Rat der
Europäischen Union

Brüssel, den 18. November 2014
(OR. en)

15585/14

COPS 303
POLMIL 103
CYBER 61
RELEX 934
JAI 880
TELECOM 210
CSC 249
CIS 13
COSI 114

BERATUNGSERGEBNISSE

des	Rates
vom	17./18. November 2014
Nr. Vordok.:	15193/14 + COR 1 COPS 287 POLMIL 97 CYBER 58 RELEX 897 JAI 845 TELECOM 196 CSC 242 CIS 12 COSI 111
Betr.:	EU-Politikrahmen für die Cyberabwehr

Die Delegationen erhalten anbei den EU-Politikrahmen für die Cyberabwehr in der Fassung, die der Rat am 18. November 2014 angenommen hat.

ANLAGE

EU-POLITIKRAHMEN FÜR DIE CYBERABWEHR

Hintergrund und Ziele

Der Cyberraum wird häufig als der fünfte Bereich für militärische Aktivitäten beschrieben, der für die Umsetzung der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) der Europäischen Union (EU) gleichermaßen wichtig ist wie die Bereiche Land, See, Luft und Weltraum. Für die erfolgreiche Umsetzung der GSVP ist es immer stärker entscheidend, dass ein sicherer Cyberraum verfügbar und zugänglich ist. Robuste und belastbare Fähigkeiten im Bereich der Cyberabwehr sind jetzt erforderlich, um die GSVP-Strukturen und die GSVP-Missionen und -Operationen unterstützen zu können.

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.

Mit dem vorliegenden Dokument sollen die Schlussfolgerungen des Europäischen Rates und des Rates sowie die Aspekte der Cyberabwehr in der Cybersicherheitsstrategie der EU[1] einen Rahmen erhalten. Im Dokument werden vorrangige Bereiche für die Cyberabwehr im Rahmen der GSVP festgelegt und die Rollen der verschiedenen europäischen Akteure näher bestimmt, wobei die jeweiligen Verantwortlichkeiten und Zuständigkeiten der Unionsakteure und der Mitgliedstaaten sowie der institutionelle Rahmen der EU und ihre Autonomie bei der Entscheidungsfindung uneingeschränkt geachtet werden. Die Umsetzung der Cybersicherheitsstrategie der EU wurde von der für Fragen des Cyberraums zuständigen Gruppe der Freunde des Vorsitzes vereinbart.

[1] Gemeinsame Mitteilung an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: "Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum" vom 7. Februar 2013, und die entsprechenden Schlussfolgerungen des Rates (Allgemeine Angelegenheiten) vom 25. Juni 2013.

Ein Schwerpunkt dieses Politikrahmens wird die Entwicklung von Fähigkeiten im Bereich der Cyberabwehr sein, die von den Mitgliedstaaten für die Zwecke der GSVP sowie zum Schutz der für die GSVP relevanten Kommunikations- und Informationsnetze des Europäischen Auswärtigen Dienstes (EAD) bereitgestellt werden. Im Ausbildungsbereich steht die Entwicklung von Programmen für verschiedene Zielgruppen in der GSVP-Befehlskette im Mittelpunkt. Es ist wichtig, dass die Cyberdimension bei Übungen angemessen aufgegriffen wird, um die Reaktionsfähigkeit der EU bei einer Cyberkrise im GSVP-Kontext und die Verfahren für die strategische Beschlussfassung zu verbessern und die Architektur der Informationsinfrastruktur zu stärken. Der Cyberraum ist ein sich rasch entwickelnder Bereich, in dem Fähigkeiten mit doppeltem Verwendungszweck eine sehr wichtige Rolle spielen, weshalb es erforderlich ist, die zivil-militärische Zusammenarbeit und Synergien mit der übergreifenden Cyberpolitik der EU weiterzuentwickeln, um den mit dem Cyberraum verbundenen neuen Herausforderungen begegnen zu können, wobei die interne Organisation und die Zuständigkeiten der Mitgliedstaaten zu achten sind.

