Arbeitspapier
Arbeitspapiere sind Online-Veröffentlichungen der Forschungsgruppen.
Sie durchlaufen kein förmliches Gutachterverfahren wie SWP-Studie,
SWP-Aktuell und SWP-Zeitschriftenschau.

SWP

FORSCHUNGSGRUPPE EU / EUROPA | AP NR. 01, JANUAR 2023

Deutsche Cybersicherheit in Europa

Öffentliche Anhörung „Cybersicherheit - Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland“ am Mittwoch, 25. Januar 2023, 14:00 – 16:00 Uhr.

Dr. Annegret Bendiek

Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Inhalt

Executive Summary

Die Abwehr von Cybersicherheitsbedrohungen erfordert eine koordinierte europäische Antwort. Diese Antwort sollte nach dem Prinzip der Sorgfaltsverantwortung erfolgen. Hierbei gilt es, sich des strategischen Vakuums zwischen Cyberdiplomatie und Cyberverteidigung bewusst zu sein. Die zukünftige Cybersicherheitspolitik kann daher weder rein defensiv noch offensiv ausgerichtet sein, sondern muss dem Leitbild einer aktiven defensiven Cyberabwehr folgen. Hierbei gilt es die zivile Verteidigung zu betonen und gleich-zeitig die Resilienz der nationalen und europäischen Infrastrukturen zu verstärken. Für die hierzu notwendigen Kompetenzübertragungen auf die EU-Ebene sollten die nationalen Parlamente den Einsatz der Solidaritätsklausel nach Art. 222 AEUV in Erwägung ziehen, um eine Grundlage für europäisches Handeln zu schaffen.

Reformimplikationen

Deutschland benötigt eine Stärkung von Bundeskompetenzen im Bereich der aktiven Cyberabwehr bei Gefahrenlage. Vergleichbar zur Terrorismusbekämpfung sind die Befugnisse für das BKA im Nationalen Cyberabwehrzentrum zu stärken. Gleichzeitig ist eine stärkere Unabhängigkeit des BSI vom Bundesministerium des Innern sinnvoll. Bei-de Reformen würden die für die europäische Handlungsfähigkeit zur Cyberabwehr not-wendigen Vorbedingungen für die EU-Zusammenarbeit schaffen. Europol (EC3) und die ENISA sind in ihren Kompetenzen für die europäische Cyberabwehr-Koordination sowie für den internationalen Kapazitätsaufbau zu stärken.

Die Cyberdiplomatie im Europäischen Auswärtigen Dienst (EAD) und im Auswärtigen Amt müssen eine zentrale Position und neue personelle und fachliche Kompetenzen erhalten. Die EU-Zusammenarbeit zur Umsetzung des Stufenplans der Cyber Diplomacy Toolbox sollte durch Qualifizierte Mehrheitsentscheidungen erleichtert werden. Der Kapazitätenaufbau, die Normenbildung sowie die sicherheits- und vertrauensbildende Cyberdiplomatie sollten weiter vorangetrieben werden.

Die Bundesregierung und die EU brauchen ein je nach Intensität klar definiertes Reaktionsverfahren, um auf staatlich motivierte, unterstützte oder geduldete Cyberangriffe aus dem Cyberraum reagieren zu können. Sicherheitsbehörden der inneren und äußeren Sicherheit sollten nach dem Push-Prinzip ihre Erkenntnisse auf EU-Ebene insbesondere im EU-Intcen (SIAC) im EAD für eine gemeinsame Bedrohungsanalyse auch im Kontext von hybriden Bedrohungen austauschen.

Die EU Cyber Unit in der EU-Kommission ist zentral für die Cluster orientierte Cybersicherheitsforschung. Die Forschung wäre auf die Resilienz des digitalen Binnenmarkts zu konzentrieren. Schwachstellen müssen systematisch erfasst, der Umgang mit ihnen verbessert und die Zeit von Entdeckung bis zur Beseitigung verringert werden. Die Einheit sollte international angelegte Mechanismen der Exportkontrolle und die Aufnahme von Überwachungstechnologien in Sanktionsregimen überprüfen.

Die Umsetzung von Cybersicherheitsstrategien auf nationaler und EU-Ebene bedürfen einer jährlichen Berichtspflicht gegenüber der Legislative.

Die Herausforderungen

Laut dem ENISA Threat Landscape Report vom November 2022 sind Cyberangriffe in den letzten zwei Jahren massiv angestiegen[1].[2] Cyberangriffe sind nicht nur ein bundesdeutsches, sondern auch ein gesamteuropäisches Problem (Annex EuRePoC Statistiken).[3] Grundsätzlich ist dabei davon auszugehen, dass die Umsetzung der von Bundeskanzler Olaf Scholz angemahnten „neuen strategischen Kultur“[4] in der Cybersicherheit nur dann gelingen kann, wenn nationale Cybersicherheit einer europäischen bzw. transatlantischen Bündnisfähigkeit unterliegt und dem Vorrang der Diplomatie in einer „kooperativen Sicherheit“ (Christopher Daase) verpflichtet ist.

Die deutsche Cybersicherheit ist ein Kernbereich der künftigen umfassenden Nationalen Sicherheitsstrategie Deutschlands.[5] Diese Bemühungen sind in die EU, G7 und Nato-Zusammenarbeit eingebunden. Den aktuellen EU-Rahmen setzt die im Dezember 2020 von der EU-Kommission und dem Hohen Vertreter für die Außen- und Sicherheitspolitik, Joseph Borrell, vorgestellte EU-Strategie für Cyber-Sicherheit und Resilienz.[6] Diese ist eng mit anderen Initiativen der EU verbunden, etwa der digitalen Zukunft des Binnenmarktes, dem Konjunkturprogramm der Kommission und der Strategie der Sicherheitsunion 2020-2025.

[1] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2022*, November 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (eingesehen am 18.1.2023).

[2] Ich bedanke mich bei allen Kolleg:innen des EuRePoC-Teams (www.eurepoc.eu) für ihre wertvolle Unterstützung für diese Stellungnahme. Das European Repository über Cybervorfälle in Europa hat zum Anspruch die technische, politische und rechtliche Attribution von Cybervorfällen, die für die Cyberaußen- und Sicherheitspolitik von Relevanz sind nach wissenschaftlichen Kriterien zu erheben.

[3] Einige Überlegungen basieren im Folgenden auf zahlreiche SWP-Schriften, die die Autorin in alleiniger oder in Ko-Autorenschaft mit Matthias Schulze verfasst hat. Hierzu zählen: Annegret Bendiek und Matthias Schulze, *Attribution als Herausforderung für EU-Cybersanktionen. Eine Analyse von WannaCry, NotPetya, Cloud Hopper, Bundestag-Hack, OVCW*, Berlin: Stiftung Wissenschaft und Politik (SWP), Oktober 2021 (SWP-Studie 2021/S 17), https://www.swp-berlin.org/publikation/attribution-als-herausforderung-fuer-eu-cybersanktionen; Annegret Bendiek und Matthias Schulze: *Schwachstellen der deutschen Cybersicherheitsstrategie 2021*, Berlin: Stiftung Wissenschaft und Politik (SWP), September 2021 (Kurz Gesagt), https://www.swp-berlin.org/publikation/schwachstellen-der-deutschen-cybersicherheitsstrategie-2021; Annegret Bendiek, *Sorgfaltsverantwortung im Cyberraum. Leitlinien für eine deutsche Cyber-Außen- und Sicherheitspolitik*, Berlin: Stiftung Wissenschaft und Politik (SWP), März 2016 (SWP-Studie 2016/S 03), https://www.swp-berlin.org/publikation/sorgfaltsverantwortung-im-cyberraum (alle eingesehen am 18.1.2023).

