Frankreich, Tschechien), auf die rasche Zunahme bösartiger Cyberangriffe (Estland 2007, Georgien 2008) sowie die Kompromittierung von industrieller Steuerungssoftware im Rahmen der *Stuxnet*-Attacke, welche die wachsende Verwundbarkeit kritischer Infrastrukturen offenlegte.[4] Zentrales Ziel war die Etablierung eines grundlegenden Schutzniveaus für die vernetzten Informationsstrukturen auf deutschem Territorium bei gleichzeitiger Wahrung der umfassenden wirtschaftlichen und gesellschaftlichen Nutzung des Cyberraums. Im Vergleich zu den genannten Partnerstaaten verwies die Cybersicherheitsstrategie aber bereits auf die 2010 erschienene *Digital Agenda for Europe* der EU; sie unterließ es aber noch Cybersicherheit als potenzielle Bedrohung der nationalen Sicherheit zu adressieren.[5]

Die Cybersicherheitsstrategien von 2016 und 2021 differenzierten stärker zwischen kriminellen, staatlichen und hybriden Bedrohungen und führten zu einem raschen Ausbau der institutionellen Cybersicherheitsarchitektur. Zu den neuen Institutionen gehörten zuvorderst das BSI als *National Cyber Defense Authority* und das Nationale Cyber-Abwehrzentrum (Cyber-AZ). Zudem wurde ein nationaler Cyber-Sicherheitsrat ins Leben gerufen, um Ministerien, Bundesländer und Wirtschaftsvertreter zusammenzubringen. In der Cybersicherheitsforschung ist diese Institutionenzunahme und deren wachsende Kompetenzüberschneidung weitgehend kritisch rezipiert worden, indem etwa auf die (technische) Engführung des Cybersicherheitsbegriffs, die Fokussierung des BSI auf technische Grundlagen des Cyberschutzes und die stärkere (verantwortliche) Einbindung der Betreiber von kritischer Infrastruktur hingewiesen wurde.[6]

Die Verabschiedung der dritten Cybersicherheitsstrategie im September 2021 sorgte erstmalig für erheblichen zivilgesellschaftlichen Widerstand, insbesondere wegen der geplanten Ausweitung staatlicher Überwachungsbefugnisse. In einem offenen Brief forderten zahlreiche Unterzeichner Änderungen und kritisierten die Strategie als »Vertrag zu Lasten Dritter«, da sie unter anderem kurz vor der anstehenden Bundestags-

4 Eric Luiijf / Kim Besseling / Patrick de Graaf, »Nineteen national cyber security strategies« in: *International Journal of Critical Infrastructures*, Nr. 9 (2013); Tillmann Schulze, *Bedingt abwehrbereit. Schutz kritischer Informations-Infrastrukturen in Deutschland und den USA,* Wiesbaden 2007; Stefan Steiger, *Cybersicherheit in Innen- und Außenpolitik: Deutsche und britische Policies im Vergleich. Deutsche und britische Policies im Vergleich,* Bielefeld 2022, S. 100ff.

5 Luiijf / Besseling / Graaf, Nineteen national cyber security strategies, aaO. (FN 4).

6 Die Stiftung Neue Verantwortung veröffentlicht regelmäßig grafische Aufarbeitungen der institutionellen Verflechtungen auf nationaler und internationaler Ebene, vgl. Sven Herpig / Frederic Dutke, *Deutschlands staatliche Cybersicherheitsarchitektur* 2023; Eric Luiijf / Kim Besseling / Patrick de Graaf, »Nineteen national cyber security strategies« in: *International Journal of Critical Infrastructures*, Nr. 9 (2013); Dennis Kipker, *Stellungnahme Cybersicherheit Digitalausschuss,* https://www.bundestag.de/resource/blob/929758/9725e00cad76feaa54527f0130050b14/Stellungnahme-Kipker.pdf, (Zugriff am 28.08.2024); Dennis-Kenji Kipker / Sebastian Mayr, »Zur Unabhängigkeit des BSI« in: *Datenschutz und Datensicherheit – DuD* 47, Nr. 12 (2023), S. 790–795.

wahl verabschiedet werden würde.[7] Besonders beanstandet wurden im Rahmen des Konzepts der »aktiven Cyberabwehr« die erweiterten Strafverfolgungsmaßnahmen bei Computerdelikten, die Stärkung der Zentralstellenaufgabe des BKA, operative Lösungen für den Zugriff auf verschlüsselte Kommunikation, der Ausbau der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) sowie die Ausweitung der nachrichtendienstlichen Befugnisse. Besonders umstritten war der geplante Einbau von »Hintertüren« in verschlüsselte Kommunikation, da diese Sicherheitslücken auch von ausländischen Akteuren für Angriffe genutzt werden könnten. Konkret verdeutlichte die weltweite *WannaCry*-Kampagne nordkoreanischer Hacker (2017) diese Gefahr: Die Schadsoftware nutzte einen von der *NSA* entwickelten und später gestohlenen *Exploit* (Befehlsfolge zur Ausnutzung von Sicherheitslücken, in diesem Fall mit dem Namen *Eternalblue),* der auch in (späteren) russischen und chinesischen Cyberoperationen wiederverwendet wurde.[8] Kritiker argumentierten, dass selbst Länder mit umfassenden Cyberfähigkeiten, wie die *USA*, ihre Hintertüren nicht ausreichend schützen können, und somit auch nicht deutsche Sicherheitsbehörden.[9]

Die Enthüllungen von Edward Snowden über die *NSA*-Überwachungsprogramme im Jahr 2013 hatten die deutsche Cybersicherheitsdebatte noch auf die Zielkonflikte zwischen persönlicher Freiheit und nationaler Sicherheit fokussiert. Im Vergleich arbeitete sich der deutsche Diskurs über die Cybersicherheitsstrategie 2021 dann stärker an der Frage ab, ob Cybersicherheit primär mittels institutioneller Reformen oder durch technische Lösungen erlangt werden könne. Ein Zielkonflikt, der zwei Jahre später im Rahmen der Nationalen Sicherheitsstrategie wieder aufgegriffen wurde.

Die Formulierung und Umsetzung der Cyber-Sicherheits-, Außen- und Verteidigungspolitik obliegt prinzipiell den Mitgliedstaaten internationaler Organisationen. Seit Anfang der 2000er koordinieren diese aber zunehmend ihre Politiken, sodass nationale Strategien durch multilaterale Institutionen zunehmend geformt und in diese eingebettet sind.[10]

In der *EU* kamen die Mitgliedstaaten und die Kommission erstmals 2002 überein, mit Vertretern der IT-Industrie Informationssicherheit zu stärken. 2004 wurde die *European Network and Information Security Agency* (*ENISA*) gegründet, welche heute als *European Union Agency for Cybersecurity* fungiert. Nach zahlreichen Angriffen veröffentlichte die Hohe Repräsentantin 2013 die erste *EU-Cybersecurity*-Strategie »An Open, Safe and Secure Cyberspace«, die infolge des Bundestagshacks 2015 zur ersten Richtlinie

7 O. A., »Offener Brief an die Deutsche Bundesregierung« (2021), https://www.interface-eu.org/storage/archive/files/offener_brief_-_cybersicherheitsstrategie2021.pdf, (Zugriff am 13.08.2024).

8 Gordon Corera, *Cyber-attack: US and UK blame North Korea for WannaCry,* https://www.bbc.com/news/world-us-canada-42407488, (Zugriff am 06.10.2021).

