EUROPÄISCHE
KOMMISSION

HOHER VERTRETER
DER UNION FÜR
AUSSEN- UND
SICHERHEITSPOLITIK

Brüssel, den 10.11.2022
JOIN(2022) 49 final

GEMEINSAME MITTEILUNG AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

EU-Cyberabwehrpolitik

I. EINLEITUNG

Die Rückkehr des Krieges nach Europa durch Russlands ungerechtfertigten und unprovozierten militärischen Angriff war ein Weckruf für alle, die das Sicherheits- und Verteidigungskonzept der EU und ihre Fähigkeit, ihre Vision voranzutreiben und ihre Interessen – auch im Cyberraum – zu verteidigen, infrage stellen. Autoritäre Regierungen versuchen, die auf Regeln basierende internationale Ordnung im Cyberraum infrage zu stellen und zu untergraben. Der Cyberraum ist daher wie auch der Land-, See-, Luft- und Weltraum immer stärker umkämpft. Das böswillige Verhalten im Cyberraum, das sowohl von staatlichen als auch von nichtstaatlichen Akteuren ausgeht, hat sich in den letzten Jahren verstärkt. Dazu gehören zunehmend auch Cyberangriffe auf militärische und zivile kritische Infrastruktur in der EU sowie im Rahmen von Missionen und Operationen.

Zwischen der zivilen und der militärischen Dimension des Cyberraums besteht keine klar Grenze, wie die jüngsten Angriffe auf Energienetze, Verkehrsinfrastruktur und Weltraumressourcen gezeigt haben. Dadurch wird auch deutlich, wie die physische und die digitale Infrastruktur miteinander verflochten sind und wie durch schwerwiegende Cybersicherheitsvorfälle kritische Infrastrukturen gestört oder beschädigt werden können. Dies erinnert eindringlich daran, dass die EU eine enge militärische und zivile Zusammenarbeit im Cyberraum braucht, um zu einem stärkeren Sicherheitsgarant zu werden.

Die EU muss mehr Verantwortung für ihre eigene Sicherheit übernehmen. Dies erfordert moderne und interoperable europäische Streitkräfte. Die Mitgliedstaaten müssen sich deshalb dringend und vorrangig dazu verpflichten, mehr in ihre Fähigkeiten im Bereich der Cyberabwehr, einschließlich aktiver Verteidigungsfähigkeiten, zu investieren. Die EU sollte sich weiterhin uneingeschränkt für das Völkerrecht und die internationalen Normen im Cyberraum einsetzen, aber auch ihre Bereitschaft signalisieren, diese Fähigkeiten im Falle eines Cyberangriffs auf einen Mitgliedstaat in koordinierter Weise zu nutzen.

Damit dies gelingt, muss die EU ihre technologische und digitale Souveränität im Cyberbereich sicherstellen. Die Handlungsfähigkeit der EU hängt davon ab, ob sie in der Lage ist, Spitzentechnologien für Cybersicherheit und Cyberabwehr in der EU zu nutzen und weiterzuentwickeln. Da bei Cybertechnologien ein großes Dual-Use-Potenzial gegeben ist, müssen zwischen den im Bereich Cybersicherheit und Cyberabwehr tätigen Unternehmen und den Forschungs-, Entwicklungs- und Innovationstätigkeiten viel mehr Synergien entwickelt werden, um die bessere Fähigkeiten zu entwickeln.

Die gemeinsame Prävention und Erkennung ist ein wichtiger Bestandteil der Verteidigungsfähigkeiten der EU. Die EU muss in der Lage sein, Angriffe frühzeitig zu erkennen. Erkennungsdaten müssen in verwertbare Informationen umgewandelt werden, die sowohl der Cybersicherheit als auch der Cyberabwehr dienen können. Eine solche Zusammenarbeit zwischen den militärischen und zivilen Cybergemeinschaften stellt die Grundlage für eine verbesserte gemeinsame Lageerfassung im Cyberraum dar und ist ebenso wichtig für koordinierte Krisenreaktionen auf technischer und auf operativer Ebene.

Der bewaffnete Konflikt in der Ukraine hat auch gezeigt, wie wertvoll eine enge Zusammenarbeit mit dem Privatsektor ist und wie wichtig es ist, Zugang zu privaten vertrauenswürdigen Anbietern zu haben, die als Cyberreserven fungieren und es ermöglichen, die Reaktion auf größere Cyberangriffe zu verbessern. Daher muss sichergestellt werden, dass

sich die Mitgliedstaaten auf die Unterstützung durch vertrauenswürdige Cyberreserven verlassen können und dass dies auf sichere und koordinierte Weise geschieht.

In dieser Gemeinsamen Mitteilung wird auf der Grundlage des Politikrahmens für die Cyberabwehr[1] eine ehrgeizige Strategie vorgeschlagen, die es der EU und ihren Mitgliedstaaten ermöglichen soll, im Cyberraum mit Selbstvertrauen und Durchsetzungsvermögen zu handeln. Ziel ist es, die Cyberabwehrfähigkeiten durch individuelle oder gemeinsame Maßnahmen der Mitgliedstaaten zu fördern und die Koordinierung und Zusammenarbeit zwischen den Cybergemeinschaften der Union zu stärken. Außerdem soll darauf hingearbeitet werden, die strategischen Abhängigkeiten der EU in Bezug auf kritische Cybertechnologien zu verringern und die technologische und industrielle Basis der europäischen Verteidigung (EDTIB) zu stärken. Im Rahmen der Strategie werden die Spielregeln der EU festgelegt und Möglichkeiten zur Stärkung der Solidarität innerhalb der Union im Hinblick auf die Cyberabwehr sowie für die Zusammenarbeit mit dem Privatsektor vorschlagen, um die Reaktion auf größere Cyberangriffe zu verbessern. Angesichts des länderübergreifenden Charakters von Cyberbedrohungen werden für beide Seiten vorteilhafte und maßgeschneiderte Partnerschaften im Bereich der Cyberabwehr, einschließlich des Aufbaus von Kapazitäten im Bereich der Cyberabwehr, entwickelt und die Cyberresilienz der Partnerländer gestärkt.

Wie in dem im März 2022 vom Rat angenommenen Strategischen Kompass für Sicherheit und Verteidigung[2] 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[3], der Ankündigung von Präsidentin von der Leyen in ihrer Rede zur Lage der Union 2021[4] und den Schlussfolgerungen des Rates zur Entwicklung der Cyberabwehr der Europäischen Union[5] vom 23. Mai 2022. In der Gemeinsamen Mitteilung über die Defizite bei den Verteidigungsinvestitionen aus dem Jahr 2022[6] wurden die EU und ihre Mitgliedstaaten darüber hinaus aufgefordert, die Arbeiten zur Schaffung einer vollwertigen Fähigkeit zur Cyberabwehr – angefangen bei Forschung, Erkennung und Schutz bis hin zur Reaktion – aufzunehmen.

[1] EU-Politikrahmen für die Cyberabwehr (Aktualisierung 2018) vom 19. November 2018, http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/de/pdf.
[2] Ein Strategischer Kompass für Sicherheit und Verteidigung – Für eine Europäische Union, die ihre Bürgerinnen und Bürger, Werte und Interessen schützt und zu Weltfrieden und internationaler Sicherheit beiträgt.
[3] Die Cybersicherheitsstrategie der EU für die digitale Dekade, JOIN(2020) 18 final.
[4] https://ec.europa.eu/commission/presscorner/detail/de/SPEECH_21_4701
[5] 9364/22 (auf Englisch).
[6] JOIN(2022) 24 final.

II. EU-CYBERABWEHR: SCHUTZ, AUFDECKUNG, ABSCHRECKUNG UND VERTEIDIGUNG

1. Gemeinsames Handeln für eine stärkere Cyberabwehr

Cyberangriffe sind häufig grenzüberschreitender Art und können sich physisch auf kritische Infrastrukturen in der EU auswirken. Schwerwiegende Cybersicherheitsvorfälle können zu erheblich sein, als dass die von einem oder mehreren betroffenen Mitgliedstaaten allein bewältigt werden können. Sie können auch Teil größerer hybrider Angriffe von Drittländern sein, die darauf abzielen, Wirtschaft und Gesellschaft zu destabilisieren, kritische Infrastrukturen, die für die Sicherheit der EU erforderlich sind, zu schwächen oder das Funktionieren von Demokratien zu untergraben und zu beeinträchtigen, unter anderem durch Angriffe auf Wahlinfrastrukturen.

Im Jahr 2018 benannte die EU den Cyberraum als einen Bereich für militärische Einsätze. In der 2021 angenommenen „militärischen Vision und Strategie für den Cyberraum als Einsatzbereich“[7] werden die Rahmenbedingungen festgelegt und die Ziele, Wege und Mittel beschrieben, die erforderlich sind, um den Cyberraum als Einsatzbereich zur Unterstützung der Operationen im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) der EU zu nutzen. Die Cyberabwehr und die Nutzung damit zusammenhängender Fähigkeiten im gesamten Spektrum militärischer Cyberraum-Einsätze sind ein nationales Vorrecht der Mitgliedstaaten und stützen sich auf ein umfassenderes Ökosystem, einschließlich einer starken industriellen Basis, die durch die Entwicklung von Fähigkeiten auf EU-Ebene unterstützt wird.

Die Cyberabwehrgemeinschaft der EU, die sich aus den Verteidigungsbehörden der Mitgliedstaaten zusammensetzt und von den Organen, Einrichtungen und sonstigen Stellen der EU (EU-OESS) unterstützt wird, weist im Vergleich zu den anderen Cybergemeinschaften[8] gewisse Besonderheiten auf und folgt einem anderen Governance-Modell. Das Fehlen eines Rahmens für den Informationsaustausch und die Zusammenarbeit zwischen den militärischen IT-Notfallteams der EU (milCERT), auch zur Unterstützung militärischer GSVP-Missionen und -Einsätze, ist angesichts des erhöhten Ausmaßes der Cyberbedrohungen durch staatliche und nichtstaatliche Akteure problematisch.

Die Zusammenarbeit zwischen der zivilen, der diplomatischen und der Cybergemeinschaft im Bereich der Strafverfolgung mit der Cyberabwehrgemeinschaft wird zu einem großen Mehrwert für alle beteiligten Akteure führen. Daher ist es von entscheidender Bedeutung, eine solche Zusammenarbeit zu ermöglichen, indem geeignete und sichere Mittel für den Informationsaustausch bereitgestellt und Übungen und andere Aktivitäten durchgeführt werden, die Vertrauen und ein gegenseitiges Verständnis schaffen.

Darüber hinaus gibt es derzeit nur eine begrenzte gegenseitige operative Unterstützung zwischen den Mitgliedstaaten. Die weitere Ausdehnung des Konzepts der Soforteinsatzteams für Cybervorfälle in der gesamten EU sollte auf der Grundlage des damit verbundenen Projekts

[7] EEAS(2021) 706 REV 4.
[8] Die zivile und die diplomatische Cybergemeinschaft sowie die Cybergemeinschaft im Bereich der Strafverfolgung.

für Teams für die rasche Reaktion auf Cybervorfälle und die gegenseitige Unterstützung im Bereich der Cybersicherheit (CRRT)[9] im Rahmen der Ständigen Strukturierten Zusammenarbeit (SSZ) geprüft werden, auch im Zusammenhang mit Artikel 42 Absatz 7 des Vertrags über die Europäische Union (EUV)[10] („Klausel über die gegenseitige Verteidigung“) und Artikel 222 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV)[11] („Solidaritätsklausel“). Die entscheidende Rolle des Privatsektors ist eine der Lehren, die aus der erfolgreichen Cyberabwehr der Ukraine im Zusammenhang mit dem russischen Angriffskrieg gezogen werden konnten. Daher sollte geprüft werden, inwieweit der Privatsektor auch zur Verbesserung der Cyberabwehr beitragen könnte.

1.1 Stärkung der gemeinsamen Lageerfassung und der Koordinierung innerhalb der Abwehrgemeinschaft

Angesichts des Ausmaßes des mit Cyberangriffen verbundenen Risikos müssen die Mitgliedstaaten über eine möglichst vollständige kollektive Lageerfassung verfügen, die auch die Fähigkeit zur Früherkennung sowie die Ressourcen für eine angemessene, solidarische und koordinierte Erholung umfasst.

