Rat der
Europäischen Union

Brüssel, den 18. Juni 2018
(OR. en)

10135/18

HYBRID 9	**ENER 238**
COPS 212	**EUMC 104**
PROCIV 39	**CIVCOM 111**
CSDP/PSDC 334	**TRANS 267**
CYBER 140	**COEST 121**
CFSP/PESC 568	**ESPACE 30**
JAI 646	**COTER 77**
ECOFIN 625	**CSC 194**
POLMIL 83	**IPCR 14**

ÜBERMITTLUNGSVERMERK

Absender:	Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag des Generalsekretärs der Europäischen Kommission
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	JOIN(2018) 14 final
Betr.:	Gemeinsamer Bericht an das Europäische Parlament, den Europäischen Rat und den Rat zur Umsetzung des Gemeinsamen Rahmens für die Abwehr hybrider Bedrohungen von Juli 2017 bis Juni 2018

Die Delegationen erhalten in der Anlage das Dokument JOIN(2018) 14 final.

Anl.: JOIN(2018) 14 final

EUROPÄISCHE
KOMMISSION

HOHE VERTRETERIN
DER UNION FÜR
AUSSEN- UND
SICHERHEITSPOLITIK

Brüssel, den 13.6.2018
JOIN(2018) 14 final

Gemeinsamer Bericht an das Europäische Parlament, den Europäischen Rat und den Rat

zur Umsetzung des Gemeinsamen Rahmens für die Abwehr hybrider Bedrohungen von Juli 2017 bis Juni 2018

EINFÜHRUNG

Der Gemeinsame Rahmen für die Abwehr hybrider Bedrohungen – eine Antwort der Europäischen Union[1] stellt Lagebewusstsein, Resilienz und Reaktion in das Zentrum der EU-Maßnahmen gegen hybride Bedrohungen. Der Ausbau unserer Kapazität, böswillige hybride Aktivitäten frühzeitig zu erkennen und zu verstehen, sowie die Stärkung der Resilienz kritischer Infrastrukturen (z. B. Verkehr, Kommunikation, Energie, Weltraum und Finanzen) unserer Gesellschaften und Einrichtungen sind für die Verbesserung unseres Vermögens, Angriffen standzuhalten und uns davon zu erholen, von grundlegender Bedeutung. Die Abwehr hybrider Bedrohungen erfordert Maßnahmen sowohl aufseiten der Mitgliedstaaten als auch der Organe der Union. Der erste Bericht über die Umsetzung der 22 im Gemeinsamen Rahmen genannten Maßnahmen wurde dem Rat am 19. Juli 2017 vorgelegt.[2] Dieser aktualisierte Bericht für 2018 bietet einen Überblick über die seit Sommer vergangenen Jahres erzielten Fortschritte.

In allen vier prioritären Maßnahmenbereichen wurden erhebliche Fortschritte erzielt:

- Verbesserung des Lagebewusstseins
- Stärkung der Resilienz
- Stärkung der Fähigkeit der Mitgliedstaaten und der Union auf den Gebieten Krisenverhütung und -bewältigung und Sicherstellung einer schnellen und koordinierte Erholung von Krisen
- Intensivierung der Zusammenarbeit mit der NATO zur Gewährleistung der Komplementarität von Maßnahmen

ERKENNUNG DER HYBRIDEN NATUR VON BEDROHUNGEN

<u>Maßnahme 1</u>: Einleitung einer Untersuchung über hybride Risiken durch die Mitgliedstaaten

Der Rat hat eine Gruppe der Freunde des Vorsitzes eingesetzt, der jeweils der turnusmäßig wechselnde Vorsitz vorsteht und die die Arbeit voranbringen soll. Im Dezember 2017 leiteten die Mitgliedstaaten eine Untersuchung ein, um zu ermitteln, wo sie am stärksten verwundbar für hybride Bedrohungen sind. Auf der Grundlage der Antworten der Mitgliedstaaten wird der Vorsitz – wahrscheinlich noch vor Ende Juni 2018 – dem Ausschuss der Ständigen Vertreter der Regierungen der Mitgliedstaaten (AStV) einen Bericht vorlegen.

Angesichts des Auslaufens des Mandats der Gruppe Ende Juni 2018 begann die Gruppe der Freunde des Vorsitzes bei ihrem Treffen im April, auf der Grundlage des Vorschlags des Vorsitzes ihr zukünftiges Mandat zu erörtern. Das laufende Mandat würde dadurch bis 2020 verlängert und sein Umfang ausgeweitet; nach dem gegenwärtigen Entwurf könnte das Mandat Aufgaben im Zusammenhang mit der Analyse von Optionen zur Stärkung der Vorsorge und der Resilienz der Mitgliedstaaten, der Beobachtung nationaler Entwicklungen und der Hilfe bei der Koordinierung politischer Ansätze im Bereich hybrider Bedrohungen, der Unterstützung bei der Arbeit des Rates hinsichtlich der Zusammenarbeit zwischen EU und NATO im Bereich Abwehr hybrider Bedrohungen sowie dem Austausch von Informationen und der Entwicklung eines gemeinsamen Verständnisses zu hybriden Bedrohungen umfassen.

---

1 JOIN(2016) 18 final.

2 Gemeinsamer Bericht an das Europäische Parlament und den Rat zur Umsetzung des Gemeinsamen Rahmens für die Abwehr hybrider Bedrohungen – eine Antwort der Europäischen Union, JOIN(2017) 30 final.

GESTALTUNG DER ANTWORT DER EU: STÄRKERE SENSIBILISIERUNG

Maßnahme 2: Schaffung einer EU-Analyseeinheit für hybride Bedrohungen

Die EU-Analyseeinheit für hybride Bedrohungen, die als Teil des zivilen/militärischen Einheitlichen Analyseverfahrens im EU-Zentrum für Informationsgewinnung und -analyse angesiedelt ist, stützt sich sowohl auf zivile und militärische Analytiker als auch auf Beiträge der Nachrichten- und Sicherheitsdienste der Mitgliedstaaten. Sie erreichte im Juli 2017 volle Einsatzfähigkeit, was sie während der parallelen und koordinierten Übung mit der NATO 2017 (PACE17) unter Beweis stellte. Die EU-Analyseeinheit für hybride Bedrohungen nimmt geheime und offen zugängliche Informationen über hybride Bedrohungen von verschiedenen Interessenträgern entgegen und analysiert sie. Die Berichte und Analysen werden anschließend mit den EU-Organen und den Mitgliedstaaten geteilt, um eine fundierte Entscheidungsfindung zu ermöglichen. Die EU-Analyseeinheit für hybride Bedrohungen hat bisher bereits über 100 Unterlagen im Zusammenhang mit hybriden Bedrohungen erstellt. Das IT-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der EU (CERT-EU) leistet einen Beitrag zur Arbeit der EU-Analyseeinheit für hybride Bedrohungen, indem es Informationen über bevorstehende oder bestehende hybride Cyberbedrohungen übermittelt. Die Kenntnisse in den Bereichen chemische, biologische, radiologische und nukleare Bedrohungen sowie Cyberaufklärung und Spionageabwehr sind jedoch gegenwärtig begrenzt.

Die EU-Analyseeinheit für hybride Bedrohungen hat ein Netz nationaler Kontaktstellen eingerichtet, um diesbezügliche Arbeiten auszuweiten. Bisher haben 26 von 28 Mitgliedstaaten Kontaktstellen benannt, mit denen regelmäßige Treffen stattfinden, um ihr Fachwissen mit der Analyseeinheit zu teilen.

Ferner gibt es in Form des gemeinsamen Netzes des EAD und der Kommission, das sich auf Ergebnisse bei verschiedenen Resilienzmaßnahmen konzentriert, ein gleichwertiges Pendant. Diese Treffen finden monatlich statt und dort werden vorrangig thematische Fragen unter anderem zu Verkehr, Infrastruktur, Energie sowie Cybersicherheit und Tätigkeiten feindlicher Nachrichtendienste behandelt.

Auf strategischer Ebene baut die EU-Analyseeinheit für hybride Bedrohungen ihre Beziehungen zum Europäischen Kompetenzzentrum für die Abwehr hybrider Bedrohungen in Helsinki aus, indem sie an Workshops und Übungen teilnimmt und regelmäßige Besprechungen zu einschlägigen Themen abhält, um Kompetenzen im Bereich Abwehr hybrider Bedrohungen aufzubauen.