9 Annegret Bendiek / Matthias Schulze, *Attribution als Herausforderung für EU-Cybersanktionen* 2021, S. 20.

10 Darius Štitilis / Paulius Pakutinskas / Inga Malinauskaitė, »EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis« in: *Security Journal* 30, Nr. 4 (2017), https://link.springer.com/article/10.1057/s41284-016-0083-9, S. 1151–1168.

zur Netzwerk- und Informationssicherheit (NIS-1) führte.[11] Seither hat die EU eine Vielzahl legislativer und operativer Initiativen gestartet, darunter die erweiterte Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2), die Richtlinie zur Resilienz kritischer Einrichtungen (*CER 2023*), die Richtlinie zur digitalen operativen Resilienz von Finanzinstitutionen (*DORA, 2023*), der *Cybersecurity Act* (2019) und das EU-Gesetz zur Cyberfähigkeitsakademie (2023).[12] Für diesen Abschnitt ist besonders die NIS-2, als zweite EU-Richtlinie zur Netz- und Informationssicherheit von Bedeutung. Sie wurde im Amtsblatt der Europäischen Union L333 veröffentlicht. Die Mitgliedstaaten müssten die Richtlinie bis Oktober 2024 in nationales Recht umsetzen, jedoch hinken viele Staaten, so auch Deutschland, diesem Zeitplan weit hinterher. Die aktuelle NIS-2-Richtlinie stellt eine Weiterentwicklung der (ersten) NIS-Richtlinie aus dem Jahr 2016 dar. In der *EU*-Cybersicherheitsstrategie von 2020 verpflichteten sich die Union und ihre Mitgliedstaaten zudem, ihre operativen Fähigkeiten, Krisenreaktionsteams und die Zusammenarbeit mit internationalen Partnern und gesellschaftlichen Akteuren zu verbessern. Dazu baute die EU unter anderem eine *Joint Cyber Unit* (2021–24) und ein Zentrum für die Analyse hybrider Bedrohungen mit der *NATO* auf (2017).[13]

Nach den Cyberangriffen auf Estland (2007) formulierten die *NATO* und ihre Mitgliedstaaten 2008 zunächst eine »Politik zur Cyberverteidigung«, die sodann 2014 auf dem Gipfel in Wales revidiert wurde. Cyberangriffe, die in Ausmaß und Wirkung kinetischen Angriffen gleichen, können danach den Bündnisfall auslösen.[14] In Warschau (2016) verpflichteten sich die Mitgliedstaaten durch einen *Cyber Defense Pledge,* ihre Abwehrfähigkeiten auszubauen und mithilfe von »best practices« den Schutz der Truppen und des Bündnisterritoriums zu stärken. Auf den *NATO*-Gipfeln von Brüssel (2021) und Vilnius (2023) wurden umfassende Cyberverteidigungspolitiken beschlossen, welche die Fähigkeiten zur Abschreckung, Verteidigung und Gegenwehr stärkten und eine gemeinsame Lagebewertung hervorhoben. Zusätzlich einigten sich die Mitglieder auf eine *Virtual Cyber Incident Support Capability* (VCISC) und eine *NATO Cyber Defence Conference* (2023) in Berlin. Ein *NATO Integrated Cyber Defense Center (NiCC)* wurde beim *Supreme Headquarters Allied Powers Europe* (SHAPE) in Mons eingerichtet, um Schwachstellen in der Verteidigungsfähigkeit aufzudecken.[15]

Vor diesem Hintergrund lässt sich festhalten, dass die Bundesrepublik wesentliche Elemente der Strategieentwicklung von *NATO* und *EU* mitgestaltet und teilweise auch selbst initiiert hat. Dies betrifft die Anwendbarkeit des Völkerrechts im Cyberraum, das Recht auf Selbstverteidigung nach einem schweren Cyberangriff, den Ausbau der eigenen

11 Bendiek / Schulze, Attribution als Herausforderung für EU-Cybersanktionen, aaO. (FN 9).

12 Christina Rupp, *Navigating the EU Cybersecurity Policy Ecosystem,* https://www.stiftung-nv.de/publications/navigating-the-eu-cybersecurity-policy-ecosystem, (Zugriff am 28.08.2024); André Barrinha / G. Christou, »Speaking sovereignty: the EU in the cyber domain« in: *European Security* 31, Nr. 3 (2022), S. 356–376.

13 Annegret Bendiek / Jakob Bund, »Hardening Norms and Networks: Europe's Cyber Defence Posture« in: *Intereconomics* 59, Nr. 4 (2024), S. 198–203.

14 NATO, *The Secretary General's Annual Report 2014, 30-Jan.-2015,* https://www.nato.int/cps/en/natohq/opinions_116854.htm, (Zugriff am 28.08.2024).

15 Suzanne Spaulding / Mark Montgomery, *NATO and Cyber: Outrunning the Bear,* https://www.csis.org/analysis/nato-and-cyber-outrunning-bear, (Zugriff am 28.08.2024).

Lagebild- und Abwehrfähigkeiten sowie die engere Verzahnung staatlicher Einheiten mit privatwirtschaftlichen Fähigkeiten. Die operative Erkennung und Abwehr in den eigenen Systemen werden dabei priorisiert. Erhebliche Schwächen zeigt die Bundesrepublik allerdings in der Umsetzung internationaler Regelwerke, insbesondere der NIS-2-Richtlinie für den Schutz kritischer Infrastruktur, weil bei der nationalen Umsetzung zahlreiche Ausnahmetatbestände zugelassen wurden (siehe Abschnitt 3.1).

3 Cyber in der Nationalen Sicherheitsstrategie

Der »integrierte Sicherheitsbegriff« der Sicherheitsstrategie betont zunächst den Schutz der physischen Integrität öffentlicher Netzinfrastrukturen und Systeme sowie privatwirtschaftlicher Unternehmen und Bürger. Weiterhin fordert die Strategie den Schutz der Freiheit zur unabhängigen Entscheidung über politische Ziele ohne Zwang, etwa durch Sabotage, Erpressung oder hybride Bedrohungen, und bekräftigt die Bedeutung der Abstimmung mit Partnern und multilateralen Institutionen. Schließlich hebt sie den Schutz der natürlichen Lebensgrundlagen, insbesondere den Klimaschutz, hervor, mit besonderem Fokus auf marginalisierte Gruppen, wie Frauen und Kinder.[16]

Vor der Veröffentlichung standen Expertenanhörungen im Fokus, welche die veränderte internationale Lage, vor allem den russischen Angriffskrieg auf die Ukraine, die zunehmende EU-Regulierung des Cyberraums und die veränderten Angriffsmethoden von staatlichen und nichtstaatlichen Akteuren thematisierten.[17] Im Digitalausschuss des Bundestags wurden Ende Januar 2023 Strategien zur Stärkung der Cybersicherheitsarchitektur in Deutschland erörtert.[18] Diese umfassten primär innerstaatliche Maßnahmen, wie die Stärkung des BSI, verbesserte Kontrollrechte und Prozessoptimierungen sowie die Zusammenarbeit mit Unternehmen und Bürgern. Ein Vorschlag betraf die Einberufung einer Expertenkommission zur Reform der Sicherheitsarchitektur. Viele dieser Vorschläge basierten auf der 2022 vom Bundesministerium des Innern und für Heimat (BMI) vorgestellten Cybersicherheitsagenda für die 20. Legislaturperiode, die unter anderem die Weiterentwicklung der Cyberfähigkeiten des Bundesamtes für Verfassungsschutz (BfV) und den Ausbau der ZITiS zur Stärkung der digitalen Ermittlungswerkzeuge für Sicherheitsbehörden vorsah.[19]

16 Bundesregierung, *Nationale Sicherheitsstrategie: Wehrhaft. Resilient. Nachhaltig. Integrierte Sicherheit für Deutschland,* https://www.bmvg.de/resource/blob/5636374/38287252c5442b786ac5d0036ebb237b/nationale-sicherheitsstrategie-data.pdf, (Zugriff am 30.11.2023), S. 6f.

17 Siehe in diesem Band: Thomas Dörfler / Holger Janusch, »Einleitung: Die Nationale Sicherheitsstrategie Deutschlands, ihre Entstehung und Funktionen« in: *Zeitschrift für Politik* 72, Sonderband (2025).

18 Deutscher Bundestag, *Anhörung zur Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland,* https://www.bundestag.de/ausschuesse/a23_digitales/Anhoerungen/928388-928388, (Zugriff am 28.08.2024).

19 Bundesministerium des Innern und für Heimat, *Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat,* https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.pdf?__blob=publicationFile&v=5, (Zugriff am 28.08.2024).

