Rat der
Europäischen Union

Brüssel, den 19. November 2018
(OR. en)

14413/18

CYBER 285
CSDP/PSDC 669
COPS 444
POLMIL 214
EUMC 193
RELEX 978
JAI 1154
TELECOM 415
CSC 328
CIS 13
COSI 290

BERATUNGSERGEBNISSE

Absender:	Generalsekretariat des Rates
vom	19. November 2018
Empfänger:	Delegationen
Betr.:	EU-Politikrahmen für die Cyberabwehr (Aktualisierung 2018)

Die Delegationen erhalten anbei den EU-Politikrahmen für die Cyberabwehr (Aktualisierung 2018), den der Rat auf seiner 3652. Tagung vom 19. November 2018 angenommen hat.

ANLAGE

EU-POLITIKRAHMEN FÜR DIE CYBERABWEHR

(Aktualisierung 2018)

Geltungsbereich und Ziele

Um auf sich ändernde Sicherheitsherausforderungen zu reagieren, müssen die EU und ihre Mitgliedstaaten ihre Cyberabwehrfähigkeit stärken und robuste Cybersicherheits- und Cyberabwehrfähigkeiten entwickeln.

Der EU-Politikrahmen für die Cyberabwehr unterstützt die Entwicklung der Cyberabwehrfähigkeiten der EU-Mitgliedstaaten sowie die Stärkung des Cyber-Schutzes der Sicherheits- und Verteidigungsinfrastruktur der EU, unbeschadet der nationalen Rechtsvorschriften der Mitgliedstaaten und der Rechtsvorschriften der EU, einschließlich des Umfangs der Cyberabwehr, sofern dieser festgelegt ist.

Der Cyberspace ist der fünfte operative Bereich neben den Bereichen Land, See, Luft und Weltraum. Die erfolgreiche Durchführung der EU-Missionen und Operationen hängt immer stärker vom ununterbrochenen Zugang zu einem sicheren Cyberraum ab und erfordert daher robuste und widerstandsfähige operative Fähigkeiten.

Ziel des aktualisierten Politikrahmens für die Cyberabwehr ist es, die Cyberabwehrstrategie der EU weiterzuentwickeln, indem einschlägige Entwicklungen in anderen maßgeblichen Foren und Politikbereichen und die Umsetzung des EU-Politikrahmens für die Cyberabwehr seit 2014 berücksichtigt werden. Im Politikrahmen werden vorrangige Bereiche für die Cyberabwehr festgelegt und die Rollen der verschiedenen europäischen Akteure näher bestimmt, wobei die Verantwortlichkeiten und Zuständigkeiten der Unionsakteure und der Mitgliedstaaten sowie der institutionelle Rahmen der EU und deren Beschlussfassungsautonomie uneingeschränkt geachtet werden.

Hintergrund

In den Schlussfolgerungen des Europäischen Rates zur GSVP vom Dezember 2013 und den Schlussfolgerungen des Rates zur GSVP vom November 2013 wurde gefordert, auf der Grundlage eines Vorschlags der Hohen Vertreterin in Zusammenarbeit mit der Europäischen Kommission und der Europäischen Verteidigungsagentur (EDA) einen EU-Politikrahmen für die Cyberabwehr auszuarbeiten. Der EU-Politikrahmen für die Cyberabwehr wurde vom Rat am 18. November 2014[1] angenommen, und seitdem wurden durch konkrete Ergebnisse im Rahmen seiner Umsetzung die Cyberabwehrfähigkeiten der Mitgliedstaaten wesentlich verstärkt. Als Teil des Jahresberichts über die Umsetzung des Politikrahmens für die Cyberabwehr 2017[2] und unter Berücksichtigung von EU-Initiativen im Bereich Sicherheit und Verteidigung – insbesondere der Koordinierten Jährlichen Überprüfung der Verteidigung, der Ständigen Strukturierten Zusammenarbeit, des Europäischen Verteidigungsfonds und des Pakts für die zivile GSVP sowie der 2018 erfolgten Überarbeitung des Fähigkeitenentwicklungsplans und des Plans zur Entwicklung der zivilen Fähigkeiten – forderten die Mitgliedstaaten eine Aktualisierung des EU-Politikrahmens für die Cyberabwehr.

Die Cybersicherheit ist eine Priorität im Rahmen der Globalen Strategie für die Außen-und Sicherheitspolitik der Europäischen Union und der Zielvorgaben für die EU[3]. In der Globalen Strategie wird die Notwendigkeit betont, die Fähigkeiten zum Schutz der EU und ihrer Bürgerinnen und Bürger und zur Reaktion auf externe Krisen zu steigern. Darüber hinaus wird darin hervorgehoben, wie wichtig es ist, die EU als Sicherheitsgemeinschaft zu stärken. In diesem Zusammenhang sollten die Bemühungen im Bereich Sicherheit und Verteidigung die strategische Rolle der Union und zugleich ihre Fähigkeit stärken, eigenständig zu handeln, wann und wo immer dies erforderlich sein sollte, und gemeinsam mit Partnern tätig zu werden, wenn immer dies möglich ist. Diese Ziele erfordern eine stärkere Zusammenarbeit bei der Entwicklung der Fähigkeiten, die die Wirksamkeit und Interoperabilität der daraus entstehenden zivilen und militärischen Fähigkeiten fördern wird.

---

1 Ratsdokument 15585/14 vom 18.11.2014.
2 Ratsdokument 15870/17 vom 19.12.2017.
3 Schlussfolgerungen des Rates zur Umsetzung der Globalen Strategie der Europäischen Union im Bereich der Sicherheit und der Verteidigung vom 14.11.2016.

Das gemeinsame Paket von Vorschlägen zur Umsetzung der am 8. Juli 2016 in Warschau von dem Präsidenten des Europäischen Rates, dem Präsidenten der Europäischen Kommission und dem Generalsekretär der Nordatlantikvertrags-Organisation (NATO) unterzeichneten Gemeinsamen Erklärung[4] beinhaltet konkrete Maßnahmen zur Ausweitung der Zusammenarbeit zwischen EU und NATO im Bereich der Cybersicherheit und -abwehr, auch im Zusammenhang mit Missionen und Operationen sowie in Bezug auf die Entwicklung der Fähigkeiten in den Bereichen Cyberabwehr, Forschung und Technologie, Ausbildung, Schulung, Übungen und der durchgehenden Einbindung der Aspekte der Cybersicherheit in das Krisenmanagement. Diese Zusammenarbeit findet unter uneingeschränkter Achtung der Grundsätze der Offenheit, der Transparenz, der Inklusivität, der Gegenseitigkeit und der Beschlussfassungsautonomie der EU statt. Eine technische Vereinbarung zwischen dem IT-Notfallteam der EU (CERT-EU) und der Computer Incident Response Capability der NATO vom Februar 2016 ermöglicht den Austausch von technischen Informationen mit dem Ziel, die Verhütung und Aufdeckung von Cybervorfällen sowie die Reaktion darauf in beiden Organisationen zu verbessern.

