SWP

SWP-Aktuell

NR. 49 JULI 2023

# Paradigmenwechsel in der europäischen Cyberabwehr

**Für den Sprung von der reaktiven zur aktiven Abwehr braucht es Transparenz über die normativen Grenzen und Grundlagen**

*Annegret Bendiek / Jakob Bund*

**Für EU-Staaten, die in Abstimmung mit Verbündeten eine aktive Cyberabwehr betreiben wollen, sind die rechtlichen und politischen Befugnisse noch nicht ausreichend ausbuchstabiert worden. Im Sinne des Prinzips der Sorgfaltsverantwortung sind die EU und ihre Mitgliedstaaten in der Pflicht, die normativen Grundlagen für einen Einsatz aktiver Cyberabwehrmaßnahmen festzulegen, bevor diese ergriffen werden. Eine Militarisierung des Cyber- und Informationsraums gilt es zu vermeiden.**

Seit November 2022 gehen die australische Bundespolizei und das Australian Signals Directorate (ASD) in einem neu geschaffenen Einsatzverbund (JSO) gegen Cyberkriminelle vor. Zuvor hatten Hacker die größte landesweite australische Krankenkasse Medibank und einen der führenden Telekommunikationsanbieter des Landes, Optus, angegriffen. Im großen Maßstab wurden dabei persönliche und sensible Gesundheitsdaten von rund 40 Prozent der australischen Bevölkerung gestohlen und veröffentlicht. Im Unterschied zu klassischen Strafverfolgungsmethoden der Polizei reagiert die hundertköpfige JSO nicht mehr erst, nachdem Verbrechen begangen wurden, sondern versucht Cyberkriminelle bereits vorher an ihren Taten zu hindern.

Ereignisse wie die in Australien verdeutlichen, wie zunehmend wichtig es ist, Cyberangriffe zu entschärfen und international zu kooperieren, um Cyberkriminelle zur Rechenschaft zu ziehen. Die jüngsten Entwicklungen standen auch im Hintergrund der Beratungen über die Nationale Sicherheitsstrategie, in deren Rahmen neben Überlegungen zur Stärkung der Resilienz auch über aktive Cyberabwehrmaßnahmen nachgedacht wurde, um Schäden durch Cyberangriffe schon im Vorfeld zu verhindern. Dafür wäre eine Grundgesetzänderung erforderlich, die die Bundesregierung auch anstrebt. In der im Juni 2023 vorgestellten Nationalen Sicherheitsstrategie bekennt sie sich dazu, die bestehenden Befugnisse zur Cyberabwehr und die dafür erforderlichen Fähigkeiten zu überprüfen. Anerkannte Rechtsprinzipien der Sorgfaltsverantwortung, der Verhältnismäßigkeit von Gegenmaßnahmen und internationale Normen zum verantwortlichen Staatenverhalten im Cyberraum sind

Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

hierbei handlungsleitend. Hackbacks als Mittel der Cyberabwehr schließt die Bundesregierung dem Dokument zufolge aus. Die deutsche Cyberbotschafterin Regine Grienberger weist nicht ohne Grund auf die hohen rechtlichen Hürden eines proaktiven Einschreitens gegen Gefahren aus dem Cyberraum hin. Bedingung dafür ist die verlässliche und belastbare Zuordnung von Angriffen, was wiederum eine Identifizierung des Angreifers in technischer, politischer und rechtlicher Hinsicht voraussetzt. Die Durchsetzung des bestehenden Rechts hängt zwangsläufig auch davon ab, ob die dafür notwendigen Fähigkeiten zur Cyberkriminalitätsbekämpfung und zur Strafverfolgung vorhanden sind.

Das 2022 beschlossene neue strategische Konzept der Nato beschreibt den Cyberraum als fortlaufend umkämpft. David van Weel, der Stellvertretende Generalsekretär für neue Sicherheitsherausforderungen, machte vor kurzem deutlich, dass diese Einschätzung unabhängig davon gelte, ob man sich in einem bewaffneten Konfliktaustrag befindet. Im Rahmen des Bündnisgipfels in Vilnius stellten sich die Nato-Mitgliedstaaten im Juli daher hinter ein neues Cyberverteidigungskonzept mit dem Ziel, zu jeder Zeit — sei es in Friedens-, Krisen- oder Konfliktsituationen — eine zivil-militärische Zusammenarbeit zu gewährleisten, auch unter Einbeziehung privatwirtschaftlicher Akteure.