3.1 Stärkung nationaler Cyberabwehrfähigkeiten, jedoch lückenhafte europäische Einbettung

Die Sicherheitsstrategie beschreibt Deutschland als Gemeinwesen, das digitale Netze und Technologien für gesellschaftliche, wirtschaftliche und politische Zwecke nutzt, aber zunehmend Bedrohungen vonseiten staatlicher und nicht-staatlicher Akteure ausgesetzt ist.[20] Im Zentrum der Bedrohungsanalyse stehen öffentliche Infrastrukturen und *Ransomware*-Angriffe gegen Unternehmen und Verwaltungen, während die Risiken durch digitale Lieferketten, Drittparteien und Clouddienste nicht explizit thematisiert werden. Diese Risiken hätten eine differenziertere Analyse nahegelegt, da den Vorteilen ihrer Nutzung, auch erhebliche Nachteile, wie eine erhöhte Anfälligkeit aufgrund erweiterter Zugriffsmöglichkeiten gegenüberstehen. Auffällig ist ferner, dass die Strategie undifferenziert von wachsenden Bedrohungen durch »Kriminalität, Terrorismus, Spionage und Sabotage« spricht, ohne deren unterschiedliche Prävalenz in Deutschland und der EU zu berücksichtigen. Eine mögliche Priorisierung der Maßnahmen anhand der evidenzbasierten Cybersicherheitsforschung wird nicht vorgenommen. In Anbetracht der stetigen Warnungen vor böswilligen Aktivitäten in IT-Sicherheitssystemen und angesichts knapper menschlicher, zeitlicher und finanzieller Ressourcen wäre dies jedoch zwingend notwendig. Hierfür hätte zunächst eine Risikoeinschätzung der unterschiedlichen Cyberoperationstypen vorgenommen werden müssen, d.h. konkret die Eintrittswahrscheinlichkeit muss in Bezug zum vermuteten Schaden modelliert werden. Der Fokus auf technische Vorfallstypen (Spionage, *DDoS, Wiper, Hack-and-Leak, Ransomware*) im Gegensatz zur generischen Differenzierung zwischen »Kriminalität, Terrorismus, Spionage und Sabotage« wäre hierbei zielführender gewesen, da laut Forschung nicht nur Kriminelle erpresserische Operationen wie *Ransomware* vornehmen und umgekehrt nicht nur staatlich assoziierte Akteure Datendiebstahl oder disruptive Operationen durchführen.[21]

Die Sicherheitsstrategie betont zudem die Stärkung der gesamtgesellschaftlichen Resilienz zur Abwehr von Cyberbedrohungen. Es bleibt jedoch konzeptionell unklar, ob dies die Wiederherstellung des Status quo oder eine dynamische Anpassung an neue Technologien und Bedrohungen bezweckt.[22] Zwar fehlt es an einer klaren Priorisierung der Maßnahmen zur Eindämmung und Bekämpfung von Cybergefahren. Aber aus der Strategie selbst kann ein »Implementierungsnarrativ Cyberabwehr« herausgelesen werden: Danach soll zunächst ein *Whole-of-Society-Approach* durch gesteigertes gesellschaftliches Risikobewusstsein und umfassendere Lagebilder der Behörden die Cybersicherheit erhöhen. Das BSI soll unabhängiger und als Zentralstelle im Bund-

20 Bundesregierung, *Nationale Sicherheitsstrategie: Wehrhaft. Resilient. Nachhaltig. Integrierte Sicherheit für Deutschland, aaO. (FN 16), S. 59.*

21 Kerstin Zettl-Schabath / Sebastian Harnisch, *One Year of Hostilities in Ukraine: Nine Notes on Cyber Operations*, https://eurepoc.eu/wp-content/uploads/2023/06/One_Year_of_Hostilities_in_Ukraine_EuRepoC.pdf, *(Zugriff am 03.02.2025).*

22 Siehe in diesem Band: Thomas Dörfler, »Gefahr erkannt, Gefahr gebannt? Bedrohungen und der effektive Mitteleinsatz in der Nationalen Sicherheitsstrategie« in: *Zeitschrift für Politik* 72, Sonderband (2025).

Länder-Verhältnis gestärkt werden. Eine engere Anbindung von KRITIS-Unternehmen an die Lagebeurteilung des BSI sowie sektorspezifische *CERT*-Teams (Computer Emergeny Response Team) sollen geprüft werden. Ferner sollen die Cyber- und Weltraumfähigkeiten Deutschlands zur kollektiven Abschreckung und Verteidigung in der *NATO* beitragen.[23]

Konkret geplant sind der Ausbau des Informationssicherheitsmanagements der Bundesverwaltung, die hochsichere Vernetzung mit Partnerstaaten und die Sicherstellung der Arbeitsfähigkeit der Bundesregierung im Krisenfall. Eine Grundgesetzänderung zur Bundeskompetenz bei schwerwiegenden Cyberangriffen wird angestrebt, wobei zwischen der Erkennung und Abwehr von Angriffen und *Hackbacks* unterschieden wird, letztere werden abgelehnt.[24]

Die Sicherheitsstrategie betont zudem, dass Deutschland »regelwidriges und aggressives Verhalten von Cyberakteuren nicht hinnehmen« wird und Cyberangriffe, wenn möglich, attribuieren und sanktionieren will, auch in Zusammenarbeit mit *EU*-Partnern und der *NATO*.[25] Neben dem Ausbau nationaler Kapazitäten werden auch die Umsetzung europäischer Regulierung (z.B. NIS-2), der Kapazitätsaufbau bei Partnern und die internationale Zusammenarbeit in der *Counter Ransomware Initiative* genannt. Erstaunlicherweise erwähnt die Strategie jedoch nicht explizit den Ausbau völkerrechtlich verbindlicher Normen oder den Schutz von Dissidenten vor digitaler transnationaler Repression, ebenso wenig wie die *CDT* der *EU*. So verpasst es Deutschland auf außenpolitischer Ebene die europäische Cyberdiplomatie zu stärken, indem die *CDT* nicht als integraler Bestandteil der Nationalen Sicherheitsstrategie verankert wurde. Hinzu kommen die von ExpertInnen bislang als lückenhaft und defizitär beschriebenen Planungen für das deutsche Umsetzungsgesetz von NIS-2: So sieht der aktuelle Gesetzesentwurf umfangreiche Ausnahmen für staatliche Behörden, etwa auf der Landes- und Kommunalebene, vor, was einerseits deren Cybersicherheitsniveau eher schaden könnte und andererseits ein falsches Signal an weitere, weniger befähigte und finanziell ausgestattete Mitgliedstaaten, aber auch die umfassend von der Regulierung betroffene deutsche Wirtschaft sendet.[26]

23 Bundesregierung, *Nationale Sicherheitsstrategie: Wehrhaft. Resilient. Nachhaltig. Integrierte Sicherheit für Deutschland, aaO. (FN 16), S. 61.*

24 Bundesregierung, *Nationale Sicherheitsstrategie: Wehrhaft. Resilient. Nachhaltig. Integrierte Sicherheit für Deutschland, aaO. (FN 16),* S. 62.

25 Bundesregierung, *Nationale Sicherheitsstrategie: Wehrhaft. Resilient. Nachhaltig. Integrierte Sicherheit für Deutschland, aaO. (FN 16),* S. 60.

26 AG Kritis, *Schriftliche Stellungnahme zum Referentenentwurf des NIS2UmsuCG vom 07.05.2024,* https://ag.kritis.info/2024/05/30/stellungnahme-nis2umsucg/ (Zugriff am 03.02.2025).