In diesem Dokument werden die Grundsätze dargelegt, mit denen die Zusammenarbeit mit dem Privatsektor bei der Entwicklung von Fähigkeiten im Bereich der Cyberabwehr erleichtert werden soll; dabei wird ein besonderer Schwerpunkt auf die Stärkung von Forschung und Technologie (FuT) und der technologischen und industriellen Basis der europäischen Verteidigung (EDTIB) gelegt. Außerdem sorgt dieses Dokument für Kohärenz bei den Anstrengungen der EU und der Nordatlantikpakt-Organisation (NATO) im Bereich der Cyberabwehr und enthält Vorschläge für Bereiche der Zusammenarbeit zwischen ihnen.

Schließlich sollten die Ziele der Cyberabwehr besser in die Mechanismen der Union für Krisenmanagement einbezogen werden. Um die Auswirkungen einer Cyberkrise zu bewältigen, können gegebenenfalls die einschlägigen Bestimmungen des Vertrags über die EU und des Vertrags über die Arbeitsweise der EU[2] Anwendung finden.

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

Prioritäten des EU-Politikrahmens für die Cyberabwehr

1. Unterstützung der Entwicklung von Fähigkeiten der Mitgliedstaaten im Bereich der Cyberabwehr im Zusammenhang mit der GSVP

Um die Widerstandsfähigkeit der Netze zur Unterstützung der Umsetzung der GSVP zu gewährleisten, sollte der Schwerpunkt darauf liegen, den Schutz der vom EAD verwalteten Kommunikationsnetze der GSVP-Strukturen zu verbessern und seitens der Mitgliedstaaten Fähigkeiten im Bereich der Cyberabwehr, die den GSVP-Missionen und -Operationen zur Verfügung stehen, zu entwickeln. In diesem Sinne sollten die Mitgliedstaaten, der EAD und die EDA zusammenarbeiten, damit sie wirksame Fähigkeiten im Bereich der Cyberabwehr bereitstellen können.

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.

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 bei den Aktivitäten im Bereich der Cyberabwehr das Hauptaugenmerk auf die Erhaltung der Funktionsweise der Kommunikations- und Informationsnetze der GSVP gerichtet sein, soweit in den Mandaten der Operationen oder Missionen nichts anderes bestimmt ist.

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 EAD/die EDA und die Mitgliedstaaten Folgendes unternehmen:

- Nutzung des Plans zur Fähigkeitenentwicklung und anderer Instrumente, die die Zusammenarbeit zwischen Mitgliedstaaten erleichtern und fördern, 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;
- Unterstützung bestehender und künftiger Projekte zur Bündelung und gemeinsamen Nutzung im Bereich der Cyberabwehr bei Militäroperationen (z.B. Forensik, Ausbau der Interoperabilität, Festlegung von Standards);
- Entwicklung von Standards für Ziele und Anforderungen zwecks Festlegung eines Mindestmaßes an Cybersicherheit und Vertrauen, das von den Mitgliedstaaten zu erreichen ist, wobei auf vorhandene unionsweite Erfahrungen zurückgegriffen wird;
- Erleichterung des Informationsaustauschs zwischen den Mitgliedstaaten über nationale Doktrinen im Bereich der Cyberabwehr, über Ausbildungsprogramme und Übungen sowie über auf die Cyberabwehr ausgerichtete Rekrutierungs-, Weiterbeschäftigungs- und Reservistenprogramme;
- Verbesserung der freiwilligen Zusammenarbeit zwischen militärischen IT-Notfallteams (Computer Emergency Response Teams – CERTs) der Mitgliedstaaten, um die Prävention gegen Sicherheitsvorfälle und den Umgang mit ihnen zu verbessern;
- Prüfung der Entwicklung von Ausbildungsmaßnahmen im Bereich der Cyberabwehr im Hinblick auf die Zertifizierung von Gefechtsverbänden der EU.
- Soweit die Verbesserung der Fähigkeiten im Bereich der Cyberabwehr von ziviler Expertise im Bereich Netz- und Informationssicherheit abhängt, können die Mitgliedstaaten die ENISA um Unterstützung ersuchen.