Es ist darauf hinzuweisen, dass mehrere politische Strategien der EU zum Ziel der Cyberabwehr im Sinne dieses Dokuments beitragen, und dass dieser Politikrahmen auch die entsprechenden Regelungen, politischen Strategien und technologische Unterstützung im Zivilbereich berücksichtigt. So haben das Europäische Parlament und der Rat beispielsweise im Juli 2016 die Richtlinie zur Netz- und Informationssicherheit[5] (NIS-Richtlinie) erlassen, die die allgemeine Abwehrbereitschaft der Mitgliedstaaten gegen Cyberbedrohungen erhöhen und die unionsweite Zusammenarbeit stärken soll. Mit dieser Richtlinie werden Maßnahmen festgelegt, mit denen ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der Union erreicht werden soll, um so das Funktionieren des Binnenmarkts zu verbessern. Die Frist zur Umsetzung der Richtlinie ist am 9. Mai 2018 abgelaufen.

---

4 Schlussfolgerungen des Rates zur Umsetzung der Gemeinsamen Erklärung des Präsidenten des Europäischen Rates, des Präsidenten der Europäischen Kommission und des Generalsekretärs der Nordatlantikvertrags-Organisation (NATO) (6. Dezember 2016) – Dok. 15283/16; 5. Dezember 2017, Dok. 14802/17).

5 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

Der Vorschlag vom September 2017 für einen EU-Rechtsakt zur Cybersicherheit beinhaltet das neue Mandat für die EU-Agentur für Cybersicherheit (ENISA) und die Schaffung eines unionsweiten Rahmen für Zertifizierungen. Durch diesen Zertifizierungsrahmen sollen künftig hohe Standards für IKT-Prozesse, -Produkte und -Dienstleistungen gefördert und Wettbewerbsvorteile geschaffen werden und ferner das Vertrauen auf Seiten der Verbraucher und Auftraggeber gestärkt werden. Darüber hinaus hat die Kommission im September 2017 einen weiteren Schritt unternommen, um die EU auf etwaige schwerwiegende grenzüberschreitende Cybervorfälle vorzubereiten ("Blue-Print"-Entwurf) und arbeitet nun gemeinsam mit den Mitgliedstaaten und anderen Organen, Agenturen und Einrichtung an der Entwicklung einer europäischen Zusammenarbeit bei Cybersicherheitskrisen, indem die praktische Einsatzfähigkeit und Dokumentation aller betroffenen Akteure, Prozesse und Verfahren im Rahmen bereits bestehender Krisen- und Katastrophenbewältigungsmechanismen der EU, insbesondere der Integrierten Regelung für die politische Reaktion auf Krisen, hergestellt bzw. erstellt wird.

In den Schlussfolgerungen des Rates zur Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit vom November 2016 ist das gemeinsame Ziel festgelegt, auch in Bezug auf den Cyberraum einen Beitrag zur strategischen Autonomie Europas zu leisten, wie es in den Schlussfolgerungen des Rates zur Globalen Strategie für die Außen- und Sicherheitspolitik der Europäischen Union vom November 2016 dargelegt ist. Der Europäische Rat hat diese Botschaft im Juni 2018 nochmals bekräftigt und außerdem betont, dass die Abwehrfähigkeiten gegen Cyberbedrohungen von außerhalb der Union gestärkt werden müssen.

2017 hat der Rat einen Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten, die sogenannte "Cyber Diplomacy Toolbox", angenommen[6]. Dieser Rahmen soll die Zusammenarbeit fördern, Bedrohungen eindämmen und auf lange Sicht Einfluss auf das Verhalten potenzieller Angreifer nehmen. Der Rahmen nutzt die GASP-Maßnahmen, einschließlich restriktiver Maßnahmen, um böswilligen Cyberaktivitäten vorzubeugen und darauf zu reagieren. Die Urheber böswilliger Cyberaktivitäten müssen für ihre Taten zur Rechenschaft gezogen werden, und die EU-Mitgliedstaaten werden angehalten, ihre Reaktionsfähigkeit bezüglich böswilliger Cyberaktivitäten auf koordinierte Weise und in Abstimmung mit der Cyber Diplomacy Toolbox weiterzuentwickeln. Die Staaten sollten von Tätigkeiten mit Hilfe von Informations- und Kommunikationstechnologien, die ihren völkerrechtlichen Verpflichtungen zuwiderlaufen, absehen bzw. diese nicht wissentlich unterstützen sowie nicht wissentlich zulassen, dass auf ihrem Hoheitsgebiet mit Hilfe dieser Technologien völkerrechtswidrige Handlungen begangen werden.

Im September 2017 stellten die Kommission und die Hohe Vertreterin/Vizepräsidentin eine Gemeinsame Mitteilung[7] zu Cyberfragen vor, die darauf abzielt, die aufgrund der neuen Bedrohungen auftretenden Risiken zu senken. Darin ist die Cyberabwehr als einer der wichtigsten Tätigkeitsbereiche und der Politikrahmen für die Cyberabwehr als eine der Säulen der konkreten Umsetzung enthalten[8].

In den Schlussfolgerungen des Rates vom November 2017 zu Cyberfragen wurde die immer engere Verknüpfung zwischen Cybersicherheit und Cyberabwehr anerkannt und dazu aufgerufen, die Zusammenarbeit bei der Cyberabwehr unter anderem durch die Förderung der Zusammenarbeit zwischen den zivilen und militärischen Gemeinschaften, die für die Reaktion auf Vorfälle zuständig sind, zu verstärken. Außerdem wurde betont, dass besonders schwere Cybersicherheitsvorfälle oder -krisen für die Mitgliedstaaten einen hinreichenden Grund darstellen könnten, die "Solidaritätsklausel" der EU und/oder die Beistandsklausel geltend zu machen.

---

6 Schlussfolgerungen des Rates zu einem Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten ("Cyber Diplomacy Toolbox"), Dok. 9916/17 vom 7. Juni 2017.

7 Gemeinsame Mitteilung an das Europäische Parlament und den Rat: "Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen" (13. September 2017, Dok. JOIN(2017), 450 final).

8 Schlussfolgerungen des Rates zur Gemeinsamen Mitteilung an das Europäische Parlament und den Rat: "Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen" (20. November 2017, Dok. 14435/17).

Am 11. Dezember 2017 wurde die Ständige Strukturierte Zusammenarbeit (SSZ) ins Leben gerufen. Dieser ehrgeizige, verbindliche und inklusive Rahmen für die Zusammenarbeit wurde von 25 Mitgliedstaaten geschaffen und umfasst auch die Zusage verstärkter Bemühungen bei der Zusammenarbeit im Bereich Cyberabwehr und damit verbundener Projekte der SSZ. Das erste Paket an SSZ-Projekten, die von den an der SSZ teilnehmenden Mitgliedstaaten 2017 bestimmt wurden, enthält zwei Projekte im Bereich Cyberabwehr: "Teams für die rasche Reaktion auf Cybervorfälle und die gegenseitige Unterstützung im Bereich der Cybersicherheit" und "Plattform für den Austausch von Informationen über die Reaktion auf Cyberbedrohungen und -vorfälle". Es sind weitere SSZ-Projektbündel vorgesehen. Durch die SSZ werden die Cyberabwehrfähigkeiten entwickelt, was die Zusammenarbeit zwischen den teilnehmenden Mitgliedstaaten stärken und die Interoperabilität erhöhen wird.

