EUROPÄISCHE
KOMMISSION

HOHE VERTRETERIN
DER UNION FÜR
AUSSEN- UND
SICHERHEITSPOLITIK

Brüssel, den 19.7.2017
JOIN(2017) 30 final

GEMEINSAMER BERICHT AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

zur Umsetzung des Gemeinsamen Rahmens für die Abwehr hybrider Bedrohungen – eine Antwort der Europäischen Union

1. EINFÜHRUNG

Die EU steht vor einer der größten Herausforderungen, die sie in ihrer Geschichte im Sicherheitsbereich zu bewältigen hatte. Die Bedrohungen nehmen immer unkonventionellere Formen an: Einige sind physisch greifbar, wie neue Arten des Terrorismus, bei anderen wird der digitale Raum für komplexe Cyberangriffe genutzt. Bei wieder anderen subtileren Formen wird – auch durch Kampagnen zur Verbreitung von Fehlinformationen – Zwang ausgeübt und damit Druck aufgebaut und zudem kommt es zu Medienmanipulationen. Auf diese Weise sollen europäische Grundwerte, wie Menschenwürde, Freiheit und Demokratie, untergraben werden. Die kürzlich weltweit verübten und nur schwer zuordenbaren koordinierten Cyberangriffe haben gezeigt, dass unsere Gesellschaften und Institutionen verwundbar sind.

In April 2016 nahmen die Europäische Kommission und die Hohe Vertreterin eine Gemeinsame Mitteilung für die Abwehr hybrider Bedrohungen[1] (Gemeinsamer Rahmen) an. In diesem Rahmen wird die grenzüberschreitende und komplexe Natur hybrider Bedrohungen anerkannt und ein ressortübergreifender Ansatz vorgeschlagen, durch den die Resilienz unserer Gesellschaften insgesamt gestärkt werden soll. Der Rat[2] begrüßte die Initiative und regte Maßnahmen an, ferner forderte er die Kommission und die Hohe Vertreterin auf, im Juli 2017 einen Fortschrittsbericht vorzulegen. Zwar kann die EU die Mitgliedstaaten beim Aufbau ihrer Resilienz gegenüber hybriden Bedrohungen unterstützen, die Hauptverantwortung liegt aber insofern bei ihnen selbst, als ein Zusammenhang zwischen der Abwehr hybrider Bedrohungen und der nationalen Sicherheit und Verteidigung besteht.

Dieser Gemeinsame Rahmen für die Abwehr hybrider Bedrohungen ist ein wichtiger Bestandteil des insgesamt stärker integrierten Sicherheits- und Verteidigungskonzepts der EU. Er trägt dazu bei, ein „Europa, das schützt“ zu schaffen, das von Präsident Juncker in seiner Rede zur Lage der Union im September 2016 gefordert wurde. Im Jahr 2016 hat Europäische Union auch den Grundstein für eine bessere europäische Verteidigungspolitik gelegt, um den gestiegenen Sicherheitserwartungen der Bürgerinnen und Bürger Rechnung zu tragen. In der Globalen Strategie für die Außen- und Sicherheitspolitik der Europäischen Union[3] wird herausgearbeitet, dass es eines integrierten Konzepts zur Verknüpfung der internen Resilienz mit dem auswärtigen Handeln der EU bedarf. Zudem werden Synergien zwischen der Verteidigungspolitik und den Politikbereichen, unter die die Themen Binnenmarkt, Industrie, Strafverfolgung und Nachrichtendienste fallen, gefordert. Nachdem der Europäische Aktionsplan im Verteidigungsbereich im November 2016 angenommen worden war, stellte die Kommission konkrete Initiativen vor, mit denen die Fähigkeit der EU, auf hybride Bedrohungen zu reagieren, verbessert werden soll: Es gilt, die Resilienz der Lieferketten der europäischen Verteidigungswirtschaft zu fördern und den Binnenmarkt für Verteidigungsgüter auszubauen. Insbesondere stellte die Kommission am 7. Juni 2017 den Europäischen Verteidigungsfonds vor, der bis 2020 mit 600 Mio. EUR und ab 2020 mit 1,5 Mrd. EUR jährlich ausgestattet werden soll. In der Mitteilung zur Sicherheitsunion[4] wird