[4] Olaf Scholz, »Die globale Zeitenwende«, in: *Foreign Affairs* (online), 5.12.2022, https://www.foreignaffairs.com/germany/die-globale-zeitenwende (eingesehen am 18.1.2023).

[5] Gesprächskreis Nachrichtendienste in Deutschland e. V., *Nationale Sicherheitsstrategie zwischen Ressortprinzip und gesamtstaatlicher Aufgabenwahrnehmung - Anmerkungen zur aktuellen Diskussion um die Erarbeitung der ersten Nationalen Sicherheitsstrategie*, 05.01.2023, https://www.gknd.org/uploads/1/3/8/1/138195092/230109_gknd_stellungnahme_nationale_sicherheitsstrategie.pdf (eingesehen am 18.1.2023).

[6] Europäische Kommission, *The EU's Cybersecurity Strategy for the Digital Decade*, 16.12.2020, https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (eingesehen am 18.1.2023). Siehe hierzu: Annegret Bendiek, Matthias Kettemann: *EU-Cybersicherheitsstrategie: Desiderat Cyberdiplomatie*, Berlin: Stiftung Wissenschaft und Politik (SWP), Februar 2021 (SWP-Aktuell 2021/A 12), https://www.swp-berlin.org/publikation/eu-strategie-zur-cybersicherheit-desiderat-cyberdiplomatie (eingesehen am 18.1.2023).

Eine gemeinsame Cyber-Einheit mit der Aufgabe, die IT-Fähigkeiten von Verteidigungskreisen im Bereich der Cyber-Sicherheit und der Strafverfolgungsbehörden in Kooperation zu stärken, befindet sich im Aufbau. Die EU soll ein "echtes Cyber-Sicherheits-Schutzschild" erhalten, um Gefahren frühzeitig zu erkennen und Gegenmaßnahmen einzuleiten, bevor Schäden entstehen.

Die bestehende Cybersicherheitsstrategie 2021 für Deutschland ist in ihrer außen- und sicherheitspolitischen Dimension zu europäisieren und die wichtigsten bundesdeutschen und föderalen Institutionen sind auf die Einhaltung des europäischen Kohärenzgebotes hin zu überprüfen. Die Cybersicherheit ist vorwiegend Aufgabe der Bundesländer, die eine wichtige Funktion im Resilienzaufbau, der Strafverfolgung und im kritischen Infrastrukturschutz übernehmen. Das Bundesministerium des Inneren kann als ressortführendes Ministerium nur indirekt darauf achten, inwiefern europäische Vorgaben umgesetzt werden. Es ist fraglich, ob sich die föderale Struktur in eine effektive Cybersicherheit für Deutschland und europäische Handlungsfähigkeit umsetzt.[7]

[7] Christoph Koopmann: »IT-Sicherheit; wie es um die deutsche Cybersicherheit steht«, in: *Süddeutsche Zeitung* (online), 2. Juni 2022, https://www.sueddeutsche.de/politik/cybersicherheit-sondervermoegen-1.5595776?reduced=true; Jana Ballweber: »Faesers Digital-Pläne machen Deutschland unsicherer: Die Politik hat nichts verstanden«, in: *Frankfurter Rundschau* (online), 12. Juli 2022, https://www.fr.de/meinung/kommentare/cyber-unsicherheit-91663064.html (beides eingesehen am 18.1.2023).

Sorgfaltsverantwortung als Prinzip

Die Bundesregierung, die Mitgliedstaaten der EU und die Union folgen prinzipiell der Idee von »Due Diligence«[8] bei der Umsetzung ihrer Cybersicherheitsstrategien. Diese Norm verpflichtet Staaten, in Friedenszeiten dafür zu sorgen, dass von ihrem Territorium keine Handlungen ausgehen, welche die Rechte anderer Staaten verletzen. Die Cybersicherheitsstrategie 2021 und die Cybersicherheitsagenda des Bundesministeriums des Innern vom Juli 2022 folgen dieser Leitidee. Sie weisen darauf hin, dass Cybersicherheit für einen modernen, hochtechnologisierten und digitalisierten Industriestaat wie Deutschland essentiell ist. Infrastrukturresilienz, die Abwehr und Aufklärung von (auch staatlich gelenktem) Cybercrime sowie die Sensibilisierung für Desinformationskampagnen müssen gestärkt werden. Deutschland verfolgt eine auf internationalen Übereinkünften aufbauende grundsätzlich defensiv ausgerichtete Cybersicherheitsstrategie. Dieser Weg liegt in der außenpolitischen Kontinuität und ist der militärischen Zurückhaltung verpflichtet.

Die Betonung von Sorgfaltsverantwortung steht nicht im Widerspruch zur Cyberabwehr und Cyberverteidigung.[9] Cybersicherheit im Sinne der Sorgfaltsverantwortung schließt vielmehr die Art und Weise politischer Regulierung ein.[10] Zur Gewährleistung der Cybersicherheit sollte daher sowohl die deutsche Cybersicherheitspolitik in die europäische Cybersicherheitsarchitektur eingebunden sein (2.1.) als auch die Cyberfähigkeit zur „kooperativen Sicherheit“ der Sicherheitsbehörden (2.2.) und die öffentliche-private Partnerschaft (2.3.) gestärkt werden.

[8] Zum Völkerrecht des Netzes, siehe Christian Schaller, *Internationale Sicherheit und Völkerrecht im Cyberspace*, Berlin: Stiftung Wissenschaft und Politik (SWP), Oktober 2014 (SWP-Studie 2014/S 18), https://www.swp-berlin.org/publikation/internationale-sicherheit-und-voelkerrecht-im-cyberspace (eingesehen am 18.1.2023).

[9] Christian Schaller: »Aktive Cyberabwehr und Notstand im Völkerrecht«, *Zeitschrift für das Gesamte Sicherheitsrecht (GSZ)*, 1 2018, 57–61 S. 58: „Ein Staat, der sich unterhalb der Schwelle des Selbstverteidigungsrechts gegen eine Cyberattacke zur Wehr setzt und dabei in die Rechte unbeteiligter Staaten eingreift, denen im Zusammenhang mit der Attacke nicht einmal eine Sorgfaltspflichtverletzung nachzuweisen ist, kann sich allenfalls auf Notstand berufen, um diesen Eingriff zu rechtfertigen. Im Rahmen des Notstands sind digitalen Gegenschlägen prinzipiell enge völkerrechtliche Grenzen gesetzt.“

[10] Annegret Bendiek, *Sorgfaltsverantwortung im Cyberraum*, Berlin: Stiftung Wissenschaft und Politik (SWP), März 2016 (SWP-Studie 2016/S 03) Siehe auch Annegret Bendiek, Eva Pander Maat, The EU's Regulatory Approach to Cybersecurity, Berlin: Stiftung Wissenschaft und Politik (SWP), Oktober 2019 (Research Division EU/Europe, WP Nr. 02), https://www.swp-berlin.org/publications/products/arbeitspapiere/WP_2019_Bendiek_Pander_Maat_EU_Approach_Cybersecurity.pdf (eingesehen am 18.1.2023).

Europäische Zusammenarbeit

Die EU-Abstimmung stellt einen zentralen rechtlichen und politischen Rahmen für die deutsche Reformagenda in der Cybersicherheit dar.[11] Der Angriffskrieg Russlands gegen die Ukraine verlangt den Ausführungen des Strategischen Kompass vom März 2022 folgend eine aktive Cyberabwehr.[12] Der Begriff der Cyberabwehr wird auf polizeiliche und nachrichtendienstliche, nicht aber auf militärische Maßnahmen angewandt.[13] Er verbindet eine investigative mit einer aktiven Komponente. Die investigative Komponente umfasst die Durchsetzung rechtsstaatlicher Prinzipien, den wechselseitigen Rechtsbeistand und die Auslieferung von Straftätern. Zur aktiven Komponente gehören restriktive Maßnahmen (Sanktionen) sowie alle notwendigen nicht-militärischen Instrumente, die bei Gefahr im Verzug anzuwenden sind. Hierzu kann allerdings auch die Manipulation ausländischer Ressourcen, die elektronische Zerstörung von Servern und die Störung von Datenverkehr im Ausland gehören (siehe Schaubild).

