SWP-Aktuell

NR. 43 SEPTEMBER 2026

Multilaterale Kooperation und Vertrauensbildung im Cyberbereich

Die OSZE als Laboratorium kooperativer Cybersicherheit

Nadja Douglas/Jonas Hemmelskamp/Simon Muschick

Die Zahl der Cybervorfälle durch staatliche und von Staaten kontrollierte Akteure steigt weltweit an – insbesondere im OSZE-Raum –, während die diplomatischen Instrumente zu ihrer Eindämmung wenig Aufmerksamkeit erfahren. Die OSZE (Organisation für Sicherheit und Zusammenarbeit in Europa) und andere Regionalorganisationen haben eine Reihe von vertrauensbildenden Maßnahmen (VBMs) im Cyberbereich verabschiedet, welche die Grundlage für eine tiefergehende multilaterale Kooperation darstellen. Doch es ist unklar, inwieweit diese Maßnahmen den Anforderungen einer sich wandelnden Bedrohungslandschaft Rechnung tragen. Auch gibt es nach wie vor strukturelle Defizite in der Cyberdiplomatie und unterschiedliche Bedrohungsperzeptionen in den jeweiligen Regionen. Prinzipiell stellt sich die Frage, in welchen Konstellationen Staaten im Kontext von Cybervorfällen zusammenarbeiten und wann nationale Souveränitätsinteressen überwiegen.

Die Sicherheitslage in der OSZE-Region wird seit 2014 durch die russische Aggression gegen die Ukraine geprägt. Seit Beginn des Angriffskriegs 2022 haben zahlreiche Cyberangriffe (wie z. B. auf das Satellitenkommunikationsunternehmen Viasat zu Kriegsbeginn, auf den Mobilfunkanbieter Kyivstar oder auch jüngst auf den polnischen Energiesektor) gezeigt, dass sich der Konflikt längst auf den Cyberraum ausgedehnt hat.

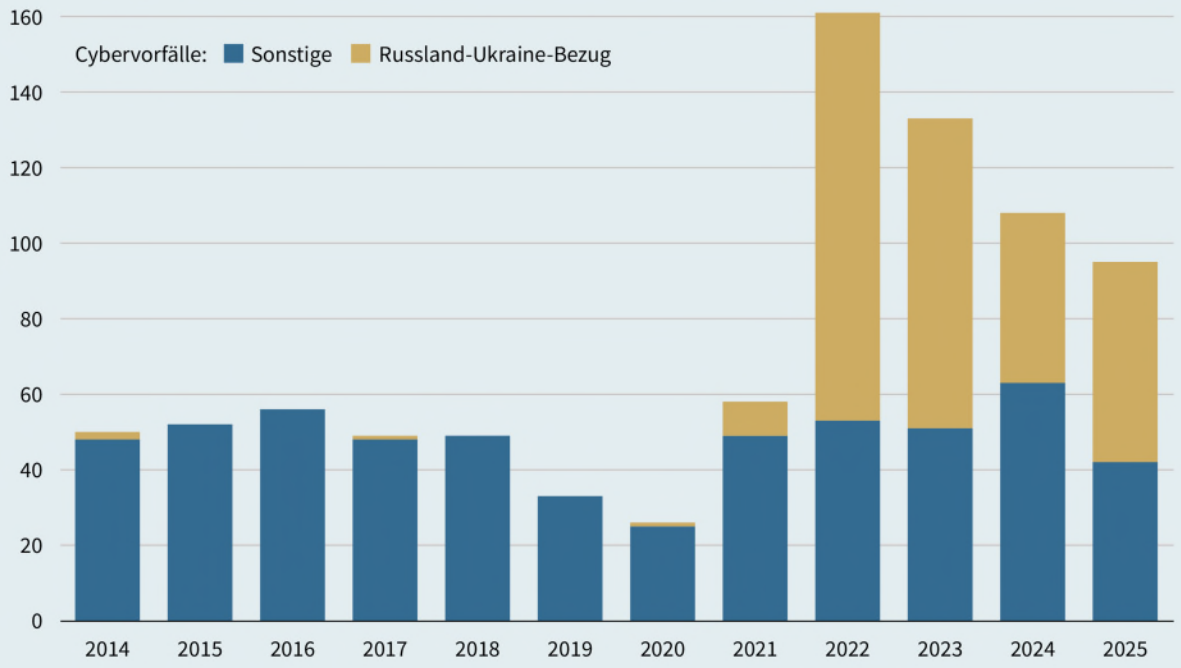
Betrachtet man die Cyberangriffe in der OSZE-Region, die durch staatliche, staatsnahe oder vorgeblich aktivistische Akteure verübt wurden, so kann auf Grundlage von Daten des EuRepoC-Projekts für 67 Prozent der Fälle 2022 ein Bezug zum Krieg festgestellt werden (siehe Grafik 1). Über 60 Prozent der öffentlich bekannten Vorfälle im OSZE-Raum entfallen auf sechs Staaten: Neben der Ukraine sind dies die USA, Russland, Deutschland, Großbritannien und Frankreich. Die Ukraine und ihre Unterstützer sind fortwährend von russischen Angriffen betroffen. Russland wird wiederum regelmäßig von pro-ukrainischen Gruppierungen angegriffen. Mit Kriegsbeginn hat sich die Zielsetzung der Angriffe in der gesamten Region gewandelt. Vor 2022 dienten die Angriffe der genannten Akteure primär der Spionage (44,6 Prozent). Mittlerweile ist

Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Grafik 1

Politisch motivierte Cybervorfälle im OSZE-Raum mit Bezug zum Russland-Ukraine-Krieg

Anzahl der Vorfälle pro Jahr



Quelle: EuRepoC

das Operationsmuster heterogener und wird von disruptiven (32,4 Prozent) und zerstörerischen Angriffen (10,3 Prozent) dominiert, wobei die Intensität der Vorfälle relativ niedrig bleibt. Tatsächlich scheint der Cyberraum in gewissen Konstellationen auch als Substitut für konventionelle kinetische Angriffe zu fungieren. So kann mit Hilfe von Signalisierungsstrategien eine Eskalationsdynamik eher gebremst als verstärkt werden (*Off-Ramp*-These). Typische Angriffsziele sind kritische Infrastrukturen, Kommunikationsnetzwerke und Wahlsysteme.

Neben dem Einfluss des Krieges stellen die fortschreitende digitale Transformation, die gestiegene Bedeutung von Künstlicher Intelligenz, die Krise und Erosion multilateraler Sicherheit sowie eine zunehmende regionale Fragmentierung die OSZE-Teilnehmerstaaten vor große Herausforderungen in der Cybersicherheit.

In dem vorliegenden SWP-Aktuell wird analysiert, wie die Schaffung von technischen Kommunikationskanälen zusammen mit Bemühungen um Capacity Building (Fähigkeitsaufbau) zu einer Stärkung der internationalen Kooperation im Cyberraum beitragen kann. Die Untersuchung basiert auf Interviews mit Vertreter:innen der Wissenschaft, ausgewählter OSZE-Teilnehmerstaaten in Wien, des OSZE-Sekretariats und anderer Regionalorganisationen. Ergänzend wurden Daten des European Repository of Cyber Incidents (EuRepoC) ausgewertet.

Kooperation und Governance im Cyberraum

Die zunehmenden Angriffe auf kritische Informationsinfrastrukturen verdeutlichen, dass sich digitale Netzwerke zu Austragungsorten von Konflikten entwickelt haben. Entsprechend gewinnt der Cyberraum auch für militärische und sicherheitspolitische Fragen an Bedeutung. Während die Versicherheitlichung des Cyberraums durch staatliche Akteure von einigen Expert:innen kritisch betrachtet wird, sehen andere in ihm einen legitimen Schauplatz für Macht-

politik und Abschreckung. Da Cyberangriffe nur schwer eindeutig zurückzuverfolgen sind, ist die Attribution, das heißt die politische oder technische Zuordnung eines Vorfalls zu einem bestimmten Akteur, mit erheblichen Unsicherheiten verbunden. Die Komplexität dieses Verfahrens stellt Staaten mit geringerer Cyber-Reife vor große Herausforderungen. Entsprechend gibt es bereits verschiedene Empfehlungen zur Einrichtung multilateraler Attributionsmechanismen. Die Attribution betrachten die Staaten aber nach wie vor als nationales Prärogativ.