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

Unbeschadet der Rolle des CERT-EU als für alle Organe, Einrichtungen und sonstige Stellen der Union zuständiger zentraler Struktur für die Koordinierung der Reaktion auf Cybervorfälle sollte 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 EAD-Direktion für Ressourcen 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 Operationen und Missionen 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 den Schutz der Kommunikationsnetze der GSVP zu verbessern, werden die Direktion für Ressourcen, der EUMS, die CMPD und der CPCC in Zusammenarbeit mit dem Zentrum für Informationsgewinnung und -analyse (INTCEN) Folgendes unternehmen:

- Stärkung der Kapazitäten für IT-Sicherheit innerhalb des EAD auf der Grundlage der bestehenden technischen Fähigkeiten und Verfahren 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 ausgearbeitet oder in den Fällen, in denen eine solche vorhanden ist, weiter verbessert werden;
- Entwicklung kohärenter Maßnahmen und Leitlinien für die IT-Sicherheit, 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;
- aufbauend auf bestehenden Strukturen Ausbau der Bewertung der Bedrohungslage im Cyberbereich und der Fähigkeit der Nachrichtengewinnung, 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;
- Förderung des Echtzeit-Austauschs von Informationen über Cyberbedrohungen zwischen den Mitgliedstaaten und einschlägigen EU-Stellen. Zu diesem Zweck sollen 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;
- Ausarbeitung eines einheitlichen Konzepts im Bereich der Cyberabwehr für militärische Operationen[3] und zivile Missionen im Rahmen der GSVP und Einbeziehung dieses Konzepts in die strategische Planung;
- Verbesserung der Koordinierung im Bereich der Cyberabwehr, 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;
- regelmäßige Überprüfung des Ressourcenbedarfs und anderer einschlägiger politischer Entscheidungen vor dem Hintergrund des sich verändernden Bedrohungsumfeldes in Konsultation mit den einschlägigen Ratsarbeitsgruppen und anderen EU-Organen.

[3] Bei militärischen Operationen sollte das derzeitige EU-Konzept für die Cyberabwehr bei EU-geführten militärischen Operationen unter Berücksichtigung dieses Politikrahmens aktualisiert werden.

3. Förderung der zivil-militärischen Zusammenarbeit und der Synergien mit der übergreifenden Cyberpolitik der EU und den einschlägigen Organen und Agenturen der EU sowie mit dem Privatsektor

Der Cyberraum ist ein sich rasch weiterentwickelnder Bereich, in dem Fähigkeiten mit doppeltem Verwendungszweck eine wichtige Rolle spielen und in dem der vorliegende Rahmen die Synergien zwischen der GSVP und anderen horizontalen Politikbereichen (wie die Raumfahrtpolitik und die Politik im Bereich der maritimen Sicherheit) und Strategien der EU (wie die Strategie für maritime Sicherheit und der zugehörige Aktionsplan) verbessern wird. Unbeschadet der internen Organisation und der Rechtsvorschriften der Mitgliedstaaten werden die Weiterentwicklung der Fähigkeiten mit doppeltem Verwendungszweck, Forschung und Technologie (FuT), der Austausch bewährter Verfahren, der Informationsaustausch und Frühwarnmechanismen sowie Risikobewertungen in Bezug auf die Reaktion auf Sicherheitsvorfälle und Sensibilisierungsmaßnahmen der zivil-militärischen Zusammenarbeit im Cyberbereich zugute kommen. Gemeinsame Aktivitäten in Bezug auf Schulungen und Übungen werden die Zusammenarbeit fördern und die Kosten über die verschiedenen Politikbereiche hinweg senken.