Aktuelle Überlegungen in der Allianz, auf EU-Ebene, aber auch in einigen EU-Staaten bewegen sich weg von einem reaktiven Verständnis der Cyberabwehr und hin zu einem proaktiven Vorgehen bei Gefahrenlage bzw. zu einer aktiven Cyberverteidigung im militärischen Bereich. Die definitorische und exekutive Hoheit darüber, welche Maßnahmen der (in die Sphäre der zivilen Strafverfolgung fallenden) aktiven Cyberabwehr und welche der (militärischen) aktiven Cyberverteidigung zuzuordnen sind, liegt bei den Mitgliedstaaten. Zeichnet sich also aktuell ein Paradigmenwechsel im europäischen Umgang mit Cyberbedrohungen ab — von einem reaktiven hin zu einem verstärkt proaktiven Abwehransatz? Der Blick auf die bisherige Staatenpraxis lässt Rückschlüsse darauf zu, in welchen Fragen Europa zu einer Position finden muss, denn enge Partner wie die USA, das Vereinigte Königreich, Australien oder Japan zeigen bereits, welche aktiven Einwirkmittel zur Gefahrenabwehr im Einsatz sind. Die Staatenpraxis muss grundsätzlich dem Prinzip der Sorgfaltsverantwortung Rechnung tragen.

## Unklare Definitionen

In der im November 2022 vorgelegten Mitteilung über eine EU-Cyberabwehrpolitik fordert die Europäische Kommission die Mitgliedstaaten dazu auf, Fähigkeiten im Bereich der Cyberabwehr zu entwickeln, und zwar innerhalb des gesamten Spektrums von defensiven bis hin zu aktiven Maßnahmen. In den Schlussfolgerungen des Rates zur Cyberabwehrpolitik vom Mai 2023 wird zudem die Bedeutung der militärisch-zivilen Zusammenarbeit betont. Fähigkeiten zur Früherkennung, Abwehr und Abschreckung von Cyberbedrohungen müssten das Portfolio der Verteidigungsinstrumente ergänzen. Der Rat unterstreicht auch, dass es sich hierbei um nationalstaatliche Kompetenzen handelt, der Einsatz von Cyberabwehrmaßnahmen allein von den Regierungen der Mitgliedstaaten verantwortet werden muss und entsprechende Akte defensiven Charakter haben. Welcher Techniken und Vorgehensweisen sich eine aktive Cyberabwehr bzw. aktive Cyberverteidigung bedienen soll, wird in den Schlussfolgerungen offengelassen. Stattdessen werden die Mitgliedstaaten aufgefordert, selbst Ziele anzugeben und Maßnahmen auf dem Weg dorthin zu umreißen. Die bisher in Policy Papers, Interviews und durch spärliche Beispiele aus der Staatenpraxis dokumentierten Methoden der aktiven Cyberabwehr umfassen unter anderem die Ableitung schädlichen Datenverkehrs, die Deaktivierung von Botnetzen und die Übernahme von Servern oder Internet-Domänen durch Strafverfolgungsbehörden, so dass die Angreifer den Zugriff

auf ihre Infrastruktur verlieren. Zum Abwehrinstrumentarium zählen darüber hinaus die Identifikation und Deaktivierung von Schadsoftware in IT-Systemen und die Intervention in angreifende IT-Infrastrukturen außerhalb der Systeme der betroffenen Opfer. In den Bereich der aktiven Cyberverteidigung fallen des Weiteren die Manipulation ausländischer Medien, die elektronische (Zer-)Störung von Servern und die Unterbindung von Datenverkehr im Ausland.

## Das Prinzip der Sorgfaltsverantwortung

Die Bundesregierung, die Mitgliedstaaten der EU und die Union orientieren sich bei der Umsetzung ihrer Cybersicherheitsstrategien prinzipiell am Gebot der »Due Diligence«. Diese Norm verpflichtet Staaten, in Friedenszeiten dafür zu sorgen, dass von ihrem Territorium keine Handlungen ausgehen, welche die Rechte anderer Staaten verletzen. Alle Cybersicherheitsstrategien der Union weisen darauf hin, dass der Schutz von Computersystemen und Netzwerken für einen modernen, hochtechnologisierten und digitalisierten Industriestaat essentiell ist. Deshalb sollen die Resilienz der Infrastruktur, die Fähigkeit zur Abwehr und Aufklärung von (auch staatlich gelenkter) Cyberkriminalität und die Sensibilität für Desinformationskampagnen gestärkt werden.