Traditionelle Instrumente der Sicherheitsgovernance greifen aufgrund des grenzüberschreitenden Charakters von Cyberangriffen und der Grauzone zwischen zivilem und militärischem Handeln im Cyberraum zu kurz. Gefordert ist deshalb ein transnationaler Ansatz. Cybergovernance lässt sich als mehrstufiges Modell verstehen, in dem globale, regionale und nationale Prozesse ineinandergreifen. Ideen der Kooperation und Governance im Cyberraum gehen zurück auf das Bestreben, Cybersicherheitsrisiken als Bedrohung für die internationale Sicherheit zu werten und auf multilateraler Ebene Antworten zu finden. Seit 2004 werden durch die Vereinten Nationen in unregelmäßigen Abständen Groups of Governmental Experts (GGE) eingesetzt, um Fragen der internationalen Sicherheit im Bereich der Informations- und Kommunikationstechnologien zu diskutieren und Normen für verantwortungsvolles staatliches Verhalten zu entwickeln. Neben den GGE, denen nur eine begrenzte Zahl von Expert:innen angehören, wurde 2018 mit der Open-ended Working Group ein weiteres Verhandlungsformat geschaffen. Im Jahr 2026 wurde der Prozess dann durch einen Ständigen Globalen Mechanismus institutionell verstetigt. Zwar hat sich auf diese Weise auf VN-Ebene ein gemeinsamer institutioneller Rahmen für verantwortungsvolles staatliches Verhalten herausgebildet. Die konkrete Umsetzung ist jedoch weiterhin politisch umstritten.

Ein Instrument der multilateralen Cyberdiplomatie zur Wahrung von Stabilität im Cyberraum sind Vertrauensbildende Maßnahmen (VBMs). Sie bieten einen Weg, um das Risiko von Fehlwahrnehmungen, unintendierten Zwischenfällen und Spannungen im Cyberraum zu reduzieren. Staatliche Cyberfähigkeiten lassen sich im Unterschied zu konventionellen Waffensystemen nur begrenzt quantifizieren und überprüfen, da sie überwiegend immateriell und informationsgebunden sind und vielfach auf Dual-Use-Technologien beruhen. Während Transparenz bei konventionellen VBMs in der Regel stabilisierend wirkt, kann sie im Cyberbereich Verwundbarkeiten und mögliche Angriffsziele offenlegen. Cyber-VBMs konzentrieren sich deshalb stärker auf Kommunikation, Kooperation und Krisenmanagement unter Bedingungen technischer Unsicherheit. Ihre Umsetzung erfordert die Zusammenarbeit verschiedener staatlicher Stellen auf politischer und technischer Ebene.

Cyberdiplomatische Ansätze erfahren von den Regierungen und Privatakteuren insgesamt jedoch wenig Aufmerksamkeit. Das allgemeine politische Klima und der gängige Cyber-Diskurs sind maßgeblich von der Frage der politischen Zuweisung von Verantwortung für Cyberangriffe (Attribution) und der Idee der aktiven Cyberabwehr geprägt. Umso bemerkenswerter ist es, dass die Cybersicherheitsdebatte in der OSZE zu den wenigen Bereichen gehört, in denen ein zwischenstaatlicher Austausch mit russischer Beteiligung weiterhin aufrechterhalten wird und vertrauensbildende Maßnahmen diskutiert werden.

Regionale Umsetzung von Normen und VBMs

Regionalorganisationen kommt eine besondere Bedeutung bei der Konkretisierung und praktischen Umsetzung global vereinbarter Normen und vertrauensbildender Maßnahmen zu. Umgekehrt sollen regionale Erfahrungen und Best Practices in den globalen VN-Prozess zurückfließen. Derzeit wird unter anderem nach Möglichkeiten und Modalitäten gesucht, diesen interregionalen Austausch insbesondere zum Thema

VBMs zu verstetigen. Neben den Vereinten Nationen beschäftigen sich verschiedene Regionalorganisationen, darunter die OSZE, die Organisation Amerikanischer Staaten (OAS), das ASEAN Regional Forum (ARF) und afrikanische Regionalorganisationen, mit der Entwicklung und Umsetzung von Regeln, Kooperationsmechanismen und VBMs im Cyberraum.