[1] Gemeinsame Mitteilung an das Europäische Parlament und den Rat – *Gemeinsamer Rahmen für die Abwehr hybrider Bedrohungen – eine Antwort der Europäischen Union*, JOIN(2016) 18 final.
[2] *Schlussfolgerungen des Rates zur Bewältigung hybrider Bedrohungen*, Pressemitteilung 196/16, 19. April 2016.
[3] Wurde dem Europäischen Rat von der Hohen Vertreterin am 28. Juni 2016 präsentiert.
[4] COM(2016) 230 final vom 20.4.2016.

anerkannt, dass hybride Bedrohungen abzuwehren sind, und dass es von Bedeutung ist, das interne und externe Handeln auf dem Gebiet der Sicherheit kohärenter zu gestalten.

Die Spitzenvertreter der EU haben die Sicherheit und Verteidigung in der Debatte über die Zukunft Europas in den Vordergrund gerückt.[5] Dies wurde am 25. März 2017 in der **Erklärung von Rom** anerkannt, in der die Vision einer sicheren und geschützten Union, die sich zur Stärkung ihrer gemeinsamen Sicherheit und Verteidigung bekennt, dargelegt wird. Die Präsidenten des Europäischen Rates und der Europäischen Kommission sowie der Generalsekretär der NATO unterzeichneten am 8. Juli 2016 in Warschau eine gemeinsame Erklärung, durch die die strategische Partnerschaft zwischen EU und NATO neue Impulse und Inhalte erhalten soll. In der gemeinsamen Erklärung werden sieben konkrete Bereiche, unter anderem die Abwehr hybrider Bedrohungen, genannt, in denen die Zusammenarbeit zwischen den beiden Organisationen zu intensivieren wäre. Ein gemeinsames Paket von 42 zur Umsetzung anstehenden Vorschlägen wurde in der Folge sowohl vom EU-Rat als auch vom Nordatlantikrat gebilligt, und ein erster Bericht, demzufolge beträchtliche Fortschritte erzielt wurden, wurde im Juni 2017 vorgelegt.[6]

In dem im Juni 2017 vorgestellten Reflexionspapier der Kommission zur Zukunft der europäischen Verteidigung[7] werden verschiedene Szenarien erläutert. Es geht um die Frage, wie man mit den wachsenden Bedrohungen umgeht, mit denen Europa im Sicherheits- und Verteidigungsbereich konfrontiert ist, und wie Europa seine eigene Verteidigungsfähigkeit bis 2025 ausbauen kann. Bei allen drei Szenarien werden Sicherheit und Verteidigung als Elemente des europäischen Projekts betrachtet, die für den Schutz und die Förderung unserer Interessen innerhalb und außerhalb unserer Grenzen unerlässlich sind. Europa muss ein Garant für Sicherheit werden und Schritt für Schritt seine eigene Sicherheit gewährleisten. Kein Mitgliedstaat kann die künftigen Herausforderungen – und insbesondere die Abwehr hybrider Bedrohungen – allein bewältigen. Die Zusammenarbeit im Verteidigungs- und Sicherheitsbereich ist keine Option, sondern eine Notwendigkeit, wenn dafür gesorgt werden soll, dass ein „Europa, das schützt", Wirklichkeit wird.

Der Bericht soll Aufschluss geben über die bisherigen Fortschritte sowie über die nächsten Schritte zur Umsetzung der Maßnahmen, die in den vier im Gemeinsamen Rahmen vorgeschlagenen Bereichen geplant sind, nämlich verbessertes Lagebewusstsein, Stärkung der Resilienz, Stärkung der Fähigkeit der Mitgliedstaaten und der Union auf den Gebieten Krisenverhütung und -bewältigung und koordinierte Erholung von Krisen sowie Intensivierung der Zusammenarbeit mit der NATO zur Gewährleistung der Komplementarität von Maßnahmen. Er sollte in Verbindung mit den monatlichen Fortschrittsberichten mit dem Titel „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion" gelesen werden.