Im überarbeiteten EU-Fähigkeitsentwicklungsplan, der vom Lenkungsausschuss der Europäischen Verteidigungsagentur im Juni 2018 gebilligt wurde, wird die Cyberabwehr als Schlüsselelement ausgewiesen und die Notwendigkeit von Cyberabwehroperationen in jedem beliebigen operativen Kontext anerkannt; diese Operationen sollten auf einer hochentwickelten Erfassung der aktuellen Lage des Cyberraums bzw. einer entsprechenden Prognose beruhen, wozu unter anderem auch die Fähigkeit gehört, große Mengen an Daten und Erkenntnissen aus zahlreichen Quellen für eine rasche Entscheidungsfindung und eine zunehmende Automatisierung der Datenerfassung, der Analyse und des Entscheidungshilfeprozesses zu kombinieren. Der Fähigkeitsentwicklungsplan 2018 legt die Schwerpunkte der Cyberabwehrfähigkeiten folgendermaßen fest: Zusammenarbeit und Synergien mit relevanten Akteuren aus den Bereichen Cyberabwehr und Cybersicherheit; Tätigkeiten in Bezug auf Forschung und Technologie im Bereich der Cyberabwehr; Systemtechnikrahmen für Cyberoperationen; Aus- und Fortbildung, Evaluierung und Übung (ETEE); Bewältigung von Herausforderungen für die Cyberabwehr in der Luft, im Weltraum, auf See und an Land.

Schließlich ist in den letzten Jahren klar geworden, dass die internationale Gemeinschaft Konflikte verhüten, zusammenarbeiten und den Cyberraum stabilisieren muss. Die EU fördert in enger Zusammenarbeit mit anderen internationalen Organisationen, insbesondere den VN, der OSZE und dem ASEAN-Regionalforum, einen strategischen Rahmen für die Konfliktverhütung, die Zusammenarbeit und die Stabilität im Cyberraum, der folgendes beinhaltet: i) die Anwendung des Völkerrechts, insbesondere der gesamten Charta der Vereinten Nationen, im Cyberraum; ii) die Einhaltung universeller, nicht bindender Normen, Regeln und Grundsätze für ein verantwortungsvolles Verhalten der Staaten; iii) die Entwicklung und Umsetzung regionaler vertrauensbildender Maßnahmen. Der Politikrahmen für die Cyberabwehr sollte dieses Vorhaben auch unterstützen.

Prioritäten

Im aktualisierten Politikrahmen für die Cyberabwehr wurden sechs vorrangige Bereiche festgelegt. Hauptschwerpunkt dieses Politikrahmens ist die Entwicklung von Cyberabwehrfähigkeiten sowie der Schutz der für die GSVP der EU genutzten Kommunikations- und Informationsnetze. Weitere vorrangige Bereiche sind die Folgenden: Schulung und Übungen, Forschung und Technologie, zivil-militärische Zusammenarbeit und internationale Zusammenarbeit. Im Bereich der Ausbildung wird es vor allem darum gehen, die Cyberabwehr-Ausbildung in den Mitgliedstaaten und die Cyber-Sensibilisierungsschulung für die GSVP-Befehlskette zu intensivieren. Es ist zudem wichtig, dass die Cyberdimension bei Übungen angemessen aufgegriffen wird, um die Reaktionsfähigkeit der EU bei Cyberkrisen und hybriden Krisen durch verbesserte Beschlussfassungsverfahren und bessere Verfügbarkeit von Informationen zu stärken. Der Cyberraum ist ein sich rasch entwickelnder Bereich, und neue technologische Entwicklungen müssen erfasst werden, sowohl im zivilen als auch im militärischen Umfeld. Die zivil-militärische Zusammenarbeit in diesem Bereich ist entscheidend für die Gewährleistung einer kohärenten Reaktion auf Cyber-Bedrohungen. Nicht zuletzt könnte eine verstärkte Zusammenarbeit mit internationalen Partnern dazu beitragen, die Cybersicherheit sowohl innerhalb als auch außerhalb der EU zu stärken und die Grundsätze und Werte der EU zu fördern.

In diesem Politikrahmen werden Vorschläge und Möglichkeiten für eine Koordinierung zwischen den einschlägigen Organen, Einrichtungen und Agenturen der EU umrissen. Der Rahmen berücksichtigt auch die wichtige Rolle des Privatsektors bei der Entwicklung von Technologien für Cybersicherheit und Cyberabwehr.

Zudem unterstützt er die weitere Integration der Cyberabwehr in die Krisenbewältigungsmechanismen der Union, wenn zur Bewältigung der Auswirkungen einer Cyberkrise die einschlägigen Bestimmungen des Vertrags über die EU und des Vertrags über die Arbeitsweise der EU[9] Anwendung finden können.

1. Unterstützung der Entwicklung von Fähigkeiten der Mitgliedstaaten im Bereich der Cyberabwehr

Bei der Entwicklung von Fähigkeiten und Technologien im Bereich der Cyberabwehr sollten alle Aspekte der Fähigkeitenentwicklung, so unter anderem Doktrin, Leitung, Organisation, Personal, Ausbildung, Technologie, Infrastruktur, Logistik und Interoperabilität, einbezogen werden. Zu diesem Zweck sollten die Mitgliedstaaten ihre Anstrengungen beim Aufbau wirksamer Cyberabwehrfähigkeiten intensivieren. Der EAD, die Kommission und die EDA sollten zusammenarbeiten und diese Anstrengungen unterstützen.

Es ist erforderlich, die Schwachstellen der Informationsinfrastrukturen, die die GSVP-Missionen und -Operationen unterstützen, laufend zu bewerten, was mit echtzeitnahen Kenntnissen der Wirksamkeit des Schutzes einhergehen muss. Aus operativer Sicht wird einer der Schwerpunkte im Bereich der Cyberabwehr darin bestehen, Verfügbarkeit, Integrität und Vertraulichkeit der Kommunikations- und Informationsnetze der GSVP aufrecht zu erhalten, soweit in den Mandaten der Operationen oder Missionen nichts anderes bestimmt ist. Zudem wird der EAD, in Zusammenarbeit mit den Mitgliedstaaten, die Integration von Cyberabwehrfähigkeiten in GSVP-Missionen und -Operationen vorantreiben.

Akteure, die böswillige Cyberaktivitäten verüben, müssen dafür zur Rechenschaft gezogen werden. Es ist wichtig, dass sich die EU-Mitgliedstaaten mit Unterstützung des EAD für ein gemeinsames Vorgehen gegen böswillige Cyberaktivitäten einsetzen. Die Cyber Diplomacy Toolbox wurde mit dem Ziel entwickelt, die Verwirklichung einer derartigen gemeinsamen Reaktion zu unterstützen. Der EAD und die EDA werden regelmäßige Übungen auf Grundlage der Cyber Diplomacy Toolbox veranstalten, die es den EU-Mitgliedstaaten ermöglichen, sich damit vertraut zu machen.