Für die deutsche Europapolitik sind eine schnelle und verbindliche Verabschiedung von Rechtsakten zum Resilienzaufbau, zur Cyberkriminalitätsbekämpfung und nun eben auch zur Cyberabwehr notwendig. Die transnationale Energieinfrastruktur ist laut ENISA-Threat Report ein besonders attraktives Ziel für Cyberangriffe, da die Folgen für die EU weitreichend sein und als Hebel für Erpressungen in Form von Ransomware-Angriffen oder als Ausgangspunkt für militärische Operationen genutzt werden können. Für die Unternehmen des Energiesektors bedeuten die Neuauflagen der Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2) strengere Berichtspflichten. Mitgliedstaaten sollen zudem Registrierungsdaten von TLD-Registries und Domain-Registries erfassen — dies umfasst eine Datenbank von Domain-Namen sowie Namen und Kontaktdaten der Registranten. Weiterhin sollen sie striktere Regeln zur Erfassung und Aktualisierung von Daten innerhalb des Registers erlassen und eine anonyme Domain-Registrierung ausschließen.[14]

Das Europäische Parlament hat in der Einigung mit dem Rat der Version P9_TA(2022)0394 der CER-Richtlinie der EU („Critical Entities Resilience“) am 22. November 2022 zugestimmt. Die Durchführung nationaler Risiko-Analysen zur Identifizierung von critical enti-

[11] Angefangen mit der ersten Cybersicherheitsstrategie 2011, die im Wesentlichen formuliert wurde, um die EU-Strategie von 2013 maßgeblich inhaltlich zu formen. Das IT-Sicherheitsgesetz 2015 sollte die Neuauflage der EU-Strategie 2015 und die erste Netzwerk- und Informationssicherheitsrichtlinie auf den Weg bringen. Das gleiche gilt aktuell für das IT-Sicherheitsgesetz 2.0, welches in die NIS 2.0 überführt wurde

[12] Europäische Kommission, *Gemeinsame Mitteilung an das Europäische Parlament und den Rat: EU-Cyberabwehrpolitik*, 10.11.2022 , https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52022JC0049&from=DE (eingesehen am 18.1.2023): „Wie in dem im März 2022 vom Rat angenommenen Strategischen Kompass für Sicherheit und Verteidigung vorgeschlagen, wird durch die vorliegende Cyberabwehrstrategie die Fähigkeit verbessert, gegen die EU und ihre Mitgliedstaaten gerichtete Cyberangriffe mit allen verfügbaren Mitteln zu verhindern, aufzudecken und abzuwehren sowie sich davon zu erholen und davon abzuschrecken. Dies steht im Einklang mit den digitalen Prioritäten der Kommission, dem ehrgeizigen Ziel der EU-Cybersicherheitsstrategie 2020, der Ankündigung von Präsidentin von der Leyen in ihrer Rede zur Lage der Union 2021 und den Schlussfolgerungen des Rates zur Entwicklung der Cyberabwehr der Europäischen Union vom 23. Mai 2022.“

[13] Zum Folgenden vgl. https://www.athene-center.de/aktuelles/news/whitepaper-zur-aktive-cyberabwehr-1514.

[14] Friedhelm Greis: »NIS2-Richtlinie: Domaininhaber müssen künftig Adressdaten hinterlegen«, in: *Golem.de*, 10.11.2022, https://www.golem.de/news/nis2-richtlinie-domaininhaber-muessen-kuenftig-adressdaten-hinterlegen-2211-169666.html (eingesehen am 18.1.2023)

ties soll im Hinblick auf den "disruptiven Effekt", auf die Anzahl betroffener Nutzer, auf Auswirkungen auf andere Essential Services und weitere Faktoren erweitert werden. Elf Sektoren (wie im Entwurf für das KRITIS-Dachgesetz) sind hierzu vorgesehen, wobei die Finanzmarktinfrastruktur und digitale Infrastrukturen von den Pflichten zur Kooperation ausgenommen sind. Die Eckpunkte für ein neues deutsches Gesetz zum Schutz der kritischen Infrastruktur folgen dem europäischen Rechtsakt. Bei der Erarbeitung des KRITIS-Dachgesetzes und der damit verbundenen Umsetzung der CER-Richtlinie sowie der NIS-2-Richtlinie werden die Schnittstellen zwischen Cybersicherheit und physischem Schutz von KRITIS angeglichen.

Neben dem verstärkten Resilienzaufbau ist die Cyberkriminalitätsbekämpfung ein wichtiger Baustein in der EU-Cyber-Taxonomie[15]. Europol und EC3 wird eine Vorbildfunktion in der Koordination der internationalen Cyberkriminalitätsbekämpfung zugesprochen. Das BKA leistet hier unterstützende Arbeit in der Ermittlung und dient oftmals als *Point of Contact*. Deutschland zählt zu den potenten EU-Staaten in der europäischen Cybersicherheit. Weniger gut aufgestellte EU-Staaten sollten auf Expert:innen aus anderen Staaten zurückgreifen können, die über Europol in Abstimmung mit dem Cybersecurity Research Center und der ENISA vermittelt werden sollten. Europol hat (noch) keine exekutiven Befugnisse und kann deshalb Ermittlungen, die mehr als ein Land betreffen, auch nicht an sich ziehen. Es kann aber koordinieren. Die Cyberabwehr in der EU wäre in einer operativen Kompetenz von Europol aber auch von EU INTCEN und ENISA auf EU-Ebene zu stärken. Diese Institutionen sind zentral, um das strategische Vakuum zwischen Cyberdiplomatie und Cyberverteidigung schließen zu können.

Kooperative Sicherheit

Im Bereich der Cyberaußen- und Sicherheitspolitik standen bisher die Cyber Diplomacy Toolbox und die PESCO-Projekte für die zivile Friedensmacht der EU im Cyber- und Informationsraum im Zentrum. Die zivile Komponente war gegenüber der militärischen Komponente bis zum 24. Februar 2022 im Mittelpunkt der deutschen Außen- und Sicherheitspolitik. Systeme kollektiver Verteidigung wie die Nato oder PESCO spielen seither eine größere Rolle.[16] Zur Umsetzung des neuen Verständnisses wurde im Februar 2022 ein Sondervermögen in Höhe von €100 Milliarden für die Bundeswehr bereitgestellt. Der Bund hat der Cyberagentur hingegen lediglich 30 Millionen Euro für die Erforschung von Hackerangriffen auf kritische Infrastruktur bereitgestellt. Um hinreichende Ressourcen für die Cybersicherheit zu garantieren sollte das Sondervermögen auch Maßnahmen im Bereich der Cybersicherheit finanzieren können.

Die Bündelung von Informationen zur Gefahrenlage im Cyber- und Informationsraum auf EU-Ebene – sei es im EU-Nachrichten- und Lagezentrum (EU-INTCEN) oder in der EU Cyber

[15] European Union Agency For Network and Information Security (ENISA), *Reference Incident Classification Taxonomy*, 26.1.2021, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy/@@download/fullReport (eingesehen am 18.1.2023)

[16] Die Außenministerin Annalena Baerbock hat sich in einer Grundsatzrede Ende September 2022 am Hasso-Plattner Institut in Potsdam für eine zentrale deutsche Cyberabwehr ausgesprochen, so dass der Bund eine Zuständigkeit und Kompetenz für die Gefahrenabwehr im zivilen Bereich erhält, die derzeit bei den Ländern liegt. Vgl. auch Josef Keinberger und Paul-Anton Krüger: »Europäische Union; Wie Europa sich auf Cyberkrieg einstellen will«, in: *Süddeutsche zeitung* (online), 10.11.2022, https://www.sueddeutsche.de/politik/eu-hack-backs-cyberangriffe-1.5693869 (eingesehen am 18.1.2023).

