SWP

SWP-Aktuell

NR. 39 AUGUST 2025

Das Janus-Prinzip: Fünf zentrale Reformansätze für die europäische Cybersicherheitspolitik

Annegret Bendiek / Jakob Bund

Die Bedrohung im Cyber- und Informationsraum geht maßgeblich von autoritären Staaten wie Russland, China, Nordkorea und Iran aus, die hybride Netzwerke aus staatlichen und nichtstaatlichen Akteuren einsetzen, um Verantwortung zu verschleiern und Konflikte zu eskalieren. Langfristige Analysen verdeutlichen ihre hohe operative Aktivität und die zunehmende Vermischung von Akteursrollen. Die EU reagiert darauf mit einem umfangreichen diplomatischen Reaktionsrahmen, dessen Wirkung aber höchst umstritten ist. Eine grundlegende Reform der europäischen Cybersicherheitspolitik sollte daher dem Janus-Prinzip folgen: Sie sollte sich konsequent einem Check-up ineffizienter Strukturen und Prozesse stellen und dabei gleichzeitig die technologischen Entwicklungen in den Blick nehmen. Fünf konkrete Reformansätze bieten sich für die EU Cyber Posture an, um Synergien zu heben und eine wirksame, belastbare Antwort auf die dynamischen Bedrohungen zu finden.

Die Bewertung technologiegetriebener Bedrohungen, wie sie sich im Cyber- und Informationsraum (CIR) ergeben, kreist häufig um den Fortschritt des technisch Machbaren. In zugespitzter Form zeigt sich das an der Diskussion über die Auswirkungen von KI-Entwicklungen auf die Cybersicherheit. Diese Debatten vermitteln den Eindruck, dass sich Sicherheit im Wettstreit um einen technologischen Durchbruch und einen damit verbundenen, nicht auszugleichenden Vorteil entscheidet. Diese Wahrnehmung führt dann in der Regel zu dem Schluss, die künftige Bedrohungslandschaft gestalte sich danach, ob es gelingt, ein technisches Gleichgewicht zwischen Offensive und Defensive herzustellen. Aus dem Impuls, dieses neue Gleichgewicht zu bestimmen, ergibt sich die Tendenz, in Analysen die Aufmerksamkeit allein auf den technologischen Entwicklungshorizont zu richten. Über den Einsatz von Cyberfähigkeiten entscheiden indes vielmehr strategische Überlegungen, institutionelle Pfadabhängigkeiten und diplomatische Verhaltensweisen, die langfristigen Trendlinien folgen.

Eine umfassende Bewertung der Bedrohungen im CIR erfordert aber nicht nur eine vorwärtsgewandte Einschätzung künftiger technologischer Entwicklungen (ex-ante),

Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

sondern auch eine rückwärtsgerichtete kritische Selbstevaluation, also Ex-post-Betrachtung, der eingeschlagenen institutionellen Pfade, die eine zielgerichtete europäische Cyberabwehr hemmen. Dieser Janusblick in beide Richtungen ist die Bedingung dafür, das technisch Mögliche mit dem eigenen strategischen Anspruch, eine europäische Cybersicherheitspolitik zu entwickeln, in Abstimmung zu bringen. Gerade gegenüber den strategischen Herausforderern ist es unverzichtbar, den Blick auf eine vorwärtsgewandte Gefahrenabwehr zu richten und zugleich die Fehler der Vergangenheit in der europäischen Cybersicherheitspolitik nicht zu wiederholen. Insbesondere im Hinblick auf jene Reaktionen auf EU-Ebene, die mit einem hohen Kommunikationsaufwand zwischen den Politikebenen von der EU-Ebene bis hin zur föderalen Ebene in der Bundesrepublik Deutschland einhergehen, ist ein derartiger Janusblick die Voraussetzung dafür, dass erwogene Schutz- und Gegenmaßnahmen auf ihre tatsächliche Wirksamkeit hin überprüft werden können.