In diesem Zusammenhang gilt die OSZE als erste multilaterale Organisation, die auf Anregung der UN GGE 2013 begann, praktische VBMs zu verabschieden und umzusetzen. Das Ziel des ersten Pakets über 11 freiwillige bzw. politisch nicht bindende Maßnahmen bestand darin, Vertrauen und Transparenz aufzubauen. Dazu gehören Konsultationsmechanismen zur Verringerung des Risikos von Fehlwahrnehmungen und Eskalation im Zusammenhang mit Cybervorfällen (VBM 3) sowie der Aufbau eines Netzwerks nationaler Kontaktstellen (Points of Contact, PoC) für direkte Kommunikation zwischen den teilnehmenden Staaten (VBM 8). Weitere fünf Maßnahmen kamen 2016 dazu. Ursprünglich sollte noch ein drittes Paket über Stabilitätsmaßnahmen den Prozess abschließen, gemäß dem die teilnehmenden Staaten von destabilisierenden Aktivitäten Abstand genommen hätten, beispielsweise von Angriffen auf zivile und kritische Infrastruktur. Doch es gab in der Folge keinen politischen Willen mehr, die Maßnahmen zu erweitern. Auf VN-Ebene entwickelte sich zwischen 2022 und 2024, ergänzend zu den Normen verantwortungsvollen staatlichen Handelns, ein Rahmenwerk von acht freiwilligen vertrauensbildenden Maßnahmen, das insbesondere Transparenz, zwischenstaatliche Kommunikation und Kooperation fördern und Eskalationsrisiken mindern soll.

Die Organisation Amerikanischer Staaten (OAS) konzipierte, ergänzend zu den konventionellen VBMs, ebenfalls spezifische Cyber-VBMs. Allerdings richtet sich die Agenda der OAS stärker auf den Fähigkeitsaufbau, das heißt auf die Unterstützung von Staaten mit geringen Cyberfähigkeiten. Auch Einrichtung und Vernetzung nationaler Computer Security Incident Response Teams (CSIRTs) spielen eine wichtige Rolle. Im Vergleich zur OSZE ist die Arbeit der OAS bislang weniger stark von geopolitischen Blockaden geprägt.

Auch die ASEAN-Staatengruppe (Association of Southeast Asian Nations) bzw. ihr Regional Forum (ARF) verbindet vertrauensbildende Maßnahmen mit der regionsspezifischen Tradition präventiver Diplomatie. Der Schwerpunkt liegt auf Dialog, Fähigkeitsaufbau und technischer Zusammenarbeit, wobei vor allem die Vernetzung von CSIRTs eine wichtige Rolle spielt. Die Zusammenarbeit technischer Reaktionsstellen in Südostasien gilt dabei als ein Beispiel dafür, wie Vertrauen zunächst auf funktionaler und technischer Ebene aufgebaut werden kann. Auf dem afrikanischen Kontinent verfolgt die subregionale Economic Community of West African States (ECOWAS) beispielsweise Ansätze zur Stärkung regionaler Cybersicherheit, insbesondere indem sie die Erarbeitung regionaler Cyber-VBMs fördert. Eine besondere Herausforderung besteht in der Region weiterhin darin, Cybersicherheit nicht ausschließlich als technisches oder sicherheitspolitisches Problem zu behandeln, sondern als eine staatliche Aufgabe, die in Verbindung mit sozioökonomischer Entwicklung und der Stärkung der gesellschaftlichen Resilienz gedacht werden muss.