Im Rahmen der gemeinsamen Erklärung wird außerdem der tägliche Kontakt der Mitarbeiter zu denen der NATO-Analyseeinheit für hybride Bedrohungen fortwährend gepflegt. Im September 2017 wurde eine bahnbrechende parallele und koordinierte Bewertung zu einem hybridbezogenen Thema veröffentlicht und für 2018 werden Dokumente zu hybriden Herausforderungen mit Ursprung in der südlichen und östlichen Nachbarschaft erwartet.

Maßnahme 3: strategische Kommunikation

Die strategische Kommunikation hat in der EU dadurch zusätzliche Impulse erhalten, dass viele verschiedene Akteure Fähigkeiten aufbauen. In der Mitteilung „Bekämpfung von Desinformation im Internet: ein europäisches Konzept“[3] vom 26. April 2018 wird Desinformation als hybride Bedrohung erkannt und eine Reihe von Maßnahmen, unter anderem eine stärkere Vernetzung zwischen der Kommission, dem Europäischen Auswärtigen Dienst und den Mitgliedstaaten, festgelegt. Die positiven Erfahrungen der East StratCom Task Force, die im März 2015 aufgrund eines Mandats des Europäischen Rates eingesetzt wurde, müssen unterstützt und verstärkt werden, wie es in der gemeinsamen

[3] COM(2018) 236 final.

Mitteilung Reaktion auf hybride Bedrohungen: Schutz der europäischen Bürgerinnen und Bürger[4] vorgeschlagen wurde.

Der Schwerpunkt der Arbeit der East StratCom liegt auf der Unterstützung von EU-Delegationen in der Region der östlichen Partnerschaft und in Russland sowie in gewissem Umfang in Zentralasien; damit sollen positive Botschaften besser übermittelt und die Reichweite bei inländischem und regionalem Publikum verbessert werden. Die Kommission unterstützt diese Tätigkeiten über ein mehrjähriges regionales Informations- und Kommunikationsprogramm. Die East StratCom Task Force koordiniert ihre Tätigkeiten regelmäßig mit den Mitgliedstaaten und der NATO. Zusätzlich zur Überwachung von Desinformation führt die East StratCom Task Force Sensibilisierungsaktivitäten für die Auswirkungen russischer Desinformation in Ländern der östlichen Partnerschaft und Mitgliedstaaten durch. Des Weiteren hat sie Schulungen für Beschäftigte in Ländern der östlichen Partnerschaft aufgestockt, mit denen ihre StratCom-Fähigkeiten und ihre Resilienz gegenüber Desinformation gestärkt werden sollen. Für die Zukunft ist eine stärkere Zusammenarbeit mit den NATO-Hauptquartieren und den Kompetenzzentren in Riga und Helsinki geplant, in deren Rahmen beispielsweise Analysen geteilt und Schulungsseminare für Journalisten aus der Region der östlichen Partnerschaft oder Russland veranstaltet werden.

Gemäß der neuen EU-Strategie für den westlichen Balkan wurde eine Taskforce mit dem Schwerpunkt westlicher Balkan eingesetzt, die für eine wirksamere Kommunikation von EU-Maßnahmen an ein breiteres Publikum in der Region zuständig ist und gleichzeitig für auf den westlichen Balkan ausgerichtete Desinformationen sensibilisiert und gegen diese vorgeht. Die Taskforce und die Kommission arbeiten eng zusammen, um eine strategischere und gezieltere Kommunikation und Nachrichtenübermittlung in die Region zu erreichen, wofür sie auf bewährten Verfahren aufbauen und den Schwerpunkt auf thematische Kampagnen legen. Trotzdem mangelt es an Bewusstsein für zunehmende Bedrohungen, die sich speziell gegen die Organe richten. Es muss eine Kultur des Sicherheitsbewusstseins aufgebaut werden und die Fähigkeiten der Organe zur Bewältigung der hybriden Bedrohungen müssen verstärkt werden.

Die 2017 eingerichtete Task Force South passte ihr Mandat an, um einer Verlagerung vom Fokus auf Terrorismusbekämpfung hin zu einem nuancierteren Ansatz zur Verbesserung der Kommunikation und der Reichweite in der arabischen Welt, auch in arabischer Sprache, Rechnung zu tragen. Da Da'esh – oder ISIS – nicht die einzige Bedrohung in Bezug auf Radikalisierung darstellt, arbeitet die Taskforce daran, gegen die verbreiteten Fehlinformationen und die falsche Wahrnehmung der EU vorzugehen. Das geschieht – in enger Zusammenarbeit mit der Kommission – über die Entwicklung positiver Botschaften über die Europäische Union und ihre politischen Maßnahmen, um ein besseres Verständnis von der Union zu erreichen, strategischer über die Aktivitäten der Union in der arabischen Welt zu kommunizieren und gemeinsame Werte und Interessen zu fördern. Die Kommission unterstützt diese Tätigkeiten über ein mehrjähriges regionales Informations- und Kommunikationsprogramm.

<u>Maßnahme 4:</u> Kompetenzzentrum für die „Abwehr hybrider Bedrohungen"

Das 2017 eingerichtete Europäische Kompetenzzentrum für die Abwehr hybrider Bedrohungen dient als Drehscheibe für Fachwissen zur Unterstützung der individuellen und kollektiven Bemühungen der teilnehmenden Länder bei der Abwehr hybrider Bedrohungen mithilfe von Forschung, Schulungen, Bildung und Übungen. An dem Zentrum können sich sowohl EU-Mitgliedstaaten als auch NATO-Verbündete beteiligen. Vor Kurzem wurden Italien, die Niederlande, Dänemark und die Tschechische Republik Mitglieder, womit

[4] Referenz einfügen sobald bekannt.

nunmehr 16 Länder beteiligt sind. Sowohl die EU als auch die NATO nehmen als Beobachter am Lenkungsausschuss teil.

2018 einigte sich das Zentrum auf einen Haushalt und ein Arbeitsprogramm; außerdem hat es seinen konzeptionellen Rahmen erarbeitet und drei Interessengemeinschaften gegründet: zu hybrider Beeinflussung, zu Verwundbarkeiten und Resilienz sowie zu Strategie und Verteidigung. Es wurde eine Untergruppe für nichtstaatliche Akteure eingesetzt, die sich damit beschäftigt, wie verschiedene terroristische Vereinigungen und deren staatliche Förderer vorgehen. Das Zentrum hat eine Reihe von Analysen hybrider Bedrohungen veröffentlicht und mehrere hochrangige Treffen veranstaltet, um ein gemeinsames Verständnis hybrider Bedrohungen zu erreichen, bewährte Verfahren zu teilen und gemeinsame Reaktionen in der gesamten EU und der NATO-Gemeinschaft anzustreben.

GESTALTUNG DER ANTWORT DER EU: STÄRKUNG DER RESILIENZ

Zur Stärkung der Resilienz sind Maßnahmen in zahlreichen Politikbereichen erforderlich. Diese Maßnahmen müssen sich nicht unbedingt speziell auf die hybride Natur der Bedrohungen beziehen, können jedoch in der Summe sicherstellen, dass eine resilientere EU besser für hybride Bedrohungen gewappnet ist. Daher wird, sofern es für die Beschreibung der Fortschritte der nachfolgend beschriebenen Maßnahmen relevant ist, auf den spezifischen politischen Rahmen und die von der Union ergriffenen Maßnahmen verwiesen, insbesondere auf diejenigen Maßnahmen, die im Rahmen der Arbeiten hin zu einer Sicherheitsunion ergriffen wurden. Daher sollte dieser Bericht in Verbindung mit den monatlichen Fortschrittsberichten mit dem Titel „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion“[5], die am selben Tag angenommen wurden, gelesen werden.

Maßnahme 5: Schutz und Resilienz kritischer Infrastrukturen

Die Kommission hat einen Entwurf für ein Handbuch zu Verwundbarkeitsindikatoren und Resilienz bei hybriden Bedrohungen für kritische Infrastrukturen in der EU ausgearbeitet. Dieser Entwurf eines Handbuchs wird derzeit in Konsultationen mit den Mitgliedstaaten validiert. Die endgültige Fassung des Handbuchs soll voraussichtlich im November 2018 angenommen werden. Ferner werden die Verwundbarkeitsindikatoren im Laufe der parallelen und koordinierten Übung mit der NATO 2018 (PACE18) sowie von einzelnen Mitgliedsstaaten, die Interesse angemeldet haben, getestet. Besondere Aufmerksamkeit sollte der weiteren Entwicklung von Erkennungsindikatoren gelten, mit denen die Frühwarnung in der Anfangsphase hybrider Angriffe auf kritische Infrastrukturen erleichtert wird. Bei der anstehenden Bewertung der EU-Richtlinie über den Schutz kritischer Infrastrukturen werden hybride Bedrohungen ebenfalls berücksichtigt. Außerdem verstärkt die Kommission die wissenschaftliche Unterstützung, um die zahlreichen und transversalen Merkmale hybrider Bedrohungen zu bekämpfen; der Schwerpunkt liegt dabei auf der Ermittlung von Verwundbarkeiten, Früherkennung und Indikatoren, Resilienz, Sensibilisierung und Übungen.