Die strategischen Herausforderer

Kontinuierliche Auswertungen, wie sie das European Repository of Cyber Incidents (EuRepoC) über einen Zeitraum von nahezu 25 Jahren ermöglicht, stellen für ein (öffentlich zugängliches) Lagebild der europäischen Cybersicherheit eine wichtige Grundlage bereit. In diesen Langzeitbeobachtungen zeichnet sich eine anhaltend hohe Aktivität von Seiten eines Clusters von autoritären Staaten ab. Knapp drei Viertel der seit 2000 öffentlich berichteten Cyberoperationen mit staatlichem Hintergrund sind nach EuRepoC-Daten auf vier Länder zurückzuführen — China, Iran, Nordkorea und Russland. Gleichzeitig belegen Daten des Repositorys für diese Zeitspanne eine Erweiterung des Akteursfelds. Staatliche Gruppen sind demnach für weniger als ein Drittel der Cyberoperationen mit politischer Tragweite verantwortlich. Eine Auswertung der einzelnen Operationen zeigt allerdings, dass diese Trennung nach Akteurstypen gerade für Aktivitäten mit Ursprung in autoritären Staaten weit weniger statisch ist. Der Konstante eines Clusters autoritärer Staaten als Bedrohungsquelle steht eine Dynamisierung des Verhältnisses zwischen staatlichen und nichtstaatlichen Akteuren gegenüber, welche die Grenzen zwischen diesen Gruppen zunehmend verschwimmen lässt.

Insbesondere Russland und China haben gezielt hybride Strukturen entwickelt, in denen staatliche und nichtstaatliche Akteure — etwa kriminelle Gruppen oder private Hacker-Dienstleister — eng miteinander verzahnt vorgehen. Kriminelle Gruppen, die in Russland ein Rückzugsgebiet gefunden haben und von dort gegen ausländische Ziele straffrei agieren können, werden im Gegenzug von russischen Diensten in staatlich gesteuerte Operationen einbezogen. In China hat sich unter Führung des Ministeriums für Staatliche Sicherheit ein verzweigtes Netzwerk kommerzieller Dienstleister ausgebildet. Im staatlichen Auftrag spähen diese Firmen Schwachstellen aus und erschließen Zugänge zu Hochwertzielen im Ausland. Über die Einbindung solcher Proxy-Gruppen ohne vermeintlichen Staatsbezug versuchen Staaten, die Aufklärung ihrer Cyberaktivitäten zu behindern und die dahinterstehenden Absichten zu verschleiern. Hinter dieser Kulisse starten sie gezielte Angriffe auf kritische Infrastrukturen, politische Institutionen oder zivilgesellschaftliche Akteure in der EU. Zu beobachten ist eine strategisch bewusst angelegte Integration nichtstaatlicher Ressourcen in staatliche Planungs- und Kommandostrukturen. Diese Vorgehensweise erschwert die politische Attribution, unterminiert internationale Normen und setzt die Resilienz offener Gesellschaften permanent unter Druck.

Die EU Cyber Posture: Ungenutzte Synergiepotentiale

Gerade Europa steht vor der besonderen Herausforderung, die von der Vielschichtigkeit dieser Hybridmodelle autoritärer

Staaten ausgeht. Die EU hat dafür eine Vielzahl an Cybersicherheitsinstrumenten kreiert, darunter die Cyber Diplomacy Toolbox (CDT), das horizontale Cybersanktionsregime, militärische Reaktionsmechanismen im Rahmen von PESCO und regulatorische Initiativen zur Stärkung der Produktsicherheit wie die Cyberresilienz-Verordnung. Der neue EU Cyber Blueprint vom Juni 2025 ergänzt und integriert bestehende Initiativen wie:

- die NIS2-Richtlinie,
- den Cyber Solidarity Act,
- den Integrated-Political-Crisis-Response-Mechanismus,
- die Cyber Diplomacy Toolbox,
- sektorspezifische Vorschriften (z. B. zum Schutz der grenzübergreifenden Stromversorgung).

Diese hier nur kursorisch aufgelisteten EU-Instrumente spiegeln das breite sicherheits- und technologiepolitische Spektrum Europas wider. Zahlreiche Analysen haben aufgezeigt, dass die Wirkung der EU-Cybersicherheitspolitik durch fragmentierte Zuständigkeiten und sektorale Abschottung begrenzt bleibt. Auch ist vielfach darauf hingewiesen worden, dass durch die fehlende strategische Verknüpfung Synergiepotentiale ungenutzt bleiben, die durch eine stärkere Verzahnung von Kommissions- und Ratsinitiativen durchaus erschlossen werden könnten. Im Sinne des Janusblicks sind aber gerade die konstruktiven Elemente der EU-Cybersicherheitspolitik in den Blick zu nehmen.