Joint Unit – sollte durch konkrete nationale Gesetzgebungen flankiert werden, um die Bundesregierung dazu zu ermächtigen, gemeinsam mit den anderen Mitgliedstaaten handlungsfähig zu werden. Die Bündnissolidarität verpflichtet die Bundesregierung, eine aktive defensive Cyberabwehr und die notwenigen Ressourcen im Bereich des *Threat Hunting* und der Lagebilderstellung vorzuhalten.

Insgesamt gilt hier die These, dass Deutschland und Europa auf eine breite Palette von Szenarien vorbereitet sein müssen, um auf den „Konflikt bis hin zu militärischen Auseinandersetzungen und Kooperation bis hin zum Aufbau einer integrierten Friedens- und Sicherheitsordnung“[17] vorbereitet zu sein. Die Herausforderung einer derartigen Cyberaußen- und Sicherheitspolitik besteht darin, die zahlreichen EU und mitgliedstaatlichen Initiativen zu bündeln und den Resilienzanspruch mit der Cyberabwehr in Einklang bringen. Technokratisch gesprochen sollen Synergien zwischen den Initiativen Strategic Compass und Digital Compass hergestellt werden.[18]

Inklusivität durch privat-öffentliche Partnerschaft

Zur Sorgfaltsverantwortung[19] gehört weiterhin, dass Regelsetzungsprozesse ein hohes Maß an Inklusivität aufweisen müssen.[20] Hierzu gehören andere staatliche und nicht-staatliche Akteure. Westliche Staaten versuchten Cyberangriffe bisher vorwiegend mit zwischenstaatlichen Formaten in der VN oder innerhalb regionaler Organisationen wie der OSZE zu beantworten.[21] Zum Portfolio gehörten VN-Formate (VN GGE, OEWG) zur Etablierung freiwilliger Verhaltensnormen. Die VN-Verhandlungen orientieren sich genauso wie diejenigen im Kontext regionaler Organisationen (wie z.B. ASEAN oder Afrikanische Union) an dem Normen- und Zertifizierungsprozess der EU. Im Jahr 2015 wurden 11 Normen für verantwortungsvolles Verhalten im Cyberspace (GGE-Normen) durch die Vereinten Nationen verabschiedet.[22]

[17] Christopher Daase: »Ein freiheitlicher Sicherheitsbegriff für die Nationale Sicherheitsstrategie«, in: PRIF Blog, 27.6.2022, https://blog.prif.org/2022/06/27/ein-freiheitlicher-sicherheitsbegriff-fuer-die-nationale-sicherheitsstrategie/ (eingesehen am 18.1.2023).

[18] Schon in 2020 hat der Außenministerrat den Außenbeauftragten Josep Borrell sowie die EU-Kommission beauftragt, die verschiedenen Stränge zwischen Außen-, Sicherheits- und Verteidigungspolitik zusammenzuführen („to build a forward-looking EU external digital policy“). Digital Partnerships wurden mit Singapur und Japan sowie ein „Trade & Technology Council“ mit Indien ins Leben gerufen. Nicht zuletzt konnte eine „Declaration for the future of the Internet“ von 60 Staaten unterstützt werden, um den Stellenwert von Meinungsfreiheit und Menschenrechten online zu unterstützen.

[19] Christopher Daase, Julian Junk (Hrsg.), »Internationale Schutzverantwortung – Normative Erwartungen und politische Praxis«, in: Sonderheft der *Friedens-Warte - A Journal of International Peace and Organization*, 88 (2013); Hanns W. Maull, *What German Responsibility Means*, in *Security and Human Rights*, 26 (2015), S. 11-24.

[20] Christopher Daase, *Vortrag zum CyberLab*, September 2015.

[21] Annegret Bendiek, Matthias Schulze: »EU-Cybersicherheitspolitik und die Zeitenwende«, in: *Tagesspiegel Background* (online), 23.06.2022, https://background.tagesspiegel.de/cybersecurity/eu-cybersicherheitspolitik-und-die-zeitenwende (eingesehen am 18.1.2023).

[22] Die 77. VN-Vollversammlung im Herbst letzten Jahres hat die Resolution zur Errichtung eines „United Nations Programm of Action to Advance Responsible State Behavior in the Use of Information and Communication Technologies in the Context of Information Security“ (POA) zur Umsetzung dieser Normen verabschiedet. Das POA soll zur Plattform über globale Cybersicherheitsprobleme ausgebaut werden. Parallel laufen die Verhandlungen der „Open Ended Working Group“ (OEWG) weiter bis zu ihrem Mandatsende im Jahr 2025, siehe hierzu näher Wolfgang Kleinwächter: »Ausschuss verabschiedet drei Resolutionen zu Cybersicherheit«, in: *Tagesspiegel Background* (online),

Ein wichtiger Bereich der internationalen Normenbildung ist die Einrichtung eines staatlichen Schwachstellenmanagements am Beispiel des Vulnerabilities Equities Process (VEP).[23] Der GGE-Bericht aus dem Jahr 2015 enthält eine Norm, dass „die Staaten die verantwortungsvolle Meldung von IKT-Schwachstellen fördern und entsprechende Informationen über verfügbare Abhilfemaßnahmen für solche Schwachstellen weitergeben sollten, um potenzielle Bedrohungen für IKT und IKT-abhängige Infrastrukturen zu begrenzen und möglichweise zu beseitigen". Deutschland und die EU haben aber bis dato kein Schwachstellenmanagement eingerichtet. Eine künftige Strategie für Cybersicherheit muss nicht nur diese Normen umsetzen, sondern weitere Sorgfaltspflichten unterstützen.

Schaut man auf die akuten, von Russland gesteuerten Desinformationskampagnen, dann wird ferner die missbräuchliche Nutzung einer marktbeherrschenden Dominanz von Plattformen zu einem sicherheitspolitischen Problem.[24] Nicht nur diesen nicht-staatlichen Akteuren, sondern eben auch den Foren der Internet Governance obliegen Sorgfaltspflichten, um verantwortliches Verhalten im Cyber- und Informationsraum zu gewährleisten. Die Tatsache, dass private Unternehmen wie Starlink, Amazon Webservice oder Microsoft zu Konfliktparteien werden, unterminieren die Glaubwürdigkeit der westlichen Staaten und ihren Einsatz für das humanitäre Völkerrecht und tragen zur Fragmentierung der Internet Governance bei. [25]

Die Cybersicherheitspolitik ist gut beraten, an einem breiten Multistakeholder-Ansatz in enger Absprache mit den Betreibern von Kritischen Infrastrukturen, mit Industrievertreter:innen, der Wissenschaft und Zivilorganisationen festzuhalten. Die Resilienz erstreckt sich über Cyberhygienemaßnahmen, ein Mindestmaß an IT-Grundschutz in der Basisinfrastruktur auf der lokalen Ebene, die Cyberkriminalitätsbekämpfung, Cyberabwehr bis hin zu den vertrauens- und sicherheitsbildenden Maßnahmen in multilateralen Dialogen. Die Inklusivität von Rechtsetzungsprozessen sollte gleichzeitig dort enden, wo privatwirtschaftliche Akteure beginnen, maßgeblichen Einfluss auf gesetzgebende Organe auszuüben.[26]

[23] Alexandra Paulus: Cybernormen: Mit zweierlei Maß, in: Tagesspiegel Background, 20.4.2022, https://background.tagesspiegel.de/cybersecurity/ausschuss-verabschiedet-drei-resolutionen-zu-cybersicherheit (eingesehen am 18.1.2023).