Die EDA, die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA)[4], das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3) zusammen mit den übrigen einschlägigen Agenturen der EU sind ebenso wie die Mitgliedstaaten aufgerufen, ihre Zusammenarbeit in den folgenden Bereichen zu verstärken:

- Entwicklung gemeinsamer Kompetenzprofile für Cybersicherheit und -abwehr auf der Grundlage internationaler bewährter Verfahren und der von den EU-Organen verwendeten Zertifizierung, wobei auch die Zertifizierungsstandards des Privatsektors zu berücksichtigen sind;
- Leistung eines Beitrag zur Weiterentwicklung und Anpassung der organisatorischen und technischen Standards der Cybersicherheit und -abwehr im öffentlichen Sektor, so dass diese für den Verteidigungs- und Sicherheitssektor tauglich sind; sofern erforderlich, ist auf die laufenden Arbeiten der ENISA und der EDA aufzubauen;
- Entwicklung eines Arbeitsmechanismus für den Austausch bewährter Verfahren im Bereich Schulung und Übungen sowie in anderen Bereichen möglicher zivil-militärischer Synergien;
- Ausbau der bestehenden Präventions-, Ermittlungs- und Forensikfähigkeiten der EU im Bereich der Cyberkriminalität und deren verstärkte Nutzung bei der Entwicklung von Cyberabwehrfähigkeiten;

[4] Im Rahmen des Mandats der ENISA und in Anlehnung an den mehrjährigen Arbeitsplan der ENISA, ohne dass Überlappungen mit den Kompetenzen der Mitgliedstaaten entstehen.

Die Verbesserung der zivilen Cybersicherheit ist ein wichtiger Faktor, der zur generellen Erhöhung der Netz- und Informationssicherheit beiträgt. Es wird erwartet, dass der Vorschlag für eine Richtlinie über Netz- und Informationssicherheit die Abwehrbereitschaft auf nationaler Ebene steigern und die Zusammenarbeit auf Unionsebene zwischen den Mitgliedstaaten sowohl in strategischer wie auch operationeller Hinsicht stärken wird. Diese Zusammenarbeit sollte sowohl die nationalen Behörden, die mit der Beaufsichtigung der Cybersicherheitsstrategien befasst sind, als auch die IT-Notfallteams (Computer Emergency Response Team – CERT) der Mitgliedstaaten und der EU (CERT-EU) einschließen. Die öffentlich-private Plattform für Netz- und Informationssicherheit zielt darauf ab, technologieneutrale bewährte Verfahren zur Förderung der Cybersicherheit zu ermitteln und Anreize für die Einführung sicherer IKT-Lösungen zu schaffen.

Forschung und Technologie in Zusammenarbeit mit Privatsektor und Wissenschaft

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 FuT-Dimension. Die EDA hat im Rahmen der Forschungsagenda im Bereich der Cyberabwehr eine solide Grundlage für die Festlegung von Prioritäten bei den künftigen FuT-Ausgaben und bei der Fähigkeitenentwicklung sowohl auf nationaler wie auch auf europäischer Ebene vorgegeben.

Die Entwicklung starker 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. Deshalb ist es von größter Wichtigkeit, die enge Zusammenarbeit mit dem Privatsektor beizubehalten und dabei soweit möglich Synergien mit Lösungen, Dienstleistungen und Fähigkeiten im zivilen Bereich (insbesondere in Bezug auf Kryptographie, eingebettete IKT-Systeme, Erkennung von Schadprogrammen, Simulations- und Visualisierungstechniken, Schutz für Netze und Kommunikationssysteme, Bereiche der Identifizierungs- und Authentifizierungstechnologien) anzustreben. Es ist ferner von Bedeutung, eine gesicherte und wettbewerbsfähige europäische industrielle Lieferkette im Bereich der Cybersicherheit zu fördern, indem die Entwicklung eines robusten europäischen Cybersicherheitssektors auch über die Einbindung von kleinen und mittleren Unternehmen (KMU) gefördert wird.