Die EU und Deutschland verfolgen eine auf internationalen Übereinkünften aufbauende defensiv ausgerichtete Cybersicherheitsstrategie. Das Konzept der Sorgfaltsverantwortung steht grundsätzlich nicht im Widerspruch zur Cyberabwehr. Es schließt in jedem Fall eine Art politischer Regulierung ein. In gegnerische Cyberoperationen einzugreifen, stellt die staatliche Sorgfaltspflicht in Friedenszeiten vor neue Herausforderungen, wenngleich derartige Aktionen im Sinne einer Abwehr von »Gefahr im Verzug« begründbar sein mögen. Internationale Normen bilden einen Ankerpunkt für die Ausgestaltung aktiver Cyberabwehrmaßnahmen. Eine proaktive Cyberabwehr erfordert demzufolge die Offenlegung von normverletzendem Verhalten, um in vergleichbaren Fällen rechtfertigen zu können, dass der Eingriff zur Gefahrenabwehr bzw. im Rahmen einer Gefahrenlage erfolgte. Deutlich wird dies unter anderem an der wiederholt unter Beweis gestellten Bereitschaft der USA, nachrichtendienstliche Erkenntnisse für Anklageerhebungen gegen Bedrohungsakteure zu nutzen und öffentlich zu machen, selbst wenn sich die Verantwortlichen mit diesen Rechtsmitteln absehbar nicht belangen lassen.

Die Preisgabe dieser Informationen signalisiert die Verbindlichkeit von Attributionsbemühungen gegenüber Verbündeten. Dieses Vorgehen dient dem Aufbau einer internationalen »Koalition für Attribution« unter EU- und Nato-Staaten sowie internationalen Wertepartnern. Auf diese Weise werden Grenzen von verantwortlichem Verhalten markiert, was wiederum eine Handlungsgrundlage bildet für das Unterbinden von Aktionen, die diese Grenzen überschreiten. Ein solches proaktives Einwirken auf Cyberbedrohungen wirft unter anderem die Frage auf, in welchem Umfang es für Staaten opportun ist, ihre eigenen Bemühungen, Cyberangriffe zu unterbinden, in ihren öffentlichen Lagebeschreibungen darzulegen, um die internationalen Normen und Rechtsgrundsätze zu stärken. Denn gleichzeitig besteht das Risiko, dass sie es ihren Sicherheitsbehörden erschweren, ihre Aufgaben zu erfüllen.

## Die Staatenpraxis aktiver Cyberabwehr bzw. -verteidigung

Das US-Verteidigungsministerium gab 2018 einen Wechsel in seiner Cyberabwehrpolitik bekannt. Unter der Maxime »Defend Forward« will es böswillige Hackeraktionen künftig mit einer vorwärtsgerichteten und proaktiven Strategie bekämpfen. Das US Cyber Command, für das diese Doktrin seither handlungsleitend ist, setzt darauf, Bedrohungsaktivitäten möglichst nah an deren Ursprung zu begegnen, um Schaden

frühzeitig abzuwenden und feindlich gesinnte Akteure zu blockieren. Es verfolgt diesen Ansatz durch »persistent engagement« — dem gezielten Stoppen von Cyberbedrohungen und der Beeinträchtigung gegnerischer Fähigkeiten —, um Angreifer mit Kosten zu belegen und auf Verhaltensweisen einzuwirken, die durch andere Instrumente schwer oder nur nachträglich beeinflusst werden können. In der im März veröffentlichten Nationalen Cybersicherheitsstrategie wurde dieser Ansatz noch weiterentwickelt. Er bildet nun eine eigene Säule der Störung und Schwächung von Bedrohungsakteuren. Nach Einschätzung von General Paul Nakasone, US-Cyberkommandant und Direktor der NSA, baut die zwei Monate später beschlossene und als geheim eingestufte neue Cyberstrategie des US-Verteidigungsministeriums auf dem 2018 vorgenommenen Kurswechsel auf.