Was die militärische Lageerfassung anbelangt, so muss ein EU-Koordinierungszentrum für die Cyberabwehr (**EU Cyber Defence Coordination Centre, EUCDCC**) eingerichtet werden, das eine bessere Lageerfassung innerhalb der Verteidigungsgemeinschaft, einschließlich aller militärischen GSVP-Kommandeure der EU, unterstützt. Der Hohe Vertreter wird den Vorschlag für das EUCDCC, der auf dem Projekt des SSZ-Koordinierungszentrums für den Cyber- und Informationsbereich (CIDCC)[12] aufbaut, den Mitgliedstaaten zur Prüfung vorlegen. Ziel ist eine ganzheitliche Analyse des Cyberraums, des elektromagnetischen Umfelds und des kognitiven Bereichs, indem verschiedene Informationsquellen für die militärstrategische und operative Ebene zusammengeführt werden. Es sollten geeignete Verbindungen zwischen dem EUCDCC und dem EU-Zentrum für Informationsgewinnung und Lageerfassung (EU INTCEN) sowie der Abteilung „Aufklärung“ des Militärstabs der EU im Rahmen des Einheitlichen Analyseverfahrens hergestellt werden. Zusätzlich zu externen Informationsquellen sollte das EUCDCC ein unabhängiges aktives IT-Sensorsystem einrichten und integrieren, um die Überwachung von Knotenpunkten im Besitz der EU zur Unterstützung militärischer GSVP-Missionen und -Operationen zu stärken. Dadurch wird für bessere Erkennungsfähigkeiten gesorgt, und es wird eine neue Informationsschicht geschaffen, um die Informationsbasis für die Bewertung von Cyberrisiken und die Lageerfassung weiter zu verbessern.

Für diese Zwecke sind Fähigkeiten erforderlich, die die Erstellung und Aufrechterhaltung eines rund um die Uhr funktionierenden und nach Möglichkeit anerkannten Lagebildes des Cyberraums ermöglichen und gewährleisten, einschließlich laufender und bevorstehender

[9] Teams für die rasche Reaktion auf Cybervorfälle und die gegenseitige Unterstützung im Bereich der Cybersicherheit.
[10] Vertrag über die Europäische Union, konsolidierte Fassung: ABl. C 326 vom 26.10.2012, S. 1.
[11] Vertrag über die Arbeitsweise der Europäischen Union, konsolidierte Fassung: ABl. C 326 vom 26.10.2012, S. 1.
[12] Ziel des Projekts ist die Entwicklung, Einrichtung und der Betrieb eines multinationalen Koordinierungszentrums für den Cyber- und Informationsbereich (CIDCC) als ein dauerhaftes multinationales militärisches Element.

Cybereinsätze sowohl von gegnerischen als auch von befreundeten Kräften. Ein solches Lagebild würde zur Planung und Durchführung militärischer GSVP-Missionen und -Operationen der EU beitragen. Es wird somit der militärische Beitrag dazu sein, die EU stärker für böswillige Handlungen im Cyberraum zu sensibilisieren und darauf zu reagieren.

Um das Vertrauen zu verbessern und zuverlässige und zeitnahe strategische Informationen über größere Cybervorfälle auszutauschen, wird die **EU-Konferenz der Cyberkommandeure** weiterentwickelt und gestärkt.[13] Mit der Europäischen Verteidigungsagentur (EDA) als Sekretariat und unter Beteiligung des Militärstabs der EU wird die Konferenz mindestens zweimal jährlich stattfinden, um operative Fragen und andere relevante Themen zu erörtern.

Es wird ein operatives Netz für **milCERT (MICNET)** eingerichtet, das von der EDA unterstützt wird. Alle Mitgliedstaaten sind aufgefordert, sich an MICNET zu beteiligen, das voraussichtlich im Januar 2023 einsatzbereit sein wird.

Durch die Erleichterung des Informationsaustauschs zwischen den milCERT wird mit MICNET eine robustere und koordiniertere Reaktion auf Cyberbedrohungen gefördert, die die Verteidigungssysteme in der EU betreffen, einschließlich solcher, die bei militärischen GSVP-Missionen und -Operationen verwendet werden. MICNET wird es auch ermöglichen, die Schulungsprozesse und die kontinuierliche Ermittlung neuer Anforderungen an die milCERT-Gemeinschaft langfristig aufrechtzuerhalten. In den kommenden vier Jahren wird die EDA gemeinsam mit den Mitgliedstaaten eine Infrastruktur für den Informationsaustausch sowie entsprechende Instrumente und Verfahren entwickeln, um den Austausch von Informationen zwischen den milCERT zu unterstützen. Ferner wird MICNET den Rahmen für eine jährliche Übung zur Erprobung, Validierung und Ermittlung neuer Anforderungen und Lösungen bieten.

1.2 Verbesserung der Koordinierung mit den zivilen Gemeinschaften

MICNET sollte den Rahmen und die Infrastruktur für den Informationsaustausch zwischen den verschiedenen Ebenen der Cyberabwehrgemeinschaft und externen Interessenträgern bieten.

Wenn die Entwicklung von MICNET ein gewisses Niveau erreicht hat, wird die EDA die Mitgliedstaaten dabei unterstützen, Möglichkeiten für eine Zusammenarbeit mit dem Netzwerk von Computer-Notfallteams (**Computer Security Incident Response Teams, CSIRT**) zu sondieren, in dem die nationalen CSIRT und das IT-Notfallteam der EU-OESS (CERT-EU) zusammenkommen. Diese Zusammenarbeit könnte gemeinsame Sitzungen und Übungen umfassen. Die Einbeziehung des Privatsektors in die Bemühungen zum Austausch von einschlägigen Informationen und zur Reaktion auf Cybervorfälle sollte ebenfalls geprüft werden.

Um ein effizienteres Cyberkrisenmanagement zu ermöglichen, sollte die EU-Konferenz der Cyberkommandeure mit dem Netzwerk der Verbindungsorganisationen für Cyberkrisen (CyCLONe) kooperieren, in dem die Mitgliedstaaten und die Kommission zusammenarbeiten, um die Koordinierung und Bewältigung großer Cybersicherheitsvorfälle in der EU zu unterstützen. Dabei wird militärische Erfahrung mit ziviler Lageerfassung auf strategischer und operativer Ebene kombiniert.

[13] Aufbauend auf den ersten beiden Sitzungen der strategischen Konferenzen der europäischen Cyberkommandeure (CyberCo) im Januar und Juni 2022 haben die Cyberkommandeure der EU beschlossen, ein dauerhafteres Forum auf ihrer Ebene einzurichten.

Neben seiner Funktion als zentraler Knotenpunkt für die Sammlung, Analyse, Bewertung und anschließende Verbreitung von Informationen im Zusammenhang mit der Cyberabwehr, insbesondere für militärische GSVP-Missionen und -Operationen, könnte das EUCDCC auch mit dem interinstitutionellen Krisenstab für Cybersicherheit[14] zusammenarbeiten, der eingerichtet wurde, um eine fundierte Beschlussfassung und eine koordinierte Reaktion der EU-OESS bei größeren Cyberkrisen auf strategischer und operativer Ebene sicherzustellen.

Das EUCDCC kann auch einschlägige Informationen mit einem Cyber-Lage- und Analysezentrum austauschen, das derzeit innerhalb der Kommission mit Unterstützung der Agentur der Europäischen Union für Cybersicherheit (ENISA) und des CERT-EU eingerichtet wird, um Analysen und eine wirksamere Unterstützung des Krisenmanagements bereitzustellen.

Darüber hinaus stellt der Mangel an gemeinsam genutzten oder interoperablen sicheren Kommunikationsinstrumenten und -plattformen zwischen den Mitgliedstaaten und den einschlägigen EU-OESS nach wie vor ein großes Hindernis dar. Die Kommission und die einschlägigen Institutionen führen zurzeit eine Bestandsaufnahme der bestehenden Instrumente für eine sichere Kommunikation im Cyberbereich durch. Auf der Grundlage dieser Bestandsaufnahme der bestehenden Instrumente wird die Kommission dem Rat Ende 2022 ihre Empfehlungen vorlegen, um weitere Maßnahmen zu beschließen.

Cybersolidarität in der EU für eine bessere gemeinsame Erkennung und Lageerfassung

Zivile Unterstützungsmaßnahmen können die gemeinsame Lageerfassung weiter verbessern. Die Cyberabwehrgemeinschaft wird von besseren zivilen Fähigkeiten zur Erkennung und Lageerfassung profitieren, die für den Schutz kritischer Infrastrukturen der EU entwickelt werden. Zu diesem Zweck bereitet die Kommission eine Initiative zur Förderung des Aufbaus einer EU-Infrastruktur von Sicherheitseinsatzzentren (Security Operation Centres, SOCs) vor, deren erste Phase in den kommenden Wochen eingeleitet und die dann erweitert und in größerem Maßstab eingesetzt werden sollen.[15] Diese Infrastruktur würde sich letztlich aus mehreren länderübergreifenden SOC-Plattformen zusammensetzen, auf denen die jeweiligen nationalen SOCs zusammengeführt werden, mit Unterstützung aus dem Programm „Digitales Europa“[16] zur Ergänzung der nationalen Finanzierung. Durch legislative Änderungen am Programm „Digitales Europa“ könnte eine längerfristige finanzielle Unterstützung für die gemeinsame Beschaffung ultrasicherer Instrumente und Infrastrukturen der nächsten Generation ermöglicht werden. Dadurch könnte die geplante SOC-Infrastruktur der EU die kollektiven Erkennungsfähigkeiten durch den Einsatz der neuesten künstlichen Intelligenz (KI) und von Datenanalysen, die die zivilen Kommunikationsnetze abdecken, verbessern. Durch die so gewonnen einsetzbaren Erkenntnisse über Cyberbedrohungen könnten Behörden und einschlägige Stellen rechtzeitig gewarnt werden, damit sie größere Cybervorfälle erkennen und wirksam darauf reagieren können. Der Umfang der Infrastruktur hängt von der

[14] Eine informelle Gruppe, in der die zuständigen Kommissionsdienststellen, der EAD, die Agentur der Europäischen Union für Cybersicherheit (ENISA), das CERT-EU und Europol unter dem gemeinsamen Vorsitz der Kommission und des Hohen Vertreters vertreten sind.

[15] Die Cybersicherheitsstrategie der EU für die digitale Dekade (JOIN(2020) 18 final) und die EU-Strategie für eine Sicherheitsunion (COM(2020) 605).

[16] Im Einklang mit der Verordnung (EU) 2021/694 des Europäischen Parlaments und des Rates vom 29. April 2021 zur Einrichtung des Programms „Digitales Europa“ und zur Aufhebung des Beschlusses (EU) 2015/2240 (ABl. L 166 vom 11.5.2021, S. 1) und vorbehaltlich etwaiger Änderungen.

Gesamtfinanzierung ab, die auf nationaler Ebene und von der Union vorbehaltlich der im mehrjährigen Finanzrahmen verfügbaren Haushaltsmittel bereitgestellt werden kann.

Durch solche länderübergreifenden SOCs könnte auch die Beteiligung des Verteidigungsbereichs ermöglicht werden, indem mit Blick auf die Governance und die Art der ausgetauschten Informationen eine „Verteidigungssäule" eingerichtet wird. Diese „Verteidigungssäule" würde gemeinsam mit dem Hohen Vertreter entwickelt und könnte einen speziellen Mechanismus für den Informationsaustausch mit militärischen Akteuren, einschließlich des EUCDCC, umfassen, für den Sicherheitsstandards auf Verteidigungsebene entwickelt werden könnten.