[24] Annegret Bendiek: Integrationspolitische Bedeutung des Digital Service Act (DSA) und Digital Markets Act (DMA)
Digitalmarktregulierung als eines von fünf digitalpolitischen Großprojekten der EU, https://www.swp-berlin.org/publications/products/arbeitspapiere/AP0121_Bendiek_Digital_Service_Act_und_Digital_Markets_Act.pdf (eingesehen am 19.1.2023)

[25] Annegret Bendiek, Matthias Schulze: »Warum EU-Cyberverteidigung vor allem zivile Verteidigung ist«, in: *Tagesspiegel Background* (online), 28.04.2022, https://background.tagesspiegel.de/cybersecurity/warum-eu-cyberverteidigung-vor-allem-zivile-verteidigung-ist (eingesehen am 18.1.2023);

[26] Patrick Beuth: »Bundesregierung hofiert Lobbyisten«, in: *Zeit Online* (online), 10.03.2015, http://www.zeit.de/digital/datenschutz/2015-03/eu-datenschutzgrundverordnung-ministerrat-bundesregierung-lobbyplag (eingesehen am 18.1.2023).

Strategisches Vakuum zwischen Cyberdiplomatie und Cyberverteidigung

Der rechtliche Rahmen der Cybersicherheit wird in Europa durch die Binnenmarkt-Rechtsakte sowie das Soft Law der Gemeinsamen Außen- und Sicherheitspolitik gesetzt (siehe Tabelle).[27] Sanktionen und völkerrechtskonforme Reaktionen nach der Solidaritätsklausel (Art. 222 AEUV) oder der militärischen Beistandsklausel (Art. 42 Abs. 7 EUV) sind als letzte Stufe vorgesehen. Hierfür ist ein effektives Attributionsverfahren auf EU- und internationaler Ebene eine *conditio sine qua non*. Die technische Lokalisierung der IT-Infrastruktur von Angreifern sollte durch eine politische und rechtliche Attribution unterstützt werden.

Die Herausforderung ist, dass eine demokratische und rechtstaatliche Reaktion auf einen Cyberangriff von dessen rechtlicher Bewertung und dem Befund abhängt, ob er der Cyberkriminalitätsbekämpfung, der Cyberabwehr oder der Cyberverteidigung zuzuordnen ist. Ein Festhalten an der Priorität der Strafverfolgung bliebe dem Konzept der „kooperativen Sicherheit" folgend zentral, ist aber im Hinblick auf die staatlich unterstützten, tolerierten und geduldeten Cyberangriffe weiter auszubauen, um ihre abschreckende Wirkung zu gewährleisten.

Mit der CDT soll proportional auf Cyberangriffe bestimmter Intensität reagiert werden. Niedrigschwellige Angriffe führen etwa dazu, dass die EU eine Protestnote veröffentlicht oder eine Botschafter:in einberuft. Schwerwiegendere Angriffe wie WannaCry werden mit Cybersanktionen, also gezielten, restriktiven Maßnahmen wie Kontensperrungen und Einreisebeschränkungen beantwortet. EU-Cyber-Sanktionen sind das schärfste Schwert, das den EU-Staaten zur Verfügung steht. Für eine effektive Gefahrenabwehr ist es gleichwohl oftmals immer noch zu schwach. Die Eskalation, im Falle einer Cyberaktivität einen EU- oder Nato-Bündnisfall auszurufen und sich auf das „Recht auf Selbstverteidigung" zu berufen, wird im Hinblick auf Kollateralschäden richtigerweise gescheut. So bleiben staatlich-motivierte Cyberoperationen oder aber kumulative Cyberangriffe in einem hybriden Kontext unterhalb der Gewaltschwelle heute oftmals unbeantwortet und für Angreifer attraktiv.

[27] Annegret Bendiek, *Die EU als Friedensmacht in der internationalen Cyberdiplomatie*, Berlin: Stiftung Wissenschaft und Politik (SWP), März 2018 (SWP-Aktuell 2018/A 22), https://www.swp-berlin.org/publikation/die-eu-als-friedensmacht-in-der-internationalen-cyberdiplomatie (eingesehen am 18.1.2023) ; Annegret Bendiek und Matthias Schulze, *Attribution als Herausforderung für EU-Cybersanktionen. Eine Analyse von WannaCry, NotPetya, Cloud Hopper, Bundestag-Hack, OVCW*, Berlin: Stiftung Wissenschaft und Politik (SWP), Oktober 2021 (SWP-Studie 2021/S 17), https://www.swp-berlin.org/publikation/attribution-als-herausforderung-fuer-eu-cybersanktionen (eingesehen am 18.1.2023).

Solidaritätsklausel (Art. 222 AEUV) institutionalisieren

Eine Lösung für eine effektivere aber gleichwohl nicht-militärische Antwort auf kumulative Cyberangriffe kann die schnellere und konsequentere Anwendung der Solidaritätsklausel nach Art. 222 AEUV sein. Die rechtlichen und politischen Voraussetzungen für die Anwendung der Solidaritätsklausel auf diese „kumulierte" Cyberbedrohung in Europa sollten geprüft werden. Nach dem AEUV kann die Union bei terroristischen Bedrohungen oder Handlungen (Art. 222 Abs. 1 lit. a AEUV), Naturkatastrophen oder von Menschen verursachten Katastrophen (Art. 222 Abs. 1 lit. b AEUV) "alle ihr zur Verfügung stehenden Mittel, einschließlich der ihr von den Mitgliedstaaten bereitgestellten militärischen Mittel" einsetzen. Art. 222 AEUV begründet keine Zuständigkeit der Union in Verteidigungs- und Sicherheitsfragen, sondern enthält eine Aufgabenzuweisung zu Koordinierungszwecken. Auf der Ebene des Sekundärrechts ist Art. 222 AEUV maßgeblich durch den Beschluss 2014/415/EU des Rates vom 24. Juni 2014 ausgestaltet.

Die aktuelle Bedrohungslage im Cyberspace kann als eine auf Dauer gestellte Katastrophe verstanden werden. Die Intensität kontinuierlicher Angriffe auf private und öffentliche Einrichtungen erzeugt eine Situation struktureller Verunsicherheitlichung, die sich mit dem Begriff des Unfriedens fassen lässt und als Zustand inakzeptabel ist. Gegenwärtig besteht Unsicherheit über die staatliche oder nichtstaatliche Beteiligung an Cybervorfällen, da die Attribution komplex und oftmals nur beschränkt durchgeführt werden kann. Darüber hinaus ist davon auszugehen, dass die Bedrohung durch Cyber-Vorfälle in Zukunft noch weiter ansteigen wird. Daher scheint es überzeugend, beim derzeitigen Stand der Dinge von Art. 222 AEUV Gebrauch zu machen.[28]

Zivile Cyberverteidigung stärken

Die bisherigen Maßnahmen der EU konzentrieren sich auf die zivile Cyberverteidigung und sind von der staatlichen Logik der oben beschriebenen aktiven Cyberverteidigung zu unterscheiden. Die Maßnahmen sind rechtlich in der Gemeinsamen Außen- und Sicherheitspolitik sowie der Gemeinsamen Sicherheits- und Verteidigungspolitik angelegt. So hatte bereits im Juni 2021 der erste EU-Ukraine Cybersicherheitsdialog stattgefunden, der vor allem auf den Kapazitätsaufbau ausgerichtet war. Ferner wurden wesentliche Hilfen von Microsoft, Amazon und Starlink geleistet, um die ukrainische Infrastruktur aufrechtzuerhalten und diverse Angriffe und Wiper-Malware aus Russland abzuwehren. Konkret zeigte sich das etwa im Falle der Zusammenarbeit mit dem slowakischen IT-Unternehmen Eset. Gemeinsam mit ihnen konnte das ukrainische Computer Emergency Response Team (CERT) Anfang April einen Stromausfall verhindern, indem eine Schadsoftware namens Industroyer2 rechtzeitig identifiziert und unschädlich gemacht wurde. Auch die Europäische Union (EU) hat Unterstützung in Sachen Cyberabwehr initiiert: Kurz nach der Invasion entsandte sie ein von Litauen geführtes Cyber-Rapid-Response Team (CRRT), das die Ukraine zur „Bewältigung der wachsenden Cyberbedrohungen unterstützen wird".