Grundsätzlich ist wenig über den Einsatz aktiver Abwehrmaßnahmen bekannt. Die Vereinigten Staaten zum Beispiel haben bisher nur wenige operationelle Details öffentlich gemacht. Der erste bekannte Fall eines aktiven Einschreitens des US-Cyberkommandos zielte im Herbst 2020 darauf ab, das Botnet Trickbot von Command-and-Control-Servern zu trennen, um einer eventuellen Ransomware-Kampagne im Vorfeld der US-Wahlen entgegenzuwirken.

Die Cyberspace Solarium Commission, ein Gremium, das der US-Kongress zur Erarbeitung eines Konzepts für die Verteidigung gegen gravierende Cyberangriffe eingesetzt hat, schlug 2020 eine erweiterte Auslegung von »Defend Forward« vor. Danach erfordert eine konsequente Umsetzung der Doktrin nicht mehr länger nur den Rückgriff auf rein militärische, sondern den auf alle staatlichen Instrumente (Diplomatie, Regulierungskompetenzen etc.), insbesondere um Erkenntnisse über Bedrohungsaktivitäten zugänglich zu machen und darüber die eigene Resilienz zu steigern. Die Auslegung der Kommission zeigt deutlich, dass eine »Defend Forward«-Politik auch daran zu messen sein wird, ob und in welchem Umfang sie zur Stärkung der internationalen Verhaltensnormen beiträgt.

Um eine Verhaltensänderung des Gegners herbeizuführen, reicht es nicht aus, dessen Kampagnen zu kontern. Ebenso wichtig ist es, dem Angreifer die Fähigkeit zur Abwehrbereitschaft und die Entschlossenheit dazu zu signalisieren. Nach Angaben von General Nakasone haben die USA als Reaktion auf die russische Invasion im Frühjahr 2022 neben defensiven auch offensive Cyberoperationen zur Unterstützung der Ukraine durchgeführt.

Aber auch andere Staaten beabsichtigen, operative Einwirkungsmöglichkeiten zu nutzen, um böswillige Cyberattacken aktiv zu unterbinden. Neben der erwähnten Einsetzung der australischen JSO zur Cyberabwehr gab die australische Regierung zu Beginn des Jahres bekannt, dass sie die Investitionen in offensive Cyberabwehrkapazitäten verdreifachen wird.

Das Vereinigte Königreich hat seit dem russischen Angriff auf die Ukraine im Februar 2022 eine Reihe von Hilfsmaßnahmen öffentlich gemacht. Teil des Programms sind die Unterstützung kritischer Infrastrukturen und ukrainischer Regierungsstellen im Umgang mit Cybervorfällen, die Abwendung von Sabotageversuchen gegen die Stromversorgung, forensische Aufklärung, die Bereitstellung von Sicherheitslösungen und die Einschränkung von Angriffszugängen, um Hochwertziele vor zukünftigen Attacken zu schützen. Unter den EU-Mitgliedstaaten sind diese Hilfsleistungen nicht uneingeschränkt konsensfähig. Auch werden nicht alle dazu erforderlichen technischen Cyberfähigkeiten im gleichen Umfang von allen Mitgliedstaaten vorgehalten. Die Widerstandsfähigkeit der Ukraine gegenüber russischen Angriffsversuchen deutet indes darauf hin, dass das Land hier ebenfalls von vorausschauenden Cyberabwehrmaßnahmen profitiert hat. Kiew stützte sich bei seiner proaktiven Kalibrierung von Abwehranstrengungen unter anderem auf Ergebnisse von Hunt-Forward-Operationen (HFOs), die das US-Cyberkommando gemeinsam mit ukrainischen Partnern zwischen Dezember 2021 und März 2022 durchgeführt hat.

## Hunt Forward als aktive Gefahrenabwehr

In der Auslegung des US-Cyberkommandos sind HFOs defensive Bemühungen, bei denen interne Schutzteams auf Ersuchen befreundeter Staaten vor Ort Netzwerke auf Schadsoftware durchforsten, um etwaige neue Angriffsmuster frühzeitig zu erkennen und Sicherheitslücken und Hintertüren zu schließen. Der entscheidende Vorteil der Hunt-Forward-Methode ist nach Ansicht von General Nakasone, dass Bedrohungsakteure und ihre Werkzeuge schon im Vorfeld aufgedeckt werden können. Bisher hat das US-Cyberkommando über 47 HFOs mit mindestens 22 Ländern durchgeführt. Partner waren unter anderem mehrere EU-Mitgliedstaaten und Nato-Verbündete, darunter Albanien, Montenegro und Nordmazedonien. Kurz nach Russlands Invasion der Ukraine im Februar 2022 wurden Teams nach Litauen und später Lettland entsandt. Europäische Partner haben also nicht nur bereits bilateral an HFOs mitgewirkt, sondern fordern diese eigenständig an.