Cybersolidarität in der EU in Bezug auf Abwehrbereitschaft, Reaktion und Wiederherstellung

Cybersicherheitsvorfälle sind häufig so schwerwiegend, dass sie von einem oder mehreren betroffenen Mitgliedstaaten allein nicht bewältigt werden können. In solchen Fällen muss es den Mitgliedstaaten möglich sein, gegenseitige Unterstützung und Solidarität in Anspruch zu nehmen, auch im Zusammenhang mit Artikel 42 Absatz 7 EUV und Artikel 222 AEUV. Der Hohe Vertreter wird in Zusammenarbeit mit der Kommission und den Mitgliedstaaten Möglichkeiten für die **Ausweitung des Konzepts der Soforteinsatzteams für Cybervorfälle (CRRT)** auf der Grundlage des damit verbundenen CRRT-Projekts im Rahmen der SSZ sondieren, damit die EU-Mitgliedstaaten und die GSVP-Missionen und -Operationen besser unterstützt werden können. Aufgabe dieser Teams wäre es, auf Anfrage und je nach den spezifischen Bedürfnissen im Einzelfall maßgeschneiderte und gezielte kurzfristige Unterstützung zu leisten. Dies könnte gegebenenfalls auch Optionen für die Unterstützung durch vertrauenswürdige private Partner umfassen, um effiziente Reaktions- und Wiederherstellungsmaßnahmen zu gewährleisten.

Im Rahmen der EU-Initiative zur Cybersolidarität bereitet die Kommission Maßnahmen zur Stärkung der Abwehrbereitschaft und Reaktionsfähigkeit in der gesamten EU vor. Dies würde die Prüfung **wesentlicher Einrichtungen, die kritische Infrastruktur betreiben, auf potenzielle Schwachstellen auf der Grundlage von EU-Risikobewertungen** – aufbauend auf bereits von der Kommission gemeinsam mit der ENISA eingeleiteten Maßnahmen – sowie Bewältigungsmaßnahmen bei Cybervorfällen zur Abmilderung der Auswirkungen schwerwiegender Vorfälle, zur Unterstützung einer sofortigen Wiederherstellung und/oder zur Wiederherstellung der Funktionsfähigkeit wesentlicher Dienste umfassen.[17]

Die EU-Initiative für Cybersolidarität könnte die **schrittweise Einrichtung einer Cyberreserve auf EU-Ebene mit Dienstleistungen vertrauenswürdiger privater Anbieter** unterstützen, die bereit wäre, bei erheblichen grenzüberschreitenden Vorfällen auf Ersuchen der Mitgliedstaaten einzugreifen. Die Aufgaben und Zuständigkeiten sollten klar festgelegt und vollständig mit den bestehenden Stellen koordiniert werden, um sicherzustellen, dass die Unterstützung durch die Cyberreserve auf EU-Ebene dort bereitgestellt wird, wo sie benötigt wird, und um andere mögliche Formen der Unterstützung zu ergänzen. Zwar würde der Umfang der Maßnahmen und die Aufteilung der Kosten spezifischer Einsätze von den verfügbaren EU-Mitteln abhängen, die EU würde aber auch einen Mehrwert schaffen, indem sie die Verfügbarkeit und Bereitschaft einer solchen Reserve auf EU-Ebene sicherstellt. Um

[17] Aufruf von Nevers zur Stärkung der Cybersicherheitsfähigkeiten (auf Französisch).

ein hohes Maß an Vertrauen sicherzustellen, wird die Kommission auch die Möglichkeiten prüfen, die Entwicklung von Systemen für die Zertifizierung der Cybersicherheit für private Cybersicherheitsunternehmen zu unterstützen.

Übungen sind ein Schlüsselelement für die Herstellung der Abwehrbereitschaft. Sie fördern die Entwicklung einer gemeinsamen Wissensbasis und eines gemeinsamen Verständnisses der Cyberabwehr, wodurch wiederum die operative Abwehrbereitschaft verbessert wird. Gemeinsame Cyberabwehrübungen werden auch die Interoperabilität und das Vertrauen zwischen den Interessenträgern stärken, auch zur Unterstützung militärischer GSVP-Missionen und -Operationen. Aufbauend auf der CYBER-PHALANX-Reihe[18] und den milCERT-Übungen **wird die EDA ein neues Projekt mit der Bezeichnung „CyDef-X" einrichten, an dem alle Mitgliedstaaten teilnehmen und das als Rahmen für EU-Übungen zur Cyberabwehr dienen wird**. Dieses Projekt könnte dazu dienen, gegenseitige Unterstützung gemäß Artikel 42 Absatz 7 EUV zu leisten. Ferner sollte der Einsatz spezieller Test-, Schulungs- und Übungsumgebungen im Bereich der Cyberabwehr (z. B. Cyber-Range-Verbände) geprüft werden, unter anderem im Rahmen des SSZ-Projekts „Cyber Ranges Federations"[19].

Darüber hinaus können Übungen eine wichtige Rolle bei der Verbesserung der Zusammenarbeit zwischen zivilen und militärischen Einrichtungen spielen. Bei der Organisation von Übungen sollten ENISA, EDA und andere einschlägige Stellen daher systematisch die Einbeziehung von Teilnehmern aus anderen Cybergemeinschaften in Erwägung ziehen.

Im Rahmen der Stärkung der Fähigkeit der EU, Cyberangriffe zu verhindern, von ihnen abzuschrecken und darauf zu reagieren, und im Einklang mit der EU-Cybersicherheitsstrategie von 2020 und dem Strategischen Kompass wird der Hohe Vertreter 2023 Optionen für eine weitere Stärkung des EU-Instrumentariums für die Cyberdiplomatie[20] vorschlagen, das sich auf die Elemente der Cyberabwehr der EU und die seit der Einrichtung des Instrumentariums gewonnen Erkenntnisse stützt.

Maßnahmen zur Cyberabwehr

- Einrichtung eines EU-Koordinierungszentrums für die Cyberabwehr als Zentrum für die gemeinsame militärische Lageerfassung und Prüfung der Modalitäten für die Zusammenarbeit mit dem Lage- und Analysezentrum der Kommission.
- Weiterentwicklung und Stärkung der EU-Konferenz der Cyberkommandeure.
- Aufforderung an die Mitgliedstaaten, sich aktiv an MICNET, dem Netz militärischer CERT, zu beteiligen und auf den Aufbau einer Zusammenarbeit mit dem zivilen CSIRT-Netz hinzuarbeiten.
- Entwicklung eines neuen Rahmenprojekts (CyDef-X) zur Unterstützung von EU-Übungen im Bereich der Cyberabwehr.

[18] https://eda.europa.eu/publications-and-data/factsheets/factsheet-cyber-phalanx (auf Englisch).
[19] https://www.pesco.europa.eu/project/cyber-ranges-federations-crf/ (auf Englisch).
[20] Schlussfolgerungen des Rates zu einem Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten („Cyber Diplomacy Toolbox").

- Prüfung von Möglichkeiten zur Weiterentwicklung des Konzepts der Soforteinsatzteams für Cybervorfälle auf der Grundlage des CRRT-Projekts der SSZ.
- Prüfung von Möglichkeiten zur Weiterentwicklung von Projekten in Bezug auf Cyber-Range-Verbände (Cyber Ranges Federations).

Zivile Unterstützungsmaßnahmen

- Vorbereitung einer EU-Initiative für Cybersolidarität, einschließlich eines möglichen Rechtsakts zur Vornahme legislativer Änderungen am Programm „Digitales Europa“:
    - um die gemeinsamen Fähigkeiten der EU zur Erkennung, Lageerfassung und Bewältigung zu stärken;
    - um schrittweise eine Cyberreserve mithilfe von Dienstleistungen vertrauenswürdiger privater Anbieter aufzubauen;
    - um die Prüfung von kritischen Einrichtungen auf potenzielle Schwachstellen auf der Grundlage von EU-Risikobewertungen zu unterstützen.
- Prüfung der Entwicklung von Systemen für die Zertifizierung der Cybersicherheit auf EU-Ebene für die Cybersicherheitsbranche und private Unternehmen.
- Ausbau der Zusammenarbeit auf strategischer, operativer und technischer Ebene zwischen der Cyberabwehrgemeinschaft und anderen Cybergemeinschaften.

2. Sicherung des Verteidigungsökosystems der EU

In den letzten Jahren hat die Zahl der Cyberangriffe dramatisch zugenommen, darunter Angriffe auf Lieferketten im Zusammenhang mit Cyberspionage, Ransomware oder Störungen. Im Jahr 2020 betraf der Angriff auf die Lieferkette von SolarWinds[21] weltweit mehr als 18 000 Organisationen, darunter staatliche Stellen, große Firmen und Rüstungsunternehmen. Die Ausnutzung einer Schwachstelle in der Log4j-Software[22] von Apache hat gezeigt, dass selbst Softwarekomponenten, die nicht als hochriskant oder kritisch gelten, als Waffe dienen können, um in der EU erfolgreich Angriffe auf große Unternehmen oder Regierungen, auch im Verteidigungsbereich, durchzuführen. Dies zeigt eindeutig, dass die Cyberresilienz von Einrichtungen, die im Verteidigungsökosystem der EU aktiv sind – einschließlich militärischer Einrichtungen, der Verteidigungsindustrie und privater Akteure –, weiter gestärkt werden muss.

Streitkräfte sind in Bezug auf Bereiche wie Mobilität, Kommunikation oder Energie in hohem Maße von zivilen kritischen Infrastrukturen abhängig. Der Angriff Russlands auf das Satellitennetz KA-SAT[23], durch den die Kommunikation zwischen mehreren Behörden und

[21] https://cybernews.com/security/solarwinds-hack-the-mystery-of-one-of-the-biggest-cyberattacks-ever/ (auf Englisch).
[22] https://english.ncsc.nl/topics/log4j-vulnerability (auf Englisch).
[23] Erklärung des Hohen Vertreters im Namen der Europäischen Union zu böswilligen Cyberaktivitäten von Hackern und Hackergruppen im Zusammenhang mit der Aggression Russlands gegen die Ukraine: https://www.consilium.europa.eu/de/press/press-releases/2022/07/19/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-malicious-cyber-activities-conducted-by-hackers-and-hacker-groups-in-the-context-of-russia-s-aggression-against-ukraine/.

den ukrainischen Streitkräften gestört wurde, ist ein Beispiel für eine derartige Wechselbeziehung. Dies zeigt, dass diese kritische Infrastruktur gesichert werden muss.

Um Probleme im Zusammenhang mit der Sicherheit ihrer Kommunikations- und Informationssysteme (CIS) anzugehen, entwickeln die Mitgliedstaaten ihre eigenen Sicherheitsstandards und -anforderungen für militärische Systeme, bei denen nicht immer die Notwendigkeit der Interoperabilität oder das Vorhandensein ziviler Normen für Produkte mit doppeltem Verwendungszweck berücksichtigt werden. Dies wirkt sich negativ auf die Fähigkeit der Mitgliedstaaten aus, im Cyberraum zusammenzuarbeiten, auch im Rahmen militärischer GSVP-Missionen und -Operationen, und behindert die gegenseitige Unterstützung. Darüber hinaus müssen stärkere Synergien zwischen militärischen und zivilen Normungsprozessen gefördert werden, da der Industrie bei der Entwicklung von Produkten mit doppeltem Verwendungszweck durch die Befolgung ähnlicher, aber unterschiedlicher Normen für zivile und militärische Kunden höhere Produktionskosten entstehen.

2.1. Stärkung der Cyberresilienz des Verteidigungsökosystems

Die Stärkung der Cyberresilienz des Verteidigungsökosystems erfordert gezielte Maßnahmen und Investitionen in einem breiten Spektrum von Einrichtungen, von der militärischen Infrastruktur der Mitgliedstaaten über GSVP-Missionen und -Operationen bis hin zu kritischen Infrastrukturen, der Verteidigungsindustrie und einschlägigen Forschungseinrichtungen.

Für erfolgreiche GSVP-Missionen und -Operationen ist es notwendig, die Informationen, die für eine fundierte Entscheidungsfindung erforderlich sind, zu schützen. Die EU und ihre Mitgliedstaaten müssen ihre militärischen Kommando- und Kontrollstrukturen weiter stärken und ihre Infrastruktur weiterentwickeln und sichern. Dies gilt auch für politisch-militärische Konsultationen in den frühen Phasen der Krisenbewältigung im Hinblick auf den wirksamen Einsatz des operativen Hauptquartiers, einschließlich des militärischen Planungs- und Durchführungsstabs (MPCC). Dies wird insbesondere durch die Weiterentwicklung des „Operation Wide Area Network“ der EU angegangen.