Mit dem Ziel des Schutzes zentraler Vermögenswerte der Union hat die Kommission ferner einen Vorschlag für eine Verordnung zur Schaffung eines Rahmens für die Überprüfung von ausländischen Direktinvestitionen in der Europäischen Union[6] vorgelegt, sofern sich diese Investitionen auf die Sicherheit oder die öffentliche Ordnung auswirken dürften. Der Vorschlag der Kommission bezieht sich auf Direktinvestitionen durch Personen oder Unternehmen aus Drittländern mit möglichen Auswirkungen unter anderem auf kritische Infrastrukturen (einschließlich Energie, Verkehr, Kommunikation, Datenspeicherung, Weltraum und sonstige sensible Einrichtungen), kritische Technologien (einschließlich

5 COM(2018) 470 final.
6 COM(2017) 487 final.

künstlicher Intelligenz, Cybersicherheit, Technologien mit potenziellen Anwendungen mit doppeltem Verwendungszweck) oder die Versorgungssicherheit für kritische Ressourcen oder auf Investitionen, die Zugang zu vertraulichen Informationen oder die Möglichkeit zur Kontrolle darüber bringen.

Das Konsultationsforum für nachhaltige Energie im Verteidigungs- und Sicherheitssektor (CF SEDSS II) wird als Teil der zweiten Phase der Europäischen Verteidigungsagentur die Weiterentwicklung des Konzeptpapiers, das von der Expertengruppe für den Schutz kritischer Infrastrukturen (PCEI) vorbereitet wurde, fördern und es in ein Strategiedokument auf EU-Ebene überführen. Damit wird ein Rahmen für die Erkennung der besten Verwaltungspraktiken für Verteidigungsministerien bei der Stärkung des Schutzes und der Resilienz aller verteidigungsrelevanten kritischen Energieinfrastrukturen bereitgestellt.

Maßnahme 6: ***Verbesserung der Energieversorgungssicherheit in der EU und Erhöhung der Resilienz der nuklearen Infrastrukturen***

Im Einklang mit ihrem Versprechen von September 2017 (Gemeinsame Mitteilung „Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen“[7]) wird die Kommission auch weiterhin die Europäischen Zentren für den Informationsaustausch und Analysen im Energiesektor im Bereich Cybersicherheit unterstützen.

Zur Vorbeugung einer Krise bei der Gasversorgung setzen die Mitgliedstaaten die im vergangenen Jahr angenommene Verordnung über sichere Erdgasversorgung um, während die Kommission ihre Umsetzung und die Zusammenarbeit zwischen den Mitgliedstaaten innerhalb der Risikogruppen erleichtert. Die gemeinsamen Risikobewertungen müssen der Kommission bis zum 1. Oktober 2018 übermittelt werden. Die Kommission wird die Präventions- und Notfallpläne bis zum 1. März 2019 erhalten. Die Mitgliedstaaten sollten die bilateralen Solidaritätsvereinbarungen bis zum 1. Dezember 2018 abschließen.

Um die bestehende Regelungslücke bei der Risikovorsorge im Elektrizitätsbereich zu beheben, würde die Verordnung über Risikovorsorge, über die gegenwärtig verhandelt wird, Regeln für die Bewertung von Risiken sowie eine Verpflichtung der Mitgliedstaaten zur Ausarbeitung eines Risikovorsorgeplans mit einigen verpflichtenden Elementen darüber einführen, wie mit Krisensituationen umzugehen und wie die Versorgungssicherheit zu überwachen ist. Die Risikovorsorgepläne sollten zudem Vereinbarungen zur regionalen Zusammenarbeit und insbesondere Vereinbarungen über den Umgang mit zeitgleichen Stromversorgungskrisen treffen. Im Rahmen der Durchführung der Verordnung über Risikovorsorge hätten die Mitgliedstaaten die ersten nationalen Risikovorsorgepläne zwei Jahre nach dem Inkrafttreten der Verordnung auszuarbeiten. Anschließend sollten die Pläne alle drei Jahre aktualisiert werden. Die zukünftige Verordnung über Risikovorsorge wird auch die Durchführung regelmäßiger und gemeinsamer Übungen der Mitgliedstaaten erfordern, bei denen Stromversorgungskrisen simuliert werden. Die Kommission hat gemeinsam mit interessierten Mitgliedstaaten, der Gemeinsamen Forschungsstelle und der Koordinierungsgruppe „Strom“ bereits mit der Vorbereitung solcher gemeinsamen Übungen begonnen.

In Bezug auf die Resilienz nuklearer Infrastrukturen wird der Informationsaustausch zwischen den Mitgliedstaaten und der Kommission zu Themen der nuklearen Sicherheit kurzfristig verbessert und es ist eine Analyse im Hinblick auf zusätzliche Initiativen geplant. Es wird eine Analyse der Verordnung für Kernmaterialüberwachung und einer möglichen Anleitung zur Unterstützung der Mitgliedstaaten beim besseren Umgang mit hoch radioaktiven umschlossenen Strahlenquellen durchgeführt werden. Auf lange Sicht plant die Kommission, die Tätigkeiten im Nuklearbereich dort zu stärken, wo ein gemeinsames Interesse der

[7] JOIN(2017) 450 final.

Mitgliedstaaten und anerkannte Vorteile des Informationsaustauschs und der Zusammenarbeit bestehen. Außerdem wird sie angemessene Maßnahmen für die wirksame Umsetzung des internationalen Übereinkommens über den physischen Schutz von Kernmaterial und Kernanlagen in der EU prüfen.

Für den Verteidigungssektor hat das Konsultationsforum für nachhaltige Energie im Verteidigungs- und Sicherheitssektor mit der „Roadmap for Sustainable Energy Management in the Defence and Security" einen Fahrplan für nachhaltiges Energiemanagement in den Bereichen Verteidigung und Sicherheit aufgestellt, mit dem der Verteidigungssektor bei der Verbesserung des Infrastrukturenergiemanagements unterstützt werden soll. Das Konsultationsforum wird weiterhin daran arbeiten, wie der Verteidigungssektor effizienter mit Energieressourcen umgehen kann und eine Reihe von Technologien zur Generierung von Projekten im Hinblick auf eine potenzielle Nutzung im Verteidigungssektor überprüfen (z. B. Windenergie, Solaranlagen, intelligente Stromnetze, Energiespeicherung, Biobrennstoffe, Biomasse und Umwandlung von Abfall in Energie).

In diesem Zusammenhang wurde die Arbeit des Programms für Energie und Umwelt der Europäischen Verteidigungsagentur fortgesetzt; dabei wird im Rahmen des Forschungsprojekts „Smart Blue Water Camps" der Umfang technologischer Interventionen für nachhaltige Wasserbewirtschaftung in „heimischen" Militärlagern getestet und im Rahmen des Forschungsvertrags „Smart Camps Technical Demonstrator" die Machbarkeit der Integration einer breiteren Palette von Energie- und Umwelttechnologien in größerem Maßstab in eine militärische Umgebung im Hinblick auf Energie-, Wasser- und Abfallbelange untersucht, um gleichzeitig die Kosten- und militärische Wirksamkeit von GSVP-Missionen zu verbessern.

Maßnahme 7: Verkehr und Lieferketten

In allen Verkehrsbereichen – zivile Luftfahrt, See- und Landverkehr – hat die Kommission mit den Mitgliedstaaten, der Wirtschaft und anderen Interessenträgern die Gespräche über aufkommende Sicherheitsbedrohungen hybrider Natur intensiviert, um Kenntnisse zu sammeln und aus Erfahrungen zu lernen.