Für Deutschland und andere EU-Staaten bieten sich dabei grundsätzlich drei voneinander unabhängige Möglichkeiten, um sich zu beteiligen. Der gemeinsame Einsatz in eigenen Netzen erlaubt es, bei der Aufklärung von Angriffsaktivitäten zu einem Grad auf analytische Fähigkeiten internationaler Partner zurückzugreifen, der über einen bloßen Informationsaustausch nicht zu erreichen wäre.

In umgekehrter Richtung kann ein solcher Einsatz zur Unterstützung internationaler Partner neue Erkenntnisse über Taktiken und Angriffswerkzeuge liefern, die in Erprobung sind. Dieses Wissen erweitert die Möglichkeiten, sich auf Angriffsversuche und, im Idealfall, auf deren Vereitelung vorzubereiten, noch bevor diese Schaden anrichten können.

Europäische Staaten stellen sich zunehmend die Frage, ob der Aufbau von Fähigkeiten zur Vorausschau ähnliche Programme unter eigener Führung verlangt. Ohne dass die Mitgliedstaaten verpflichtet wären, sich unmittelbar zu beteiligen, ließe sich ein europäisches Projekt aufsetzen mit dem Ziel, eigenständige Fähigkeiten vorzuhalten und für den Bedarfsfall die Einsatzmodalitäten abgeklärt zu haben. Die Ständige Strukturierte Zusammenarbeit (SSZ) der EU bietet einen geeigneten Rahmen, innerhalb dessen die Mitgliedstaaten in HFO investieren könnten.

## Europäische Reaktionen

Eine strategische Neuausrichtung auf eine aktive Cyberabwehr ist unter den Mitgliedstaaten politisch umstritten. Der Leiter des französischen Cyberdefense-Kommandos, General Aymeric Bonnemaison, brachte in einer Anhörung der Nationalversammlung im Dezember 2022 entsprechende Vorbehalte zum Ausdruck. Selbst defensive Einsätze, die dazu dienen, gegnerische Aktionen in verbündeten Netzwerken auszukundschaften, seien aggressiv. Diese Unterstützung vor allem osteuropäischer Länder stelle für diese zwar eine Form der Beruhigung dar, setze aber einen weitreichenden Eingriff in die betreffenden Netze voraus und erfordere eine starke operative Präsenz. Unabdingbar seien ein begleitendes Engagement der Diplomatie und der Aufbau von Kapazitäten vor Ort. Nach Auffassung des französischen Cyberkommandanten wäre eine europäische Cyber-Eingreifgruppe, die wie die US-amerikanische Hilfsangebote macht, aber durchaus denkbar. Solche Unterstützungsleistungen sollten sich an Länder richten, die längerfristigen Sicherheitsherausforderungen begegnen müssen und in denen der Einsatzzeitraum somit nicht überschaubar ist. Diese Ausgangslage könne einen vorübergehend tiefgreifenden Zugriff auf sensible Netze verlangen.

Auf niedrigschwelliger Ebene bieten EU Cyber Rapid Response Teams (EU-CRRTs) bereits jetzt Drittstaaten Unterstützung an bei der Beobachtung und Bekämpfung von Cyberbedrohungen. Ein Zusammenschluss von acht Mitgliedstaaten hat im Rahmen der SSZ entsprechende Fähigkeiten aufgebaut. Die EU-CRRTs, die acht bis zwölf

nationale Experten und Expertinnen umfassen, waren die ersten einsatzfähigen Einheiten im Rahmen der SSZ. Über die Mobilisierung entscheiden allein die am SSZ-Projekt beteiligten Staaten. Obwohl seit 2019 einsatzbereit, wurde ein EU-CRRT zum ersten Mal auf Anfrage der Ukraine im Februar 2022, kurz vor Beginn des russischen Angriffskriegs, aktiviert. Nach anfänglichen Bestrebungen, die Kräfte sowohl vor Ort als auch remote einzusetzen, machte die russische Invasion einen Kurswechsel hin zu einem vollständig virtuellen Support nötig. Die Entsendung einer weiteren Truppe in die Republik Moldau befindet sich in Vorbereitung. Auch hat die EU im Rahmen der Europäischen Friedensfazilität im Dezember 2022 Ausrüstung für ein Cyberlabor an die ukrainischen Streitkräfte geliefert. Das Labor wird als Trainingsumgebung dienen, in der durch Echtzeitsimulationen weitere Fähigkeiten aufgebaut werden, um Versuche des Eindringens in ukrainische Netzwerke entdecken, nachvollziehen und abwehren zu können.