Um die zivil-militärische Zusammenarbeit bei der Entwicklung von Fähigkeiten im Bereich der Cyberabwehr zu erleichtern und die technologische und industrielle Basis der europäischen Verteidigung[5] im Einklang mit dem EU-Konzept für die Cyberindustrie zu stärken, wird die EDA zusammen mit den Kommissionsdienststellen und den Mitgliedstaaten

- Synergien zwischen den FuT-Bemühungen im militärischen Bereich und den zivilen FuE-Programmen (z.B. Horizont 2020) anstreben und dem Aspekt der Cybersicherheit und -abwehr Rechnung tragen, wenn sie die vorbereitende Maßnahme für GSVP-relevante Forschung festlegt;
- Forschungsagenden im Bereich der Cybersicherheit zwischen den Organen und Agenturen der EU austauschen (z.B. die Forschungsagenda im Bereich der Cyberabwehr), insbesondere über die Europäische Rahmenvereinbarung über Zusammenarbeit in der Sicherheits- und Verteidigungsforschung, und die daraus resultierenden Fahrpläne und Maßnahmen weitergeben;
- die Entwicklung industrieller Ökosysteme und Innovationscluster fördern, die die gesamte Wertschöpfungskette im Sicherheitsbereich betreffen, und sich dabei auf wissenschaftliche Erkenntnisse sowie Innovationen und die industrielle Produktion der KMU stützen;
- 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.);
- einen Beitrag zur besseren Einbeziehung des Aspekts der Cybersicherheit und der Cyberabwehr in Programme, die einen mit der Doppelverwendungsfähigkeit zusammenhängenden Sicherheits- und Abwehraspekt aufweisen, so etwa SESAR, leisten;
- aktiv Synergien mit der Entwicklung der Industriepolitik für die Cybersicherheit im zivilen Bereich fördern, die auf nationaler Ebene von den Mitgliedstaaten und auf europäischer Ebene von der Kommission verfolgt wird.

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

4. Verbesserung der Schulungs-, Ausbildungs- und Übungsmöglichkeiten

Schulung und Ausbildung

Um auf allen Ebenen der Befehlskette der GSVP, einschließlich Missionen und Operationen, eine gemeinsame Kultur der Cyberabwehr zu entwickeln, ist es notwendig, die Schulungsmöglichkeiten im Bereich der Cyberabwehr zu verbessern. In einer Zeit sinkender Verteidigungsausgaben ist es ferner entscheidend, dass die Mittel für Schulungen und Ausbildung 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.

Der EAD wird zusammen mit der EDA, dem Europäischen Sicherheits- und Verteidigungskolleg (ESVK) und den Mitgliedstaaten Schulungsprioritäten festlegen und

- 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;
- 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;
- anhand einer von der EDA vorgenommenen Bewertung der Durchführbarkeit die Möglichkeit und die Argumente für die Schaffung einer Schulungseinrichtung für die GSVP auf dem Gebiet der Cyberabwehr sondieren;
- weitere EDA-Kurse ausarbeiten, um die Schulungserfordernisse im Bereich der Cyberabwehr für die GSVP zu erfüllen;
- in enger Zusammenarbeit mit den einschlägigen Dienststellen der EU-Organe die etablierten Zertifizierungsmechanismen des ESVK für Schulungsprogramme auf der Grundlage der vorhandenen Standards und des vorhandenen Wissens verfolgen; die Möglichkeit prüfen, im Rahmen der militärischen Erasmus-Initiative cyberspezifische Module vorzusehen;
- Synergien mit den Schulungsprogrammen anderer Akteure, wie ENISA, Europol, Europäische Gruppe für Schulung und Ausbildung in Bezug auf Cyberkriminalität (ECTEG) und Europäische Polizeiakademie (CEPOL), herstellen;
- die Möglichkeit gemeinsamer Schulungsprogramme des ESVK und des Verteidigungskollegs der NATO im Bereich der Cyberabwehr sondieren, die allen EU-Mitgliedstaaten offenstehen, um so eine gemeinsame Kultur der Cyberabwehr zu fördern;
- 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.

Übungen

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. Nationale Streitkräfte werden so in die Lage versetzt, ihre Bereitschaft für Einsätze in einem multinationalen Umfeld zu steigern. Die Durchführung gemeinsamer Übungen zur Cyberabwehr wird auch Interoperabilität und Vertrauen fördern.