CRRTs sollen es den Mitgliedstaaten theoretisch ermöglichen, sich gegenseitig zu unterstützen, um ein höheres Maß an Cyberresilienz zu gewährleisten und gemeinsam auf Cybervorfälle zu reagieren. CRRTs können zur Unterstützung anderer Mitgliedstaaten, EU-Institutionen, GSVP-Operationen sowie von Partnern eingesetzt werden. Die CRRTs werden

[28] Annegret Bendiek, Matthias C. Kettemann, Martin Müller, »EU Cyber Diplomacy and Global Cybersecurity«, in: Tsagourias/Buchan/Franchini (Hrsg.), *The peaceful settlement of Cyber disputes*, Hart Publishing 2023, i.E..

mit einem gemeinsam entwickelten, einsatzfähigen Cyber-Toolkit ausgestattet, mit dem sie Cyberbedrohungen aufspüren, erkennen und entschärfen können. Die Teams führen beispielsweise Schwachstellenbewertungen durch.

Grundsätzlich gilt bei der Entsendung von GSVP-Operationen, dass sie nur außerhalb der EU eingesetzt werden können. Die CRRTs sind weder Battlegroups einer aktiven Cyberverteidigung noch sind sie mit den CERTS – koordiniert durch die Europäische Cybersicherheitsagentur Enisa – zu verwechseln. Sie dienen allein dem verteidigungspolitischen Kapazitätsausbau. Angesicht des längerfristigen Engagements der Europäer zur Unterstützung der Ukraine sowie anderer mittel(süd)osteuropäischen Staaten werden zusätzliche finanzielle, personelle und technische Ressourcen für derartige Einsätze, die über die europäische Friedensfazilität und Verteidigungsfond finanziert werden, nötig sein.

EU Cyberabwehr auf „Resilienz und Abwehr“ einstellen

Was tun, wenn Diplomatie scheitert und Staaten mit Cyberangriffen unterhalb der Schwelle eines bewaffneten Konflikts die staatliche Souveränität anhaltend herausfordern und die Attribution möglich ist? Die einen plädieren für aktive Gegenmaßnahmen, um die Wehrhaftigkeit des Staates zu betonen. Andere plädieren für den Resilienzaufbau und betonen Rechenschaftspflichten, um deeskalierend zu wirken. Die EU Cyber Posture vom 23. Mai 2022 sowie die Kommissionsmitteilung zur Cyberabwehr vom November 2022 verbinden beide Ansätze miteinander. Die EU schlägt damit wichtige strategische Pflöcke für eine „kooperative Sicherheit“ Europas im CIR ein. Die Tabelle zeigt einen Stufenplan der das Ziel verfolgt, die strategische Kluft zwischen Cyberdiplomatie und Cyberverteidigung zu überwinden (Siehe Schaubild).

EU Cyber Posture »Resilience by Denial«

Peace (prevent)	Peace (discourage)	Hybrid (deter)	War (respond)
Defensive (resilience)	Investigative (rule of law enforcement, mutual legal assistance, extradition)	Active Defense (restrictivemeasures, »Gefahr im Verzug«)	Offensive Defense (electroniccombat, »hackbacks«)
Joint Cyber Unit (partly included), CSIRTs-EU, EU CyCLONe, EU INTCEN	***Europol, (Regulation (EU) 2022/991)***	***ENISA, EU INTCEN, EUMS INTEL, (Art. 222 TFEU)***	***Cyber Defense Force (Cyber-Rapid-Response Team CCRT) (42, 6 EUV; 42, 7 EUV, Art. 4 and 5 Nato)***
Behebung von Schwachstellen	**Lokalisierung**	**Attribution**	**Verteidigungsfall**

Quellen: Shulman / Waidner (Tagesspiegel): https://background.tagesspiegel.de/cybersecurity/aktive-cyberabwehr
Whitepaper, das den Artikel weiterentwickelt: https://www.athene-center.de/fileadmin/Downloads/aktive-cyberabwehr.pdf
Mehrere EU-Dokumente, siehe Textbox unten

Rechtsakte:
-Directive (EU) 2022/2555 (NIS 2 Directive)
-Regulation (EU) 2022/2065 (Digital Services Act)
-Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, 2022/0272 (COD)
-Regulation (EU) 2022/1925 (Digital Markets Act)
-Regulation (EU) 2022/991
-Council Regulation (EU) 2019/796
-Council Decision (CFSP) 2019/797
-Regulation (EU) 2019/881 (Cybersecurity Act)
-Charter of Fundamental Rights of the European Union, 2012/C 326/02
-Treaty on the Functioning of the European Union (TFEU), Art. 222
-The North Atlantic Treaty (NATO), 4 April 1949

Soft Law:
-European Commission, Joint communication to the European Parliament and the Council EU Policy on Cyber Defence, JOIN(2022) 49 final
-European Commission, Code of Practice on Disinformation, 16 June 2022
-Council Conclusions on the development of the European Union's cyber posture, 9364/22
-Council Conclusions on the EU's cybersecurity strategy, 6722/21
-European Council conclusions on the MFF, climate change, disinformation and hybrid threats, external relations, enlargement and the European Semester, 20 June 2019, EUCO 9/19

Berichte, Projekte, Toolboxen von EU-Organe/Agenturen:
-European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2022, ENISA Threat Landscape 2021, ENISA Threat Landscape 2020
-Permanent Structured Cooperation (PESCO), Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT) projects
- European External Action Service, Framework for a joint EU diplomatic response to malicious cyber activities "cyber diplomacy toolbox“, 2019

Die Mitgliedstaaten haben sich auf vier Stufen der Cyberabwehr mit dem Ziel verständigt, "to increase the possibility to mobilise, on a case-by-case basis, all available tools, internal and external, to prevent, discourage, deter and respond to cyberattacks, implementing these in a swift, effective, gradual, targeted and sustained approach based on long-term strategic engagement."[29] Die entsprechende Kommissionsmitteilung zur Cyberabwehr wurde im November 2022 vorgelegt. Bisher stehen Fragen der Interoperabilität und des Informationsaustauschs zwischen den militärischen Computer-Notfallteams (milCERT) im Vordergrund. Dem Aktionsplan der EU zufolge sollen die EU-Staaten über das volle Spektrum bis hin zur Fähigkeit zur „aktiven Verteidigung" verfügen. Bei der defensiven Cyberabwehr unterscheidet Matthias Schulze nach *defensiv/passiv reaktiven* Maßnahmen, beispielsweise durch Cyberkriminalitätsbekämpfung im Rahmen der Strafverfolgung, user management patching auf der einen Seite und *pro-aktives threat hunting* durch Open Source Intelligence auf der anderen Seite. Im offensiven Bereich gibt es die aktive Cyberabwehr, DoS, Disruption, InfoOps, Sabotage auf der einen Seite und persistent engagement also Vorwärtsverteidigung oder die Vergeltung durch „Hackback" als eine militärische aktive Cyberabwehr-Maßnahme auf der anderen Seite.[30]