Im Kontext der Umsetzungstätigkeiten und der Überarbeitung des Aktionsplans für die Strategie der Europäischen Union für maritime Sicherheit analysiert die Kommission Trends in der maritimen Sicherheit (unter anderem Piraterie und Seestreitigkeiten), die Schifffahrts- und Handelswege stören und die Interessen der EU beeinträchtigen könnten. Angesichts der Tatsache, dass die EU-Mitgliedstaaten und die Mitglieder des EWR über 40 % der weltweiten Handelsflotte kontrollieren und dass die EU ein wichtiger Handelsblock ist, hätten hybride Angriffe auf die Seehandelswege erhebliche störende Auswirkungen auf die Wertschöpfungs- und Lieferketten in Europa. Risikoanalysen und die Überwachung aufkommender Bedrohungen im maritimen Bereich könnten gegebenenfalls in Vorschläge zur Aktualisierung der spezifischen Verkehrsrechtsakte münden. Außerdem bilden sie die Grundlage für die fortlaufenden Arbeiten zur Verbesserung des maritimen Lagebewusstseins, unter anderem im Kontext der Entwicklung des Fahrplans für die Schaffung des gemeinsamen Informationsraums, in dessen Rahmen bei einer neuen Aufforderung zur Einreichung von Vorschlägen zur Unterstützung der Mitgliedstaaten bei der Verbesserung der Interoperabilität der IT-Systeme zwischen nationalen Seebehörden kürzlich drei neue Projekte vergeben wurden (Anfang 2018).

Mit der Annahme des Maßnahmenpakets für eine Grenz- und Küstenwache[8] im September 2016 fügten das Europäische Parlament und der Rat in die Gründungsverordnungen der Europäischen Agentur für die Grenz- und Küstenwache, die

[8] Verordnung (EU) 2016/1624 über die Europäische Grenz- und Küstenwache.

Europäische Fischereiaufsichtsagentur (EFCA) und die Europäische Agentur für die Sicherheit des Seeverkehrs (EMSA) einen gemeinsamen Artikel ein, der sie jeweils im Rahmen ihres Mandats zur Verstärkung der Zusammenarbeit sowohl untereinander als auch mit den nationalen Behörden, die Aufgaben der Küstenwache übernehmen[9], verpflichtet, um das maritime Lagebewusstsein zu stärken und kohärentes und kosteneffizientes Handeln zu unterstützen. Zu diesem Thema wurde 2017 eine Studie über Gemeinsamkeiten und Möglichkeiten zur Verbesserung der Interoperabilität und der Zusammenarbeit im Bereich Risikobewertung unter Behörden, die Aufgaben der Küstenwache ausführen, veröffentlicht.10

Zu den Themen im Zusammenhang mit Verkehr und aufkommenden Bedrohungen – unter anderem für Häfen – gehören Cyberbedrohungen für die Flugsicherheit, gezielte Störung (Jamming) und Fälschung von GPS-Signalen (Spoofing), Bedrohungen für Satelliten oder Probleme im hohen Norden und der Arktis. Das Kompetenzzentrum für die Abwehr hybrider Bedrohungen in Helsinki leistet ebenfalls einen Beitrag zur Analyse dieser verkehrsbezogenen hybriden Bedrohungen und hat vor Kurzem eine Analyse zum Hafenschutz begonnen.

Der Zoll der EU spielt eine Schlüsselrolle bei der Gewährleistung der Sicherheit der Außengrenzen und der Lieferkette und trägt damit zur Sicherheit der Europäischen Union bei. Die Kommission modernisiert das System für Vorabinforationen über Frachtgut und für das Zollrisikomanagement erheblich, um sicherzustellen, dass die Zollbehörden in der EU alle erforderlichen Informationen erhalten, diese wirksamer zwischen Mitgliedstaaten teilen, gemeinsame und spezifische Vorschriften der Mitgliedstaaten anwenden und Risikosendungen wirksamer ermitteln. Eine zentrale Priorität des EU-Aktionsplans zur Abwehr chemischer, biologischer, radiologischer und nuklearer Bedrohungen (CBRN)[11] betrifft die Gewährleistung der Grenzsicherheit und der Aufdeckungskapazität gegen den vorschriftswidrigen Eintritt von CBRN-Materialien. Die Anpassung von Frachtinformationssystemen ist für die Stärkung der Überwachung und von risikobasierten Kontrollen internationaler Lieferketten von grundlegender Bedeutung, damit keine CBRN-Materialien vorschriftswidrig in die EU gelangen. Der fünfzehnte Bericht über die Fortschritte auf dem Weg zu einer wirksamen und echten Sicherheitsunion enthält ausführlichere Informationen über die Maßnahmen der EU zur Steigerung der Abwehrbereitschaft gegen CBRN-Risiken, insbesondere über auf EU-Ebene ergriffene Maßnahmen im Rahmen des Aktionsplans der Kommission für eine gesteigerte Abwehrbereitschaft gegen chemische, biologische, radiologische und nukleare Sicherheitsrisiken.

Die Hohe Vertreterin und die Kommission haben am 28. März 2018 einen Aktionsplan vorgestellt, der auf die Beseitigung von Hindernissen für die militärische Mobilität in der EU ausgerichtet ist und mit dem die Möglichkeiten für eine zivile und militärische Verwendung des transeuropäischen Netzes geprüft und die Zollförmlichkeiten für militärische Transporte sowie die verfahrensrelevanten Fragen für die Beförderung gefährlicher Güter für militärische Zwecke vereinfacht werden. Im Cluster „Verteidigung“ des mehrjährigen Finanzrahmens schlug die Kommission eine Mittelausstattung von 6,5 Mrd. EUR vor, die über die Fazilität „Connecting Europe“ zur Unterstützung der Verkehrsinfrastrukturen im Hinblick auf die

---

9 Zu den Aufgaben der Küstenwache gehören: 1) maritime Sicherheit und Sicherheitsmanagement, 2) Schiffsunglücke und Seerettungsdienste, 3) Fischereiaufsicht und -kontrolle, 4) Überwachung der Seegrenzen, 5) Schutz der Meeresumwelt, 6) Vorbeugung und Verhinderung von Schlepperei, Schmuggel und diesbezügliche Durchsetzung von Vorschriften des Seerechts, 7) Such- und Rettungsdienst auf See, 8) Meeresüberwachung und -aufsicht, 9) maritime Zolltätigkeiten, 10) Unfall- und Katastrophenreaktion auf See und 11) maritime, Schifffahrts- und Hafensicherheit.

10 https://publications.europa.eu/en/publication-detail/-/publication/217db2fc-15d6-11e7-808e-01aa75ed71a1/language-en

11 COM(2017) 610 final vom 18.10.2017.

Anpassung an Anforderungen der militärischen Mobilität umgesetzt wird. Dies soll eine zivile und militärische Doppelnutzung der Verkehrsinfrastrukturen ermöglichen.

Maßnahme 8: Stärkung der Resilienz bei Weltraumressourcen

Der Vorschlag der Kommission für ein Weltraumprogramm der Union[12], unter anderem das Programm Copernicus, die staatliche Satellitenkommunikation und der Rahmen zur Unterstützung der Beobachtung und Verfolgung von Objekten im Weltraum umfasst Sicherheitsaspekte, die Aspekte der Resilienz gegenüber hybriden Bedrohungen betreffen und bereits für Galileo und EGNOS ergriffene Maßnahmen ergänzen würden.

Die Beobachtung und Verfolgung von Objekten im Weltraum (SST)[13] ist auf die Unterstützung einer langfristigen Verfügbarkeit europäischer und nationaler Weltrauminfrastruktur, -anlagen und -dienste ausgerichtet. Im Juli 2016 stellte die SST erste Dienste zu Kollisionsvermeidung, Zersplitterung und unkontrolliertem Wiedereintritt von Objekten aus dem Weltraum bereit. Die nationalen SST-Operationszentren und das Satellitenzentrum der EU haben Maßnahmen für die Datensicherheit ergriffen, bei denen die Empfehlungen des Rates zu Sicherheitsaspekten der Datenpolitik im Zusammenhang mit der Fähigkeit zur Weltraumlageerfassung[14] berücksichtigt wurden.

In Bezug auf Galileo ergreift die Kommission weitere Schritte, um einen besseren Schutz der Bereitstellung von Daten zu gewährleisten, die für das ordnungsgemäße Funktionieren kritischer Infrastrukturen wichtig sind, die hinsichtlich Zeitgebung und Synchronisierung auf Satellitennavigation angewiesen sind. Die Verwendung von Galileo für die Bereitstellung von Diensten in kritischen Infrastrukturen wie Energienetzen, Telekommunikationsnetzen und Finanzmarktplätzen wird erwogen. In diesem Zusammenhang werden im Vorschlag der Kommission für eine Verordnung zur Schaffung eines Rahmens für die Überprüfung ausländischer Direktinvestitionen die europäischen Programme für globale Satellitennavigationssysteme (GNSS) – Galileo und EGNOS – als Beispiele für Projekte oder Programme von Unionsinteresse genannt, die für die Überwachung ausländischer Direktinvestitionen im Rahmen der vorgeschlagenen Verordnung[15] relevant sein könnten.