Grundsätzlich legt die Cyber Posture vom Mai 2022 die Aufgaben der EU richtigerweise breit an, indem sie fünf Arbeitsbereiche definiert: Stärkung der Widerstandsfähigkeit und der eigenen Schutzkapazitäten; Stärkung der Solidarität und Verbesserung des umfassenden Krisenmanagements; internationale cyberpolitische Positionierung der EU; Intensivierung der Zusammenarbeit mit Partnerländern und internationalen Organisationen; und Prävention, Abwehr und Reaktion auf Cyberangriffe. Der Aufbau und die Ausrichtung dieser Cyber Posture unterstreicht auch den spezifischen kollektiven Beitrag von EU-Institutionen und -Akteuren bei der Koordination, die ein gemeinsames Vorgehen in der europäischen Cybersicherheitspolitik überhaupt erst ermöglicht. Diese vielfach unterschätzten Koordinationsbemühungen erstrecken sich über mehrere Ebenen. Im November 2024 verständigten sich die Mitgliedstaaten auf eine gemeinsame Erklärung zur Anwendung des Völkerrechts im Cyberraum, an der sich auch andere Drittstaaten außerhalb der EU orientieren. Der im Juni 2025 angenommene Cyber Blueprint zur Verbesserung des Cyberkrisenmanagements regelt die Verantwortlichkeiten zwischen Akteuren auf Unionsebene. Auch dieses Konzept dient insbesondere anderen Regionalorganisationen als Vorbild. Die Einbindung der Ukraine in Überlegungen, wie sich die CDT noch wirkungsvoller zur Abschreckung von Cyberangriffen einsetzen lässt, verdeutlicht nicht zuletzt, wie intensiv sich die EU um die Abstimmung mit internationalen Partnern bemüht. Auch die EU-Initiativen zur horizontalen, vertikalen und drittstaatsorientierten Kohärenzsteigerung ihrer Cybersicherheitspolitik sind Beleg für den Ansatz, Sorgfaltspflichten und das internationale Recht zu stärken. Als normativer Ausgangspunkt der EU-Cybersicherheitspolitik kommt ihnen darüber hinaus eine zentrale Bedeutung zu.

Sorgfaltsverantwortung als Ausgangspunkt

Angesichts der systematischen Offensive autoritärer Akteure im CIR hat die EU vor allem Maßnahmen ergriffen, um ihren eigenen cybersicherheitspolitischen Sorgfaltspflichten nachzukommen. Die EU will im CIR auf internationaler Ebene eine regelbasierte Strategie verfolgen, die auf der Achtung des Völkerrechts und der UN-Normen basiert und von vertrauens- und sicherheitsbildendem Handeln begleitet ist. Diese Haltung soll Erwartungsverlässlichkeit erzeugen und wird durch zentrale Dokumente und Instrumente wie die EU Cyber Posture (2022), die überarbeitete Cyber Diplomacy Toolbox (2023), den Strategischen Kompass,

die Mitteilung zur Cyberverteidigung (2024) und die Erklärung zur Anwendung des Völkerrechts im Cyberraum (2024) bekräftigt. Diese Dokumente betonen die Geltung humanitärer und internationaler Normen, die Bedeutung normsetzender Diplomatie und die Verpflichtung der EU zu verantwortungsvollem staatlichem Handeln im digitalen Raum. Im Zentrum des diplomatischen Reaktionsrahmens der EU steht die überarbeitete Cyber Diplomacy Toolbox (CDT) mit ihren bisher vier verabschiedeten Sanktionspaketen.

Daneben gibt es, wie bereits weiter oben aufgelistet, eine Vielzahl von verbindlichen Rechtsakten der EU-Kommission, die vor allem seit 2022 erlassen wurden. Verbunden sind sie durch das übergeordnete Ziel, die Resilienz innerhalb des Binnenmarkts zu steigern. Durch Vorgaben für Hard- und Software, für die Netzwerkinfrastruktur und durch die Festschreibung internationaler Verpflichtungen aus der Grundrechtecharta und dem internationalen Recht werden alle Marktteilnehmer im Binnenmarkt damit mittelbar an europäische Normen und Standards gebunden.