Im Zusammenhang mit militärischen Missionen und Operationen sind Cyberabwehrakteure mit Informationen unterschiedlicher Formate und Klassifikationen aus unterschiedlichen Quellen befasst. Daher ist die Anwendung sicherer, modernster Technologien wie KI mit Unterstützung der Industrie äußerst wichtig.

Die Sicherheit der CIS-Infrastruktur muss durch die Anwendung einvernehmlich vereinbarter Verwaltungsverfahren verbessert werden, um das Vertrauen in die Integrität der verfügbaren Informationen bei den Beteiligten zu stärken. Darüber hinaus wird der Hohe Vertreter, auch in seiner Eigenschaft als Leiter der EDA, mit Unterstützung der Kommission die Mitgliedstaaten bei der Ausarbeitung **nicht rechtsverbindlicher Empfehlungen für die Verteidigungsgemeinschaft unterstützen, die sich an der Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2)**[24] orientieren, da die

[24] Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148, auf die sich die Mitgesetzgeber kürzlich geeinigt haben und die voraussichtlich bis Ende dieses Jahres förmlich angenommen wird.

Verteidigung vom Anwendungsbereich der Richtlinie ausgenommen ist. Dies wird dazu beitragen, dass die Cyberabwehr insgesamt ausgereifter wird.

Die Kommission hat ein Cyberresilienzgesetz[25] vorgeschlagen, das Anforderungen an die Cybersicherheit für Produkte mit digitalen Elementen enthalten soll und mit dem die Angriffsfläche bei Produkten mit doppeltem Verwendungszweck, die beispielsweise von der Verteidigungsindustrie und staatlichen Akteuren im Verteidigungsbereich in Kommunikations- und Informationssystemen eingesetzt werden, weiter verringert werden soll. Dem Vorschlag zufolge wären die Hersteller verpflichtet, innerhalb von 24 Stunden aktiv ausgenutzte Schwachstellen der ENISA zu melden, die die zuständigen nationalen CSIRT informieren wird. In diesem Zusammenhang wäre es auch wichtig, dafür zu sorgen, dass die Verteidigungsgemeinschaft rasch über Schwachstellen bei Produkten mit digitalen Elementen sowie über verfügbare und/oder angewandte Korrekturen und Abhilfemaßnahmen informiert wird.

Angesichts der Abhängigkeit des Militärs von kritischen zivilen Infrastrukturen ist es umso wichtiger, **den Schutz kritischer Infrastrukturen vor groß angelegten Cyberangriffen weiter zu verbessern**. Auf Ersuchen des Rates[26] entwickeln die Kommission, der Hohe Vertreter und die NIS-Kooperationsgruppe[27] Risikoszenarien für die Sicherheit der digitalen Infrastruktur. Der Schwerpunkt wird in erster Linie auf der Cybersicherheit in den Bereichen Energie, Telekommunikation und Verkehr sowie Raumfahrt liegen. Darüber hinaus werden gezielte Risikobewertungen im Hinblick auf die Cybersicherheit für Kommunikationsinfrastruktur und Kommunikationsnetze in der EU (einschließlich fester und mobiler Infrastruktur, Satellitenkabel, Unterseekabel und Internet-Routing) erstellt.[28] In Bezug auf den Schutz kritischer Infrastrukturen vor vom Menschen verursachten Bedrohungen, einschließlich hybrider Bedrohungen, werden die Mitgliedstaaten in dem Vorschlag für eine Empfehlung des Rates für eine koordinierte Vorgehensweise der Union zur Stärkung der Resilienz kritischer Infrastruktur[29] unter anderem aufgefordert, für angemessene Stresstests und Krisenkoordinierung zu sorgen. Die kritische maritime Infrastruktur, einschließlich des Schutzes von unterseeischen Datenkabeln, wird im Rahmen der bevorstehenden Überarbeitung der EU-Strategie für maritime Sicherheit und des dazugehörigen Aktionsplans weiter angegangen. Weitere Maßnahmen zur Stärkung der Cybersicherheit kritischer Infrastruktur im Energiesystem sind im EU-Aktionsplan zur Digitalisierung des Energiesystems[30] festgelegt.

Weltraumgestützte Dienste sind von zunehmender Bedeutung für die Verteidigung, sei es für die Überwachung, die Lageerfassung, die genaue Positionierung oder die ultrasichere Kommunikation. Sie stellen daher wichtige strategische Vorteile für die technologische Souveränität dar. Die Störung weltraumgestützter Dienste könnte erhebliche Auswirkungen auf die Verteidigungssysteme, aber auch auf die Gesellschaft und die Wirtschaft insgesamt haben. Ihre Resilienz ist für die allgemeine Cyberresilienz von zentraler Bedeutung, da sie Ziel

[25] Vorschlag für eine Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020, COM(2022) 454 final.
[26] Schlussfolgerungen zur Entwicklung der Cyberabwehr der Europäischen Union; ST09364/22, 23. Mai 2022.
[27] https://digital-strategy.ec.europa.eu/de/policies/nis-cooperation-group
[28] Aufruf von Nevers zur Stärkung der Cybersicherheitsfähigkeiten (auf Französisch).
[29] Vorschlag für eine Empfehlung des Rates für eine koordinierte Vorgehensweise der Union zur Stärkung der Resilienz kritischer Infrastruktur, COM(2022) 551 final.
[30] Digitalisierung des Energiesystems – EU-Aktionsplan (COM(2022) 552 final).

böswilliger Angriffe sein können. Wie vor allem auch die Angriffe auf KA-SAT-Netze zeigen, sind Weltraumsysteme zunehmend Cyberbedrohungen ausgesetzt, die die Verfügbarkeit oder Kontinuität weltraumgestützter Dienste beeinträchtigen können. Dies birgt ein Risiko für die strategischen und sicherheitspolitischen Interessen der EU im Weltraumbereich sowie für Weltraumfähigkeiten, die die Cyberabwehr ermöglichen und unterstützen. In der im Strategischen Kompass[31] angekündigten EU-Weltraumstrategie für Sicherheit und Verteidigung werden Maßnahmen zur Verbesserung der Robustheit und Cyberresilienz von Weltrauminfrastrukturen und damit verbundenen Diensten sowie zur Abschreckung und zur Reaktion auf Bedrohungen sensibler Weltraumsysteme und -dienste in der EU, insbesondere zur Bewältigung von Cyberbedrohungen, dargelegt.

Die Kommission fordert die Mitgliedstaaten außerdem dringend auf, die im EU-Instrumentarium für die 5G-Cybersicherheit[32] empfohlenen Maßnahmen umzusetzen. Mitgliedstaaten, die noch keine Beschränkungen für Hochrisikoanbieter eingeführt haben, sollten dies unverzüglich tun, da durch die verlorene Zeit die Anfälligkeit der Netze in der EU zunehmen kann. Solche Risiken können für militärische Mittel relevant sein und sich auf das allgemeine Verteidigungsumfeld der Mitgliedstaaten auswirken.

Was die **Cyberresilienz der europäischen Verteidigungsindustrie sowie von Forschungs- und Entwicklungseinrichtungen im Verteidigungsbereich** betrifft, so fallen diese Einrichtungen in den Anwendungsbereich der NIS2-Richtlinie, sofern sie von den Mitgliedstaaten nicht ausdrücklich ausgeschlossen werden. Dies würde es erforderlich machen, dass diese Einrichtungen über ein Programm für das Risikomanagement der Cybersicherheit verfügen, das die Sicherheit der Lieferkette sowie die Meldung von Cybervorfällen umfasst. Da der Privatsektor bei der Erbringung von Cybersicherheitsdiensten im Verteidigungsökosystem eine wichtige Rolle spielt, sollten die Mitgliedstaaten außerdem Systeme für die Zertifizierung der Cybersicherheit nutzen. Ein **EU-System für die Zertifizierung der Cybersicherheit für Unternehmen, die Dienstleistungen für die Verteidigungsindustrie erbringen**, könnte geprüft werden, um auf der Grundlage der Erfahrungen der ENISA ein harmonisiertes Maß an Vertrauen in den Markt zu schaffen.

2.2. Gewährleistung der Interoperabilität und Kohärenz der Normen im Bereich der EU-Cyberabwehr

Interoperabilität und Einheitlichkeit sind wichtige Anforderungen, die ab der Konzeptionsphase der Cyberabwehrfähigkeiten zu berücksichtigen sind, wobei auch die Lehren aus laufenden Missionen und Operationen zu berücksichtigen sind, die unter der Leitung des Militärstabs der EU mit Unterstützung der EDA ermittelt wurden. Die Grundsätze, Verfahren und Normen, die im Rahmen der Initiative „Federated Mission Networking“ (FMN)[33] vereinbart werden, sollten als Richtschnur für die Entwicklung nationaler Cyberabwehrfähigkeiten dienen, um die Interoperabilität sicherzustellen.

---

[31] A Strategic Compass for Security and Defence (Ein strategischer Kompass für Sicherheit und Verteidigung), 21. März 2022, https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf (auf Englisch).

[32] Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures |Shaping Europe’s digital future (europa.eu) (Cybersicherheit von 5G-Netzen – EU-Instrumentarium der Risikominderungsmaßnahmen | Gestaltung der digitalen Zukunft Europas) (auf Englisch).

[33] https://dnbl.ncia.nato.int/FMNPublic/SitePages/Home.aspx (auf Englisch).

Durch die Harmonisierung der Anforderungen an die Cyberabwehrfähigkeiten der nächsten Generation können die gemeinsamen Anstrengungen erleichtert werden, was möglicherweise zu gemeinsamen Entwicklungs- und Beschaffungsinitiativen und einer integrierten Lebenszyklusunterstützung führen könnte. Aus diesem Grund werden die EDA und der Militärstab der EU **Empfehlungen zu einer Reihe von Interoperabilitätsanforderungen in Bezug auf die Cyberabwehr der EU** ausarbeiten. Diese Anforderungen müssen über alle Planungshorizonte hinweg berücksichtigt werden, um alle Aspekte der Normung als entscheidende Voraussetzung für die Interoperabilität zu garantieren. Anforderungen an die Prüfung, Bewertung und Zertifizierung sind weitere wichtige Voraussetzungen.

Harmonisierte Normen für die Cybersicherheit werden für Hardware- und Softwareprodukte und -komponenten im Rahmen des vorgeschlagenen Cyberresilienzgesetzes[34] entwickelt. Diese Normen werden für alle zivilen Produkte mit doppeltem Verwendungszweck mit digitalen Elementen gelten, was für einen großen Teil der im Verteidigungssektor verwendeten Produkte zutrifft. Soweit möglich, wird die Kommission die Kohärenz mit verteidigungsbezogenen Normen bezüglich der Cybersicherheit für digitale Produkte fördern. Wie im Aktionsplan für Synergien zwischen der zivilen, der Verteidigungs- und der Weltraumindustrie[35] (im Folgenden „Synergien-Aktionsplan“) dargelegt, wird die Kommission in enger Zusammenarbeit mit den wichtigsten Interessenträgern einen Plan zur Förderung der Nutzung bestehender hybrider ziviler/verteidigungsbezogener Normen und der Entwicklung neuer Normen vorlegen. Die Zusammenarbeit zwischen allen einschlägigen Interessenträgern, einschließlich der europäischen Normungsorganisationen, der Nordatlantikvertrags-Organisation (NATO) und anderer Partner sollte weiterentwickelt werden, wobei das Europäische Komitee für die Normung im Verteidigungsbereich bestmöglich eingesetzt werden sollte. Wenn militärische Normungsgremien neue Normen in Bezug auf die Cybersicherheit von Produkten mit digitalen Elementen für Verteidigungszwecke entwickeln, sollten harmonisierte Normen, die im Rahmen des Cyberresilienzgesetzes entwickelt wurden, als Ausgangsbasis herangezogen werden.[36]

Maßnahmen zur Cyberabwehr

- Unterstützung der Mitgliedstaaten bei der Ausarbeitung nicht rechtsverbindlicher Empfehlungen für die Verteidigungsgemeinschaft in Anlehnung an die NIS2, um die Cyberabwehr auf nationaler Ebene insgesamt ausgereifter zu machen.
- Ausarbeitung von Empfehlungen zu den Interoperabilitätsanforderungen der EU im Bereich der Cyberabwehr.
- Intensivierung der Zusammenarbeit mit allen einschlägigen Akteuren hinsichtlich verteidigungsbezogener Normen im Rahmen des Europäischen Komitees für die Normung im Verteidigungsbereich.