Die EU-Initiative zur staatlichen Satellitenkommunikation (GovSatCom) wird einen garantierten und gesicherten Zugang zu Satellitenkommunikation für Missionen, Operationen und zentrale Infrastrukturen der Union und der Mitgliedstaaten bereitstellen. Dieses Instrument ist wichtig für die Abwehr hybrider Bedrohungen von einer Reihe von Infrastrukturen, unter anderem Weltraum-, Verkehrs- und Energieinfrastrukturen.

Maßnahme 9: Anpassung der Verteidigungsfähigkeiten und Entwicklung von Verteidigungsfähigkeiten mit EU-Relevanz

Der am 7. Juni 2017 eingerichtete Europäische Verteidigungsfonds ist ein wichtiger Schritt dahin, Anreize für Anstrengungen der Mitgliedstaaten zur Vertiefung und Aufrechterhaltung der Zusammenarbeit im Bereich der Verteidigung in Europa zu schaffen, um wirksam auf strategische Herausforderungen reagieren zu können. Im Rahmen des Fähigkeitenfensters des Fonds wird die EU insbesondere nationale Finanzierungen für gemeinsame Entwicklungsprojekte in der Verteidigung ergänzen. Zu diesem Zweck hat die Kommission im Juni 2017 einen Vorschlag für eine Verordnung über ein Europäisches Programm zur industriellen Entwicklung im Verteidigungsbereich mit einem Haushalt von 500 Mio. EUR

---

12 COM 2018(447) final vom 6.6.2018.

13 Beschluss Nr. 541/2014/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Schaffung eines Rahmens zur Unterstützung der Beobachtung und Verfolgung von Objekten im Weltraum.

14 „Space Situational Awareness data policy“ (Datenpolitik im Zusammenhang mit der Fähigkeit zur Weltraumlageerfassung), (14698/12) vom 9.10.2012.

15 Siehe Anhang zu COM(2017) 487 final.

für 2019 und 2020 vorgelegt. Am 22. Mai 2018 erzielten das Europäischen Parlament und der Rat eine vorläufige Einigung über den Verordnungsentwurf. Für den nächsten mehrjährigen Finanzrahmen hat die Kommission einen integrierten Europäischen Verteidigungsfonds mit einem ehrgeizigen Haushalt von 13 Mrd. EUR vorgeschlagen, von denen mehr als 8,90 Mrd. EUR in Projekte zur Entwicklung gemeinschaftlicher Verteidigungsfähigkeiten fließen sollen. Die möglichen Auswirkungen der Abwehr hybrider Bedrohungen auf die Fähigkeitenentwicklung werden im überarbeiteten Plan zur Fähigkeitenentwicklung, auf den sich die Mitgliedstaaten im Juni 2018 einigen sollen, berücksichtigt.

***Maßnahme 10*: Vorsorge gegen Gesundheitsgefahren und Koordinierungsmechanismen**

Die Vorsorge gegen Gesundheitsgefahren ist ein sehr wichtiger Bestandteil der allgemeinen Abwehrbereitschaft gegen CBRN-Risiken. Die Kommission hat daher im Rahmen ihres Aktionsplans für eine gesteigerte Abwehrbereitschaft gegen chemische, biologische, radiologische und nukleare Sicherheitsrisiken entsprechende Schritte unternommen, wobei der Schwerpunkt auf Initiativen zur effizienten gemeinsamen Nutzung von Fachwissen lag.

Die Kommission richtete daher Chimera ein, eine Übung für Einrichtungen im Bereich des Gesundheitswesen, des Katastrophenschutzes und der Sicherheit in der gesamten EU sowie in Drittländern, mit der die Abwehrbereitschaft und die Planung der Maßnahmen bei ernsthaften grenzüberschreitenden Bedrohungen geprüft werden soll. Das fiktive Szenario der Übung umfasste die absichtliche Freisetzung einer übertragbaren Krankheit in Kombination mit Cyberangriffen auf kritische Infrastrukturen, darunter Krankenhäuser, zur Prüfung der vorhandenen Mechanismen, Systeme und Kommunikationsmittel auf nationaler und EU-Ebene bei der Reaktion auf eine hybride Bedrohung. Die EU-weite Übung fand am 30. und 31. Januar 2018 in Luxemburg statt. Sie trug dazu bei, den sektorübergreifenden Kapazitätsaufbau zu unterstützen und die Interoperabilität und Koordinierung zwischen Gesundheitswesen, Katastrophenschutz und Sicherheitssektor auf Ebene der EU und der Mitgliedstaaten sowie die Zusammenarbeit mit internationalen Partnern zu verbessern. Die Übung trug ferner dazu bei, die derzeitigen Zuständigkeiten und Rollen aller Beteiligten beim Krisenmanagement im Zusammenhang mit hybriden Bedrohungen zu ermitteln. Das Frühwarn- und Reaktionssystem (Early Warning and Response System, EWRS), das sektorübergreifende Warnsystem der Kommission ARGUS, das Gemeinsame Kommunikations- und Informationssystem für Notfälle (CECIS) sowie die Integrierte Regelung für die politische Reaktion auf Krisen (Integrated Political Crisis Response, IPCR) des Rates wurden auf ihre Interaktionsfähigkeit geprüft. Der fünfzehnte Bericht über die Fortschritte auf dem Weg zu einer wirksamen und echten Sicherheitsunion enthält ausführlichere Informationen über die Maßnahmen der EU zur Steigerung der Abwehrbereitschaft gegen CBRN-Risiken.

Im April 2018 veröffentlichte die Kommission eine Mitteilung und legte einen Vorschlag für eine Empfehlung des Rates zur Verbesserung der Zusammenarbeit in der EU gegen durch Impfungen verhütbare Krankheiten vor, damit dieser vor Ende des Jahres 2018 verabschiedet werden kann. Damit sollen gegen die Impfzurückhaltung vorgegangen, die Impfprogramme nachhaltiger gestaltet und die Effizienz von Forschung und Entwicklung im Bereich Impfstoffe erhöht werden.

Aus Sicht des Europäischen Medizinischen Korps erhielt das norwegische medizinische Notfallteam die Einstufung der Weltgesundheitsorganisation (WHO), was voraussetzt, dass bestimmte Mindestqualitätsstandards eingehalten werden. Im April 2018 fand das erste regionale Treffen der medizinischen Notfallteams der Europäischen Region der WHO statt; dieses Treffen wurde gemeinsam von der Kommission, der Weltgesundheitsorganisation sowie den belgischen Gesundheitsbehörden als Vorsitzende der Regionalgruppe ausgerichtet.

Derzeit wird in enger Zusammenarbeit mit der European Burns Association und den Mitgliedstaaten die Entwicklung eines Katastrophenmanagement-Mechanismus für den Fall massenhafter Brandverletzungen vorbereitet. Anfang Oktober 2018 kommen die Kommission und die Mitgliedstaaten zu einem Workshop zusammen, um die Arbeiten abzuschließen.

Maßnahme 11: ***Das Netzwerk der Reaktionsteams für Cybersicherheitsverletzungen (Cyber Security Incident Response Teams, CSIRTs), das CERT-EU und die NIS-Richtlinie***

Das IT-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der EU (EU institutions' Computer Emergency Response Team, CERT-EU) gibt Produkte zur Bewertung der Bedrohung durch Cyberangriffe für kritische Sektoren regelmäßig und ad hoc heraus. Für verschiedene Verkehrsträger (Luft-, See- und Landverkehr) stellt die Kommission die Kohärenz sektorbezogener Initiativen gegen Cyberbedrohungen mit den von der Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie) erfassten sektorübergreifenden Fähigkeiten sicher und führt entsprechende Kontrollen durch.

Im September 2017 veranstalteten die Europäische Verteidigungsagentur und der estnische Vorsitz des Rates der EU eine strategische Cyberplanübung namens CYBRID17 für die EU-Verteidigungsminister, um das Bewusstsein für die Cybersicherheitskoordinierung auf politischer Ebene und für die möglichen Auswirkungen offensiver Cyberkampagnen zu schärfen. Die Schwerpunkte lagen auf Lagebewusstsein, Krisenreaktionsmechanismen und strategischer Kommunikation. Die Europäische Verteidigungsagentur wird die Elemente dieser Übung in die Plattform zur Aus- und Fortbildung, Evaluierung und Übung des Europäischen Sicherheits- und Verteidigungskollegs überführen, die im September 2018 eingerichtet werden soll. Ähnliche hochrangige Übungen des jeweiligen Ratsvorsitzes werden für die Zukunft in Erwägung gezogen.