OSZE als Forum für Cyberdiplomatie

Die divergierenden Bedrohungsperzeptionen und die damit einhergehende Polarisierung innerhalb der OSZE unterscheiden sich deutlich von anderen regionalen Kontexten. Der Verlust geopolitischen Vertrauens hat die Handlungsfähigkeit der Organisation spätestens seit 2022 in zentralen sicherheitspolitischen Fragen erheblich eingeschränkt. Mit der Informellen Arbeitsgruppe (IWG) zu Cybersicherheit und Sicherheit in der Informations- und Kommunikationstechnik (IKT), die 2012 auf Grundlage des Beschlusses Nr. 1039 des Ständigen Rats eingerichtet wurde, verfügt

Grafik 2

Vertrauensbildende Maßnahmen (VBMs) der OSZE im Bereich Cyber-/IKT-Sicherheit

die OSZE jedoch über ein Gremium, das die Transparenz, Vorhersehbarkeit und Stabilität im Umgang mit IKT-Risiken fördern soll. Tagesordnungen und Diskussionen des primär technischen Organs sind weniger politisiert als die anderer OSZE-Gremien. Die teilnehmenden Staaten betrachten das Gremium, das zwei bis drei Mal pro Jahr in Wien zusammenkommt, als eine Art »Hygieneritual«, das zwar keine Schlagzeilen mache, aber nutzbringend sei. Die teilnehmenden Staaten tauschen sich hier über den Stand der Implementierung der VBMs und über aktuelle nationale Cyberstrategien, -doktrinen, und -Gesetzgebung aus. Die Inputs sind laut Interviewpartner:innen in der Regel substanziell und die Teilnahme der Delegationen, da auch online möglich, ist gewährleistet. Vieles, was im Rahmen der IWG geschieht, ist deklarativer Natur, doch bringt der Austausch mehr Transparenz und Berechenbarkeit mit sich. Ähnlich wie im VN-Kontext treten jedoch Schwierigkeiten bei der Definition zentraler Begriffe auf und es überwiegt die Zurückhaltung gegenüber rechtlich bindenden Verpflichtungen. Nichtsdestotrotz wurde eine Sprache und wurden Normen geschaffen, deren bloße Erhaltung bereits einen Mehrwert darstellt. Bemängelt wird von Interviewpartner:innen hingegen, dass das Cybermandat der OSZE jenseits von Vertrauensbildung nicht eindeutig sei. Auch, dass abrüstungskontrollpolitische Aspekte gänzlich ausgeklammert werden, wird teilweise kritisch gesehen.

Der Erfolg der insgesamt 16 VBMs (siehe Grafik 2) hängt maßgeblich davon ab, ob die teilnehmenden Staaten diese nicht nur implementieren, sondern tatsächlich anwenden. Im Rahmen der sogenannten »Adopt-a-CBM«-Initiative unterstützen einzelne Teilnehmerstaaten bei der Umsetzung bestimmter VBMs, bieten einen Erfahrungsaustausch an und entwickeln konkrete Implementierungsformate. Ein zentraler Ansatzpunkt ist hier die unter VBM 10 vorgesehene Nutzung bestehender OSZE-Plattformen, insbesondere des gesicherten OSCE Communications Network (CommsNet). Nach Einschätzung der Befragten unterscheiden sich Nutzung und Akzeptanz dieser Mechanismen durch die teilnehmenden Staaten erheblich. Auch die nationalen Voraussetzungen variieren. Einigen Staaten fehlen nach wie vor institutionelle und technische Fähigkeiten und teilweise auch das Bewusstsein für die Relevanz von VBMs,

um sich an ihrer praktischen Umsetzung beteiligen zu können.

Der Fähigkeitsaufbau erfüllt hier eine doppelte Funktion: Einerseits handelt es sich um eine eigenständige Maßnahme (VBM 5). Andererseits ist er ein Instrument, um Staaten überhaupt zur Umsetzung weiterer VBMs zu befähigen. Eine zunehmende Konzentration der OSZE auf Capacity Building kann zugleich als Reaktion auf die Grenzen politischen Handelns in der klassischen zwischenstaatlichen Vertrauensbildung interpretiert werden.

Auf nationaler Ebene wird auch der Resilienzaufbau immer wichtiger. Dies betrifft vor allem den Schutz kritischer Infrastruktur (VBM 15). Da diese häufig im privaten Sektor verortet ist, ist die Zusammenarbeit mit diesem ein Schlüssel (VBM 14 zu Öffentlich-privaten Partnerschaften). Diese VBMs verpflichten die Staaten dazu, Mechanismen für den Informationsaustausch zwischen der öffentlichen Verwaltung, Unternehmen und der Zivilgesellschaft zu etablieren. Private Unternehmen und die Zivilgesellschaft sollten daher ebenfalls Kenntnis von der Existenz von VBMs erhalten und involviert werden. Doch dies ist zwischen den zumeist westlichen Staaten und Staaten wie Russland und China umstritten. Während einige Staaten auf restriktive Akkreditierungs- und Beteiligungsverfahren drängen, setzen sich vor allem westliche Staaten für eine breite Einbindung des Privatsektors, der Wissenschaft und der Zivilgesellschaft ein. Nicht zuletzt vor diesem Hintergrund gewinnt eine regulatorisch-technische Dimension der Cybergovernance zunehmend an Bedeutung.