[34] COM(2022) 454 final.
[35] COM(2021) 70 final.
[36] Auf der Grundlage der Delegierten Verordnung (EU) 2022/30 laufen derzeit Normungsarbeiten in Bezug auf die Anforderungen an die Cybersicherheit von Funkanlagen. Sollte die Kommission die Delegierte Verordnung aufheben oder ändern, sodass sie für bestimmte Produkte, die unter das Cyberresilienzgesetz fallen, nicht mehr gilt, so sollten die Kommission und die europäischen Normungsorganisationen bei der Ausarbeitung und Entwicklung harmonisierter Normen die Normungsarbeiten, die im Rahmen des Durchführungsbeschlusses C(2022) 5637 der Kommission über einen Normungsauftrag zur genannten Delegierten Verordnung durchgeführt werden, berücksichtigen, um die Durchführung des Cyberresilienzgesetzes zu erleichtern.

Zivile Unterstützungsmaßnahmen

- Entwicklung von Risikoszenarien für kritische Infrastrukturen, die für die militärische Kommunikation und Mobilität von Bedeutung sind, um Vorsorgemaßnahmen gezielt durchzuführen, unter anderem durch Penetrationstests.
- Förderung der Zusammenarbeit zwischen zivilen und militärischen Normungsgremien bei der Entwicklung harmonisierter Normen für Produkte mit doppeltem Verwendungszweck.

3. Investitionen in Cyberabwehrfähigkeiten

In den letzten Jahren wurden die Investitionen in die Cyberabwehr in der EU vor dem Hintergrund der zunehmenden böswilligen Cyberaktivitäten staatlicher und nichtstaatlicher Akteure erhöht. Es ist von entscheidender Bedeutung, dass die EU ihre Fähigkeiten im Bereich der Cyberabwehr stärkt. Aufgrund von Russlands Angriffskrieg gegen die Ukraine sind weitere Investitionen erforderlich, um sicherzustellen, dass die Mitgliedstaaten über hochmoderne Fähigkeiten im Bereich der Cyberabwehr verfügen, sowohl vor Ort als auch bei Einsätzen.

Technologische Verbesserungen sind unerlässlich, um den Vorteil gegenüber Wettbewerbern und Gegnern, die ebenfalls massiv in neue Technologien investieren, aufrechtzuerhalten. Die EU und ihre Mitgliedstaaten müssen deshalb auch ihre Zusammenarbeit und Interoperabilität im Bereich der Cyberabwehr durch gemeinsame Fähigkeitenentwicklung und verstärkte Investitionen in Forschung und Entwicklung verbessern.

Darüber hinaus müssen Schwachstellen, die sich aus strategischen Abhängigkeiten und der Fragmentierung der EDTIB ergeben[37], angegangen werden. Insbesondere sind Fähigkeiten und Kompetenzen von entscheidender Bedeutung, um strategische Abhängigkeiten in Bezug auf die Cybersicherheit und Cyberabwehr in Europa zu überwinden. Die europäische Verteidigungsindustrie muss Schlüsselkompetenzen sichern und neue erwerben, um weiterhin in der Lage zu sein, High-Tech-Lösungen in einem globalen Umfeld anzubieten.[38] Ein Mangel an Kompetenzen wirkt sich negativ auf den Verteidigungssektor aus, da dadurch die Entwicklung von Fähigkeiten in allen Bereichen behindert wird. Alle Maßnahmen stehen voll und ganz im Einklang mit den im Aktionsplan für Synergien, dem Fahrplan für kritische Technologien für Sicherheit und Verteidigung (im Folgenden „Fahrplan“)[39] und der Lückenanalyse[40] angekündigten Ansätzen.

3.1. Entwicklung hochmoderner Fähigkeiten im Bereich der Cyberabwehr

Die Mitgliedstaaten sind dafür verantwortlich und zuständig, die Fähigkeiten im Bereich der Cyberabwehr einzusetzen, während die EU eine wichtige Rolle bei der Unterstützung der Weiterentwicklung spezifischer militärischer Fähigkeiten in den Bereichen Doktrin,

[37] Wie beispielsweise in der Analyse der Investitionslücken im Verteidigungsbereich festgestellt.
[38] Mehrere Initiativen wurden auf den Weg gebracht, z. B. die Europäische Kompetenzpartnerschaft im Verteidigungsbereich.
[39] In ihrem Fahrplan für kritische Technologien forderte die Kommission eine verstärkte Zusammenarbeit bei Technologien, die für die langfristige Sicherheit und Verteidigung Europas von entscheidender Bedeutung sind, sowie Bemühungen zur Verringerung der damit verbundenen strategischen Abhängigkeiten.
[40] In der Gemeinsamen Mitteilung über die Analyse der Defizite bei den Verteidigungsinvestitionen und die nächsten Schritte haben die Kommission und der Hohe Vertreter mehrere Maßnahmen vorgeschlagen, um sicherzustellen, dass die EU-Industrie sowohl kurz- als auch langfristig in der Lage ist, Ergebnisse zu erzielen.

Organisation, Ausbildung, Ausrüstung, Personal, Führung, Einrichtungen und Interoperabilität (DOTMLPF-I) spielt, um Handlungsfreiheit im Cyberraum zu schaffen. Der Ansatz für die Cyberabwehr muss in allen Fähigkeitsbereichen weiter vereinheitlicht und an das sich wandelnde geopolitische Umfeld angepasst werden. Daher muss ermittelt werden, welche Elemente bei den bestehenden Fähigkeiten fehlen und die Entwicklung neuer Fähigkeiten muss auf koordinierte und messbare Weise unterstützt werden.

Das Engagement der Mitgliedstaaten bei kooperativen Entwicklungsprojekten im Bereich der Cyberabwehr ist jedoch nach wie vor unzureichend und sollte verstärkt werden, um die Wirkung auf EU-Ebene zu maximieren. Alle Mitgliedstaaten müssen ihre Investitionen in die Entwicklung des gesamten Spektrums an Fähigkeiten im Bereich der Cyberabwehr erhöhen und diese gemeinsam weiterentwickeln. Die Mitgliedstaaten sollten erwägen, **eine Reihe freiwilliger Verpflichtungen für die Entwicklung nationaler Cyberabwehrfähigkeiten, auch multinationaler Fähigkeiten, zu entwickeln**, die über bestehende SSZ-Projekte im Bereich der Cyberabwehr hinausgehen.[41] Der Prozess der Koordinierten Jährlichen Überprüfung der Verteidigung (Coordinated Annual Review on Defence, CARD) könnte genutzt werden, um einen Dialog mit den Mitgliedstaaten über die Anforderungen im Bereich der Cyberabwehr und die nationalen Ziele für die Entwicklung von Cyberabwehrfähigkeiten aufzunehmen und die Umsetzung der Verpflichtungen zu bewerten. Die Entwicklung und Forschung im Bereich der Cyberabwehr, auch im Bereich der aktiven Verteidigungsfähigkeiten, wird von der Kommission über den Europäischen Verteidigungsfonds (EVF) unterstützt und kofinanziert. Die Kommission hat ihre Investitionen in die Cyberabwehr im Rahmen des EVF bereits erhöht, was zur Entwicklung gemeinsamer und/oder interoperabler europäischer Instrumente für Cyberspace-Operationen, für die Bewältigung von Cybervorfällen, für die Abwehr von Informationskriegen und Präventivmaßnahmen sowie zur Verbesserung der Widerstandsfähigkeit der CIS-Systeme führen sollte. Sie zielt auf Bereiche wie Cyberlageerfassung, Bedrohungssuche in Echtzeit und Bewältigungsmaßnahmen, Fähigkeiten bei Cyberoperationen sowie Cyberschulungen und -übungen ab.[42] Um sicherzustellen, dass die Mitgliedstaaten in der Lage sind, gemeinsame Cyberoperationen durchzuführen, werden in den kommenden Jahren im Rahmen des EVF Fähigkeiten in Bezug auf Bewältigungsmaßnahmen und Cyberoperationen gefördert. Schließlich werden die Mitgliedstaaten ermutigt, sich aktiv an den verschiedenen Kooperationsrahmen zu beteiligen und alle auf EU-Ebene eingerichteten Instrumente, einschließlich des EDA-Projektteams für Cyberabwehr[43], zu nutzen.

Die laufende Überarbeitung der EU-Prioritäten für die Fähigkeitenentwicklung 2018[44] bietet eine gute Gelegenheit, aktualisierte Prioritäten für die kooperative Entwicklung festzulegen,

[41] Soforteinsatzteams für Cybervorfälle und gegenseitige Unterstützung im Bereich der Cybersicherheit (CRRT), Koordinierungszentrum für den Cyber- und Informationsbereich (CIDCC), Plattform für den Informationsaustausch über Cyberbedrohungen und -vorfälle (CTIRISP), Cyber-Range-Verbände (CRF), EU Cyber-Akademie und Innovation Hub (EU CAIH).

[42] Im Rahmen des Europäischen Programms zur industriellen Entwicklung im Verteidigungsbereich (EDIDP) wurden sechs Projekte (PANDORA, DISCRETION, CYBER4DE, ECYSAP, SMOTANET und HERMES) mit Mitteln in Höhe von 39 Mio. EUR finanziert. Im Rahmen des EVF 2021 werden fast 40 Mio. EUR für drei kooperative FuE-Projekte im Bereich der Cyberabwehr, die für eine Finanzierung ausgewählt wurden (ACTING, AInception, EU-GUARDIAN), bereitgestellt.

[43] Das Projektteam für Cyberabwehr bietet den Mitgliedstaaten ein Forum, um Aspekte zur Cyberabwehr mit militärischen Auswirkungen zu erörtern.

[44] CDP-Informationsblatt der EDA (28.6.2018): CDP-Informationsblatt.

um die Ausweitung der kooperativen Fähigkeitenentwicklung zu ermöglichen. Bei der Überprüfung der spezifischen Priorität im Bereich der Cyberabwehr sollten die Ergebnisse der CARD 2022 sowie die Ergebnisse der den Mitgliedstaaten im Mai 2022 vorgelegten Lückenanalyse berücksichtigt werden. Anschließend wird die CARD einen regelmäßigen Rahmen bieten, um die Fortschritte bei der Umsetzung dieser aktualisierten Priorität auf nationaler Ebene zu überprüfen und neue Optionen für die gemeinsame Entwicklung von Cyberabwehrfähigkeiten mit den Mitgliedstaaten auszuloten. Die aktualisierten Prioritäten der EU für die Fähigkeitenentwicklung werden als Hauptbezugspunkt für SSZ-Projekte im Bereich der Cyberabwehr dienen.

In diesem Zusammenhang wird der Militärstab der EU auf der Grundlage der Aufgabenzuweisung des EU-Militärausschusses in enger Abstimmung mit den Mitgliedstaaten den Plan für die Durchführung von Cyberoperationen ausarbeiten, um einen Überblick über den Stand der Umsetzung der Cyberabwehrfähigkeiten zu geben und die Mitgliedstaaten dabei zu unterstützen, ihre Anstrengungen und Tätigkeiten besser abzustimmen. Diese Bemühungen stützen sich auf das EU-Konzept für die Cyberabwehr für EU-geführte militärische Operationen und Missionen, in dem die Prioritäten des Plans zur Fähigkeitenentwicklung (CDP) Berücksichtigung finden.