Maßnahme 12: ***Vertragliche öffentlich-private Partnerschaft für die Cybersicherheit***

Die Kommission unterzeichnete eine öffentlich-private Partnerschaft zur Cybersicherheit mit der European Cybersecurity Organisation (ECSO), um die Wettbewerbsfähigkeit und die Innovationskapazitäten der Branche für digitale Sicherheit und den Schutz personenbezogener Daten in Europa zu erhöhen. Die EU wird in diese Partnerschaft bis zu 450 Mio. EUR investieren, um Nutzer und Infrastrukturen vor Cyberangriffen zu schützen. Es wird erwartet, dass diese vertragliche öffentlich-private Partnerschaft bis 2020 Investitionen von 1,8 Mrd. EUR nach sich ziehen wird.

Die Gemeinsame Mitteilung „Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen"[16] aus dem September 2017 enthält Maßnahmen, mit denen die Cybersicherheitsstrukturen und -kapazitäten der EU erheblich gestärkt werden sollen. Eine wirksame Cybersicherheit wird in der EU jedoch durch einen Mangel an Investitionen und Koordinierung behindert. Wie in der Gemeinsamen Mitteilung beschrieben, versucht die Kommission, hier Abhilfe zu schaffen.

Maßnahme 13: ***Resilienz im Energiesektor***

Im Juni 2018 wird die Kommission im Rahmen der NIS-Kooperationsgruppe einen Arbeitsstrang zum Energiesektor einrichten, um den Besonderheiten des Energiesektors Rechnung zu tragen und den Mitgliedstaaten Leitlinien zur Richtlinie zur Netz- und Informationssicherheit für diesen Sektor an die Hand zu geben. Parallel dazu arbeitet die Kommission an besonderen Leitlinien zur Cybersicherheit, welche über die NIS-Richtlinie hinausgehen, um bewährte Cybersicherheitsverfahren im Energiesektor zu ermitteln, und

16 JOIN(2017) 450 final.

spricht Betreiber an, die von der NIS-Richtlinie nicht erfasst werden. Die Kommission wird weiterhin Veranstaltungen zum Informationsaustausch über Fragen der Cybersicherheit im Energiesektor initiieren, um das Bewusstsein zu schärfen, um bewährte Verfahren auszutauschen, um die Zusammenarbeit (über Grenzen hinweg und zwischen den Übertragungsnetz- und Verteilernetzbetreibern) zu verbessern und um auf physische Maßnahmen, neue Risiken sowie Ausbildung und Qualifikationen einzugehen.

Langfristig wird die Kommission, wie in der Neufassung der Elektrizitätsverordnung[17], die zurzeit das Gesetzgebungsverfahren durchläuft, vorgeschlagen, einen Netzwerkkodex für sektorspezifische Cybersicherheitsvorschriften einführen.

Maßnahme 14: ***Resilienz im Finanzsektor: Plattformen und Netze für den Informationsaustausch***

Mit ihrem Aktionsplan zur Finanztechnologie (FinTech) sucht die Kommission potenzielle Hemmnisse zu ermitteln, die den Informationsaustausch zwischen Finanzmarktakteuren über Cyberbedrohungen beschränken, und mögliche Lösungen für deren Beseitigung aufzuzeigen. Das CERT-EU spielt ebenfalls eine Rolle beim Austausch von Informationen über Zwischenfälle.

Maßnahme 15: ***Resilienz gegen Cyberangriffe im Verkehrssektor***

Der Schutz von Verkehrsträgern vor Angriffen auf die Cybersicherheit genießt für die Kommission hohe Priorität. In der Zivilluftfahrt wurden vom Standpunkt der Cybersicherheit gute Fortschritte erzielt, doch eine Verwundbarkeit des Systems gegen technische Störungen oder Bedrohungen der Cybersicherheit kann niemals ausgeschlossen werden, wie der jüngste IT-Zwischenfall bei EUROCONTROL, von dem die Hälfte der Flüge in Europa betroffen war, beweist. Die Kommission arbeitet im Verkehrssektor eng mit der Europäischen Agentur für Flugsicherheit zusammen. Das CERT-EU hat mit EUROCONTROL eine Leistungsvereinbarung und mit der Europäischen Agentur für Flugsicherheit eine Kooperationsvereinbarung abgeschlossen, um diese Einrichtungen und die mit ihnen verbundenen Interessenträger beim Umgang mit Cyberbedrohungen zu unterstützen.

Im Seeverkehr gab die Schifffahrtsbranche Richtlinien zur Cybersicherheit heraus, die auf Ebene der Internationalen Seeschifffahrtsorganisation erörtert und anschließend verabschiedet wurden, wobei ein globaler Blickwinkel und Ansatz vorherrschten. Die Cybersicherheit in europäischen Häfen und Hafenanlagen bliebt eine hohe politische Priorität, die mit den Mitgliedstaaten, der Industrie und Interessenträgern im Zusammenhang mit der Umsetzung der Richtlinie zur Netz- und Informationssicherheit und den entsprechenden Folgemaßnahmen erwogen und regelmäßig erörtert wird.

Die Kommission beabsichtigt, ein ganzheitliches und interaktives Instrumentarium mit Kenntnissen im Bereich der Cybersicherheit zu entwickeln, welches empfohlene bewährte Verfahren enthält, mit denen Sicherheitsmanager und Fachleute im Verkehrssektor bei der besseren Ermittlung, Bewertung und Verringerung von Cyberrisiken unterstützt werden sollen.

Maßnahme 16: ***Bekämpfung der Terrorismusfinanzierung***

Wie in den regelmäßigen Berichten über die Sicherheitsunion beschrieben, hat die Kommission im letzten Jahr erhebliche Anstrengungen unternommen, um die Terrorismusfinanzierung zu unterbinden. Zuletzt hat die Kommission in ihrem

[17] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den Elektrizitätsbinnenmarkt (Neufassung), COM/2016/0861 final.

Sicherheitspaket vom April 2018[18] weitere Maßnahmen ergriffen, um die Zusammenarbeit zwischen den für die Bekämpfung von schwerwiegenden Straftaten und Terrorismus zuständigen Behörden zu verbessern und deren Zugang zu und Nutzung von Finanzdaten zu fördern; die Kommission hat dafür einen Vorschlag für eine Richtlinie[19] zur Erleichterung der Nutzung von Finanz- und sonstigen Informationen für die Verhütung, Aufdeckung, Untersuchung oder Verfolgung schwerer Straftaten vorgelegt. Weitere Einzelheiten über die jüngsten Maßnahmen auf EU-Ebene gegen die Terrorismusfinanzierung enthält der fünfzehnte Fortschrittsbericht „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion".

Zwecks Harmonisierung der Sanktionen für Geldwäschedelikte schlug die Kommission Rechtsvorschriften vor, die Mitte 2018 verabschiedet werden sollten. Überdies wurde im Mai dieses Jahres die fünfte Richtlinie zur Bekämpfung der Geldwäsche verabschiedet, um eine Reihe von Maßnahmen wie verstärkte Kontrollen von Drittländern mit hohem Risiko, Kontrollen von Umtauschplattformen für virtuelle Währungen, Transparenzmaßnahmen für Zahlungsinstrumente auf Guthabenbasis, neue Befugnisse für die zentralen Meldestellen und rascher Zugang zu Informationen über die Inhaber von Bank- und Zahlungskonten durch zentralisierte Register oder elektronische Datenabrufsysteme für zentrale Meldestellen zu stärken.

***Maßnahme 17:* Maßnahmen gegen die Radikalisierung und Prüfung der Notwendigkeit, die Verfahren zur Entfernung illegaler Inhalte auszubauen**

Die Verhinderung einer in Gewaltbereitschaft mündenden Radikalisierung, sowohl online als auch offline, war in den letzten Jahren ein vordringliches Anliegen der Kommission. Zur Intensivierung der Arbeiten auf EU-Ebene richtete die Kommission eine hochrangige Expertengruppe zum Thema Radikalisierung ein, die Empfehlungen über die Koordinierung der Vorsorgepolitik der EU sowie über ihre Öffentlichkeitswirksamkeit und ihre Auswirkungen geben soll. Am 18. Mai 2018 legte die hochrangige Expertengruppe zum Thema Radikalisierung ihren Abschlussbericht vor, in dem die Einrichtung eines EU-Kooperationsmechanismus empfohlen wird.

Bei der Bekämpfung illegaler Online-Inhalte lag der Schwerpunkt im Anschluss an die Verabschiedung der Empfehlungen der Kommission vom 1. März 2018 auf der Erschwerung des Online-Zugangs zu solchen Inhalten. Die Kommission hat eine Folgenabschätzung gestartet, um festzustellen, ob die derzeitigen Anstrengungen ausreichen oder zusätzliche Maßnahmen erforderlich sind, um die rasche und proaktive Erkennung und Entfernung illegaler Online-Inhalte zu gewährleisten, einschließlich eventueller Legislativmaßnahmen zur Ergänzung des bestehenden Rechtsrahmens. Die Arbeit der Kommission in diesem Bereich wird im fünfzehnten Fortschrittsbericht „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion" ausführlicher dargestellt.