3.2 Die Nationale Sicherheitsstrategie im Lichte der Cyberkonfliktforschung

Die Cyberkonfliktforschung ist ein wachsendes, angloamerikanisch geprägtes Forschungsfeld.[27] Nur wenige Arbeiten untersuchen bislang die Effektivität nationaler Attribuierungsprozesse, der *CDT* und der institutionellen Reform der deutschen Cybersicherheitspolitik. Vergleichende Arbeiten blieben bisher weitgehend aus, während zahlreiche Studien die Voraussetzungen für erfolgreiche technische Attribuierungen analysieren, rechtliche Zuschreibungen untersuchen und politische Verantwortlichkeiten beleuchten.[28]

Einzelfallstudien zu den Attribuierungsprozessen in den USA, Deutschland und begrenzt vergleichende internationale Studien sind verfügbar.[29] So analysieren Paulus und Rupp vier staatliche Attribuierungsprozesse hinsichtlich technischer, rechtlicher und politischer Elemente. Armelli et al. und Efrony[30] kommen zu dem vorläufigen Schluss, dass insbesondere kollektive Attribuierungen kaum Einfluss auf das Verhalten der adressierten Akteure haben. Als Gründe identifiziert Efrony die mangelnde Transparenz und die wechselnden beteiligten bürokratischen Akteure, welche die Legitimität und Effektivität von Attribuierungen einschränken, selbst wenn sie mithilfe von Sanktionen unterstützt werden.

Ähnliche Befunde gelten für die Wirkung der *CDT*: Einige Studien befassten sich mit der Genese und den Inhalten der *CDT*; andere untersuchten die Effekte eines Sanktionsregimes oder gemeinsamer Attribuierungen.[31] Die Nutzung der *CDT*-Ins-

27 James Shires / Robert Chesney / Max Smeets (Hg.), *Cyberspace and Instability* 2023. Tim Stevens / Joseph Devanny (Hg.), *Research handbook on cyberwarfare,* Cheltenham, UK, Northampton, MA 2024.

28 David D. Clark / Susan Landau, »Untangling attribution«, in: National Research Council (Hg.), *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.*, Washington, D.C. 2010, S. 25–40; Thomas Rid / Ben Buchanan, »Attributing Cyber Attacks« in: *Journal of Strategic Studies* 38, 1–2 (2015), S. 4–37; Kristen Eichensehr, »The Law & Politics of Cyberattack Attribution« in: *UCLA Law Review* 67 (2020); Florian J. Egloff, »Public attribution of cyber intrusions« in: *Journal of Cybersecurity* 6, Nr. 1 (2020), S. 484.

29 Heajune Lee, *Strategic Publicity?: Understanding US Government Cyber Attribution* 2021; Rebecca Beigel, »Attribution von Cyberoperationen – Deutschlands öffentliche Zuschreibungen«, in: *Asymmetrien in Cyberkonflikten* 2022, S. 169–198; Alexandra Paulus / Christina Rupp, *Official Public Political Attribution of Cyber Operations: State of Play and Policy Options,* https://www.stiftung-nv.de/publications/official-public-political-attribution-of-cyber-operations, (Zugriff am 16.08.2024).

30 Matthew Armelli et al., *Named but hardly shamed. The Impact of Information Dislosures on APT Operations* 2020; Dan Efrony, »Collective Attribution in Cyberspace: A Rebranded Version of Attribution Does Not Make It More Effective« in: *International Law Studies* 103, Nr. 270 (2024), https://digital-commons.usnwc.edu/ils/vol103/iss1/9/¸ »Enhancing Accountability in Cyberspace Through a Three-Tiered International Governance Regime« in: *International Law Studies*, Nr. 103 (2024), https://digital-commons.usnwc.edu/ils/vol103/iss1/13/.

31 Erica Moret / Patryk Pawlak, *The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?,* https://www.jstor.org/stable/pdf/resrep06815.pdf; Siim Alatalu, »Alliance attribution of global cyber attacks : The European Union«, in: *National Cyber Emergencies* 2020,

trumente durch *EU*-Institutionen und Mitgliedstaaten wird nur in sehr wenigen Studien behandelt:[32] hier zeigt sich zum einen, dass die beteiligten *EU*-Institutionen und Mitgliedstaaten eine Präferenz für präventive Maßnahmen haben und zum anderen, dass nur (sehr) wenige *CDT*-basierte Sanktionen verhängt wurden. Ferner zeigen diese Studien deutlich, dass bislang zwischen der Intensität des Angriffs und Robustheit der Gegenmaßnahme kein erkennbarer Zusammenhang besteht, sodass die Forschung hier ganz konkret Hilfestellung geben kann, wie eine »verhältnismäßige(re) Reaktion« der betroffenen *EU*-Staaten ausgestaltet werden könnte.

Die Debatte um aktive (oft auch offensive) Verteidigung und Sicherung kritischer digitaler Infrastrukturen wird in der Bundesrepublik seit 2017 intensiv geführt.[33] Es wird unterschieden zwischen aktiver Cyberabwehr von Angriffen unterhalb der Schwelle eines bewaffneten Angriffs und Cyberverteidigung gegen Angriffe darüber, die bislang in der Realität jedoch kaum vorkommen, ein Beispiel wäre die sogenannte *Stuxnet*-Operation, bekanntgeworden 2010. *Hackbacks*, offensive Maßnahmen ohne definitorische Einschränkungen, werden von der Bundesregierung indes abgelehnt.[34] Einige Experten halten die Abgrenzung zwischen aktiver Cyberabwehr und *Hackbacks* für praktisch unmöglich.[35] Die meisten politisch Verantwortlichen setzen jedoch auf eine Differenzierung der Maßnahmen in vier Stufen: Umleitung des Datenverkehrs, Blockierung, Infiltration und Manipulation von Daten, und Abschaltung des angreifenden Systems.[36]

Die Sicherheitsstrategie greift diese Debatte auf, indem sie die Bundesregierung auffordert, »eine Bundeskompetenz zur Gefahrenabwehr bei schwerwiegenden Cyberangriffen durch Änderung des Grundgesetzes« anzustreben.[37] Nach Medienberichten sieht ein erster Reformschritt unter Federführung des BMI eine Bundeskompetenz des BKA zur aktiven Gefahrenabwehr vor, die auch Maßnahmen wie Datenmanipulation

---

S. 171–185; Stefan Soesanto, *Europe Has No Strategy on Cyber Sanctions,* https://www.lawfaremedia.org/article/europe-has-no-strategy-cyber-sanctions, (Zugriff am 28.08.2024).

32 Annika Sachs / Imke Schmalfeldt / Kerstin Zettl-Schabath, *Right Thoughts Right Words Right Actions? The EU´s application of the Cyber Diplomacy Toolbox* 2024.

33 Janine Schmoldt, »Von der Defensive zur Cyberoffensive? Aktive Cyberabwehr, Hackbacks und der Diskurs der Akteure in der deutschen Cybersicherheitspolitik« in: *Zeitschrift für Außen- und Sicherheitspolitik* 17, Nr. 2 (2024), S. 165–182.

34 SPD / Bündnis 90/Die Grünen und FDP, *Mehr Fortschritt wagen – Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit,* https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf, (Zugriff am 28.08.2024), S. 16f.

35 Sven Herpig, *Warum das Bundesinnenministerium den Begriff „Hackback" umdefiniert,* https://www.interface-eu.org/publications/warum-das-bundesinnenministerium-den-begriff-hackback-umdefiniert, (Zugriff am 28.08.2024). Johannes 'Ijon' Rundfeldt, *Kommentar: Aktive Abwehr defensiver Offensive ist Cybersicherheitsfantasie,* https://www.heise.de/meinung/Kommentar-Aktive-Abwehr-defensiver-Offensive-ist-Cybersicherheitsfantasie-7474597.html, (Zugriff am 28.08.2024).

36 Hakan Tanriverdi, *Internes-Papier: Die Hackback-Pläne der Bundesregierung,* https://cyber-peace.org/wp-content/uploads/2019/05/Internes-Papier_-Die-Hackback-Pl%C3%A4ne-der-Bundesregierung-_-tagesschau.de_.pdf, (Zugriff am 28.08.2024).