Intensivierung der Forschungsanstrengungen zu Schlüsseltechnologien für die Cyberabwehr

Um sicherzustellen, dass die Fähigkeiten im Bereich der Cyberabwehr stets auf dem neusten Stand sind, müssen die technologischen Entwicklungen und ihre Anwendungen in verteidigungsbezogenen Systemen auf dem Laufenden gehalten werden, insbesondere in Bezug auf neu entstehende und disruptive Technologien (EDT, z. B. KI, Verschlüsselung und Quanteninformatik).[45] Insbesondere muss die EU in die Post-Quanten-Kryptografie investieren, um dafür zu sorgen, dass ihre Verteidigungssysteme sicher bleiben. Angesichts der rasanten Weiterentwicklung der Technologien müssen die Bemühungen im Bereich der gemeinsamen Forschung und technologischen Entwicklung so gestaltet werden, dass sie ein ausreichend fortgeschrittenes Technologieniveau erreichen, damit ihre Ergebnisse schneller in bestehende und künftige Fähigkeiten integriert werden können.

Die Kommission finanziert im Rahmen des EVF technologische Innovationen im Verteidigungsbereich und unterstützt die Entwicklung neu entstehender und disruptiver sowie modernster Technologien, auch im Bereich der Cyberabwehr. Bis zu 8 % der EVF-Mittel werden für Themen bereitgestellt, die sich mit disruptiven Technologien für die Verteidigung befassen, darunter auch einige Aspekte, die für die Cyberabwehr relevant sind. Besondere Aufmerksamkeit wird im Rahmen des EVF in den kommenden Jahren Forschungsmaßnahmen und -projekten gewidmet, die sich mit neuen Technologien befassen, die gegen aufkommende und sich weiterentwickelnde Bedrohungen entwickelt werden, sowie der Stärkung der Resilienz, der Cybersicherheit und ihrer Integration in die Verteidigungsfähigkeiten.

[45] Gemäß der strategischen Forschungsagenda für die Cyberabwehr und der übergeordneten strategischen Forschungsagenda (OSRA).

Im Einklang mit dem EDT-Aktionsplan[46] wird die EDA die Mitgliedstaaten jährlich über das Umfeld neu entstehender Technologien, einschließlich der Technologien im Zusammenhang mit der Cyberabwehr, informieren. Darüber hinaus wird die EDA eine strategische Bewertung für die europäischen EDT entwickeln, um die Mitgliedstaaten bei der Festlegung langfristiger strategischer Richtungen und der Ermittlung von Synergien und Kooperationsmöglichkeiten zu unterstützen. Das Europäische Kompetenzzentrum für Cybersicherheitsforschung (ECCC) wird eine strategische Agenda für Investitionen in Schlüsselbereiche der Cybersicherheit annehmen, die wiederum als Richtschnur für die Ausarbeitung künftiger Arbeitsprogramme der Programme „Digitales Europa“ und „Horizont Europa“ im Zusammenhang mit der Cybersicherheit bzw. zur Unterstützung von Forschung, Innovation und Markteinführung dienen wird. Um Synergien zu fördern, werden das ECCC und die EDA auch eine Arbeitsvereinbarung entwickeln, um den Informationsaustausch zwischen den jeweiligen Mitarbeitern über die Prioritäten im Bereich der zivilen Technologien, der doppelten Verwendung und der Verteidigungstechnologien zu erleichtern.

Umgang mit dem Technologiebedarf für die Cyberabwehr

Um sicherzustellen, dass die rasante technologische Entwicklung im Cyberbereich rechtzeitig vom Verteidigungssektor aufgegriffen wird, sind weitere Maßnahmen und Koordinierungsbemühungen erforderlich. Dazu gehören verstärkte Anstrengungen zur Ermittlung kritischer Technologien für die Cyberabwehr und Cybersicherheit, denen Vorrang eingeräumt werden sollte, um die technologischen Abhängigkeiten der EU zu verringern, und es wird bewertet, ob die derzeitigen Prioritätensetzungs- und Finanzierungsinstrumente diesen Abhängigkeiten ausreichend Rechnung tragen.

Zu diesem Zweck wird die Kommission im Jahr 2023 gemeinsam mit der EDA und den Mitgliedstaaten auf der Grundlage einschlägiger Konsultationen, gegebenenfalls auch mit der Industrie, einen **Technologiefahrplan für kritische Cybertechnologien** vorschlagen. Der Technologiefahrplan wird Cybertechnologien umfassen, die für die technologische Souveränität der EU wichtig sind, sowohl die Cyberabwehr als auch die Cybersicherheit abdecken, technologische Entwicklungen und strategische Abhängigkeiten erfassen und Maßnahmen zu ihrer Verringerung enthalten. Der Fahrplan für die Cybertechnologie wird in die strategischen Prioritäten für die Finanzierungsinstrumente der EU einfließen, und darin wird vorschlagen, die Programme und Finanzierungsinstrumente im Bereich der zivilen und verteidigungsbezogenen Forschung und Entwicklung sowie der Fähigkeitenentwicklung im Einklang mit ihren jeweiligen Governance-Vorschriften in vollem Umfang zu nutzen. Darüber hinaus werden weitere Möglichkeiten vorgeschlagen, um die Entwicklung der Forschung zur doppelten Verwendung, die Technologieentwicklung und Innovationen im Bereich Cybersicherheit und Cyberabwehr auf EU-Ebene und auf der Ebene der Mitgliedstaaten zu fördern.

In diesem Zusammenhang wird die Kommission[47] im Jahr 2023 in Zusammenarbeit mit dem ECCC und der EDA Technologien prüfen, die bereits als kritisch für die Cyberabwehr

[46] Der Aktionsplan mit dem Titel „Emerging Disruptive Technologies (EDTs): A capability-driven Action Plan“ (Neu entstehende disruptive Technologien (EDT): Ein fähigkeitsorientierter Aktionsplan) wurde am 16. Dezember 2021 vom EDA-Lenkungsausschuss in der Zusammensetzung der Forschungs- und Technologiedirektoren gebilligt.

[47] Einschließlich der Gemeinsamen Forschungsstelle.

eingestuft wurden, und wird – möglicherweise mit Unterstützung der Beobachtungsstelle für kritische Technologien[48] – weitere bestehende Abhängigkeiten erfassen und ermitteln. Dabei werden die Arbeiten berücksichtigt, die im Rahmen des jährlichen Monitoring-Dokuments der EDA[49] und der strategischen Bewertung der europäischen EDT[50] durchgeführt wurden. Darüber hinaus könnte das ECCC ein spezielles Projekt zur politischen Unterstützung auf den Weg bringen, das in den Technologiefahrplan einfließen und einschlägige Akteure aus dem zivilen und militärischen Bereich einbeziehen und zusammenbringen könnte.

Einige der im Aktionsplan für Synergien, im Fahrplan und in der Lückenanalyse beschriebenen Maßnahmen zur Stärkung der Synergien laufen bereits, um das volle Potenzial von Technologien mit doppeltem Verwendungszweck, auch im Cyberbereich, besser auszuschöpfen.

Ferner werden die Mitgliedstaaten aufgefordert, die bestehenden Initiativen zur Unterstützung der Forschung und der technologischen Entwicklung in vollem Umfang zu nutzen; im Verteidigungsbereich sind das insbesondere die CapTech-Gruppen der EDA für Verteidigungstechnologien[51] und die damit verbundenen OSRA-Technologie-Bausteine[52], der Ad-hoc-Rahmen der EDA[53], der EVF und die SSZ. Im Hinblick auf zivile Technologien und Technologien mit doppeltem Verwendungszweck können das ECCC und das Netzwerk Projekte verwalten, die gemäß ihrer Rechtsgrundlage[54] sowohl eine verteidigungsbezogene als auch eine zivile Dimension aufweisen. Wie im Aktionsplan für Synergien und im Fahrplan angekündigt, wird sich die Kommission auch darum bemühen, die Synergien zwischen den Tätigkeiten des ECCC und des EVF in den Bereichen Cybersicherheit und Cyberabwehr im Einklang mit den Governance-Regeln des EVF zu stärken.

3.2. Eine flexible, wettbewerbsfähige und innovative europäische Verteidigungsindustrie

Die EU braucht eine starke, flexible, wettbewerbsfähige und innovative europäische Verteidigungsindustrie, die in der Lage ist, ein vollständiges Spektrum modernster

[48] Beobachtungsstelle für kritische Technologien, die im Aktionsplan für Synergien zwischen der zivilen, der Verteidigungs- und der Weltraumindustrie angekündigt wurde.
[49] Erste Phase des EDT-Aktionsplans 2021 der EDA.
[50] Zweite Phase des EDT-Aktionsplans 2021 der EDA.
[51] CapTechs bieten Experten aus den Mitgliedstaaten ein Netzwerkforum und einen flexiblen Rahmen für kooperative Projekte. Weitere Informationen zu den CapTechs im Cyberbereich (Cyber, Information, Components) sind abrufbar unter: https://eda.europa.eu/what-we-do/research-technology/capability-technology-areas-(captechs) (auf Englisch).
[52] Die OSRA erfasst die einschlägigen Forschungs- und Technologiebereiche im Zusammenhang mit der Verteidigung und zeigt konkrete Möglichkeiten der Zusammenarbeit auf. Es gibt 17 Technologie-Bausteine mit ihren Technologiefahrplänen im Zusammenhang mit Cybertechnologien, die sich mit der Lageerfassung im Bereich der Cyberabwehr, dem Schutz militärischer Kommunikationssysteme, der Verarbeitung von Informationen aus heterogenen Quellen, Modellierung und Simulation, Quanteninformatik und Kryptografie befassen sowie Synergien zwischen Cyberoperationen und elektronischer Kriegsführung untersuchen. Künstliche Intelligenz und Big Data spielen bei der Informationsverarbeitung eine Schlüsselrolle.
[53] Der Ad-hoc-Rahmen der EDA ist im Beschluss (GASP) 2015/1835 des Rates festgelegt. Derzeit werden in diesem Rahmen sechs Projekte mit Elementen der Cybertechnologie durchgeführt, die mit einem Budget von etwa 20 Mio. EUR ausgestattet sind (ANQUOR, CERERE, EDA SOC 2, MASFAD II, PASEI II, ASSAI).
[54] Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren.

Verteidigungsfähigkeiten, auch im Bereich der Cyberabwehr, bereitzustellen. Bei der Cyberabwehr ist die Verteidigungsindustrie der EU derzeit jedoch in hohem Maße auf zivile Lösungen und externe Märkte angewiesen, um hochmoderne Lösungen anbieten zu können. Obwohl der technologische Fortschritt im zivilen Bereich rasch voranschreitet und der Markt für zivile Informations- und Cybersicherheitsprodukte schnell wächst, gibt es spezifische militärische Anforderungen, die von zivilen Standardprodukten nicht erfüllt werden. Wichtige Hardware- und Software-Elemente, die derzeit für die Cyberabwehr verwendet werden, werden in der EU nicht hergestellt, was zu industriellen und technologischen Abhängigkeiten führen kann. Die EU verfügt auch nicht über eine starke Präsenz in der globalen Cybersicherheits- und Cyberabwehrindustrie. Aufgrund der stark fragmentierten **EDTIB** ist ihre Fähigkeit zur Verbesserung ihrer Wettbewerbsfähigkeit[55] erheblich eingeschränkt. Die Mehrheit der Cybersicherheitsunternehmen in der EU sind kleine und mittlere Unternehmen (KMU).[56] Eine technologisch souveräne industrielle Kapazität ist ein Eckpfeiler der Handlungsfähigkeit der EU.

Die EU unterstützt die Entwicklung einer starken EDTIB durch eine Reihe von Programmen und Initiativen. Während im Rahmen des EVF technologische Innovationen im Verteidigungsbereich finanziert und die Entwicklung von Technologien unterstützt werden, die letztlich zu gemeinsam entwickelten modernsten militärischen Fähigkeiten führen und zur Wettbewerbsfähigkeit der Verteidigungsindustrie der EU beitragen, unterstützen die Programme „Horizont Europa“ und „Digitales Europa“ die Forschung im Bereich der Cybersicherheit und die Entwicklung von Technologien mit doppeltem Verwendungszweck, einschließlich Quantentechnologien, Verschlüsselung, gesicherter Cloud und KI.[57]

Weitere Maßnahmen im Zusammenhang mit kritischen Technologien für die Cyberabwehr und den industriellen Bedarf, wie sie im **Technologiefahrplan für kritische Cybertechnologien** ermittelt wurden, sollten angegangen werden. Es ist notwendig, geeignete Unterstützungsströme zu ermitteln, um beispielsweise gemeinsame Beschaffungsbemühungen anzuregen, z. B. durch das künftige Programm für Europäische Verteidigungsinvestitionen, oder den Zugang zu Beteiligungskapital und Darlehen über den Europäischen Investitionsfonds und die Europäische Investitionsbank zu erleichtern.