## Normative Grundlagen fehlen

Die bisherige Staatenpraxis zeigt, dass es durchaus gute Gründe gibt, bei einer Gefahrenlage eine aktive Cyberabwehr zu betreiben. Die Vereinigten Staaten, das Vereinigte Königreich und Australien haben bereits aktive Abwehrmaßnahmen ergriffen. Diese Akteure müssen im Sinne der Sorgfaltsverantwortung sicherstellen, dass derartige Einsätze angemessen sind, und Rechenschaftspflichten einhalten. Aktive Cyberabwehr setzt zunächst eine Auseinandersetzung mit der Frage voraus, welche Maßnahmen von welchen Akteuren in welchen Partnerschaften sinnvollerweise verfolgt werden sollen. Daneben braucht es Klarheit darüber, in welcher Weise diese Aktionen dazu geeignet sind, zur eigenen Sicherheit und zur Stärkung von Partnern beizutragen. In einem zunehmend unübersichtlichen strategischen Umfeld der EU sind die normativen Grundlagen einer aktiven Gefahrenabwehr legitimierbar, jedoch mangelt es derzeit mindestens noch in folgenden Punkten an Transparenz:

- Aktive Abwehrmaßnahmen sollten eng an feste Einsatzprinzipien und eine sorgfältige Folgenabschätzung geknüpft werden. Das stellt hohe Anforderungen vor allem an die Einordnung des notwendigerweise vorwärts gerichteten Charakters von defensiven und zugleich disruptiven Aktionen. Ihr Zweck, offensive Operationen zu stören, ist klar von solchen Aktionen mit gezielter Schadensabsicht abzugrenzen. Überlegungen zu den Auswirkungen dürfen sich nicht allein auf die Beeinflussung des gegnerischen Kalküls beschränken, sondern sollten nachgelagerte Konsequenzen für die globale Stabilität im Cyber- und Informationsraum miteinbeziehen. Analog braucht es Evaluationsgrundlagen und Metriken, die eine integrierte strategische, operative und taktische Auswertung jenseits der bloßen Anzahl der durchgeführten Operationen oder ihrer unmittelbaren taktischen Effekte ermöglichen.
- Die Solarium-Kommission hebt hervor, dass die taktische und operative Umsetzung der Defend-Forward-Policy den Einsatz in Netzwerken von Partnern und Verbündeten miteinschließt, wenn disruptive Maßnahmen nur auf diesem Weg ihr Ziel erreichen können. Wie das Beispiel der Löschung von Propagandamaterial des »Islamischen Staats« von einem deutschen Server zeigt, setzen solche grenzüberschreitenden aktiven Cyberabwehreingriffe eine Verständigung voraus. Vor diesem Hintergrund verwies die Kommission darauf, dass entsprechende Aktionen, wann immer möglich, mit der Unterstützung von Verbündeten und Partnern durchzuführen seien. Unabhängig von deren Bereitschaft, aktive Cyberabwehrfähigkeiten zu entwickeln, erfordert dies aus US-Perspektive eine enge Koordination mit Alliierten und anderen gleichgesinnten Regierungen. Auf EU-Seite könnte das geplante Cyberabwehr-Koordinationszentrum (EUCDCC) zukünftig eine Plattform zur Abstimmung mit internatio-

nalen Partnern sein. Dessen Bemühungen, ein Lagebild über laufende Cyberoperationen zu erstellen, werden sich zunächst auf GSVP-Missionen und -Operationen konzentrieren.