37 Bundesregierung, *Nationale Sicherheitsstrategie: Wehrhaft. Resilient. Nachhaltig. Integrierte Sicherheit für Deutschland, aa*O. *(FN 16),* S. 62.

und Abschaltung von Servern umfassen könnte. Ein zweiter Schritt zielt auf die Aufwertung des BSI zu einer Bundesoberbehörde, die jedoch eine Grundgesetzänderung und die Zustimmung des Bundesrats erfordert.[38] Eine solche Änderung ist zwar dringlich, da das BKA bei der Bekämpfung des *Emotet*-Netzwerks 2021 möglicherweise schon seine Kompetenzen überschritten hat, als es Schadsoftware auf angegriffenen Systemen veränderte und unschädlich machte.[39] Die Umsetzung dieser Reformschritte konnte vor dem Bruch der Ampelregierung im November 2024 auf den Weg gebracht, aber nicht mehr abgeschlossen werden.

4 Deutschlands Cybersicherheitsansatz zwischen »aktiver Diplomatie« und »aktiver Abwehr«

Sind die Ziele und Instrumente der Strategie im bisherigen Cybersicherheitsverhalten Deutschlands erkennbar? Die Bundesregierung war aktiv innerhalb der *UN* und der *EU* in der Normentwicklung im Cyberspace beteiligt (»aktive Cyberdiplomatie«), konnte ihre Fähigkeiten (»aktive Cyberabwehr«) jedoch nur eingeschränkt umsetzen. Zudem ist die langfristige Effektivität zur Stärkung der gesamtstaatlichen Resilienz fraglich, in Anbetracht der nationalen Umsetzungslücken bei NIS-2 sowie der wenig umfänglichen Adressierung und Anwendung der *CDT*. Um Cyberoperationen verhindern, ihnen standhalten und sich von ihnen erholen zu können, wären diese Maßnahmen jedoch zur effektiven und effizienten Allokation öffentlicher und privater Ressourcen notwendig; aufbauend auf einem umfassenden Cyber-Bedrohungslagebild für ganz Deutschland als Basis sämtlicher Cybersicherheitsmaßnahmen.

4.1 Deutschlands Cyberdiplomatie: Globale Normbildung, EU-Cybersanktionen und Attribution

Auf diplomatischer Ebene setzt sich Deutschland seit den ersten Konsultationen der *United Nations Group of Governmental Experts on Information Security* (*UNGGE*) 2004 für die Anwendung des internationalen Rechts im Cyberspace ein. Ausgehend vom Zivilmachtkonzept[40] spiegelt dies das historische Engagement der Bundesrepublik für eine regelbasierte internationale Ordnung wider. Die Bundesregierung unterstützt die Anwendung der *UN*-Charta und der Menschenrechte im digitalen Raum.

38 Christian Rath, Faeser für aktive Cyberabwehr im Grundgesetz, 3.4.2023, https://www.rnd.de/politik/hackbacks-durch-bka-nancy-faeser-will-aktive-cyberabwehr-im-grundgesetz-M53ZE4MU3VEZBB3VEVQZSEF44A.html, (Zugriff am 29.08.2024).

39 Jakob Bund, *Bureaucratic initiative redefines German law enforcement cyber operations,* https://bindinghook.com/articles-hooked-on-trends/bureaucratic-initiative-redefines-german-law-enforcement-cyber-operations/, (Zugriff am 26.08.2024).

40 Hanns W. Maull, »Deutschland als Zivilmacht«, in: Siegmar Schmidt / Gunther Hellmann / Reinhard Wolf (Hg.), *Handbuch zur deutschen Außenpolitik*, Wiesbaden 2007, S. 73–84. Siehe in diesem Band: Patrick Mello, »Strategische Zeitenwende? Die Nationale Sicherheitsstrategie als Wendepunkt deutscher Außenpolitik« in: *Zeitschrift für Politik* 72, Sonderband (2025).

Wichtige Diskussionsthemen der *UNGGE* waren seit 2009 das Verbot völkerrechtswidriger Handlungen und die Sorgfaltspflicht der Staaten, um die Nutzung ihres Territoriums für illegale IKT-Aktivitäten (Informations- und Kommunikationstechnologie) zu verhindern.[41]

Trotz der Verabschiedung dieser Prinzipien im Jahr 2013 scheiterte die Umsetzung oft aufgrund technischer, politischer und rechtlicher Herausforderungen. Besonders der fehlende politische Wille, offensive Cyberfähigkeiten einzuschränken, hinderte technologisch fortgeschrittene Demokratien daran, Verantwortung zu übernehmen.[42] Die *UNGGE*-Runden 2010, 2013 und 2015 formulierten freiwillige Normen für verantwortungsvolles staatliches Verhalten im Cyberspace, wie den Schutz kritischer Infrastrukturen. Die Verhandlungen von 2017 unter deutscher Führung scheiterten jedoch wegen verschlechterter geopolitischer Beziehungen zwischen Russland und den *USA* nach den *US*-Wahlen 2016.[43]

Nach dem Scheitern der *UNGGE* 2017 verfolgte Deutschland seine Ziele im Rahmen der *CDT*, die Sanktionen gegen Verantwortliche für Cyberoperationen ermöglicht. Die Toolbox enthält jedoch keinen gemeinsamen Attributionsprozess, wie die damalige deutsche Cyberbotschafterin Regine Grienberger 2023 in einem Positionspapier betonte.[44] Die Formalisierung des deutschen Attribuierungsprozesses erfolgte dabei erst fünf Jahre nach dem Bundestagshack von 2015, als die Bundesregierung erstmals offiziell russische Akteure des Militärgeheimdienstes *GRU* beschuldigte.[45]

Deutschland erkennt die Notwendigkeit einer stärkeren europäischen Koordination bei der Attribution von Cyberoperationen an. Ein prominentes Beispiel war die EU-Reaktion auf die russische »*Ghostwriter*«-Kampagne, die von Deutschland vorangetrieben wurde. Um die EU-Mitgliedstaaten von einer gemeinsamen Erklärung zu überzeugen, war ein hinreichender Austausch von Attributionsevidenzen nötig, wozu die Bundesregierung offensichtlich bereit war.[46] Auch bei der ersten Anwendung der *CDT* spielte Deutschland eine zentrale Rolle, als die *EU* gemeinsam Sanktionen gegen Verantwortliche für Cyberangriffe wie *WannaCry* und *NotPetya* verhängte.

Bemerkenswert ist jedoch, dass die *CDT* in der Nationalen Sicherheitsstrategie nicht eigens erwähnt wird, entgegen dem Bekenntnis zu verstärkten Attributions- und Sank-

41 Heli Tirmaa-Klaar, »The Evolution of the UN Group of Governmental Experts on Cyber Issues. From a Marginal Group to a Major International Security Norm-Setting Body« in: *Cyberstability Paper Series: New Conditions and Constellations in Cyber* (2021), https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf, (Zugriff am 19.08.2024), 5.

42 Tim Maurer, »A Dose of Realism: The Contestation and Politics of Cyber Norms« in: *Hague Journal on the Rule of Law* 12, Nr. 2 (2020), https://link.springer.com/article/10.1007/s40803-019-00129-8, S. 283–305, 283–305.

43 Tirmaa-Klaar, The Evolution of the UN Group of Governmental Experts on Cyber Issues, aaO. (FN 41), S. 11.

44 Regine Grienberger, *Cyberangreifer benennen, globale Normen stärken: Erfahrungen mit dem Attributionsverfahren der Bundesregierung* 2023.

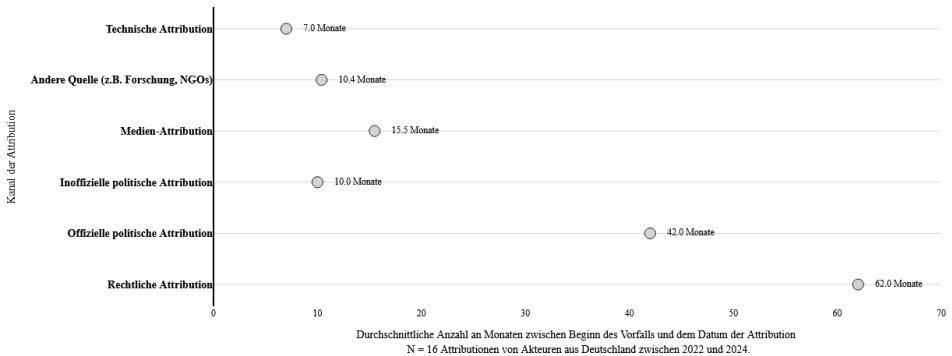
45 Bundesregierung, *Regierungsbefragung mit Kanzlerin Merkel,* https://www.bundesregierung.de/breg-de/aktuelles/regierungsbefragung-kanzlerin-1752666, (Zugriff am 16.08.2024).