---

[9] Artikel 222 AEUV und Artikel 42 Absatz 7 EUV unter gebührender Berücksichtigung von Artikel 17 EUV.

In Anbetracht dessen, dass in den nationalen Rechtsvorschriften der Mitgliedstaaten sowie im Unionsrecht der Umfang der Cyberabwehr, insoweit er festgelegt ist, breit gefasst und vielfältig ist, sollte ein gemeinsam aggregiertes Verständnis des Umfangs der Cyberabwehr ausgearbeitet werden.

Da sich die GSVP-Militäroperationen auf die von den Mitgliedstaaten bereitgestellte Kommando-, Kontroll-, Kommunikations- und Computerinfrastruktur stützen, ist im Bereich der Cyberabwehr bei der Planung in Bezug auf den Bedarf für die Informationsinfrastruktur ein gewisses Maß an strategischer Konvergenz notwendig.

Auf der Grundlage der vom EDA-Projektteam zur Cyberabwehr durchgeführten Arbeit zur Entwicklung von Fähigkeiten im Bereich der Cyberabwehr werden der EDA und die Mitgliedstaaten

- den CDP (Plan zur Fähigkeitenentwicklung) und andere Instrumente wie CARD (Koordinierte Jährliche Überprüfung der Verteidigung), die die Zusammenarbeit zwischen Mitgliedstaaten erleichtern und fördern, nutzen, um das Maß an Konvergenz bei der Planung in Bezug auf den Bedarf der Mitgliedstaaten im Bereich der Cyberabwehr auf strategischer Ebene zu erhöhen, und zwar insbesondere in den Bereichen Überwachung, Lageeinschätzung, Prävention, Aufdeckung und Schutz, Informationsaustausch, forensische Fähigkeiten und Fähigkeiten in Bezug auf die Analyse von Schadsoftware, gewonnene Erkenntnisse, Eindämmung von Schäden, Fähigkeiten in Bezug auf die dynamische Datenwiederherstellung, verteilte Datenspeicherung und Sicherung von Daten;
- bestehende und künftige Projekte zur Bündelung und gemeinsamen Nutzung im Bereich der Cyberabwehr bei Militäroperationen (z.B. Forensik, Ausbau der Interoperabilität, Festlegung von Standards) nutzen;
- Standards für Ziele und Anforderungen entwickeln zwecks Festlegung eines von den Mitgliedstaaten zu erreichenden Mindestmaßes an Cybersicherheit und Vertrauen, wobei auf vorhandene unionsweite Erfahrungen zurückgegriffen wird.

Der EAD und die Mitgliedstaaten werden

- den Informationsaustauschs zwischen den Mitgliedstaaten über nationale Doktrinen im Bereich der Cyberabwehr sowie über auf die Cyberabwehr ausgerichtete Rekrutierungs-, Weiterbeschäftigungs- und Reservistenprogramme erleichtern.

Die EDA wird

- die unterschiedlichen Anwendungsbereiche der militärischen Anforderungen im Bereich der Cyberabwehr in den nationalen Rechtsvorschriften der Mitgliedstaaten sowie bei ihren bewährten Verfahren untersuchen. Hauptziel dieser Untersuchung wird die Ausarbeitung einer Unternehmensstruktur für die Cyberabwehr sein, unter Einbeziehung des Anwendungsbereichs, der Funktionen und der Anforderungen, wie sie in diesem Bereich von den Mitgliedstaaten gehandhabt werden, auf der Grundlage der nationalen und EU-Rechtsvorschriften.

Die Mitgliedstaaten werden auf freiwilliger Basis

- die Zusammenarbeit zwischen ihren militärischen IT-Notfallteams (Computer Emergency Response Teams – CERT) im Hinblick auf eine bessere Vorbeugung gegen Sicherheitsvorfälle und den Umgang mit ihnen verbessern;
- zur weiteren Intensivierung der Zusammenarbeit im Bereich Cyberabwehr, einschließlich neuer Projekte, auf die SSZ zurückgreifen;
- den Europäischen Verteidigungsfonds zur gemeinsamen Entwicklung von Cyberabwehrfähigkeiten nutzen;
- ein gemeinsames Verständnis der Beistandsklausel im Bereich der Cybersicherheit schaffen, wobei auf die Wahrung ihrer Flexibilität zu achten ist;
- grundlegende Anforderungen an die Cyberabwehr-Informationsinfrastruktur ausarbeiten;
- – soweit die Verbesserung der Cyberabwehrfähigkeiten von ziviler Expertise im Bereich Netz- und Informationssicherheit abhängt – das Fachwissen der ENISA, der in der NIS-Kooperationsgruppe vertretenen Behörden der Mitgliedstaaten sowie etwaiger anderer EU-Stellen mit Expertise im Bereich der zivilen Cybersicherheit nutzen.

Die Mitgliedstaaten, der EAD/Militärstab der EU, das ESVK und die EDA werden

- die Entwicklung von Ausbildungsmaßnahmen im Bereich der Cyberabwehr im Hinblick auf die Zertifizierung von Gefechtsverbänden der EU prüfen.

Die Kommission wird in Zusammenarbeit mit den Mitgliedstaaten

- die Cyberabwehr in den Arbeitsprogrammen des Europäischen Programms zur industriellen Entwicklung im Verteidigungsbereich und des Europäischen Verteidigungsfonds berücksichtigen.

2. Verbesserung des Schutzes der von EU-Stellen genutzten Kommunikationsnetze der GSVP

Unbeschadet der Rolle des IT-Notfallteams für die Organe, Einrichtungen und sonstigen Stellen der EU (CERT-EU) als für alle Organe, Einrichtungen und sonstige Stellen der Union zuständiger zentraler Struktur für die Koordinierung der Reaktion auf Cybervorfälle wird der EAD im Rahmen der einschlägigen Vorschriften zum Unionshaushalt ein angemessenes und autonomes Verständnis der Sicherheits- und Netzwerkverteidigungsfragen entwickeln und eine eigene IT-Sicherheitskapazität aufbauen. Damit soll die Widerstandsfähigkeit der EAD-Netze für die GSVP verbessert werden, wobei die Prävention, die Aufdeckung, die Reaktion auf Sicherheitsvorfälle, die Lageeinschätzung, der Informationsaustausch und Frühwarnmechanismen im Mittelpunkt stehen werden.

Der Schutz der Kommunikations- und Informationssysteme der GSVP und der Aufbau von Kapazitäten im Bereich der Sicherheit der Informationstechnologien (IT) werden von der Generaldirektion Haushalt und Verwaltung (BA) des EAD geleitet. Zusätzliche zweckgebundene Mittel und Unterstützung werden auch vom Militärstab der Europäischen Union (EUMS), von der Direktion Krisenbewältigung und Planung (CMPD) und vom Zivilen Planungs- und Durchführungsstab (CPCC) zur Verfügung gestellt. Diese Fähigkeit im Bereich der IT-Sicherheit wird sowohl gesicherte als auch frei zugängliche Systeme betreffen und Bestandteil der bestehenden operativen Einheiten sein.