Der Cyberkapazitätsaufbau über die EU hinaus findet häufig im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) statt, vor allem über zivile Ausbildungsmissionen (z. B. EUAM Ukraine, EUCAP Sahel). Diese Missionen bieten Anknüpfungspunkte zur normengebundenen Cyberdiplomatie, etwa durch die Vermittlung europäischen Rechts oder technischer Schutzmaßnahmen, zum Teil über private IT-Sicherheitsanbieter. Jedoch ist das Potential solcher Missionen als Beitrag zur gesamtstrategischen Cybersicherheitsarchitektur der EU bislang kaum genutzt worden.

Während der regulatorische Anspruch der EU weltweit Beachtung findet, wird ihre Fähigkeit, Cyberbedrohungen abzuwehren, von einer Reihe von Defiziten beschränkt, unter denen vor allem zu nennen wären: fehlende horizontale Strategiekohärenz, die einseitige Fokussierung auf die Attribution, Schwächen bei der Anschlussfähigkeit zur aktiven Kooperation mit anderen Partnern, ein Mangel an EU-interner vertikaler Kohärenz und die starre Trennung zwischen zivil und militärischer Zusammenarbeit. Reformansätze sollten stärker nach den Konfliktstrukturen unterscheiden, weniger auf die Attribution und Sanktionen abheben und auf die Verbesserung der internationalen Anschlussfähigkeit durch öffentlich-private Partnerschaften sowie eine Vertiefung der zivil-militärischen Kooperation abzielen.

Erstens: Stärker zwischen Bedrohungen differenzieren

Die Reform der CDT 2023 war ein wichtiger Schritt, aber sie hat keine substantiellen Durchbrüche bei Attribution, Sanktionierung oder operativer Resilienz gebracht. Der diplomatische Reaktionsrahmen der GASP fokussiert stark auf staatliche Bedrohungsakteure, vor allem auf Advanced Persistent Threats (APTs), die staatlichen Stellen zugeschrieben werden können. Diese Engführung blendet jedoch die zunehmende Verwischung der Trennlinie zwischen staatlichem und nichtstaatlichem Handeln aus. Autoritäre Staaten wie Russland und China integrieren kriminelle Strukturen systematisch in ihre Cyberoperationen, sei es durch Schutzräume oder operative Koordination.

Zentrale Herausforderungen ergeben sich aus der fortschreitenden Verwässerung der Grenzen zwischen staatlichem und nichtstaatlichem Handeln — insbesondere im russischen Fall, wo kriminelle Gruppen als verlängerter Arm des Staates agieren und Schutzräume genießen. Dies reduziert die Wirksamkeit der bisherigen EU-Instrumente gegenüber Cyberkriminalität, besonders im Bereich von Ransomware, wie die jüngsten Operationen gegen Krankenhäuser und Wasserwerke zeigen.

Die EU hat zwar mit der Toolbox ein Instrumentarium zur Reaktion auf hybride Bedrohungen beschlossen, das unter anderem Cyberoperationen umfasst; doch auch hier fehlt es an einer systematischen Integration mit CDT-Maßnahmen. Auch der Einsatz hybrider Rapid Response Teams wird bisher weder strategisch gesteuert

noch regelmäßig geübt — ein Missstand, der im Cyber Blueprint 2025 selbstkritisch benannt wird.

Bislang mangelt es an einer institutionellen horizontalen Kohärenz in der europäischen Cybersicherheit: Während beispielsweise in Großbritannien das National Cyber Security Centre landesweit Einsatzmöglichkeiten für Täuschungsmaßnahmen (Honeypots etc.) prüft, verfügt die EU noch über keinen vergleichbaren Ansatz, obwohl die Größe des Binnenmarkts hier einen Vorteil darstellen würde. Zwar sehen die 2023 überarbeiteten Leitlinien der CDT zum Beispiel den gemeinsamen Einsatz von Maßnahmen aus den EU-Toolboxen für den Umgang mit hybriden Bedrohungen und ausländischen Beeinflussungsversuchen vor. Die Schaffung von Synergien zwischen den verschiedenen EU-Strategien verharrt allerdings bislang auf konzeptioneller Ebene. Auch dieses Defizit hat die EU Cyber Posture benannt.