46 Stefan Soesanto, *The limits of like-mindedness in cyberspace,* https://www.realinstitutoelcano.org/en/analyses/the-limits-of-like-mindedness-in-cyberspace/, (Zugriff am 15.12.2022).

tionierungsprozessen mit Partnerstaaten. Denn trotz der Bedeutung dieser Sanktionen bleibt die Kohärenz und Geschwindigkeit der politischen und rechtlichen Reaktionen auf Cybervorfälle in Deutschland weiterhin eine Herausforderung.[47] Insbesondere die Geschwindigkeit offizieller politischer und rechtlicher Attributionen durch Bundesbehörden ist trotz der erhöhten Anzahl von Vorfällen seit 2022 immer noch deutlich geringer als die Geschwindigkeit (und Anzahl) technischer Attributionen vonseiten privatwirtschaftlicher Akteure (Abbildung 1).

Konkret heißt dies: während privatwirtschaftliche Akteure Cyberangriffe auf deutsche Ziele immer schneller aufdecken – im Durchschnitt nach zehn Monaten, Tendenz sinkend – braucht eine offizielle und öffentliche politische Zuschreibung der gleichen Angriffe nach wie vor viermal so lang; geht es um die Zuweisung völkerrechtlicher Verantwortung, braucht der deutsche Attributionsprozess im Durchschnitt sogar mehr als sechsmal so lang, sprich über fünf Jahre.

Abbildung 1: Attributionsgeschwindigkeit deutscher Akteure je Attributionskanal seit 2022



Erklärung: Die Grafik zeigt die durchschnittliche Anzahl der Monate zwischen dem Beginn eines Cybervorfalls und der ersten öffentlich gemachten Attribution seitens deutscher Akteure. Unterschieden wird dabei zwischen der Art der Attribution, wobei »Technische Attributionen« regelmäßig von Threat Intelligence Unternehmen im Rahmen technischer Analysen veröffentlicht werden. Quelle: Eigene Darstellung auf Basis von European Repository of Cyber Incidents, 2025.

Die politische und rechtliche Attribution von Cyberoperationen bleibt auch deshalb eine Herausforderung, weil es oft schwer ist, die Verantwortlichen technisch klar zu identifizieren. Und selbst wenn eine Regierung eine öffentliche Attribution vornimmt, führt dies nicht zwangsläufig zu Sanktionen oder Gegenmaßnahmen, da Attributionen verschiedene Ziele und Adressaten haben.[48] Demokratische Staaten sind zudem oft zögerlich, Cyberangriffe einem Akteur öffentlich zuzuordnen, um geopolitische Spannungen zu vermeiden, geheimdienstliche Quellen zu schützen oder aufgrund man-

47 Paulus / Rupp, *Official Public Political Attribution of Cyber Operations: State of Play and Policy Options, aaO. (FN 29).*

48 Florian J. Egloff / Max Smeets, »Publicly attributing cyber attacks: a framework« in: *Journal of Strategic Studies* (2021), S. 1–32.

gelnder Reaktionsmöglichkeiten.[49] Dies erschwert grundsätzlich die Schaffung einer regelbasierten Ordnung im Cyberspace.

Multilaterale Sanktionen, wie die der *EU*, erfordern zusätzlichen Informationsaustausch, Koordination und Verhandlungen zwischen den Mitgliedstaaten, da die Attribution und Reaktion auf Cyberoperationen eine nationale Angelegenheit sind.[50] Dabei strebt die Bundesregierung durchaus an, Sanktionen und diplomatische Maßnahmen schneller durchzuführen als noch beim Bundestagshack 2015. Zwei Beispiele verdeutlichen dies: Am 3. Mai 2024 attribuierte Außenministerin Annalena Baerbock während einer Australien-Reise eine russische Cyberspionage-Operation des *GRU* gegen die SPD-Parteizentrale vom Januar 2023.[51] Noch am selben Tag wurde der Geschäftsträger der russischen Botschaft in Berlin ins Auswärtige Amt einbestellt, und der deutsche Botschafter in Russland, Alexander Graf von Lambsdorff, wurde zu Konsultationen nach Deutschland zurückgerufen.[52] Der Vorfall war bereits im Juni 2023 bekannt geworden. Im zweiten Fall beschuldigte das Auswärtige Amt in einer Pressekonferenz am 31. Juli 2024 staatlich geförderte chinesische Hacker der Spionage gegen das Bundesamt für Kartografie und Geodäsie (BKG).[53] Die zuständige Ministerin Nancy Faeser bezeichnete die Operationen zudem als Bedrohung für die »digitale Souveränität Deutschlands und Europas«.[54] Auch hier war der Vorfall bereits ein Jahr vor der politischen Attribution öffentlich bekannt geworden.

Diese Unterschiede in den Attributionspraktiken illustrieren das deutsche Vorgehen: Erstens verzichtet das Auswärtige Amt als federführendes Ministerium oft darauf, konkrete Normverletzungen zu benennen, zu denen sich Deutschland auf UN-Ebene aber bekennt. Zweitens lässt das deutsche Attributionsverfahren Spielraum für andere Bundesbehörden, wenn eine Cyberoperation ihren Geschäftsbereich direkt betrifft, wie im Fall der Spionage gegen das BKG. Auch hier wurde vom BMI kein Bezug auf *UN*-Normen genommen, die Cyberoperationen gegen kritische Infrastrukturen verbieten. Ein möglicher Grund für diese Zurückhaltung könnte sein, dass der Zusam-

49 Kerstin Zettl-Schabath, *Staatliche Cyberkonflikte. Proxy-Strategien von Autokratien und Demokratien im Vergleich,* Bielefeld 2023.

50 Sven Herpig / Thomas Reinhold, »Spotting the bear: credible attribution and Russian operations in cyberspace«, in: Nicu Popescu / Stanislav Secrieru (Hg.), *Hacks, Leaks and Disruptions. Russian Cyber Strategies*, Brussels 2018, S. 33–42.

51 Paul-Anton Krüger / Markus Balser, *Putins Hacker,* https://www.sueddeutsche.de/politik/russland-spd-cyberattacke-hacker-fancy-bear-apt-28-annalena-baerbock-1.6877406?reduced=true, (Zugriff am 19.08.2024).

52 Paul-Anton Krüger, *Alexander Graf Lambsdorff: Deutschland zieht Botschafter aus Moskau ab,* https://www.sueddeutsche.de/politik/russland-cyberattacke-lambsdorff-botschafter-abzug-1.6979111, (Zugriff am 19.08.2024).

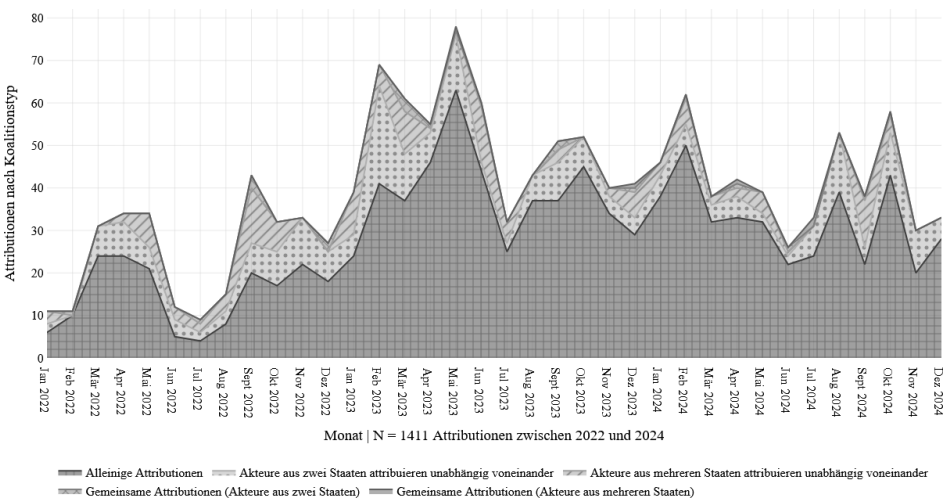
53 Auswärtiges Amt, *Erklärungen des Auswärtigen Amts in der Regierungspressekonferenz vom 31.07.2024,* https://www.auswaertiges-amt.de/de/newsroom/regierungspressekonferenz/2669268#content_1, (Zugriff am 19.08.2024).