Technische und politische Kooperation

Die informelle Arbeitsweise der OSZE bietet das Potential, die Kooperation im Cyberraum maßgeblich zu verbessern. Anhand einer Analyse des staatlichen Reaktionsverhaltens im Cyberraum lässt sich aufzeigen, wo angesichts der verschärften geopolitischen Situation eine Kooperation in der OSZE und anderen Regionalorganisationen noch möglich sein könnte. Entscheidend ist dabei, welche Formen der Zusammenarbeit auch bei geringem politischem Vertrauen tragfähig sind.

Im Rahmen des EuRepoC-Projekts wurden 412 staatliche Reaktionen von Nato-Mitgliedstaaten auf Cyberangriffe aus den Jahren 2021 bis 2025 untersucht (Berechnungen auf Grundlage des bisher unveröffentlichten EuRepoC-Reaktionsdatensatzes). Die Daten lassen erkennen, dass die Kooperation alles in allem selbst unter Verbündeten begrenzt ist, aber auch, dass die Etablierung von Kooperationsmechanismen auf der technischen Ebene, also jenseits der politisch umstrittenen kollektiven Zuweisung von Schuld, besonders erfolgversprechend ist. Insgesamt ist das Reaktionsverhalten im Bündnis stark vom Sicherheitsdiskurs geprägt. 45 Prozent aller erfassten Reaktionen entfallen auf sogenannte Sicherheitshinweise *(Security Advisories)*, in denen Behörden zum Beispiel auf Sicherheitslücken, deren Ausnutzung oder Kampagnen bestimmter Akteure hinweisen, auf die formale Zuweisung von Verantwortung oder operative Handlungen. Und trotz der zunehmend kritischen Cybersicherheitslage wird nur auf einen kleinen Teil der erfassten Cybervorfälle überhaupt reagiert (17 Prozent). Unabhängig von ihrer Form bleiben die meisten Reaktionen (69 Prozent) auf einer kommunikativen Ebene. Sie laufen also ohne unmittelbare operative Konsequenzen ab.

Bemerkenswert ist die Differenz zwischen der technischen und der politischen Ebene. Im Gegensatz zur politischen Attribution wird im Rahmen der technischen Attribution regelmäßig nicht der verantwortliche Staat, sondern (manchmal ausschließlich) die verantwortliche Hackergruppe benannt. Die politische Zuweisung von Verantwortung wird dabei durch eine rein technische Warnung ersetzt, die sich mit Informationen zum Angriffsvektor in erster Linie an Verteidiger richtet, parallel jedoch auch dem Angreifer signalisiert, dass er »gesehen« wird. In diesem Sinne können Regierungen die Attribution auch an IT-

Sicherheitsunternehmen auslagern, um sich einen diplomatischen Spielraum zu schaffen und Eskalationsdynamiken besser kontrollieren zu können. Dabei unterscheiden sich die beiden Ebenen der Attribution auch in der Intensität der internationalen Zusammenarbeit: Die technische Ebene erlaubt oftmals eine engere Zusammenarbeit. Insgesamt haben 21,6 Prozent aller erfassten Reaktionen eine multilaterale Komponente. Besonders häufig sind dabei koordinierte Reaktionen, also solche, an denen mehrere Staaten beteiligt sind und aufeinander verweisen, dabei aber weiterhin eigene Statements veröffentlichen. Etwas weniger häufig sind gemeinsame Reaktionen, bei denen mehrere Staaten im Verbund handeln und schließlich ein gemeinsames Statement abgeben.