Um die EDTIB zu stärken, muss sichergestellt werden, dass Synergien zwischen zivilen und Verteidigungsunternehmen genutzt und wirksam eingesetzt werden. Die im Rahmen des EU-Innovationsprogramms im Verteidigungsbereich (EUDIS) vorgeschlagenen Innovationsmaßnahmen, einschließlich der Einbeziehung von KMU und des Technologie-Scoutings, könnten sich positiv auf die Verteidigungsindustrie der EU und die EDTIB auswirken.

[55] Wie in der Gemeinsamen Mitteilung über die Analyse der Defizite bei den Verteidigungsinvestitionen und die nächsten Schritte dargelegt.

[56] Die Gesamtzahl der KMU in der EU, die in den mehrschichtigen und häufig grenzüberschreitenden Rüstungslieferketten tätig sind, wird auf 2500 geschätzt. Sie haben Kunden im Verteidigungsbereich und 7,8 % ihrer Geschäftstätigkeit liegt im Cyberbereich.

[57] Wie im Programm „Horizont Europa“ vorgesehen, profitieren die zivile Forschung und die Verteidigungsforschung von Synergien mit dem EVF, obwohl die Aktivitäten des Rahmenprogramms ausschließlich auf zivile Anwendungen ausgerichtet sind.

Die Kommission wird auch einen Dialog mit der Industrie aufnehmen, um die Cyberabwehrindustrie der EU weiterzuentwickeln, gegebenenfalls unter Einbeziehung der EDA.

Die Kommission und der Hohe Vertreter schlagen mehrere Maßnahmen vor, um sicherzustellen, dass die Industrie in der Lage ist, kurz- und langfristig Ergebnisse zu erzielen. Dies erfordert in naher Zukunft eine eingehende Bestandsaufnahme der industriellen Fertigungskapazitäten im Verteidigungsbereich in der EU, um Lücken und Bereiche genau zu ermitteln, in denen ein Ausbau erforderlich ist.

Die Verringerung kritischer Abhängigkeiten im Cyberbereich, wie sie in technologischen Fahrplänen aufgezeigt werden könnten, könnte auch durch den neuen Europäischen Souveränitätsfonds angegangen werden, der von Präsidentin von der Leyen in ihrer Rede zur Lage der Union im September 2022 angekündigt wurde.

Der EU-Rahmen für die Überprüfung ausländischer Direktinvestitionen wird weiterhin genutzt, um die Risiken beim Erwerb europäischer Technologien oder Lösungen, die Verteidigungs- und Sicherheitsrisiken bergen, zu mindern. Mitgliedstaaten, die noch keine nationalen Überprüfungsmechanismen eingerichtet haben, sollten dies unverzüglich tun.

3.3. Arbeitskräfte der EU im Bereich der Cyberabwehr

Europa ist mit einem tatsächlichen und alarmierenden Mangel an Cyberkompetenzen konfrontiert, und die Europäische Cybersicherheitsorganisation (ECSO) schätzt, dass bereits 2022 insgesamt 500 000 Fachkräfte benötigt werden. Durch diese Kompetenzlücke wird die Fähigkeit der EU beeinträchtigt, neue Technologien zu entwickeln und ihre kritische Infrastruktur zu verteidigen. Für staatliche Stellen wie die Verteidigungsministerien und das Militär verschärfen der harte Wettbewerb um Qualifikationen und die attraktiven Gehälter des Privatsektors die Schwierigkeiten, Talente im Cyberbereich anzuziehen und zu halten.

Im Zusammenhang mit dem Europäischen Jahr der Kompetenzen 2023 **wird die Kommission eine Initiative für eine Akademie für Cyberkompetenzen (Cyber Skills Academy) auf den Weg bringen**. Sie wird als Dachinitiative mit dem Ziel dienen, die Zahl der im Bereich Cybersicherheit ausgebildeten Fachkräfte zu erhöhen. In ihr werden die zahlreichen verschiedenen Initiativen zu Cyberkompetenzen zusammengeführt, um die Koordinierung, Integration und eine gemeinsame Kommunikation um sie herum zu gewährleisten. Die Cyber Skills Academy, die sich auf mehrere Handlungsschwerpunkte wie Finanzierung, gemeinschaftliche Unterstützung, Schulung und Zertifizierung, Einbeziehung der Interessenträger und Wissensgenerierung stützt, wird auch den Fachkräften im Bereich der Cyberabwehr zugutekommen. Das Europäische Sicherheits- und Verteidigungskolleg (ESVK) wird prüfen, wie der Austausch bewährter Verfahren und weiterer Synergien zwischen dem militärischen und dem zivilen Bereich in Bezug auf die Ausbildung und die Entwicklung weltraumspezifischer militärischer Fähigkeiten erleichtert werden kann.

Auf der Grundlage einer Analyse des Schulungsbedarfs der EU werden das ESVK, die EDA und die Mitgliedstaaten Ausbildungsmaßnahmen und Übungen im Bereich der Cyberabwehr für EU-Organe, GSVP-Operationen und -Missionen sowie Beamte der Mitgliedstaaten weiterentwickeln und organisieren. Außerdem werden Möglichkeiten zur **Weiterentwicklung der ESVK-Plattform zur Aus- und Fortbildung, Evaluierung und Übung im Cyberbereich (ETEE)** geprüft, um mehr Schulungskapazitäten zu schaffen. Dies sollte auch

Schulungen für Einsätze in bestimmten operativen Bereichen und bereichsübergreifende Einsätze umfassen. Insbesondere sollten Synergien mit dem SSZ-Projekt „EU Cyber-Akademie und Innovation Hub“ (EU CAIH)[58] angestrebt werden.

Die Mitgliedstaaten werden aufgefordert, spezifische Bildungsprogramme im Bereich der Cyberabwehr zu entwickeln, und zu diesem Zweck Hochschulen und akademische Einrichtungen (zivil und militärisch) zusammenzubringen, um gemeinsame Lehrpläne in Bezug auf die Cyberabwehr zu erstellen, bewährte Verfahren auszutauschen, Partnerschaften und gemeinsame Projekte zu entwickeln und den Austausch von Ausbildern und Auszubildenden zu erleichtern. Um Interoperabilität und eine gemeinsame Kultur in der gesamten EU zu gewährleisten, wird das ESVK den Austausch zwischen den Mitgliedstaaten im Rahmen der ETEE fördern.

Die Mitgliedstaaten sollten die Zusammenarbeit zwischen den Akteuren der allgemeinen und beruflichen Bildung verstärken, indem sie sowohl zivile als auch militärische Aspekte in den technischen, operativen, strategischen und rechtlichen Bereichen miteinander verbinden und die Grundlage für die Einrichtung gemeinsamer und standardisierter Ausbildungsprogramme auf verschiedenen Ebenen für die zivile und die diplomatische Cybergemeinschaft, die Cybergemeinschaft im Bereich der Strafverfolgung und die Cyberabwehrgemeinschaft schaffen. Darüber hinaus sollten die Mitgliedstaaten mit europäischen Ausbildungsanbietern aus dem Privatsektor sowie mit akademischen Einrichtungen zusammenarbeiten, um das Niveau der Kompetenzen und Fähigkeiten des Personals bei militärischen GSVP-Missionen und -Operationen zu verbessern.

Darüber hinaus sollte die Zusammenarbeit bei Ausbildungsstandards und Zertifizierung im Bereich der Cyberabwehr zwischen den Mitgliedstaaten, den EU-OESS, internationalen Partnern und anderen Akteuren, einschließlich des Privatsektors und der Wissenschaft, gefördert werden. Aufbauend auf bestehenden zivilen Initiativen wie dem von der ENISA entwickelten Europäischen Kompetenzrahmen für Cybersicherheit (ECSF) wird das ESVK einen Rahmen für die Zertifizierung von Kompetenzen im Bereich der Cyberabwehr erarbeiten. Die Kommission würde auch Ansätze für die Zertifizierung von Cyberkompetenzen prüfen, die auf dem Markt und in der Wissenschaft verfügbar sind, und gleichzeitig versuchen, über die Cyber Skills Academy Synergien zwischen diesen Ansätzen zu fördern und Lücken zu schließen, insbesondere mit gezielt eingesetzten EU-Mitteln.

Maßnahmen zur Cyberabwehr

- Entwicklung der strategischen Bewertung für die EDT zur Unterstützung langfristiger strategischer Investitionsentscheidungen.
- Entwicklung eines Technologiefahrplans für kritische Cybertechnologien für die EU, der kritische Technologien für die Cyberabwehr und Cybersicherheit umfasst, um das Ausmaß der Abhängigkeiten zu bewerten.
- Vorschläge für das weitere Vorgehen zur Verringerung von Abhängigkeiten unter Nutzung aller EU-Instrumente, einschließlich der Programme „Digitales Europa“ und „Horizont Europa“ sowie des Europäischen Verteidigungsfonds, und Einschätzung technologischer

[58] https://www.pesco.europa.eu/project/eu-cyber-academia-and-innovation-hub-eu-caih/ (auf Englisch).

Entwicklungen, um die technologische Souveränität zu stärken und die Handlungsfähigkeit sicherzustellen.
- Unterstützung der Entwicklung eines Zertifizierungsrahmens für Kompetenzen im Bereich der Cyberabwehr.
- Entwicklung von Übungen der EU im Bereich der Cyberabwehr und Prüfung der Frage, wie die ETEE-Plattform des ESVK weiterentwickelt werden kann, um mehr Schulungskapazitäten zu schaffen.

Zivile Unterstützungsmaßnahmen

- Einrichtung einer EU-Akademie für Cyberkompetenzen unter Berücksichtigung des Bedarfs an spezifischen Kompetenzen für verschiedene Berufsprofile und Tätigkeitsbereiche, auch bei den Arbeitskräften im Verteidigungsbereich.
- Analyse von Ansätzen für die Zertifizierung von Cyberkompetenzen bei gleichzeitiger Förderung von Synergien und Schließung von Lücken, auch mit EU-Mitteln.

4. Partner für die Bewältigung gemeinsamer Herausforderungen

Die Partner werden von einer leistungsfähigeren und widerstandsfähigeren EU im Cyberraum sowie von der Unterstützung durch die EU im Bereich der Cyberabwehr und dem Aufbau von Kapazitäten im Rahmen der einschlägigen EU-Instrumente profitieren. Die EU wird sich bemühen, maßgeschneiderte Partnerschaften im Bereich der Cyberabwehr aufzubauen, sofern diese für beide Seiten von Vorteil sind. Partnerschaften im Bereich der Cyberabwehr werden auch im Zusammenhang mit der Beteiligung der Partnerländer an militärischen GSVP-Missionen und -Operationen thematisiert.

Dabei wird gegebenenfalls auf bestehenden Cyberdialogen sowie Sicherheits- und Verteidigungsdialogen aufgebaut. Der Hohe Vertreter wird auch Synergien zwischen dem **informellen EU-Netz für Cyberdiplomatie und dem Netz der Militärattachés in den EU-Delegationen** ausloten.

4.1. Zusammenarbeit mit der NATO

Die strategische Partnerschaft der EU mit der NATO ist nach wie vor von entscheidender Bedeutung für die euro-atlantische Sicherheit, wie im Strategischen Kompass und im Strategischen Konzept[59] der NATO für 2022 hervorgehoben wird. Die EU ist nach wie vor fest entschlossen, diese wichtige Partnerschaft, auch im Bereich der Cyberabwehr, zu stärken, und es müssen weitere Schritte unternommen werden, um gemeinsame Lösungen für gemeinsame Bedrohungen und Herausforderungen zu entwickeln. Im Einklang mit den gemeinsamen Erklärungen von Warschau und Brüssel über die Zusammenarbeit zwischen der EU und der NATO[60] und basierend auf den Grundsätzen der Transparenz, der Gegenseitigkeit, der Inklusivität, der Offenheit und der Beschlussfassungsautonomie beider Organisationen gehören Cybersicherheit und Cyberabwehr für die EU zu den wichtigsten Prioritäten bei der Zusammenarbeit.