54 Bundesministerium des Innern und für Heimat, *Schwerer Cyberangriff auf das BKG ist staatlichen chinesischen Angreifern zuzuordnen und diente der Spionage,* https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/07/cyberangriff-bkg.html, (Zugriff am 19.08.2024).

menhang zwischen Cyberspionage und Sabotage bei kritischen Infrastrukturen im Fall des BKG weniger direkt ist.

Die Sicherheitsstrategie stellt indes mehr gemeinsame Attributionen mit europäischen und internationalen Partnern in Aussicht: »*Deutschland wird regelwidriges und aggressives Verhalten von Cyberakteuren nicht hinnehmen. Wo immer möglich wird die Bundesregierung die Urheber von Cyberangriffen ermitteln und durch Attribuierung auf nationaler Basis, gemeinsam mit EU-Partnern, unseren Verbündeten in der NATO oder anderen betroffenen Staaten benennen und mittels Sanktionen gezielt gegen sie vorgehen.*«[55] Der Einschub »wo immer möglich« lässt dabei aber Raum für Situationen, in denen keine öffentliche oder gemeinsame Attribution erfolgen soll und dies ist nach wie vor der Fall für eine große und wachsende Anzahl der öffentlich bereits bekanntgewordenen Vorfälle. Trotz dieses Bekenntnisses zu verstärkten *joint attributions* und der Tendenz zu gemeinsamer Attributionskoordination seit 2022,[56] sind unilaterale Attributionen global (und europäisch) betrachtet indes weiterhin das vorherrschende Politikinstrument (Abbildung 2). Gemeinsame Attributionen Deutschlands mit weiteren *EU*-Mitgliedstaaten könnten den Weg ebnen hin zu kohärenten und effektiveren Attributionsprozessen, die auf einem gemeinsamen Bedrohungsverständnis basieren. Wenn dies regelmäßig gelänge, so könnten konsistentere, und damit wirkungsvollere Gegenmaßnahmen gegenüber feindlichen Cyberoperationen angewandt werden, als dies in der Vergangenheit der Fall war:

Abbildung 2: Globale Attributionsmuster seit 2022



Quelle: Eigene Darstellung auf Basis von European Repository of Cyber Incidents, 2025.

55 Bundesregierung, *Nationale Sicherheitsstrategie: Wehrhaft. Resilient. Nachhaltig. Integrierte Sicherheit für Deutschland, aaO. (FN 16),* S. 60.

56 Paulus / Rupp, *Official Public Political Attribution of Cyber Operations: State of Play and Policy Options, aaO. (FN 29).*

Erschwerend kommt hinzu, dass die ansteigende Zahl deutscher (öffentlicher) Attributionen mit der Anzahl und Intensität der Vorfälle nicht schritthält. Konkret bedeutet dies: Deutschland wird häufiger im Cyberraum angegriffen, es wird auch öffentlich darüber berichtet, aber die Bundesregierung setzt sich dagegen nur in einigen Fällen öffentlich zur Wehr. Selbst wenn die zuständigen Ministerien und Agenturen die Täter(gruppen), oder die sie schützenden Regierungen (diplomatisch) nicht-öffentlich adressieren, verbleibt in der Öffentlichkeit möglicherweise der Eindruck der Taten- oder Hilflosigkeit zurück. Diesem Eindruck kann und muss besser begegnet werden.

4.2 »Aktive Cyberabwehr« als Reaktion auf eine verschärfte Cyberkonfliktlage

Deutschland hat in den letzten Jahren seine operativen Gegenmaßnahmen zur Bekämpfung von Cyberkriminalität erheblich ausgeweitet, insbesondere vonseiten des BKA. Im Bundeslagebild Cyberkriminalität 2023 werden Ransomware und politisch motivierter Hacktivismus als die größten Bedrohungen identifiziert.[57] Diese Einschätzung kann für den zumeist wenig schadhaften Hacktivismus, etwa mittels *DDoS*- oder *Defacement*-Operationen, kritisch gesehen werden, Stichwort »Priorisierung«. Zu den Gefahrenabwehrmaßnahmen zählen die Beschlagnahmung von Cyberinfrastruktur, Verhaftungen, die Bereitstellung von Entschlüsselungstools, die Beschlagnahmung von Lösegeldzahlungen und die Verhängung von Sanktionen. Während Sanktionen hauptsächlich auf europäischer Ebene koordiniert werden, führt das BKA operativ die übrigen Maßnahmen durch, oft in Zusammenarbeit mit europäischen Partnern.

Die verstärkten Bemühungen Deutschlands und anderer *ICRI*-Länder (*International Counter Ransomware Initiative*) unter *US*-Führung konzentrieren sich auf die permanente Störung krimineller Aktivitäten, ähnlich der US-Doktrinen *Defending Forward* und *Persistent Engagement*.[58] Ein aktuelles Beispiel für die operative Zusammenarbeit ist die *Operation Cronos,* bekannt geworden im Februar 2024, bei der die *Ransomware*-Gruppierung *Lockbit* geschwächt wurde. Laut Angaben des Threat Intelligence Unternehmens *TrendMicro* war *Lockbit* 2023 für 25 bis 33 Prozent aller globalen *Ransomware*-Operationen verantwortlich.[59]

Neben der konkreten Unterstützung für Opfer stand bei *Operation Cronos* nicht das Ziel im Vordergrund, die konkrete Gruppierung endgültig zu zerschlagen und deren Mitglieder festzunehmen, sondern vielmehr das Vertrauen der kriminellen Akteure untereinander und zu deren *affiliates* sukzessive zu unterminieren. Dies entspricht der *doctrine of cognitive effect,* die die britische *National Cyber Force* (*NCF*) 2023 geprägt

57 Bundeskriminalamt, *Im Fokus: Bundeslagebild Cybercrime 2023,* https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2023/CC_2023.html, (Zugriff am 28.08.2024).

58 Michael P. Fischerkeller / Richard J. Harknett, »Persistent engagement, agreed competition, and cyberspace interaction dynamics and escalation« in: *The Cyber Defense Review* (2019), S. 267–287.

59 Christopher Boyton, *Auswirkungen der Operation Cronos auf LockBit,* https://www.trendmicro.com/de_de/research/24/d/auswirkungen-der-operation-cronos-auf-lockbit.html, (Zugriff am 25.08.2024).

hat. Die Strategie kombiniert technische und Informationsoperationen, um Misstrauen innerhalb krimineller Netzwerke zu säen.[60] Die langfristige Effektivität solcher Strafverfolgungsoperationen muss zwar erst noch bewertet werden. Einige ExpertInnen aus Wissenschaft und Industrie gehen jedoch davon aus, dass solche *Counter Cyber Operations* zur Strafverfolgung durchaus einen zeitweiligen Effekt haben und so auch Teil einer erfolgreichen Abschreckungsstrategie gegen cyberkriminelle Gruppen sein können.[61]