Darüber hinaus besteht die Notwendigkeit, die Sicherheitsvorschriften für Informationssysteme, die von verschiedenen institutionellen EU-Akteuren während der Durchführung von Missionen und Operationen und im Rahmen der GSVP bereitgestellt werden, zu straffen. In diesem Zusammenhang könnte die Einrichtung einer einheitlichen Befehlskette in Betracht gezogen werden, damit die Widerstandsfähigkeit der im Rahmen der GSVP genutzten Netze verbessert wird.

Um die Koordinierung zu verbessern und den Schutz und die Widerstandsfähigkeit der für die GSVP genutzten Kommunikations- und Informationssysteme und -netzwerke zu erhöhen, wurde 2017 ein Lenkungsausschuss für Cybersicherheit (Cyber Governance Board) eingesetzt, der vom Generalsekretär des EAD geleitetet wird.

Die Generaldirektion Haushalt und Verwaltung (BA) des EAD wird

- die Kapazitäten für IT-Sicherheit innerhalb des EAD auf der Grundlage der bestehenden technischen Fähigkeiten und Verfahren stärken, mit Schwerpunkt auf Prävention, Aufdeckung, Reaktion auf Sicherheitsvorfälle, Lageeinschätzung, Informationsaustausch und Frühwarnmechanismen. Zudem sollte eine Strategie für die Zusammenarbeit mit dem CERT-EU und den bestehenden Fähigkeiten der EU im Bereich der Cybersicherheit weiter verbessert werden.

Die Generaldirektion Haushalt und Verwaltung (BA) des EAD wird gemeinsam mit dem EUMS, dem MPCC, der CMPD und dem CPCC

- kohärente Maßnahmen und Leitlinien für die IT-Sicherheit entwickeln, auch unter Berücksichtigung des technischen Bedarfs im Bereich der Cyberabwehr im GSVP-Kontext bei Strukturen, Missionen und Operationen und unter Beachtung der in der EU bestehenden Kooperationsrahmen und -maßnahmen, um bei den Vorschriften, den Maßnahmen und der Organisation Konvergenz zu erreichen.

Der EAD/Das Einheitliche Analyseverfahren (SIAC) wird

- aufbauend auf bestehenden Strukturen die Bewertung der Bedrohungslage im Cyberbereich und die Fähigkeit der Nachrichtengewinnung ausbauen, um neue Cyberrisiken erkennen und regelmäßig Risikobewertungen durchführen zu können, die die Bewertung strategischer Bedrohungen und echtzeitnahe Informationen über Sicherheitsvorfälle umfassen, deren Bereitstellung zwischen den einschlägigen EU-Strukturen koordiniert wird und die nach verschiedenen Geheimhaltungsstufen zugänglich gemacht werden.

Der EAD/das SIAC und das CERT-EU werden

- den Echtzeit-Austausch von Informationen über Cyberbedrohungen zwischen den Mitgliedstaaten und einschlägigen EU-Stellen fördern. Zu diesem Zweck werden Mechanismen für den Informationsaustausch und vertrauensbildende Maßnahmen von den zuständigen nationalen und europäischen Behörden entwickelt werden, und zwar anhand eines auf Freiwilligkeit beruhenden Ansatzes, der sich auf bereits bestehende Formen der Zusammenarbeit stützt.

Der EAD/das EUMS und der MPCC werden

- ein Cyberabwehr-Konzept für militärische Missionen und Operationen im Rahmen der GSVP weiterentwickeln und dieses Konzepts in die strategische Planung einbeziehen;
- generische Standard-Einsatzverfahren für die operative Ebene in Zusammenarbeit mit den operativen Hauptquartieren ausarbeiten.

Der EAD/der CPCC und der MPCC werden

- ein Cyberabwehr-Konzepts für zivile Missionen im Rahmen der GSVP weiterentwickeln und dieses Konzepts in die strategische Planung einbeziehen;
- die Cyberabwehrfähigkeiten ziviler GSVP-Missionen unter Nutzung bestehender Infrastrukturen verstärken und Standardisierung und Harmonisierung der bei GSVP-Missionen und Operationen eingesetzten Technologien fördern, gegebenenfalls unter Nutzung der Expertise des CERT-EU, der ENISA und der EDA;
- – im Rahmen der Stärkung der zivilen GSVP – eine möglichen Unterstützung von Aufnahmeländern bei der Cyberabwehr durch zivile GSVP-Missionen weiter prüfen.

Der EAD wird

- gemeinsame Anforderungen für militärische und zivile Missionen und Operationen im Rahmen der GSVP weiterentwickeln;
- die Koordinierung im Bereich der Cyberabwehr verbessern, um die Ziele in Bezug auf den Schutz der Netze, die von institutionellen EU-Akteuren zur Unterstützung der GSVP genutzt werden, zu verwirklichen, wobei auf vorhandene unionsweite Erfahrungen zurückgegriffen wird;
- den Ressourcenbedarf und andere einschlägige politische Entscheidungen vor dem Hintergrund des sich verändernden Bedrohungsumfeldes in Konsultation mit den Mitgliedstaaten und anderen EU-Organen regelmäßig überprüfen.

3. Förderung der zivil-militärischen Zusammenarbeit

Der Cyberraum ist ein sich rasch weiterentwickelnder Bereich: Die technologischen Entwicklungen müssen sowohl im zivilen als auch im militärischen Umfeld durch Sicherheitssysteme verstärkt werden. Es sollte eine möglichst weitgehende Koordinierung zwischen dem zivilen und dem militärischen Bereich vorgesehen werden für Fälle, in denen ähnliche technologische Entwicklungen Lösungen für zivile und militärischen Anwendungen bieten. In anderen Fällen sind militärische Fähigkeiten und Waffensysteme so spezifisch, dass kein Spielraum für eine gemeinsame Nutzung mit zivilen Technologien vorhanden ist. Unbeschadet der internen Organisation und der Rechtsvorschriften der Mitgliedstaaten kann die zivil-militärische Zusammenarbeit im Cyberbereich beispielsweise in Betracht gezogen werden für den Austausch bewährter Verfahren, den Informationsaustausch und Frühwarnmechanismen, Risikobewertungen in Bezug auf die Reaktion auf Sicherheitsvorfälle, Sensibilisierungsmaßnahmen sowie für Schulungen und Übungen.

Die Verbesserung der zivilen Cybersicherheit ist ein wichtiger Faktor, der zur generellen Erhöhung der Netz- und Informationssicherheit beiträgt. Die NIS-Richtlinie steigert die Abwehrbereitschaft auf nationaler Ebene und stärkt die Zusammenarbeit auf Unionsebene zwischen den Mitgliedstaaten sowohl in strategischer wie auch operativer Hinsicht. Diese Zusammenarbeit sollte sowohl die nationalen Behörden, die mit der Beaufsichtigung der Cybersicherheitsstrategien befasst sind, als auch die CERT der Mitgliedstaaten und das CERT-EU einschließen. Die Zusammenarbeit zwischen den zivilen und den militärischen CERT sollte unter gebührender Berücksichtigung dieser Entwicklungen vertieft werden. Der neue europäische Rechtsakt zur Cybersicherheit soll die Cyber-Resilienz Europas verbessern und einen Rahmen für die Cybersicherheitszertifizierung für Produkte und Dienste bieten und damit das Vertrauen in den zivilen digitalen Raum erhöhen.