Shulmann und Waidner (2022) zählen als konkrete Beispiele der nicht-militärischen Cyberabwehr auf: Die Manipulation des Internetverkehrs, die Deaktivierung von Botnetzen und die Übernahme einer angreifenden Server-Infrastruktur oder von Internet-Domänen durch Strafverfolgungsbehörden, so dass die Angreifer den Zugriff auf ihre Infrastruktur verlieren. Hierzu zählt auch die Identifikation und Deaktivierung von sogenannten Schläfern in IT-Systemen und die Intervention auf angreifende IT-Infrastrukturen außerhalb der Systeme der angegriffenen Opfer.[31] Hackbacks dürften nach diesem Verständnis allein im Rahmen des Gewaltmonopol des Staates und in europäischer Absprache ausgeführt werden.[32]

Das Problem der strategischen Fähigkeitslücke zur Reaktion auf Cyberangriffe unterhalb der Gewaltschwelle bleibt institutionell und rechtlich weiterhin bestehen. Im Kontinuum zwischen Frieden und Krieg werden Cyberangriffe dann als hybrid eingestuft, wenn Angriffe auf Infrastrukturen zielgerichtet kumulativ oder mit der böswilligen Absicht zur Manipulation oder Störung ausgerichtet werden. Zur Feststellung ist nach wie vor die Einstimmigkeit im Rat gefordert. Qualifizierte Mehrheitsentscheidungen würden die Prozesse beschleunigen.[33]

[29] Punkt 26. Siehe: Rat der EU, *Council conclusions on the development of the European Union's cyber Posture - Council conclusions approved by the Council at its meeting on 23 May 2022*, 23.5.2022, https://www.consilium.europa.eu/media/56358/st09364-en22.pdf (eingesehen am 18.1.2023).
[30] Matthias Schulze, *Militärische Cyber-Operationen - Nutzen, Limitierungen und Lehren für Deutschland*, Berlin: Stiftung Wissenschaft und Politik (SWP), August 2020 (SWP-Studie 2020/S 15), https://www.swp-berlin.org/publikation/militaerische-cyber-operationen (eingesehen am 18.1.2023).
[31] Haya Shulman, Michael Waidner, Aktive Cyberabwehr, in: Tagesspiegel Background (online), 13.10.2022, https://background.tagesspiegel.de/cybersecurity/aktive-cyberabwehr (eingesehen am 18.1.2023). Whitepaper, das den Artikel weiterentwickelt: Haya Shulman, Michael Waidner, Aktive Cyberabwehr, ATHENE Whitepaper, 10.10.2022, https://www.athene-center.de/fileadmin/Downloads/aktive-cyberabwehr.pdf (eingesehen am 18.1.2023).
[32] Siehe zur durchaus überzeugenden kritischen Betrachtung von Hackbacks Florian Deutsch und Tobias Eggendorfer, IT-Grundschutz mit staatlicher IT-Security-Schutzpflicht; Hackbach, Update IT-Sicherheitsrecht 2021/2022, 5.12.2022
[33] Annegret Bendiek, Raphael Bossong: Hybride Bedrohungen, Berlin: Stiftung Wissenschaft und Politik (SWP), Juni 2022 (SWP-Aktuell 2022/A 40), https://www.swp-berlin.org/publikation/hybride-bedrohungen-vom-strategischen-kompass-zur-nationalen-sicherheitsstrategie (eingesehen am 18.1.2023).

Hybrid markiert im EU-Denken die Grauzone zwischen Krieg und Frieden. Wann aber wird die Schwelle überschritten, die die Beistandsklausel in der EU oder den Nato-Bündnisfall auslöst? Aktuell gilt im Cyberraum das Konzept der strategischen Doppeldeutigkeit. Die Nato hat festgelegt, dass ein Cyberangriff den Artikel 5 des Nato-Vertrages, also den Bündnisfall, auslösen kann und hat – wie bei konventionellen Angriffen – bewusst offengelassen, wann genau dieser Fall eintritt. In der EU ließe sich der Artikel 222 AEUV oder die militärische Beistandsklausel nach Artikel 42.7 EUV aktivieren. Diese Logik verkennt jedoch, dass es einen „großen Cyberangriff" nicht braucht, da die vielen kleinen „Cyber-Nadelstiche" kumulativ ausreichend Schaden anrichten können.

Die Europäer stehen angesichts der hohen Kosten für die Wirtschaft[34] unter dem Zwang, eine angemessene Reaktion auf Cyberangriffe unterhalb der Gewaltschwelle zu finden. Zur wehrhaften Demokratie gehöre es, so der BDI, dass Interventionen in fremden Netzen im Rahmen der völkerrechtlichen Bestimmungen in engen Grenzen nicht ausgeschlossen sein dürften, wenn etwa ein unmittelbar bevorstehender Angriff abzuwehren sei.[35] Die Gefahr ist sonst groß, dass Konzerne und Plattformen die aktive Cyberabwehr in die eigene Hand nehmen und eine faktische Privatisierung internationaler Konflikte befördern. In der aktiven Cyberabwehr muss es daher darum gehen, den Instrumentenkasten über die bloße Resilienzbeförderung hin auszuweiten und die aktive Cyberabwehr zu inkludieren. Hierzu gehören drei Kategorien von Maßnahmen:

Unter dem Begriff der Entmutigung lässt sich eine europäische Cyberabwehr verstehen, die zum Ziel hat, das Angreifer-System zu deaktivieren, um eine Cyberattacke zu beenden. Etwaig gestohlene Daten können vom System des Angreifers gelöscht werden. Ziel sollte es dabei immer sein, durch die aktive Cybergegenmaßnahme Täter zu identifizieren und strafrechtlich zu verfolgen.[36]
Die nächst-schärfere Handlungsmöglichkeit fällt unter den Begriff der Abschreckung und beinhaltet weitergehende Maßnahmen wie die Zerstörung von Servern im Ausland, von denen Angriffe ausgehen. Hierfür wäre es sinnvoll, IT-Sicherheitsunternehmen in Europa für die Cyberabwehr zu zertifizieren und die EU-Cybersicherheitsagentur ENISA sowie Europol mit einer operativen Kompetenz auszustatten. Als Rechtsgrundlage wäre hier gegebenenfalls auf Art. 222 AEUV, aber eben nicht auf die militärische Beistandsklausel, zurückzugreifen. Parlamentarische Rechenschaftspflichten müssen dabei gelten.[37]
Militärische Gewalt – also auch eine offensive Cyberverteidigung inklusive Hackbacks – wäre nach der Cyber Diplomacy Toolbox nur zur Selbstverteidigung sowie europäisch und

[34] Schäden liegen bei rund 203 Milliarden Euro, 84 Prozent aller Unternehmen waren betroffen. Bitkom, »203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen 2022«, 31.8.22, https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022 (eingesehen am 18.1.2023).
[35] BDI Positionspapier zur aktiven Cyberabwehr siehe https://bdi.eu/artikel/news/deutschland-muss-effiziente-staatliche-cyberabwehr-schaffen/ oder https://bdi.eu/artikel/news/digitale-gegenangriffe-sollte-der-staat-zurueckhacken-duerfen/ (eingesehen am 19.1.2023)
[36] Hierzu siehe Haya Shulmann und Michael Waidner Aktive Cyberabwehr, in: *Tagesspiegel Background* (online), 13.10.2022, https://background.tagesspiegel.de/cybersecurity/aktive-cyberabwehr (eingesehen am 18.1.2023). auch erschienen in *Frankfurter Allgemeinen Zeitung*, 25.4.2022.
[37] Vgl. hierzu die kanadische Parlamentskontrolle: National Security and Intelligence Committee of Parliamentarians, *Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack. Submitted to the Prime Minister on August 11, 2021 pursuant to subsection 21(1) of the National Security and Intelligence Committee of Parliamentarians Act (Revised version pursuant to subsection 21(5) of the NSICOP Act),* 14.2.2022, https://www.nsicop-cpsnr.ca/reports/rp-2022-02-14/2022-cyber-attack-framework-report-en.pdf (eingesehen am 18.1.2023).

parlamentarisch abgestimmt vertretbar. Äußerst heikel wäre es, Cyberattacken mit automatischen Gegenangriffen und digitalen Vergeltungsschlägen zu beantworten. Diese Maßnahme kann nur die ultima ratio sein. Die offensive Cyberverteidigung birgt die Gefahr eines digitalen Rüstungswettlaufs (etwa durch Advanced Persistent Threats, APTs) mit nur schwer kalkulierbaren Konsequenzen für verwundbare kritische Infrastrukturen.