[59] https://www.nato.int/strategic-concept/ (auf Englisch).
[60] Unterzeichnet 2016 bzw. 2018.

Auf der Grundlage der Gegenseitigkeit wird sich die EU weiterhin mit der NATO über das militärische Rahmenkonzept für die Einbeziehung von Aspekten der Cyberabwehr in die Planung und Durchführung militärischer GSVP-Missionen und -Operationen austauschen. Die EU wird sich um eine größtmögliche Kompatibilität mit den Konzepten und der Doktrin der NATO zur Cyberabwehr bemühen.

Angesichts der hohen Nachfrage nach Cyberabwehrfähigkeiten wird die EU Synergien und Komplementarität mit der NATO über organisatorische und nationale Grenzen hinweg fördern. Die EU wird mit der NATO zusammenarbeiten, um die technische und verfahrenstechnische Interoperabilität der Cyberabwehrfähigkeiten zu stärken, einschließlich der Entwicklung von Fähigkeiten im Einklang mit der FMN-Initiative. Damit wird der Weg für die sich möglichst gegenseitig unterstützende Entwicklung und Nutzung von Cyberabwehrfähigkeiten geebnet. Besondere Aufmerksamkeit sollte der Interoperabilität von Normen gewidmet werden, durch die zur Cyberresilienz und zur Interoperabilität militärischer Kommunikations- und Informationssysteme beigetragen wird, gegebenenfalls unter Einbeziehung der Industrie.

Um für eine kohärente Ausbildung des jeweiligen Personals im Bereich der Cyberabwehr zu sorgen, wird die EU gegebenenfalls auch die Zusammenarbeit mit der NATO bei der Harmonisierung des Schulungsbedarfs und bei der Analyse der Anforderungen verstärken und gemeinsame Lehrpläne, Kurse und Übungen entwickeln. Basierend auf den Grundsätzen der Gegenseitigkeit und der Nichtdiskriminierung wird das ESVK seine Schulungen im Bereich der Cyberabwehr für NATO-Mitarbeiter öffnen und eine Plattform einrichten, um für gemeinsame Kurse zu werben. Die EU wird auch die Beteiligung des NATO-Personals an Cyberübungen und Übungen zum Krisenmanagement mit Cyber-Elementen fördern.

Die EU und die NATO werden sich auch für die weitere Verbesserung der gegenseitigen Lageerfassung einsetzen und Möglichkeiten der Koordinierung sondieren, unter anderem durch eine verstärkte Zusammenarbeit zwischen dem NCIRC und dem CERT-EU. Um die Zusammenarbeit in Bezug auf die Cyberaspekte und die Auswirkungen des Krisenmanagements und der Krisenbewältigung zu fördern, wird die EU zum Austausch zwischen den Bediensteten über militärische, zivile und gemeinsame Initiativen und gegebenenfalls zur Schaffung potenzieller Synergien innerhalb der jeweiligen Krisenbewältigungsrahmen und -initiativen, auch bei Vorfällen mit großem Ausmaß, beitragen. Um gegenseitige Komplementarität zu gewährleisten und unnötigen doppelten Aufwand zu vermeiden, wird die EU eine engere Zusammenarbeit und einen engeren Informationsaustausch mit der NATO über die Bemühungen um den Aufbau von Kapazitäten im Bereich der Cyberabwehr in Partnerländern anstreben.

4.2. Zusammenarbeit mit gleich gesinnten Partnern

Der Hohe Vertreter wird Fragen der Cyberabwehr systematischer in bestehende und künftige Cyberdialoge sowie Sicherheits- und Verteidigungsdialoge mit Partnern einbeziehen. Wenn die Aspekte der Cyberabwehr im Rahmen von bilateralen Dialogen weiterentwickelt werden, werden sich mehr Möglichkeiten ergeben, solche Aspekte in andere Formen der Zusammenarbeit mit EU-Partnern aufzunehmen.

Im Rahmen der strategischen Partnerschaft der EU mit den **Vereinigten Staaten** wird die Zusammenarbeit in den Bereichen Sicherheit und Verteidigung auf für beide Seiten vorteilhafte Weise weiter vertieft, unter anderem durch einen strukturierten Austausch von Informationen

über die Lageerfassung. Regelmäßige Cyberdialoge sowie Sicherheits- und Verteidigungsdialoge zwischen der EU und den USA untermauern die starke transatlantische Partnerschaft. Der Hohe Vertreter wird gegebenenfalls relevante Aspekte der Cyberabwehr in diese Dialoge aufnehmen.

Gemeinsam mit ihren internationalen Partnern wird die EU die **Ukraine** weiterhin unterstützen, unter anderem durch einen Cyberdialog. In Anbetracht der Erfahrungen der Ukraine mit dem Aufbau von Cyberresilienz- und Cyberabwehrkapazitäten wird der Austausch bewährter Verfahren im Bereich der Cyberabwehr, einschließlich Informationen über die Bedrohungslage und die Lageerfassung, sowie einschlägige politische Entwicklungen von gemeinsamem Interesse fortgesetzt und ausgeweitet werden.

Gleichgesinnte Partner spielen eine wichtige Rolle bei der Aufrechterhaltung eines globalen, offenen, stabilen und sicheren Cyberraums und können die EU in ihrer Fähigkeit ergänzen, böswilliges Verhalten im Cyberraum zu verhindern, davon abzuschrecken und darauf zu reagieren. Die EU ist nach wie vor offen für ein breit angelegtes, ehrgeiziges und für beide Seiten vorteilhaftes Engagement in den Bereichen Sicherheit und Verteidigung, auch im Bereich der Cyberabwehr, mit allen gleich gesinnten Partnern.

4.3. Unterstützung des Kapazitätsaufbaus im Bereich der Cyberabwehr in Partnerländern

Durch globale und regionale Herausforderungen hat sich die gegenseitige Abhängigkeit der EU und ihrer Partner vergrößert, und es ist deutlich geworden, dass engere Partnerschaften in den Bereichen Sicherheit und Verteidigung aufgebaut werden müssen. Von besonderer Bedeutung ist dies für die EU-Kandidatenländer. Die jüngsten groß angelegten Cyberangriffe zeigen die Notwendigkeit eines verstärkten Engagements der EU und einer verstärkten Partnerschaft in den Bereichen Cybersicherheit und Cyberabwehr, die auf bestehenden Programmen aufbauen sollte. Aufgrund des länderübergreifenden Charakters von Cyberbedrohungen wird die Stärkung der Cyberresilienz der Partnerländer, insbesondere derjenigen mit weniger ausgereiften Cyberfähigkeiten, zu einem sichereren Cyberraum beitragen. Dadurch wäre die EU besser in der Lage, Cyberangriffe zu verhindern, aufzudecken, abzuwehren und von ihnen abzuschrecken. Die EU wird die Zusammenarbeit mit Partnerländern in den Bereichen Sicherheit und Verteidigung intensivieren, um deren Cyberresilienz zu stärken, unter anderem im Rahmen von bestehenden Dialogen. Soweit möglich und für beide Seiten vorteilhaft, wird die EU bei ihren Bemühungen um den Aufbau von Kapazitäten im Bereich der Cyberabwehr mit Partnern und insbesondere mit den EU-Kandidatenländern, die sich an der Gemeinsamen Außen- und Sicherheitspolitik und der Gemeinsamen Sicherheits- und Verteidigungspolitik der EU orientieren, zusammenarbeiten. Dies könnte die Unterstützung der politischen und rechtlichen Rahmenbedingungen, Ausbildung, Beratung, Anleitung und Ausrüstung der Streitkräfte und Sicherheitskräfte der Partner umfassen. Die Mitgliedstaaten könnten beschließen, den Partnern operative Unterstützung im Bereich der Cyberabwehr zu leisten. Darüber hinaus wird die EU die Partner dabei unterstützen, ihre Fähigkeit, zu militärischen GSVP-Missionen und -Operationen beizutragen, zu stärken, da dies ein wertvoller Beitrag zu den gegenseitigen Bemühungen zur Förderung von Frieden und Sicherheit ist.

Die Europäische Friedensfazilität wird weiterhin die Bemühungen der EU unterstützen, den Aufbau von Verteidigungskapazitäten, einschließlich der Cyberabwehr, in Partnerländern, insbesondere in der Nachbarschaft der EU, zu fördern, um die Bemühungen zur

Krisenbewältigung im Rahmen der GSVP zu ergänzen. In diesem Zusammenhang wird die EU erforderlichenfalls die Unterstützung der Cyberabwehr besser mit dem Aufbau ziviler Kapazitäten im Bereich der Cybersicherheit verknüpfen, insbesondere über das EU-Gremium für den Cyberkapazitätsaufbau. Für den Erfolg der Maßnahmen zur Cyberabwehr und zum Kapazitätsaufbau im Bereich der Cybersicherheit wird eine effiziente Koordinierung zwischen den einschlägigen Programmen und Instrumenten der EU, einschließlich der Europäischen Friedensfazilität, und den Mitgliedstaaten erforderlich sein.

Die EU wird die Partnerländer bei ihren Bemühungen um den Aufbau von Kapazitäten im Bereich der Cyberabwehr unterstützen und eng mit anderen Gebern zusammenarbeiten, um die Lageerfassung und Koordinierungsplattformen zu entwickeln, damit die bestmögliche maßgeschneiderte Unterstützung geleistet und für Kohärenz gesorgt und doppelter Aufwand vermieden werden kann.

Maßnahmen zur Cyberabwehr

- Stärkung der Zusammenarbeit zwischen der EU und der NATO bei Ausbildung, Schulungen, Lageerfassung und Übungen im Bereich der Cyberabwehr.
- Aufnahme von Aspekten der Cyberabwehr in EU-geführte Cyberdialoge sowie Sicherheits- und Verteidigungsdialoge mit Partnerländern.
- Zusammenarbeit mit gleich gesinnten Staaten, auch im Zusammenhang mit der Entwicklung von Cyberabwehrfähigkeiten und Cyberresilienz.
- Verstärkung der Unterstützung für Partner bei der Entwicklung von Cyberabwehrfähigkeiten, unter anderem im Rahmen der Europäischen Friedensfazilität, insbesondere in der Nachbarschaft der EU und zur Unterstützung der EU-Kandidatenländer.

Zivile Unterstützungsmaßnahmen

- Stärkung der Zusammenarbeit zwischen der EU und der NATO bei der Cybersicherheit in den Bereichen Lageerfassung, Krisenreaktion, Schutz kritischer Infrastruktur sowie Normung und Zertifizierung.

III. SCHLUSSFOLGERUNGEN

Der Hohe Vertreter, auch in seiner Eigenschaft als Leiter der EDA, und die Kommission fordern die Mitgliedstaaten auf, die relevanten Aspekte dieser Strategie zur Cyberabwehr weiterzuentwickeln und sie werden mit den Mitgliedstaaten zusammenarbeiten, um praktische Umsetzungsmaßnahmen zu ermitteln. In Zusammenarbeit mit den Mitgliedstaaten könnte ein Umsetzungsplan erstellt werden. Die Ergebnisse der Umsetzung der EU-Strategie zur Cyberabwehr werden zu den allgemeinen Zielen der EU-Cybersicherheitsstrategie und des Strategischen Kompasses beitragen.

Dem Rat wird jährlich ein Bericht vorgelegt, um die Fortschritte bei der Umsetzung der Strategie für die Cyberabwehr zu überwachen und zu bewerten. Die Mitgliedstaaten sind aufgefordert, die Fortschritte bei den Umsetzungsmaßnahmen, die auf nationaler Ebene oder in Kooperationsformaten umgesetzt werden, mit ihren Beiträgen zu unterstützen.