Die EDA, die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA), das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3) und das CERT-EU in Zusammenarbeit mit anderen einschlägigen Einrichtungen und Agenturen der EU – im Rahmen ihrer jeweiligen Mandate und ohne dass Überschneidungen mit den Kompetenzen der Mitgliedstaaten entstehen – sowie die Mitgliedstaaten werden ermutigt, ihre Zusammenarbeit in den folgenden Bereichen weiter zu vertiefen:

- Entwicklung gemeinsamer Kompetenzprofile für Cybersicherheit und -abwehr auf der Grundlage internationaler bewährter Verfahren und der von den Organen, Einrichtungen und Agenturen der EU verwendeten Zertifizierung, wobei auch die Zertifizierungsstandards des Privatsektors zu berücksichtigen sind.
- Leistung eines Beitrags zur Weiterentwicklung und Anpassung der organisatorischen und technischen Standards der Cybersicherheit und -abwehr im öffentlichen Sektor, sodass diese für den Verteidigungs- und Sicherheitssektor tauglich sind. erforderlichenfalls Aufbau auf die laufenden Arbeiten der ENISA und der EDA;
- Einführung oder Weiterentwicklung von Arbeitsmechanismen und Vereinbarungen für den Austausch bewährter Verfahren, insbesondere in Bezug auf Ausbildung, Schulung, Übungen, Forschung und Technologie sowie andere Bereiche, die zivil-militärische Synergien ermöglichen;
- Aufbau auf den bestehenden Präventions-, Ermittlungs- und Forensikfähigkeiten der EU im Bereich der Cyberkriminalität und auf deren verstärkter Nutzung bei der Entwicklung von Cyberabwehrfähigkeiten.

Die Mitgliedstaaten werden auf freiwilliger Basis

- die Zusammenarbeit zwischen den Mitgliedstaaten in Bezug auf die zivilen und die militärischen CERT verstärken.

Der EAD und die Mitgliedstaaten werden

- die Cyberabwehr in die Verfahren der EU für Krisenbewältigung und Katastrophenmanagement (nach dem "Blueprint"-Verfahren) einbeziehen.

4. Forschung und Technologie

Die Betreiber von Infrastruktur und die Anbieter von IKT-Dienstleistungen für zivile und für Verteidigungszwecke sind infolge gemeinsamer Technologien und Anforderungen an die operativen Fähigkeiten mit ähnlichen Herausforderungen im Bereich der Cybersicherheit konfrontiert. Um die Interoperabilität der Systeme auf Dauer zu verbessern und die Kosten für die Entwicklung geeigneter Lösungen zu senken, wird von gemeinsamen Bedürfnissen bei Forschung und Technologie sowie gemeinsamen Anforderungen an die Systeme ausgegangen. Es ist unbedingt notwendig, größenbedingte Kostenvorteile zu erreichen, um der ständig steigenden Zahl von Bedrohungen und Schwachstellen Herr zu werden. Dies dürfte wiederum den Erhalt und das Wachstum einer wettbewerbsfähigen Industrie für Cyberabwehr in Europa begünstigen.

Die Entwicklung der Fähigkeiten im Bereich der Cyberabwehr hat eine bedeutende Forschungs- und Technologie-Dimension. Die EDA hat im Rahmen der Forschungsagenda im Bereich der Cyberabwehr eine solide Grundlage für die Festlegung von Prioritäten für die künftige Finanzierung von Forschung und Technologie (FuT) im zwischenstaatlichen Rahmen vorgegeben. Die strategische Forschungsagenda, die im Anschluss daran innerhalb der zuständigen Ad-hoc-Arbeitsgruppe der EDA ausgearbeitet wurde, bietet eine sachkundige Priorisierung zu den im militärischen Bereich benötigten Cyber-Technologien, verweist zugleich aber auch auf Einsatzmöglichkeiten im Bereich des doppelten Verwendungszwecks und der Investitionen, sowohl im Kontext einer nationalen, multinationalen wie auch einer EU-Finanzierung.

Die Entwicklung technologischer Fähigkeiten in Europa ist von wesentlicher Bedeutung, wenn es darum geht, Bedrohungen und Schwachstellen zu verringern. Die Industrie wird weiterhin die Haupttriebfeder für Technologie und Innovation im Zusammenhang mit der Cyberabwehr bleiben. Kryptographie, eingebettete IKT-Systeme, Erkennung von Schadprogrammen, Simulations- und Visualisierungstechniken, Schutz für Netze und Kommunikationssysteme sowie Identifizierungs- und Authentifizierungstechnologien sind einige der Bereiche, die anzugehen sind. Ferner ist es wichtig, eine wettbewerbsfähige europäische industrielle Lieferkette im Bereich der Cybersicherheit zu fördern, indem die Einbindung von kleinen und mittleren Unternehmen (KMU) gefördert wird.

Ob gewährleistet wird, dass Europa mit seinen internationalen Konkurrenten im Bereich der cybertechnologischen Fähigkeiten Schritt halten, hängt auch von unserer Fähigkeit zur Förderung bahnbrechender Innovationen ab, sowohl durch nationale als auch durch EU-Instrumente wie dem Europäischen Investitionsrat.

Zur Erleichterung der zivil-militärischen Zusammenarbeit bei der Entwicklung von Cyberabwehr-Fähigkeiten, zur Stärkung der technologischen und industriellen Basis der europäischen Verteidigung[10] **und zur Leistung eines Beitrags zur strategischen Autonomie der EU, auch im Bereich des Cyberraums**, wann und wo dies erforderlich ist sowie nach Möglichkeit in Zusammenarbeit mit Partnern,

werden der EAD, die Kommission und die Mitgliedstaaten

- nach Synergien zwischen den FuT-Anstrengungen im militärischen Bereich und den zivilen FuE-Programmen, insbesondere solchen mit Bezug zu bahnbrechenden Innovationen, streben und den Aspekt der Cybersicherheit und -abwehr bei der Umsetzung der vorbereitenden Maßnahme der Union im Bereich Verteidigungsforschung berücksichtigen;
- die Forschungsagenden zur Cybersicherheit (z.B. Strategische Forschungsagenda der Europäischen Verteidigungsagentur) sowie die daraus hervorgehenden Fahrpläne und Maßnahmen austauschen. Zu diesem Zweck wird eine bereichsübergreifende Cyberabwehr-Forschungsagenda in enger Zusammenarbeit mit der Kommission und den Mitgliedstaaten ausgearbeitet werden;
- zur besseren Einbeziehung des Aspekts der Cybersicherheit und der Cyberabwehr in Programme beitragen, die einen mit der Doppelverwendungsfähigkeit zusammenhängenden Sicherheits- und Abwehraspekt aufweisen, so etwa das gemeinsame Unternehmen zur Entwicklung des europäischen Flugverkehrsmanagementsystems der neuen Generation (SESAR).

[10] Mitteilung der Kommission "Auf dem Weg zu einem wettbewerbsfähigeren und effizienteren Verteidigungs- und Sicherheitssektor", COM (2013) 542.