Im Hinblick auf zwischenstaatliche Konflikte hat die EU sich klar zur Geltung des humanitären Völkerrechts im Cyberraum bekannt — zuletzt in der erwähnten Erklärung vom November 2024. Um diesem Bekenntnis Wirkung zu verleihen, braucht es Konkretisierungen, wie solche roten Linien in der militärischen Verteidigungsdimension operationalisiert werden sollen. Ein wichtiger Schritt in dieser Richtung wäre die Ausarbeitung von Leitlinien zur Anwendung des humanitären Völkerrechts auf offensive Cyberoperationen im Kontext von Artikel 42(7) EUV oder Artikel 222 AEUV (Solidaritätsklausel), damit strategischen Herausforderern im Vorfeld Handlungsfähigkeit signalisiert wird.

Zweitens: Unabhängig von Attribution handeln

Der Reaktionsrahmen der EU bleibt stark attributionsabhängig, also fokussiert auf die Zuschreibung von Verantwortung. Die EU betont zwar im Hinblick auf die CDT, dass nicht alle restriktiven Maßnahmen eine Attribution voraussetzen. Faktisch aber ist die Anwendung der Tools an eine vorherige Attribution geknüpft. Obwohl die CDT 2023 überarbeitet wurde, gibt es nach wie vor kaum Maßnahmen, die ohne vorausgegangene Attribution wirksam werden können.

Auch fehlen im Arsenal der CDT bisher explizite Optionen für Maßnahmen, die sich gegen technische Infrastrukturen wie Crypto-Mixer, Anbieter von Bulletproof-Hosting-Diensten oder Botnet-Controller richten — also Instrumente, die unabhängig vom Akteur Wirkung entfalten können. Reaktive Maßnahmen wie das Unterbrechen technischer Infrastrukturen (z. B. Botnet-Zerschlagung, Serverabschaltungen, Deplatforming) können grundsätzlich unabhängig von der Attribution erfolgen und gleichzeitig effektiv zur Schadensminimierung beitragen. Dieses Potential wurde im Zuge der CDT-Reform 2023 nicht systematisch operationalisiert. Strategische Partner der EU sind in ihrer Zusammenarbeit deutlich weiter. Die USA, Großbritannien und Australien haben wiederholt in enger Abstimmung Plattformen, wie etwa die intensiv von Cyberkriminellen genutzten russischen Bulletproof-Hosting-Provider Zservers und Aeza, sanktioniert. Eine vergleichbare Option fehlt in der EU, obwohl gerade solche Maßnahmen die Fähigkeit zur Reaktion gegenüber Bedrohungsakteuren, die gezielt staatliche und nichtstaatliche Handlungsregister vermischen, erheblich steigern könnten. Die EU erkennt zwar die Rolle technischer Attribution durchaus an — etwa wenn es darum geht, den Internationalen Strafgerichtshof (IStGH) bei Ermittlungen zu Cyberkriegsverbrechen gegen die Ukraine zu unterstützen. Gleichwohl bleiben diese Ansätze isoliert. Eine systematische Verzahnung mit diplomatischen Mechanismen erfolgt nicht. Technische Attribution sollte künftig Teil der Cyberdiplomatie werden, um handlungsfähig zu bleiben, gerade dann, wenn politische Attribution nicht unmittelbar möglich ist.

Drittens: Internationale Anschlussfähigkeit verbessern

Die CDT ist eingebettet in die EU Cyber Posture von 2022. Diese enthält ein Bekenntnis zu einem regelbasierten internationalen System, das sich auf die UN-GGE- und OEWG-Berichte sowie geltendes Völkerrecht stützt. Der Verweis auf internationale Normen ist essentieller Bestandteil der diplomatischen Bemühungen der EU. Gleichzeitig bleibt unklar, wie diese Prinzipien bei konkreten Vorfällen in Europa umgesetzt werden.