Der mit Facebook, Twitter, Google (YouTube) und Microsoft vereinbarte Verhaltenskodex zur Bekämpfung von Online-Hetze zeitigt rasche und positive Ergebnisse. Dank dem Verhaltenskodex erzielten die Unternehmen erhebliche Fortschritte bei der raschen Überprüfung und Entfernung von als Hetze eingestuften Inhalten, die ihnen gemeldet wurden. Die im Januar 2018 veröffentlichte dritte Bewertung der Umsetzung des Kodex durch die Kommission zeigte, dass im Durchschnitt 70 % der hetzerischen Inhalte entfernt werden und die Überprüfung, wie im Verhaltenskodex vorgeschrieben, binnen 24 Stunden erfolgt. Der Kodex ist zu einem Branchenstandard geworden, und der jüngste Beschluss von Instagram und Google+, den Kodex ebenfalls einzuführen, ist ermutigend. Im März 2018 schlug die Kommission außerdem zusätzliche Maßnahmen für Onlineplattformen wie automatisierte

[18] COM(2018) 211 final.
[19] COM(2018) 213 final.

Entdeckung, Transparenz und Feedback an die Nutzer sowie Schutzbestimmungen zur Wahrung der Redefreiheit vor.[20]

Trotz der bereits ergriffenen Maßnahmen gegen Radikalisierung und Hetze online sollten Schritte unternommen werden, um durch den Cyberspace ermöglichte Bedrohungen für Wahlen zu verhindern und zu reduzieren.

<u>Maßnahme 18</u>: Verstärkung der Zusammenarbeit mit benachbarten Regionen und Drittländern

Die Europäische Union hat sich verstärkt darauf konzentriert, im Sicherheitssektor von Partnerländern Kapazitäten und Resilienz zu schaffen, unter anderem durch Weiterentwicklung des Sicherheitsaspekts der überarbeiteten Europäischen Nachbarschaftspolitik. Um die Kapazitäten der Partner zur Abwehr hybrider Bedrohungen zu stärken, werden eigene Untersuchungen über hybride Risiken eingeleitet, bei denen kritische Schwachstellen aufgezeigt und zielgerichtete Unterstützung bereitgestellt werden sollen. Der EAD hat in Zusammenarbeit mit der Kommission eine Untersuchung in der Republik Moldau durchgeführt. 2018 haben Jordanien und Georgien bei der EU offiziell eine Untersuchung ihrer Verwundbarkeit beantragt, wobei der erste Schritt darin bestand, die Fragebogen auf ihre speziellen Bedürfnisse zuzuschneiden. Zusätzliche Arbeiten zum Aufbau von Cybersicherheitskapazitäten, insbesondere für kritische Infrastrukturen, wurden in der Ukraine in Form technischer Unterstützungsmissionen geleistet; zugleich startete die Kommission Anfang 2018 auch ein umfassendes neues Programm zur Erhöhung der Cyberresilienz von Drittländern vor allem in Afrika und Asien.

Im Rahmen der Arbeitsgruppe für Fragen der Grenzüberwachung erörtert die EU weiter mit der Internationalen Atomenergie-Organisation und der Regierung der Vereinigten Staaten Pläne zum Aufbau von Nuklearsicherheitskapazitäten und entsprechende Programme. Das Europäische Ausbildungszentrum für Gefahrenabwehr im Nuklearbereich (European nuclear security training centre, EUSECTRA) veranstaltet Schulungen zur Vorbeugung und Gefahrenerkennung im Bereich der Nuklearsicherheit und zur Reaktion auf nukleare Zwischenfälle. Der Aktionsplan der Kommission zur Erhöhung der Abwehrbereitschaft gegen chemische, biologische, radiologische und nukleare Sicherheitsrisiken umfasst spezifische Maßnahmen zur Zusammenarbeit mit wichtigen internationalen Partnern, auch im Zusammenhang mit Terrorismusbekämpfung und Sicherheitsdialogen mit maßgeblichen Drittländern.

Die EU-finanzierte Initiative zu den CBRN-Exzellenzzentren, die nahezu alle Nachbarschaftspartner abdeckt[21], arbeitet weiter an einer Erhöhung der nationalen und regionalen Fähigkeiten der Partnerländer zur Vorbeugung gegen solche Bedrohungen, auch solche gegen militärische Sicherheitsstrukturen, an der Abwehrbereitschaft und an der Reaktionsfähigkeit.

In der östlichen und südlichen Nachbarschaft werden die Katastrophenschutzausbildung und entsprechende Übungen im Rahmen des regionalen Programms für Prävention, Einsatzbereitschaft und Reaktionsfähigkeit bei Naturkatastrophen und von Menschen verursachten Katastrophen (Prevention, Preparedness and Response to natural and man-made disasters, PPRD) organisiert. Die dritte Phase der PPRD Süd begann 2018, während die zweite Phase der PPRD Ost im November 2018 enden wird; eine Verlängerung ist möglich. Eine enge Verbindung zwischen den regionalen CBRN-Exzellenzzentren und den PPRD-Programmen Süd und Ost ist zu gewährleisten.

---

20 COM(2018) 1177 final.

21 Mit den regionalen CBRN-Exzellenzzentren in Rabat, Algier, Amman und Tiflis.

PRÄVENTION, KRISENREAKTION UND RÜCKKEHR ZUR NORMALITÄT

Die Auswirkungen lassen sich zwar durch langfristige Strategien auf nationaler und auf EU-Ebene vermindern, kurzfristig kommt es jedoch weiterhin ganz entscheidend darauf an, die Fähigkeit der Mitgliedstaaten und der Union zu stärken, rasch und koordiniert hybriden Bedrohungen vorzubeugen, darauf zu reagieren und sich davon zu erholen. Eine rasche Reaktion auf Ereignisse, die durch hybride Bedrohungen ausgelöst wurden, ist von grundlegender Bedeutung. In diesem Bereich wurden im vergangenen Jahr große Fortschritte erzielt, unter anderem wurde mit einem jetzt in der EU verfügbaren Protokoll der Ablauf des Krisenmanagements im Falle eines hybriden Angriffs festgelegt. Die regelmäßige Überwachung und die Übungen werden fortgesetzt.

Maßnahme 19: ***Ein gemeinsames Protokoll für das operative Vorgehen und Übungen zur Verbesserung der Fähigkeit zur strategischen Entscheidungsfindung im Falle komplexer hybrider Bedrohungen***

Das Protokoll für das operative Vorgehen wurde durch eine gemeinsame Arbeitsunterlage im Juni 2016 eingeführt. Es lieferte die grundlegenden Leitlinien für die institutionsübergreifende Reaktion auf Krisen. Bei der Übung EUPACE17 wurde das Protokoll gegen das Szenario einer hybriden Bedrohung geprüft und erwies sich als unschätzbares Instrument zur Erleichterung der Vernetzung der Dienststellen. Überdies lieferte es die Ansatzpunkte für das Zusammenwirken der verschiedenen Reaktionsebenen, nämlich der politisch-strategischen und der operativ-technischen Ebene sowie zwischen den drei wichtigsten Reaktionsmechanismen des Krisenreaktionssystems der EU (für externe Krisen), ARGUS (interne IT-gestützte Plattform zum Informationsaustausch) und der integrierten politischen Krisenreaktionsplattform des Rates. Das Protokoll stellte seinen Wert auch bei der parallelen Krisenmanagementübung CMX 17 mit der NATO unter Beweis. Die nächste Übung der Serie, PACE‘18, findet im November 2018 statt und es wird eine Aktualisierung des Protokolls unter Berücksichtigung etwaiger künftiger Erkenntnisse in Erwägung gezogen.