Die Kommission wird

- die Einrichtung eines Europäisches Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung mit einem Netz nationaler Koordinierungszentren zur Unterstützung der technologischen und industriellen Kapazitäten im Bereich der Cybersicherheit und zur Stärkung der Wettbewerbsfähigkeit der Cybersicherheitsbranche der Union, unter Gewährleistung der Komplementarität und unter Vermeidung von Überschneidungen innerhalb des Netzes von Kompetenzzentren für Cybersicherheit und mit anderen EU-Agenturen, prüfen. Das Kompetenzzentrum sollte unter anderem die Zusammenarbeit zwischen zivilen und militärischen Technologien und Anwendungen ausbauen und eng und in vollständiger Komplementarität mit der Europäischen Verteidigungsagentur bei der Cyberabwehr zusammenarbeiten;
- die Entwicklung industrieller Ökosysteme und Innovationscluster fördern, die die gesamte Wertschöpfungskette im Sicherheitsbereich betreffen, unter Nutzung wissenschaftlicher Erkenntnisse sowie der Innovationen und der industriellen Produktion der KMU.

Die Kommission wird in Zusammenarbeit mit den Mitgliedstaaten

- Cyberabwehr-Aspekte bei den Aufforderungen zur Einreichung von Vorschlägen für vorbereitende Maßnahmen der Union im Bereich Verteidigungsforschung berücksichtigen;
- die Cyberabwehr bei den Themen betreffend die Aufforderungen zur Einreichung von Vorschlägen im Rahmen des Europäischen Verteidigungsfonds berücksichtigen;
- die Politikkohärenz in der EU unterstützen, um sicherzustellen, dass politische und technische Aspekte des Cyber-Schutzes in der EU weiterhin eine Priorität der technologischen Innovation bleiben und in der gesamten EU harmonisiert werden (Fähigkeit zur Analyse und Bewertung von Cyberbedrohungen, Initiativen zur konzeptionsintegrierten Sicherheit ("security by design"), Abhängigkeitsmanagement in Bezug auf den Zugang zu Technologie usw.).

5. Verbesserung der Ausbildungs-, Schulungs- und Übungsmöglichkeiten

Um die Abwehrbereitschaft gegen Cyberbedrohungen zu stärken und eine gemeinsame Kultur der Cyberabwehr in der ganzen Union zu entwickeln, auch für EU-Missionen und -Operationen, bedarf es einer Verbesserung und einer Ausweitung der Schulungsmöglichkeiten im Bereich Cyberabwehr. Es ist entscheidend, dass die Mittel für Ausbildung und Schulung möglichst effizient eingesetzt werden und gleichzeitig bestmögliche Qualität gewährleistet wird. Die Bündelung und gemeinsame Nutzung – auf europäischer Ebene – von Schulungs- und Ausbildungsmaßnahmen im Bereich der Cyberabwehr sind von größter Wichtigkeit.

Das Europäische Sicherheits- und Verteidigungskolleg (ESVK), der EAD, die EDA, die Kommission und die Mitgliedstaaten werden

- auf der Grundlage der von der EDA vorgelegten Analyse des Schulungsbedarfs im Bereich der Cyberabwehr und der Erfahrungen des ESVK mit Schulungen zur Cybersicherheit GSVP-Schulungen und -Ausbildungen für unterschiedliche Adressatenkreise, darunter EAD-Personal, Personal von GSVP-Missionen und -Operationen sowie Beamte aus den Mitgliedstaaten, festlegen, was außerdem das Problem der Weiterbeschäftigung von qualifiziertem Personal kurz-, mittel- und langfristig lösen sollte;
- die Einrichtung eines Dialogs im Bereich Cyberabwehr vorschlagen, der Schulungsstandards und Zertifizierungen zum Gegenstand hat und an dem die Mitgliedstaaten, EU-Organe, Drittländer und andere internationale Organisationen sowie der Privatsektor teilnehmen;
- Verbindungen zu europäischen Schulungsanbietern im Privatsektor sowie zu wissenschaftlichen Einrichtungen knüpfen, um Kompetenzen und Fähigkeiten des an GSVP-Missionen und -Operationen beteiligten Personals zu verbessern.

Das Europäische Sicherheits- und Verteidigungskolleg wird

- die vom ESVK eingerichtete Plattform zur Aus- und Fortbildung, Evaluierung und Übung in Bezug auf Cyberfragen (Cyber ETEE Platform) weiterentwickeln;
- Synergien mit den Schulungsprogrammen anderer Akteure wie ENISA, Europol, Europäische Polizeiakademie (CEPOL) und Kompetenzzentrum der NATO für kooperativen Schutz vor Computerangriffen schaffen;
- die Möglichkeit gemeinsamer Schulungsprogramme von ESVK und NATO im Bereich der Cyberabwehr sondieren, die allen EU-Mitgliedstaaten offenstehen, um so eine gemeinsame Kultur der Cyberabwehr zu fördern.

Die Kommission wird

- die Optionen für eine Ausweitung der im Rahmen der Plattform zur Aus- und Fortbildung, Evaluierung und Übung ermittelten Schulungs- und Ausbildungsangebote in den Mitgliedstaaten bewerten.

Die EDA wird

- weitere EDA-Kurse in Zusammenarbeit mit dem ESVK entwickeln, um die Anforderungen der Mitgliedstaaten für Ausbildung und Schulung, Evaluierung und Übung im Bereich Cyberabwehr zu decken;
- die Plattform zur Aus- und Fortbildung, Evaluierung und Übung unter anderem durch eine schrittweise Einbindung der von der EDA entwickelten Ausbildungsmodule und Schulungsmodule sowie Evaluierungs- und Übungsmodule für den Cyberbereich unterstützen.

Der EAD und die Mitgliedstaaten werden

- in enger Zusammenarbeit mit den einschlägigen Dienststellen der Organe, Einrichtungen und Agenturen der EU die etablierten Zertifizierungsmechanismen des ESVK für Schulungsprogramme auf der Grundlage der bestehenden Standards und des vorhandenen Wissens verfolgen; die Möglichkeit prüfen, im Rahmen der militärischen Erasmus-Initiative cyberspezifische Module vorzusehen.

Die Übungsmöglichkeiten zur Cyberabwehr für militärische und zivile Akteure der GSVP müssen verbessert werden. Gemeinsame Übungen sind ein Instrument, mit dem das gemeinsame Wissen und Verständnis in Bezug auf Cyberabwehr weiterentwickelt werden kann. Die nationalen Streitkräfte werden so in die Lage versetzt, ihre Bereitschaft für Einsätze in einem multinationalen Umfeld zu erhöhen. Die Durchführung gemeinsamer Übungen zur Cyberabwehr wird auch Interoperabilität und Vertrauen fördern.