- Bestehende Formate für die gemeinsame Nutzung von freiwillig bereitgestellten Cyberfähigkeiten, wie zum Beispiel das SCEPVA-Programm der Nato (Sovereign Cyber Effects Provided Voluntarily by Allies), zeigen, wie schwierig es ist, Kooperationsvorhaben in diesem Bereich in die Tat umzusetzen. Alle Akteure sind daran interessiert, ihre eigenen Fähigkeiten nicht unbegrenzt offenzulegen. In der Praxis werden Fähigkeiten daher nicht gemeinsam genutzt, sondern auf Ersuchen der Verbündeten eingesetzt. Bei der aktiven Abwehr erweisen sich diese Hindernisse als besonders hoch (da sie kontinuierlich und proaktiv ist). Die aktive Abwehr nimmt Aktivitäten unterhalb der Schwelle eines bewaffneten Angriffs in den Blick und ist daher viel breiter angelegt als das Arbeitsfeld von SCEPVA, das auf Operationen und Missionen des Bündnisses beschränkt ist. Diese Dynamik erhöht den Druck, aktive Cyberabwehrmaßnahmen zumindest in Ansätzen zu verfolgen oder andernfalls zu riskieren, ins Hintertreffen zu geraten. Bei der Entwicklung nationaler Fähigkeiten stellt sich die Frage, welche Auswirkungen die Verdrängung bösartiger Aktivitäten aus dem eigenen Einsatzbereich hat, wenn diese nicht zielspezifisch sind (z. B. Ransomware, bestimmte Arten der Wirtschaftsspionage). Solche Verdrängungseffekte bergen die Gefahr, dass sich disruptive Ansätze zu einer »Beggar-thy-Neighbour«-Politik entwickeln, bei der sich Länder, die sich gegen offensive Reaktionen entscheiden, konzentrierten Bedrohungsaktivitäten ausgesetzt sehen. Ein Beispiel dafür ist Australien, dessen Motivation für den Aufbau der JSO es war sicherzustellen, dass es sich nicht als weiches Ziel präsentiert.
- Informationen darüber, wie die neuen Befugnisse ausgeübt werden, sollten ein integraler Bestandteil eines Paradigmenwechsels sein. Die Aufdeckung gegnerischer Aktivitäten und die Unterscheidung zwischen verbündeten Aktionen und feindlichen Operationen sind wichtig, um verantwortungsbewusstes Verhalten und die Einhaltung von Normen zu belegen. Ein gemeinsames stabilisierendes Verständnis von aktiven Cyberabwehrmaßnahmen ist nur dann zu erreichen, wenn Präzedenzfälle die zu unterbindenden offensiven Operationen und ergriffenen Gegenmaßnahmen in eine klare Beziehung zur Normdebatte über staatliches Verhalten im Cyberraum setzen.
- Die Offenlegung von Angriffsoperationen steht nicht zwangsläufig im Widerspruch zum Schutz von Quellen und Methoden. Im Gegenteil: Transparenz über die Gründe, das Ziel und die erzielte Wirkung einer aktiven Abwehrmaßnahme kann die Verbindlichkeit von Normen stärken und die handlungsleitende Doktrin stützen. Es mag zwar Fälle von operativen Störungen geben, bei denen die Gegner keine Einmischung von außen vermuten, doch die allgemeine Annahme, dass die Kommunikation über diese Punkte von der Preisgabe nachrichtendienstlicher Mittel abhängt, greift zu kurz.
- Ähnliche Mechanismen, die das Gebot verantwortungsvoller Transparenz bekräftigen sollen, gibt es bereits für die proaktive Nutzung von FBI-Befugnissen zur Löschung von Schadsoftware, die in Zielen hinterlegt ist. Die solchen Maßnahmen zugrundeliegende vereidigte Versicherung der Strafverfolgungsbehörde, dass die entsprechenden digitalen Säuberungsaktionen notwendig sind, wird bereits regelmäßig veröffentlicht. Ein Anfang April 2023 publik gemachtes Leitdokument der britischen National Cyber Force bewertet aktive Cyberabwehr als Ausdruck einer verantwortungsvollen Ausübung von »Cyber Power«. Das Papier liefert Ansätze, wie disruptive Abwehrmaßnahmen mit der demonstrativen Einhaltung und Stärkung von international anerkannten UN-Normen und mit