Das im Mai 2025 verlängerte horizontale Cybersanktionsregime sieht zwar explizit die Möglichkeit vor, internationale Normen durchzusetzen. Die Sanktionspraxis der EU ist allerdings von Zurückhaltung geprägt, auch wegen der hohen Anforderungen an die Beweislast und die implizite Abhängigkeit von Attribution. Darüber hinaus ist die EU bei ihren Reaktionen durch den Konsenszwang der Mitgliedstaaten eingeschränkt. Die politische Attribution erfolgt individuell durch die einzelnen Mitgliedstaaten. Eine einheitliche Außenwirkung lässt sich damit kaum erzielen.

Der Vergleich mit den Five-Eyes-Staaten zeigt: EU-Reaktionen erfolgen langsamer, weniger koordiniert und basieren seltener auf geheimdienstlicher Vorarbeit. Die Fähigkeit der EU, international abgestimmte Maßnahmen umzusetzen, ist aber von zentraler Bedeutung. Die USA und Großbritannien nutzen technische Beweismittel und Geheimdienstinformationen oft gezielt, um Sanktionen zu verhängen. Dieser pragmatische Zugriff erlaubt es ihnen, schnell zu reagieren, und zeigt, dass eine flexible Handhabung von Attributionserfordernissen ein Erfolgsfaktor im Hinblick auf die internationale Koordination ist.

Die fehlende Integration technischer Attribution in die Cyberdiplomatie schwächt die strategische Position der EU und macht es schwieriger für sie, mit Partnerstaaten abgestimmte Maßnahmen zu ergreifen. Auch operative Maßnahmen wie die koordinierten Takedowns bei der »Operation Endgame« bleiben in der EU bislang allein auf den strafrechtlichen Arbeitsbereich, beispielsweise von Europol, innerhalb der EU Cyber Posture konzentriert. Die Wirkung solcher Maßnahmen zur präventiven Zerschlagung krimineller Infrastrukturen könnte viel einschneidender und nachhaltiger sein, wenn die systematische Offenlegung von Angriffswerkzeugen unter vermehrter Einbindung von ENISA und dem EU-CSIRT-Netzwerk mit dem flankierenden Einsatz von Sanktionen über die CDT strategisch verknüpft würde. Eine solche Verschränkung von bestehenden, aber bisher nebeneinanderstehenden EU-Maßnahmen würde es ermöglichen, den strategischen Herausforderern ernsthaft die Bereitschaft zu signalisieren, sie mit Kosten zu belegen. Bisher war es eine der Limitierungen bei der Anwendung der CDT, Bedrohungsakteuren wirklich substantielle Konsequenzen aufzuerlegen. Eine Eingliederung der CDT in die operative Bedrohungsbekämpfung kann hier — auch ohne Anpassungen im Maßnahmenkatalog — neue Handlungsräume erschließen.

Viertens: Partnerschaften pragmatisch ausbauen

In bisherigen Überlegungen zur Anwendung der CDT scheinen Bezüge zu Initiativen der Europäischen Kommission zur Cybersicherheit bisher kaum eine Rolle zu spielen. Dabei ist für die Wirksamkeit der Maßnahmen des Cyber Resilience Act und des Solidarity Act die Einbindung nichtstaatlicher Stakeholder, etwa aus der Zivilgesellschaft und der Industrie, oder von Wissensträgern in Technologienischen, wie dem Blockchain-Bereich, die selbst stark von kriminellen Aktivitäten betroffen sind, zur Einhegung dieser Machenschaften zentral. Gerade diese Akteure sind entscheidend für die Umsetzung technischer Resilienz, bei der Frühwarnung vor Bedrohungen und für die effektive Attribution. Kooperationen mit Akteuren im Kryptowährungssektor sind wenig entwickelt, dabei könnten sie helfen, den Missbrauch von anonymisierenden Infrastrukturen (z. B. Crypto-Mixern) zu reduzieren. Gleichzeitig wäre ein vertrauens-

basierter Austausch mit Tech-Providern äußerst wichtig für die Identifikation von Angriffspfaden und Supply-Chain-Risiken.

Die überarbeitete CDT enthält zwar Ausführungen zur Rolle privater Akteure im Bereich der Cybersicherheit: Insbesondere Sicherheitsdienste, Computer Emergency Response Teams (CERTs) und Technologieanbieter sollen systematischer in die Lagebeurteilung (situational awareness) und vorausschauende Reaktion (preparedness) eingebunden werden. Die Implementierung bleibt jedoch fragmentiert. Wesentliche Gruppen — etwa die Krypto-Community, technische Forschungseinrichtungen oder Open-Source-Communities — sind bislang kaum Teil des Reaktionsrahmens. Dabei ist ihre Bedeutung offensichtlich: Ransomware-Gruppen nutzen zunehmend Dual-use-Technologien wie File-Transfer-Tools oder legitime Fernwartungssoftware. Ohne Einbindung der genannten Akteure lässt sich der Missbrauch solcher Systeme nicht verhindern.