Der EAD, die EDA, das CERT-EU und die Mitgliedstaaten werden sich verstärkt um die Förderung von Aspekten der Cyberabwehr im Rahmen von GSVP- und anderen Übungen bemühen und hierzu

- den Aspekt der Cyberabwehr in die bestehenden Übungsszenarien für *MILEX* und *MULTILAYER* einbeziehen;
- regelmäßig strategische/politische Übungen – wie beispielsweise *CYBRID 2017*– in Abstimmung mit der EU-geführten parallelen und koordinierten Übung (PACE) und technisch-operative Übungen wie *DEFNET* abhalten;
- gegebenenfalls eine spezielle EU-Cyberabwehrübung im Rahmen der GSVP entwickeln und eine mögliche Abstimmung mit von der ENISA organisierten gesamteuropäischen Übungen zu Cybervorfällen, wie *CyberEurope*, sondieren;
- weiterhin an anderen multinationalen Cyberabwehrübungen wie *Locked Shields* teilnehmen;
- im Einklang mit dem Übungsrahmen der EU einschlägige internationale Partner wie die NATO zu den Übungen einladen;
- regelmäßige Übungen auf der Grundlage der Cyber Diplomacy Toolbox abhalten, in denen die Mitgliedstaaten ihre Reaktion auf böswillige Cyberaktivitäten üben können.

6. Förderung der Zusammenarbeit mit den einschlägigen internationalen Partnern

Es ist im Rahmen der internationalen Zusammenarbeit notwendig, einen Dialog mit den internationalen Partnern, insbesondere der NATO und anderen internationalen Organisationen, sicherzustellen, um zur Entwicklung wirksamer Fähigkeiten im Bereich der Cyberabwehr beizutragen. Es sollte eine stärkere Beteiligung an den Arbeiten angestrebt werden, die im Rahmen der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) und der Vereinten Nationen (VN) durchgeführt werden, mit dem Ziel, einen strategischen Rahmen für Konfliktverhütung, Zusammenarbeit und Stabilität im Cyberraum zu schaffen.

In der EU besteht der politische Wille, im Bereich der Cyberabwehr stärker mit der NATO bei der Entwicklung robuster und widerstandsfähiger Fähigkeiten zur Cyberabwehr zusammenzuarbeiten, wie in der von dem Präsidenten des Europäischen Rates, dem Präsidenten der Europäischen Kommission und dem Generalsekretär der Nordatlantikvertrags-Organisation am 8. Juli 2016 in Warschau unterzeichneten Gemeinsamen Erklärung gefordert wurde. Regelmäßige Arbeitsberatungen, wechselseitige Briefings sowie etwaige Treffen zwischen der Gruppe "Politisch-militärische Angelegenheiten" und den einschlägigen Ausschüssen der NATO werden im Einklang mit dem genannten Rahmen dazu beitragen, unnötige Doppelarbeit zu vermeiden und für die Kohärenz und Komplementarität der Bemühungen zu sorgen.

Der EAD und die EDA werden zusammen mit den Mitgliedstaaten die Zusammenarbeit zwischen EU und NATO im Bereich der Cyberabwehr weiterentwickeln, wobei der institutionelle Rahmen und die Beschlussfassungsautonomie aller Organisationen gebührend geachtet werden, und hierzu

- die bestehenden Maßnahmen im Rahmen der Umsetzung der Gemeinsamen Erklärung des Präsidenten des Europäischen Rates, des Präsidenten der Europäischen Kommission und des Generalsekretärs der Nordatlantikvertrags-Organisation intensivieren;
- bewährte Verfahren in Bezug auf Krisenbewältigung sowie auf die Cyberabwehr bei militärischen und zivilen Missionen und Operationen austauschen;
- – sofern Überschneidungen vorliegen – auf Kohärenz der Ergebnisse bei der Entwicklung der Fähigkeitsanforderungen im Bereich der Cyberabwehr hinarbeiten, insbesondere bei der Entwicklung langfristiger Cyberabwehrfähigkeiten;
- auf der Grundlage angemessener Bewertungen den Rahmen für die Zusammenarbeit der EDA mit dem NATO-Kompetenzzentrum für kooperativen Schutz vor Computerangriffen als Ausgangsplattform für die verstärkte Zusammenarbeit bei multinationalen Cyberabwehrprojekten umfassender nutzen.

Das ESVK, der EAD und die EDA werden

- die Zusammenarbeit bei Konzepten für Ausbildung und Schulung im Bereich der Cyberabwehr sowie bei entsprechenden Übungen ausbauen;
- die wechselseitige Teilnahme von Personal an den Übungen im Einklang mit dem vereinbarten Rahmen sicherstellen.

Das CERT-EU wird

- die technische Vereinbarung zwischen dem CERT-EU und der NCIRC (NATO Computer Incident Response Capability) weiterhin nutzen, um Lagebeurteilung, Informationsaustausch und Frühwarnmechanismen zu verbessern und Bedrohungen vorzugreifen, die beide Organisationen betreffen könnten.

Was andere internationale Organisationen und einschlägige internationale Partner der EU anbelangt, so werden der EAD und die Mitgliedstaaten gegebenenfalls

- die strategischen Entwicklungen verfolgen und mit internationalen Partnern (internationale Organisationen und Drittländer) Konsultationen zu Fragen der Cyberabwehr führen;
- Möglichkeiten für die Zusammenarbeit in Fragen der Cyberabwehr sondieren, auch mit Drittländern, die sich an GSVP-Missionen und -Operationen beteiligen;
- sich in den einschlägigen internationalen Organisationen – insbesondere den Vereinten Nationen, der OSZE und dem ASEAN-Regionalforum – für die Anwendung des bestehenden Völkerrechts – vor allem der gesamten Charta der Vereinten Nationen – im Cyberraum sowie für die Entwicklung und Umsetzung universeller, nicht bindender Normen für ein verantwortungsvolles Verhalten der Staaten und für regionale vertrauensbildende Maßnahmen zwischen den Staaten mit dem Ziel einer erhöhten Transparenz und der Verringerung des Risikos einer falschen Einschätzung staatlichen Handelns einsetzen.

Die Kommission und der EAD werden

- gegebenenfalls den Ausbau der Cyberfähigkeiten für die EU-Partner im Rahmen des geänderten Stabilitäts- und Friedensinstruments unterstützen.

Folgemaßnahmen

Im Rahmen der Koordinierung der Umsetzung des Politikrahmens für die Cyberabwehr durch den EAD sollte der Gruppe "Politisch-militärische Angelegenheiten" – unter Teilnahme der Mitglieder der Horizontalen Gruppe "Fragen des Cyberraums" – und dem Politischen und Sicherheitspolitischen Komitee vom EAD/von der EDA/von der Kommission mit dem Ziel der Bewertung des Politikrahmens für die Cyberabwehr ein jährlicher Fortschrittsbericht über die sechs oben genannten Bereiche vorgelegt werden. Ebenso wird alle sechs Monate eine mündliche Vorstellung erfolgen.

Es ist von entscheidender Bedeutung, dass in dem Maße, wie sich die Cyberbedrohungen weiterentwickeln, neue Anforderungen im Bereich der Cyberabwehr ermittelt und anschließend in den Politikrahmen für die Cyberabwehr aufgenommen werden. Die nächste Überprüfung des Politikrahmens sollte – in enger Abstimmung mit den Mitgliedstaaten – nicht später als Mitte 2022 vorgestellt werden.