Auf der politischen Ebene erfolgen verstärkt koordinierte Reaktionen (28,3 Prozent der politischen Reaktionen). Staaten reagieren in diesen Fällen zwar prinzipiell eigenständig, stimmen ihre Reaktionen aber aufeinander ab und verweisen aufeinander. Eine engere Abstimmung bei gemeinsamen Reaktionen, bei der Staaten tatsächlich gemeinsam vorgehen, findet dagegen sehr viel stärker auf der technischen Ebene statt (41,2 Prozent der technischen Reaktionen). Dann werden gemeinsame Reaktionen oft als *Joint Advisories* von den operativen Cybersicherheitseinrichtungen getragen. Dabei entpolitisiert der technische Kanal die Frage von Schuld und Verantwortung und eröffnet somit andere Handlungsspielräume. Gemeinsame politische Erklärungen werden hingegen eher über internationale Einrichtungen wie den Nordatlantikrat der Nato oder den Hohen Vertreter bzw. den Rat der EU koordiniert und herausgegeben oder im Rahmen internationaler Konferenzen auf Außenministerebene verabschiedet. Die Beobachtung, dass selbst unter verbündeten Staaten lediglich die technische Ebene eine vertiefte Kooperation erlaubt, lässt Rückschlüsse darauf zu, welche (begrenzten) Optionen der Zusammenarbeit in anderen regionalen Kontexten denkbar sind. Gerade die technischen Formen der Kooperation, die keine gemeinsame politische Attribution voraussetzen, könnten begrenzte Handlungsspielräume offenhalten. Hieraus ergeben sich Ansatzpunkte dafür, wie die OSZE unter den Bedingungen eines anhaltenden *low trust environment* Kooperation im Cyberbereich aufrechterhalten kann.

Bezüglich der Klassifizierungen von Cybervorfällen stellt sich die Lage innerhalb der OSZE als ein Flickenteppich dar: Es fehlen gemeinsame Schwellenwerte, ab wann ein Vorfall als konsultationswürdig gilt. Gleichzeitig werden für Abstimmungen hinsichtlich Reaktionen und Attributionen unter Partnern vorhandene Formate im EU- und Nato-Rahmen bevorzugt. Letztlich entscheidet jeder Staat selbst, was ein »schwerwiegender« Vorfall ist — mit dem Ergebnis, dass im Rahmen der IWG bei den Lageberichten und der Vorstellung der Quartalszahlen erhebliche Unterschiede hinsichtlich der Berichtszahlen bestehen. Die Situation hinsichtlich berichtenswerter Cybervorfälle sei laut Beobachter:innen häufig eine ähnliche, nur die Klassifizierungssysteme unterschieden sich.

Strukturelle Defizite und Chancen

Cyberdiplomatie und -kooperation befinden sich aktuell in einem Spannungsfeld zwischen der Notwendigkeit der Aufrechterhaltung eines technischen Dialogs als Kanal für Risikominimierung und geopolitisch bedingter Stagnation.

Im derzeitigen Sicherheitsumfeld haben VBMs eine eher konservierende als transformierende Wirkung. Einige Staaten nutzen vorhandene Foren verstärkt für politisches oder vereinzelt sogar militärisches Signalling; für andere spielt der Kapazitätsaufbau eine weitaus wichtigere Rolle. Cyber-VBMs im Kontext steigender Inzidenzzahlen sind zwar nicht dazu da, gezielte Angriffe zu verhindern, aber sie bleiben wichtig, um die »Sprechfähigkeit« zwischen den Staaten zu erhalten und die Schwelle für unintendierte Eskalationen zu erhöhen. Doch der Kooperationswille und damit auch VBMs stoßen an Grenzen, wenn

es um nationale Sicherheits- und Souveränitätsinteressen oder offensive Fähigkeiten geht. Dies gilt besonders für die Klassifizierung von Vorfällen, die Koordination von Reaktionen sowie politische und technische Attributionen — in all diesen Bereichen ist kooperatives Vorgehen selbst unter verbündeten Staaten limitiert.