Auch scheinen bei den Initiativen zur Bekämpfung von Ransomware-Angriffen derartige privat-öffentliche Kooperationsformate in der Cyberdiplomatie bislang nicht im Zentrum zu stehen. Zudem fehlt ein strategischer Dialog mit Cloud-Anbietern und Plattformunternehmen — obwohl diese für Skalierung, Attribution und Interventionsmöglichkeiten maßgebliche Player sind. Die EU hätte hier die Möglichkeit, über ihre Marktregulierungskompetenz (z. B. Digital Services Act/Cyber Resilience Act) Anreize für präventive Kooperation zu schaffen, etwa im Bereich der Frühwarnung oder bei Löschungen.

Die EU hat mit ihren Kommissionsmitteilungen zur internationalen digitalen Zusammenarbeit (z. B. im Rahmen der Joint Communication on the EU's International Digital Strategy, 2023) erste Schritte in die skizzierte Richtung unternommen. Diese überwiegend entwicklungs- und handelspolitisch orientierten Vorstöße gilt es, systematisch in den diplomatischen Reaktionsrahmen zu integrieren.

Fünftens: Zivil-militärische Synergien anstreben

Die Analyse des Cyber Activity Balance Reports 2024 von EuRepoC zeigt, dass die Mehrheit der politisch motivierten Cyberoperationen gegen die EU durch Akteure erfolgt, die mit staatlicher Unterstützung handeln. Insbesondere Operationen aus Russland lassen zunehmend destruktive Absichten erkennen. In den USA werden Versuche mutmaßlich chinesischer Akteure registriert, die Störung kritischer Infrastruktur für den Krisenfall vorzubereiten. Solche Beobachtungen weisen auf ein sicherheitspolitisches Risiko hin, das eine militärische Reaktion nicht ausschließt. Dennoch wird die militärische Cyberabwehr in der Reaktionsarchitektur der EU nicht systematisch berücksichtigt.

Trotz der Ambitionen im Rahmen der EU Cyberdefence Policy (2022) und der PESCO-Projekte (z. B. Cyber Rapid Response Teams, CRRTs) fehlt es bisher an einer strategischen Integration der zivilen und militärischen Säulen europäischer Cybersicherheitspolitik. Die CDT wurde 2023 reformiert, um ein flexibleres Repertoire diplomatischer Maßnahmen gegen staatliche und nichtstaatliche Cyberakteure zur Verfügung zu haben. Allerdings bleibt ihre Wirksamkeit begrenzt, da der Rahmen der Gegenmaßnahmen, den sie umreißt, weitgehend losgelöst ist von militärischen Verteidigungsressourcen wie den PESCO-CRRTs und hybriden Reaktionsteams (HRRTs). Eine strukturelle Ankopplung an militärische Krisenreaktionsmechanismen, wie sie etwa im EU Cyber Defence Coordination Centre (EUCDCC) vorgesehen ist, befindet sich noch im Aufbau. Notwendig wäre eine enge Zusammenarbeit zwischen der militärischen und zivilen Krisenreaktionsarchitektur (EU-CyCLONe, CSIRTs Network). Sie wird aber bisher nur in Form punktueller Kooperationen und gemeinsamer Übungen angestrebt.

Die PESCO-CRRTs sind eines der wenigen Instrumente, die explizit für Cybersicherheitsoperationen konzipiert wurden. Ihre Nutzung in tatsächlichen EU-Krisenszena-

rien bleibt jedoch marginal. Der Grund dafür liegt auch in der strategischen Unklarheit über Zuständigkeiten und Einsatzdoktrinen. Die Leitlinien zur Aktivierung dieser Teams im Falle eines hybriden Angriffs oder einer Cyberkrise bleiben vage. Ihr Einsatz unterliegt der Zustimmung des Mitgliedstaats, was den Mehrwert auf Unionsebene einschränkt.