Der EAD und die Mitgliedstaaten werden sich verstärkt um die Förderung von Aspekten der Cyberabwehr im Rahmen von GSVP- und anderen Übungen bemühen; insbesondere werden sie

- den Aspekt der Cyberabwehr in die bestehenden Übungsszenarien für MILEX und MULTILAYER einbeziehen;
- sofern zweckmäßig eine spezielle EU-Cyberabwehrübung im Rahmen der GSVP entwickeln und eine eventuelle Abstimmung mit von der ENISA organisierten gesamteuropäischen Übungen zu Cybervorfällen, wie *CyberEurope*, sondieren;
- die Möglichkeit der Teilnahme an anderen multinationalen Übungen zur Cyberabwehr prüfen;
- – sobald die EU eine Cyberabwehrübung im Rahmen der GSVP entwickelt hat – im Einklang mit der Übungspolitik der EU die einschlägigen internationalen Partner wie die OSZE und die NATO einbinden.

5. 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.

In der EU besteht der politische Wille, im Bereich der Cyberabwehr stärker mit der NATO bei der Entwicklung der im vorliegenden Politikrahmen geforderten robusten und widerstandsfähigen Fähigkeiten zur Cyberabwehr zusammenzuarbeiten. Regelmäßige Arbeitsberatungen, wechselseitige Briefings sowie etwaige Sitzungen zwischen der Gruppe "Politisch-militärische Angelegenheiten" und den einschlägigen Ausschüssen der NATO werden dazu beitragen, unnötige Doppelarbeit zu vermeiden, und dafür sorgen, dass die Bemühungen kohärent sind und sich ergänzen, im Einklang mit dem bestehenden Rahmen für die Zusammenarbeit mit der NATO.

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

- bewährte Verfahren in Bezug auf Krisenbewältigung sowie in Bezug auf militärische Operationen und zivile Missionen austauschen;
- – sofern Überschneidungen vorliegen – auf Kohärenz bei der Entwicklung der Fähigkeitsanforderungen im Bereich der Cyberabwehr hinarbeiten, insbesondere bei der Entwicklung langfristiger Cyberabwehrfähigkeiten;
- bei Konzepten für Schulungen und Ausbildung im Bereich der Cyberabwehr sowie bei entsprechenden Übungen die Zusammenarbeit ausbauen;
- auf der Grundlage angemessener Bewertungen das Verbindungsabkommen der EDA mit dem NATO-Kompetenzzentrum für kooperativen Schutz vor Computerangriffen als eine erste Plattform für die verstärkte Zusammenarbeit bei multinationalen Cyberabwehrprojekten umfassender nutzen;
- die Zusammenarbeit des CERT-EU und der einschlägigen Stellen der EU für Cyberabwehr mit dem NCIRC (NATO Computer Incident Response Capability) intensivieren, 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 EDA zusammen mit den Mitgliedstaaten gegebenenfalls

- die strategischen Entwicklungen verfolgen und Konsultationen zu Fragen der Cyberabwehr mit internationalen Partnern (internationale Organisationen und Drittländer) führen;
- Möglichkeiten für die Zusammenarbeit in Fragen der Cyberabwehr sondieren, auch mit Drittländern, die sich an GSVP-Missionen und -Operationen beteiligen;
- die Entwicklung von vertrauensbildenden Maßnahmen im Bereich der Cybersicherheit weiter unterstützen, um die Transparenz zu erhöhen und das Risiko einer falschen Einschätzung staatlichen Handelns durch die Förderung der derzeit laufenden Ausarbeitung internationaler Normen in diesem Bereich zu verringern.

Folgemaßnahmen

Der Gruppe "Politisch-militärische Angelegenheiten", dem Politischen und Sicherheitspolitischen Komitee und anderen einschlägigen Ratsarbeitsgruppen sollte halbjährlich ein Sachstandsbericht, der sich unter anderem auf die fünf vorstehend umrissenen Bereiche erstreckt, vorgelegt werden, damit die Umsetzung des Politikrahmens bewertet werden kann. 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.