Im September und Oktober 2017 veranstaltete die EU die erste parallele und koordinierte Übung mit der NATO (PACE17), bei der sie die Abwehrbereitschaft und das Zusammenwirken zwischen den zwei Organisationen im Fall einer hybriden Krise im großen Maßstab prüfte. In der Vorbereitungsphase fand ein intensiver Personalaustausch in allen vier Bereichen der Hybrid-Planspiele statt: Frühwarnung/Lagebeurteilung, strategische Kommunikation, Cyberabwehr, Krisenprävention und Reaktion im Krisenfall. Die Zusammenarbeit zwischen EU- und NATO-Stäben bei der Übung EUPACE17 ist von einem bisher nicht da gewesenen Ausmaß. Es war auch das erste Mal, dass die NATO an einem runden Tisch der Integrierten EU-Regelung für die politische Reaktion auf Krisen unter Leitung der Ratspräsidentschaft teilnahm; leitende Beamte der EU nahmen wiederum an den Beratungen des Nordatlantikrats teil. Der Prozess der Erfahrungsauswertung konzentrierte sich auf mehrere Aspekte, darunter das Zusammenwirken zwischen den Krisenreaktionsmechanismen der EU und der NATO und die Herausforderungen im Zusammenhang mit dem Austausch von Verschlusssachen zwischen dem Personal der beiden Einrichtungen einschließlich der Notwendigkeit sicherer Kommunikationsverbindungen, insbesondere mit dem Ziel, zukünftig einen raschen und sicheren Austausch unter voller Beachtung der notwendigen Absenderkontrolle sicherzustellen.

Die Planungen für die parallele und koordinierte Übung 2018, bei der die EU die federführende Organisation sein wird, laufen.

<u>Maßnahme 20</u>: ***Prüfung der Anwendbarkeit und der praktischen Konsequenzen von Artikel 222 AEUV und Artikel 42 Absatz 7 EUV, falls es zu einem großangelegten, schweren hybriden Angriff kommt***

Die Anwendbarkeit der Solidaritätsklausel der EU und ihres Mechanismus zur gegenseitigen Unterstützung sowie ihr Zusammenwirken untereinander und mit den Reaktionsmechanismen der NATO einschließlich der kollektiven Verteidigung nach Artikel 5 werden in den Szenarien der Übungen zur Abwehr hybrider Bedrohungen weiter erörtert und geprüft. Das Kompetenzzentrum für die Bewältigung hybrider Bedrohungen in Helsinki ist interessiert und bereit, die Arbeiten sowohl in Bezug auf die Forschung als auch in Bezug auf Übungen voranzutreiben und so zur Entwicklung eines gemeinsamen Verständnisses zwischen den Mitgliedstaaten und den Verbündeten beizutragen.

<u>Maßnahme 21</u>: ***Integration, Nutzung und Koordinierung der militärischen Fähigkeiten zur Abwehr hybrider Bedrohungen im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik***

Nach Erteilung des Auftrags zur Integration militärischer Fähigkeiten zur Unterstützung der Gemeinsamen Außen- und Sicherheitspolitik/Gemeinsamen Sicherheits- und Verteidigungspolitik und im Anschluss an ein Seminar mit Militärexperten im Dezember 2016 sowie Leitlinien von der Arbeitsgruppe des EU-Militärausschusses im Mai 2017 wurden die militärischen Ratschläge über den militärischen Beitrag der EU zur Abwehr hybrider Bedrohungen im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik im Juli 2017 abgeschlossen. Diese Arbeiten werden im Rahmen des „Concept Development Implementation Plan“ fortgeführt. In Abstimmung mit dem Europäischen Kompetenzzentrum für die Bewältigung hybrider Bedrohungen entwickelt der Militärstab der EU derzeit ein Konzept darüber, wie das Militär zur Abwehr hybrider Bedrohungen beitragen kann, das auch Missionen und Operationen im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik umfasst.

Zusätzlich ermöglichen der Militärstab der EU und die Mitgliedstaaten täglich den Ausbau des Frühwarnsystems, indem sie der EU-Analyseeinheit für hybride Bedrohungen militärische nachrichtendienstliche Unterstützung leisten. Das Einheitliche Analyseverfahren unterstützt die StratCom Task Forces des EAD durch militärische Beratung, um zur Abwehr von gegen die EU und einzelne Mitgliedstaaten gerichteten Fehlinformationskampagnen beizutragen.

Militärische Fähigkeiten zur Abwehr hybrider Bedrohungen werden 2018 in der parallelen und koordinierten Übung mit der NATO (PACE18) geübt. Auf der Grundlage des Hybridszenarios von PACE18 werden der Militärstab der EU und der Internationale Militärstab der NATO informelle, szenariobasierte Gespräche führen, um bei sich überschneidenden Anforderungen auf der Grundlage des Grundsatzes der Inklusivität die Komplementarität bei der Abwehr hybrider Bedrohungen sicherzustellen, wobei die Autonomie jeder Organisation bei der Entscheidungsfindung und die Datenschutzvorschriften zu beachten sind.

ZUSAMMENARBEIT ZWISCHEN DER EU UND DER NATO

<u>Maßnahme 22:</u> ***Zusammenarbeit zwischen der EU und der Nato in den Bereichen Lagebewusstsein, strategische Kommunikation Cybersicherheit und „Krisenprävention und -reaktion“***

Die Abwehr hybrider Bedrohungen bleibt ein Schlüsselbereich der Zusammenarbeit zwischen EU und NATO. Sie beruht auf der Einsicht, dass die Ressourcen und Fähigkeiten, welche die zwei Organisationen bei einer hybriden Bedrohung mobilisieren können, komplementär sind und die Fähigkeit der Mitgliedstaaten und Verbündeten zur Verhütung und Abschreckung sowie zur Reaktion auf solche Bedrohungen stärken. Bei der Übung PACE17 wurden die „Planspiele" der beiden Organisationen geprüft und damit ihre Fähigkeit zur raschen und wirksamen Zusammenarbeit zur Unterstützung des betroffenen Mitglieds. Angesichts der gewonnenen Erfahrungen werden die beiden „Planspiele" überarbeitet und aktualisiert. Auf dem Gebiet der strategischen Kommunikation haben Beratungen mit dem Ziel, die Ukraine, Bosnien und Herzegowina, die Republik Moldau und Georgien zu unterstützen, stattgefunden.

Im September 2017 kamen auf einem gemeinsamen Resilienz-Workshop der EU und der NATO Experten aus kritischen strategischen Sektoren zusammen, um Informationen zu den jeweiligen Tätigkeiten auszutauschen und Vorschläge für die künftige Arbeit zu prüfen, insbesondere beim Schutz kritischer Infrastrukturen.

Im Jahr 2018 soll mit einem Projekt zur militärischen Mobilität die Bewegung von Militärmaterial und -personal erleichtert werden; hierbei könnten die wahrscheinlichen Herausforderungen durch hybride Bedrohungen berücksichtigt werden, die speziell dafür konzipiert wurden, die Reaktionszeit der Mitgliedstaaten und Verbündeten zu verlängern. Es handelt sich um ein Gebiet für künftige parallele Übungen, das in den Serien EUPACE19/20 berücksichtigt wird.

Die Koordinierung der Bemühungen im Bereich der Cyberschulungen ist ein wichtiger Bereich für eine engere Zusammenarbeit. Die NATO nahm außerdem als Beobachter an der Cyber-Europe-Planübung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) im Juni 2018 teil.

SCHLUSSFOLGERUNG

Die Verbesserung des Lagebewusstseins und der Aufbau von Resilienz gegen sich weiterentwickelnde hybride Bedrohungen aus verschiedenen Quellen bleiben eine Herausforderung und verlangen ständige Anstrengungen seitens der EU. Der Gemeinsame Rahmen umfasst eine breite Palette von Maßnahmen von der Verbesserung der Informationsverknüpfung und des Informationsaustauschs bis zum verstärkten Schutz kritischer Infrastrukturen und zur Cybersicherheit sowie zum Aufbau von Resilienz der Gesellschaften gegen Radikalisierung und gewalttätigen Extremismus. Der Rahmen der EU zur Abwehr hybrider Bedrohungen hat es ermöglicht, Mitgliedstaaten durch eine Reihe von Maßnahmen zur Stärkung der Widerstandsfähigkeit der EU und der Mitgliedstaaten gegen Stress sowie der Fähigkeit zur koordinierten Reaktion auf schädliche Angriffe und schließlich zur Erholung davon zu unterstützen.

Die Reaktion der EU auf hybride Bedrohungen wurde ebenfalls erfolgreich geprüft und war Gegenstand einer Reihe gemeinsamer Übungen mit der NATO. Es ist geplant, die Arbeiten in diesem Sinne fortzusetzen. Eine enge Zusammenarbeit aller maßgeblichen Akteure innerhalb der EU und mit der NATO ist von entscheidender Bedeutung für die Bemühungen zum Aufbau von Resilienz. Zudem trägt die Unterstützung der benachbarten Partnerländer bei der Ermittlung ihrer Verwundbarkeiten und beim verstärkten Aufbau von Kapazitäten gegen hybride Bedrohungen dazu bei, besser zu verstehen, welcher Art externe Bedrohungen sind, und führt so zu mehr Sicherheit in der Nachbarschaft der EU.