dem Völkerrecht verknüpft und in Einklang gebracht werden können.
Dazu entwirft das britische Strategiepapier ein Raster operativer Voraussetzungen und benennt Kategorien, um aktive Cyberabwehrmaßnahmen in ihrer Wirkung und am Anspruch zu messen, dass von ihnen ein stabilisierender Einfluss ausgehen muss. Wie sich die Leitlinien in der Praxis zu einem »verantwortlichen«, »präzisen« und »angepassten« Vorgehen fügen sollen, lässt sich allerdings ohne konkrete operative Beispiele nur begrenzt erfassen.
Das Leitdokument weist in diesem Zusammenhang darauf hin, dass Transparenz vor der Öffentlichkeit ein wesentlicher Baustein der »Licence to Operate« ist. Begründet wird dies unter anderem mit den zusätzlichen finanziellen Mitteln, die die Londoner Regierung in die Entwicklung von Cyberfähigkeiten investiert hat. Dieser Begründung verantwortungsvoller Transparenz ist vor allem der Sachverhalt der grundsätzlichen Vorverlagerung der Einsatzmöglichkeiten von Cyberfähigkeiten hinzuzufügen. Diese Erweiterung des Handlungsraums zeichnet sich in Deutschland nicht zuletzt durch die angestrebte Grundgesetzänderung ab, mit der neue Befugnisse erteilt werden sollen, und gewinnt mit Blick auf den Anspruch, entsprechende Fähigkeiten demokratisch abgestützt und verantwortungsvoll einzusetzen, an Gewicht.

Die USA haben in Anklageschriften und in Zusammenarbeit mit europäischen Partnern in Form von Sanktionsmitteilungen die Verantwortlichkeiten der einzelnen Akteure und die zeitliche Abfolge ihrer Aktionen detailliert dargelegt. In der Tat haben die Bemühungen, die Urheberschaft von Cyberangriffen öffentlich zuzurechnen, den Grundstein für die Kostenauferlegung gelegt, auf die sich jede Befürwortung einer aktiven Abwehr stützen müsste. Im Rahmen ihrer jeweiligen Cyberabwehrdoktrin müssen Staaten überlegen, unter welchen Umständen sie Informationen über den Einsatz aktiver Abwehrmaßnahmen veröffentlichen können, insbesondere wenn diese Informationen dem Gegner bereits bekannt sind. Solche Daten liefern auch die Grundlage für die Beurteilung, ob aktive Abwehrmaßnahmen ihren erklärten Zweck erfüllen.

Ein Paradigmenwechsel in der strategischen Kultur europäischer Cybersicherheit von einer reaktiven hin zu einer defensiv ausgelegten aktiven Cyberabwehr sollte den oben genannten Anforderungen Rechnung tragen. Die Entwicklung von Tools zur Evaluation derartiger Einsätze, insbesondere solcher, mit denen sich die Risiken einer Konflikteskalation und von Kollateralschäden bzw. negativen Folgen abschätzen lassen, ist in den Ausgestaltungsprozess neuer Befugnisse von Anfang an mit einzubeziehen. Europäische Cybersicherheit muss sich an den eigenen Prinzipien zur Einhaltung von Sorgfaltspflichten messen lassen. Ein Paradigmenwechsel von einer reaktiven hin zu einer aktiven Cyberabwehr ist nur mit demokratischem Rückhalt verantwortbar. Dieser ist nur zu bekommen, wenn ein gesellschaftliches Verständnis für das strategische Umfeld vorhanden ist und damit für die Tatsache, dass der Cyberraum inzwischen ein permanent umkämpftes Konfliktfeld darstellt. Die hierfür notwendigen Informationen können auch durch eine evidenzbasierte Cyberkonflikt- bzw. Friedensforschung generiert und vermittelt werden. Öffentliche Datenerhebungen zur Entwicklung von Cyberbedrohungen und staatlichen Reaktionen darauf, wie sie das Forschungskonsortium European Repository of Cyber Incidents (EuRepoC) betreibt, können einen wichtigen Beitrag dazu leisten, dass über Cyberabwehrüberlegungen verantwortungsvoll diskutiert wird und diese demokratisch abgestützt werden.

*Dr. Annegret Bendiek ist Stellvertretende Leiterin der Forschungsgruppe EU / Europa.*
*Jakob Bund ist Wissenschaftler im Projekt »European Repository of Cyber Incidents (EuRepoC)« und Senior Researcher der European Cyber Conflict Research Initiative (ECCRI).*



**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

ISSN (Print) 1611-6364
ISSN (Online) 2747-5018
DOI: 10.18449/2023A49