Gegenwärtig ist kaum vorstellbar, dass die OSZE oder andere übergeordnete Entitäten bei Fragen der Klassifizierung oder Attribution von Zwischenfällen unterstützen könnten. Die OSZE verfügt über kein Mandat oder Kompetenzen, um Vorfälle zu untersuchen bzw. zu klassifizieren. Deshalb sind Überlegungen geboten, wie die Harmonisierung nationaler Methodiken der Klassifizierung vorangetrieben werden kann, zum Beispiel durch subregionale Koalitionen oder Koalitionen der Willigen. Auch die Diskussion über Stabilitätsmaßnahmen sollte wieder aufgegriffen werden. Hierbei könnte es um die Konsequenzen von inakzeptablen und destabilisierenden Effekten sowie Fehlverhalten gehen, zum Beispiel um die Problematisierung von Cyberangriffen auf bestimmte zivile und kritische Infrastrukturen (in Anlehnung an Norm 13 (f) des UN GGE-Berichts zur Stärkung verantwortlichen Staatsverhaltens im Cyberraum).

Im Kontext von »low« bis »no trust« ist Risikominimierung bzw. -management auf der technischen Ebene heute aussichtsreicher als politische Vertrauensbildung. Auf der Arbeitsebene der teilnehmenden Staaten sind Handlungsspielräume größer und können einen Schutzraum für den fortlaufenden Dialog darstellen, auch weil hier ein höheres Maß an Informalität und entsprechende Kanäle vorhanden sind und die politisch brisanten Fragen der Zuordnung leichter ausgeklammert werden können. Doch sollte diese Erkenntnis nicht der weiteren Vertiefung von Silo-Strukturen auf der technischen und politischen Ebene Vorschub leisten. Tatsächlich wird in vielen Staaten Cybersicherheit noch immer als reines IT-Thema wahrgenommen. Bei schwerwiegenden Vorfällen trägt jedoch die politisch-diplomatische Ebene die Letztverantwortung. Die Analyse staatlicher Reaktionen auf Grundlage des Response-Datensatzes zeigt, dass die Muster multilateraler Kooperation überwiegen und die Staaten in der Cyberabwehr dann kooperieren, wenn es nicht um politische Zuweisung von Verantwortung, sondern um technische Warnungen geht.

Die Bereitschaft der teilnehmenden Staaten, den privaten Sektor einzubeziehen, ist höher, wenn es sich bei einem Vorfall nicht um einen politisch motivierten Cyberangriff, sondern zum Beispiel um Cyberkriminalität handelt.

Ausblick

Die Regierungen der OSZE-Teilnehmerstaaten sind gut beraten, einen zweigleisigen Ansatz zu verfolgen: Sie sollten weiter in vertrauensbildende Maßnahmen investieren und diese umsetzen, aber auch ihre nationale Cyberresilienz stärken. Maßnahmen zum Fähigkeitsaufbau können dabei eine Brücke schlagen, indem sowohl Vertrauensbildung niedrigschwellig weiterverfolgt wird als auch nationale Strukturen und Reaktionsfähigkeiten in der gesamten Region gestärkt werden. Cyber-VBMs bleiben vorerst eine wichtige substituierende Strategie, vor allem solange rüstungskontrollpolitische Maßnahmen im Cyberbereich nicht realisierbar sind. Es kann jedoch nicht erwartet werden, dass im Falle eines Waffenstillstands zwischen Russland und der Ukraine ein friedlicher Cyberraum die Folge sein wird. Gleichwohl sollte trotz aller strukturellen Defizite das Augenmerk auf die Chancen gelegt werden, die multilaterale Kooperation und Diplomatie im Cyberraum bieten.

Dr. Nadja Douglas ist Wissenschaftlerin in der Forschungsgruppe Osteuropa und Eurasien. Jonas Hemmelskamp ist Datenwissenschaftler im Projekt »European Repository of Cyber Incidents«, an der Ruprecht-Karls-Universität Heidelberg, Simon Muschick ist Informations- und Datenmanager bei der SWP.
Dieser Beitrag basiert auf Ergebnissen eines vom Auswärtigen Amt geförderten Projekts zur Rolle der OSZE in einer neuen europäischen Sicherheitsordnung. Die Autoren danken Mia Geiger für die Unterstützung beim Lektorat und der Zusammenstellung der Abbildungen sowie Alexandra Paulus für die hilfreichen Kommentare zu einem ersten Entwurf dieses Beitrags.

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: 10.18449/2026A43