Die Lageerfassung und operationale Koordination bei grenzüberschreitenden Vorfällen sind nach wie vor durch ineffiziente Kommunikationswege und eine Fragmentierung der Zuständigkeiten gekennzeichnet. Technische Lösungen könnten hier die Koordination vereinfachen. Im universitären Umfeld sind bereits Vorschläge zur Einrichtung einer gemeinsamen Plattform zur Cyber Situational Awareness (CSA) entwickelt worden, die auch militärische Stakeholder einbinden könnte. Darauf aufbauend könnte eine institutionalisierte Schnittstelle zwischen nationalen Militär-CSIRTs, zivilen Incident-Response-Teams und diplomatischen Gremien der EU etabliert werden, die in Krisenlagen gemeinsam agieren könnten.

Von der koordinierenden zur integrativen Rolle der EU

Die genannten Reformansätze versprechen erhebliche Synergiepotentiale, die allerdings von einem weiteren Schritt in dieser Koordinationskette abhängen: dem gemeinsamen Einsatz der einzelnen Instrumente, Initiativen und Mechanismen seitens der Mitgliedstaaten, der EU-Kommission und des Rates. Über einen solchen integrierten Ansatz können die Bemühungen auf Ebene der Mitgliedstaaten, der EU-Akteure und internationalen Partnern zusammengeführt werden.

Der Beitrag des EU-Reaktionsrahmens zur Eindämmung von Cyberbedrohungen bemisst sich eben nicht an den getroffenen Maßnahmen, sondern danach, wie effektiv sie sind, um die Cybersicherheit der EU zu erhöhen.

Die Einführung einer übergeordneten Ebene zur Koordination der fünf Arbeitsbereiche der EU Cyber Posture würde sicherstellen, dass einzelne Instrumente nicht in Silos gebunden werden, sondern durch ihren strategisch vernetzten Einsatz Synergien freisetzen können, die ihre Durchschlagskraft weiter steigern.

In den überarbeiteten Leitlinien zur Anwendung der CDT wird die Wirkungsverstärkung von solchen Koordinationsleistungen explizit als eine Lehre aus dem Einsatz der Toolbox erwähnt. So bekräftigen die Leitlinien ausdrücklich den Anspruch, einen »nachhaltigen, auf die Bedrohung abgestimmten, kohärenten und koordinierten« Ansatz zu verfolgen. Eine Strategie zur Wirkungsverstärkung, die dem Janus-Prinzip folgend den zunehmend vernetzten Sicherheitsherausforderungen die Verbundeffekte vorhandener Instrumente entgegensetzt, schafft dafür die Voraussetzung. Gerade angesichts der massiven Bedrohungslage, die sich aus der Vereinnahmung nichtstaatlicher Fähigkeiten durch autoritäre Akteure ergibt, liegt in der Koordination und Integration von bestehenden Instrumenten ein spezifischer Mehrwert der EU als cybersicherheitspolitischer Akteur: Mit institutioneller Kohärenz, normativer Klarheit und operativer Anschlussfähigkeit sollten die Mitgliedstaaten nicht nur auf die koordinierende Rolle der EU, sondern auf deren integratives Potential setzen, um die strategische Handlungsfähigkeit und Abwehrfähigkeit von Bedrohungen im Cyberraum zu erhöhen. Entlang der Wirkungsfelder der EU Cyber Posture sollten die Reforminitiativen dezidiert dazu beitragen, dass die EU-Cybersicherheitspolitik im Sinne der Sorgfaltsverantwortung den strategischen Herausforderern im Cyber- und Informationsraum eine kollektive Antwort entgegenzusetzen vermag.

Dr. Annegret Bendiek ist Co-Leiterin des Clusters »Cybersicherheit und Digitalpolitik« und Senior Fellow in der Forschungsgruppe EU/Europa.
Jakob Bund ist Wissenschaftler in der Forschungsgruppe EU/Europa. Die Autorin und der Autor sind Mitglieder des Forschungskonsortiums European Repository of Cyber Incidents (EuRepoC, www.eurepoc.eu). *Die Recherchen zu diesem Bericht wurden durch die Unterstützung des Auswärtigen Amtes ermöglicht.*

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: 10.18449/2025A39