Im Falle digitaler Gegenmaßnahmen gegen staatliche Cyberangreifer bestehen jedoch zumeist größere politische und rechtliche Hürden für Demokratien: Einerseits, soll eine weitere digitale oder analoge Eskalation im Regelfall vermieden werden; andererseits wird angestrebt, dass die eigenen Handlungen völkerrechtlich legitimiert sind. Anhand der international koordinierten Strafverfolgungsoperation gegen die Schadsoftware *Emotet* (2021) lassen sich die bestehenden politischen und rechtlichen Beschränkungen gut aufzeigen: So hatte das BKA im Rahmen der Operation nach eigenen Angaben den *Takedown* von *Emotet* initiiert, die Infrastruktur »übernommen und zerschlagen«.[62] BKA-Präsident Holger Münch bezeichnete die Razzia als technische Beschlagnahme, bei der installierte *Emotet*-Versionen isoliert und damit die Bedrohung neutralisiert wurde. Er betonte dabei, dass die Aktion der Informationsgewinnung gedient habe, um diese in polizeilichen Ermittlungs- und Strafverfahren zu nutzen. Der bundesrechtliche Rahmen erlaubt dem BKA bislang indes keine Bereinigung von Opfersystemen zur Gefahrenabwehr, da diese Aufgabe verfassungsrechtlich den Landespolizeibehörden obliegt. Die Deaktivierung von Malware durch das BKA ist daher nur in Kombination mit der Beweissicherung möglich und gilt rechtlich als Nebeneffekt.[63] Grundsätzlich sahen ExpertInnen die Argumentation des BKA daher kritisch, da die angeführten Rechtsgrundlagen aus der Strafprozessordnung für derlei Maßnahmen der Gefahrenabwehr nicht geeignet seien.[64] Die Bundesregierung hat wohl auch als Resultat aus dieser Debatte in der Sicherheitsstrategie den Schluss gezogen, dass sie die »Schaffung einer Bundeskompetenz zur Gefahrenabwehr bei

60 National Cyber Force, *Responsible Cyber Power in Practice (HTML),* https://www.gov.uk/government/publications/responsible-cyber-power-in-practice/responsible-cyber-power-in-practice-html, (Zugriff am 25.08.2024).

61 Diana Selck-Paulsson / Wicus Ross, *Cy-Xplorer 2024 When bits turn to blackmail: navigating the ecosystem of cyber extortion and ransomware,* https://www.orangecyberdefense.com/be/resourses/cy-xplorer-2024, (Zugriff am 25.08.2024); Erica D. Borghard / Shawn W. Lonergan, »Deterrence by denial in cyberspace« in: *Journal of Strategic Studies* 46, Nr. 3 (2023), S. 534–569.

62 Bundeskriminalamt, *Infrastruktur der Emotet-Schadsoftware zerschlagen,* https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html, (Zugriff am 26.08.2024).

63 Bund, *Bureaucratic initiative redefines German law enforcement cyber operations, aaO. (FN 39).*

64 Andre Meister, *Schadsoftware-Bereinigung: BKA nutzt Emotet-Takedown als Türöffner für mehr Befugnisse und neue Gesetze,* https://netzpolitik.org/2021/schadsoftware-bereinigung-bka-nutzt-emotet-takedown-als-tueroeffner-fuer-mehr-befugnisse-und-neue-gesetze/#2021-02-10_Innenausschuss_Protokoll_TOP-14_Emotet, (Zugriff am 26.08.2024).

schwerwiegenden Cyberangriffen aus dem In- und Ausland durch Änderung des Grundgesetzes« anstreben muss.

Gleichzeitig betont die Strategie aber weiterhin, dass die Bundesregierung die direkte und unbegrenzte Einwirkung auf Angreifer-Netzwerke und Systeme, i.e. *Hackbacks*, ablehnt. Für letztere kommen ExpertInnen zu dem Schluss, dass in Deutschland ausschließlich das Kommando Cyber- und Informationsraum (CIR) der Bundeswehr im Zuge der Erklärung eines Verteidigungsfalls hierzu legitimiert wäre. Da die Bundeswehr verfassungsrechtlich bislang eine reine Verteidigungsarmee ist, wären auch hier zahlreiche rechtliche Fragen zu klären, um solche Cybergegenmaßnahmen nicht zu völkerrechtswidrigen Vergeltungsakten werden zu lassen.[65] Auch wäre für solche offensiven Maßnahmen in den meisten Fällen eine offizielle Attribution notwendig. Schließlich stellt sich im Falle von *Hackbacks* aus Sicht der Cyberkonfliktforschung auch die Frage nach deren Effektivität und Effizienz, da offensiven Cyberoperationen keine kosteneffiziente Abschreckungs- oder nachhaltige Zerstörungswirkung zugeschrieben wird.[66]

5 Handlungsempfehlungen: Effiziente Attribution als Grundlage effektiver Cybersicherheit

Die Nationale Sicherheitsstrategie markiert einen Fortschritt in der Sicherung des Cyberraums in und für die Bundesrepublik und ihre Bürger. Die Befähigung nationaler Institutionen zu schnellerem und konsequenterem Handeln und verstärkte internationale Zusammenarbeit sind ihre Hauptelemente. Ihre Hauptschwächen liegen erstens in der mangelnden Differenzierung von Angriffsmustern und Angriffsvektoren, die einen gezielten Einsatz begrenzter Ressourcen erlauben würden. Demokratische Gemeinwesen brauchen transparente und differenzierte Risikoanalysen, um den Einsatz von Steuermitteln in einem neuen Politikfeld rechtfertigen zu können. Zweitens hat sich – historisch gewachsen – ein Netzwerk überlappender Institutionen und Kompetenzen gebildet, die eine kohärente und effiziente Cybersicherheitspolitik erschweren. Die Klärung von Kompetenzen und Koordination von neuen Bund-Länderverfahren stockt und muss – gegen parteipolitischen und institutionellen Widerstand – beherzt durchgesetzt werden. Schließlich kann und muss die Bundesregierung die Täter(-gruppen) schneller, transparenter und konsequenter benennen, um gemeinsam mit den europäischen und transatlantischen Partnern effektive (präventive und aktive operative) Gegenmaßnahmen ergreifen zu können. Wenn sie dies tut, wie im Falle des BKA, muss dies auf einer gesicherten gesetzlichen Grundlage passieren. Daraus lassen sich die folgenden Handlungsempfehlungen ableiten:

Erstens bedarf es für eine aktive Cyberabwehr mehr öffentlicher Attributionen, die direkte Bezüge zu konkreten Normverletzungen aufweisen, und stärkerer *Capacity-*

65 Dennis-Kenji Kipker, *Hackback in Deutschland: Wer, was, wie und warum?,* Bremen.

66 Matthias Schulze, *Militärische Cyber-Operationen. Nutzen, Limitierung und Lehren für Deutschland* 2020¸ Nadiya Kostyuk / Yuri M. Zhukov, »Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?« in: *Journal of Conflict Resolution* 63, Nr. 2 (2019), S. 317–347.

Building Maßnahmen bei vulnerablen Partnern, d.h. verbündeten Staaten/Institutionen mit schwacher Cybersicherheitsinfrastruktur, um so den Eigenschutz im In- und Ausland zu ertüchtigen und kollektive Sanktionen und internationale Normbildung stärker zu legitimieren. Der Gestaltungswille der Sicherheitsstrategie ist im Cyberbereich zu binnenorientiert und unterschätzt den Wert der Stärkung von Partnern und globalen *Governance*-Normen.

Zweitens muss die Bundesregierung ihre Fähigkeit zur Mitwirkung in internationalen Institutionen weiter stärken: Konkret gilt dies bei der Umsetzung von NIS-2, durch die umfassende Anwendung auf staatliche Behörden/Institutionen, um Glaubwürdigkeit und Akzeptanz in den betroffenen Sektoren zu erhöhen und das Schutzniveau politischer Akteure/Institutionen, gerade vor Wahlen, zu stärken. Des Weiteren müssen nationale Fähigkeiten in der *International Counter Ransomware Initiative* gestärkt werden, indem das BKA zur umfassenden Mitwirkung auch rechtlich befähigt wird.

Drittens sollte der Gesetzgeber das BSI auch als unabhängige Bundesoberhörde und Zentralstelle für die Bund-Länderkoordination aufstellen und mithilfe entsprechender verfassungsrechtlicher Regelung dazu befähigen, Prävention, Kapazitätsaufbau und Krisenreaktion in Bereichen der kritischen Infrastrukturen und Bundesbehörden sicherzustellen.