Eine erfolgversprechende Cybersicherheitsstrategie sollte daher nicht durch einen bloßen Paradigmenwechsel von einer defensiven hin zu einer aktiven Cyberabwehr neu ausgerichtet werden. Das wäre ein kontraproduktives Signal im Rahmen der vertrauens- und sicherheitsbildenden Maßnahmen der Cyberdiplomatie. Es braucht vielmehr ein gestaffeltes System unterschiedlicher Cyberabwehrmaßnahmen und damit die Möglichkeit, jeweils situationsangemessen reagieren zu können.

Um das für eine Umsetzung einer aktiven defensiven Strategie notwendige Klima der Sicherheit und des Vertrauens im Cyberraum zu erreichen, müssen zudem - und trotz widriger Umstände - weiterhin vertrauens- und sicherheitsbildende Maßnahmen in den UN, OSZE und Europarat verhandelt sowie internationale Standards für die Zulassung von Hard- und Software beschlossen werden. Gemeinsame Normen für staatliches Verhalten im Cyberraum sind und bleiben von zentraler Bedeutung dafür, dass der aktuelle Unfrieden nicht zu einem Krieg ausufert und damit ein einheitliches Verständnis von völkerrechtlichen Regeln weiter verfolgt werden kann. Nur so kann deutsche Handlungsfähigkeit in Europa in der Cybersicherheit gelingen.

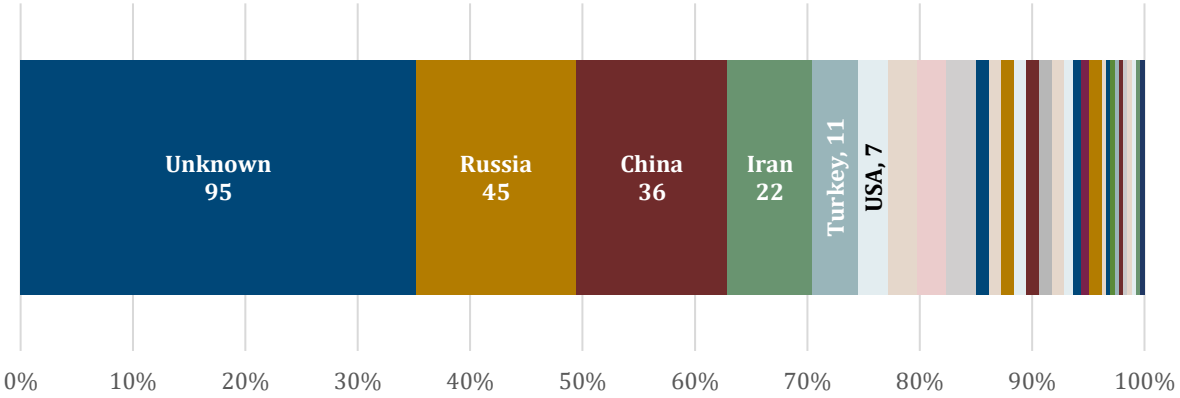
Annex

Table 1: Most targeted EU member states, 2001-2022

Member State	Count cyber incidents	% out of all incidents targeting the EU (N=279)	% when excluding incidents targeting exclusively the UK (N=214)
UK (while Member State)	82	29%	
Germany	51	18%	24%
France	40	14%	19%
Italy	27	10%	13%
Belgium	19	7%	9%
Spain	18	6%	8%
Netherlands	14	5%	7%
Poland	12	4%	6%
Austria	11	4%	5%
Sweden	11	4%	5%
EU institutions	10	4%	5%
All other EU member states combined (except Malta and Slovenia)	73	26%	34%

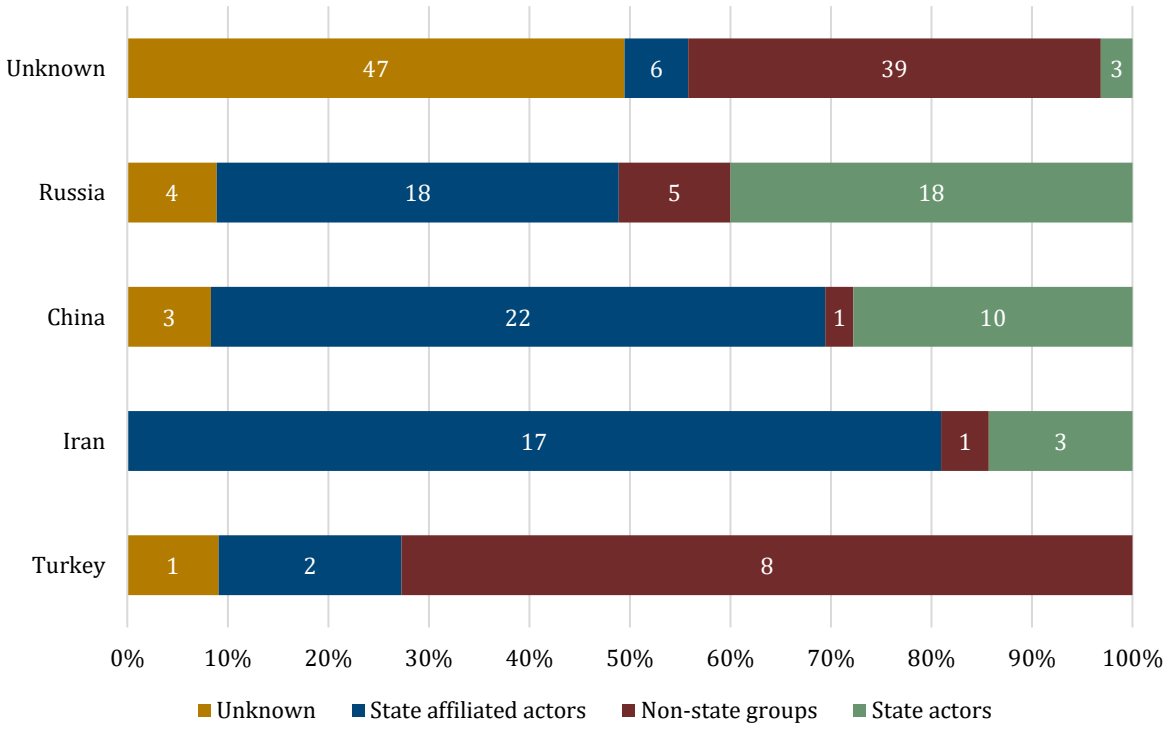
Quelle: https://eurepoc.eu/de. For detailed information on the data collection methodology see https://eurepoc.eu/methodology.

Table 2: Top attributed countries of origin of cyber incidents targeting the EU, 2001-2022 (N=279)



Quelle: https://eurepoc.eu/de. For detailed information on the data collection methodology see https://eurepoc.eu/methodology.

Table 3: Type of Actors targeting EU member states, 2001-2022 (N=279)



Quelle: https://eurepoc.eu/de. For detailed information on the data collection methodology see https://eurepoc.eu/methodology.

Dr. Annegret Bendiek ist Stellvertretende Leitung der Forschungsgruppe EU/Europa.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3–4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org