[5] Bratislava-Fahrplan des Europäischen Rats vom 16. September 2016 und Erklärung von Rom der führenden Vertreter von 27 EU-Mitgliedstaaten, des Europäischen Rates, des Europäischen Parlaments und der Europäischen Kommission vom 25. März 2017.
[6] http://www.consilium.europa.eu/de/press/press-releases/2017/06/19-conclusions-eu-nato-cooperation/
[7] Reflexionspapier zur Zukunft der europäischen Verteidigung, 7.6.2017, https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_de.pdf.

2. ERKENNEN DER HYBRIDEN NATUR EINER BEDROHUNG

Hybride Aktivitäten sind ein immer häufigeres Phänomen der europäischen Sicherheitsumgebung. Diese Aktivitäten nehmen stetig an Intensität zu und die Besorgnis wächst angesichts manipulierter Wahlen, Desinformationskampagnen, böswilliger Cyberaktivitäten und Urheber hybrider Akte, die versuchen, benachteiligte Mitglieder der Gesellschaft zu radikalisieren und zu Stellvertreterakteuren zu machen. Die Verwundbarkeit gegenüber hybriden Bedrohungen macht nicht vor nationalen Grenzen halt. Eine koordinierte Reaktion auf hybride Bedrohungen ist auch auf Ebene der EU und der NATO erforderlich. Die Entwicklungen seit April 2016 zeigen, dass Bedrohungen zwar weiterhin häufig isoliert betrachtet werden, man innerhalb der Union aber zunehmend anerkennt und versteht, dass einige beobachtete Aktivitäten hybrider Natur sind und ein koordiniertes Vorgehen erfordern. Die EU wird ihre Bemühungen zur Verbesserung des Lagebewusstseins und der Zusammenarbeit fortsetzen.

Maßnahme 1: Die Mitgliedstaaten werden aufgefordert, gegebenenfalls mit Unterstützung der Kommission und der Hohen Vertreterin eine Untersuchung über hybride Risiken zwecks Ermittlung einschlägiger Verwundbarkeiten – und spezifischer Indikatoren für hybride Bedrohungen – einzuleiten, die die nationalen und europaweiten Strukturen und Netze beeinträchtigen könnten.

Der Rat hat eine „Gruppe der Freunde des Vorsitzes“ eingesetzt, in der Sachverständige aus den Mitgliedstaaten gemeinsam eine Gesamtuntersuchung zusammenstellen, die diese in die Lage versetzen würde, wichtige Indikatoren für hybride Bedrohungen besser zu erkennen, diese in Frühwarnungs- und bestehende Risikobewertungsmechanismen einfließen zu lassen und gegebenenfalls weiterzugeben. Es kam zu einer Einigung hinsichtlich der Zuständigkeitsbereiche und die Arbeiten haben bereits begonnen. Die Gesamtuntersuchung sollte bis Ende 2017 abgeschlossen sein, die Einzeluntersuchungen werden im Anschluss daran stattfinden. Der Schutz vor hybriden Bedrohungen sollte zu einer gegenseitigen Stärkung führen. Daher werden die Mitgliedstaaten aufgefordert, diese Untersuchungen so rasch wie möglich durchzuführen, da sie wertvolle Informationen darüber liefern, wie verwundbar Europa ist und in welchem Umfang vorgesorgt wurde.

a. VERBESSERUNG DES BEWUSSTSEINS

Das Teilen nachrichtendienstlicher Analysen und Bewertungen ist ein zentrales Instrument, das zur Verringerung der Unsicherheit und zur Verbesserung des Lagebewusstseins dient. Im Verlauf des vergangenen Jahres wurden erhebliche Fortschritte erzielt. Die EU-Analyseeinheit für hybride Bedrohungen ist nach ihrer Gründung nun voll funktionsfähig, die East StratCom Task Force ist eingesetzt und Finnland hat das Europäische Zentrum zur Bewältigung hybrider Bedrohungen eingerichtet. Die Analyse der Instrumente und Hebel im Bereich Desinformation und Propaganda war sehr arbeitsaufwendig, die Kooperation zwischen EU StratCom Task Force East, der Analyseeinheit für hybride Bedrohungen und der NATO funktionierte reibungslos. Dies schafft eine gute Grundlage für das Entstehen einer Kultur, in der die Analyse und die Bewertung hybrider Bedrohungen für unsere innere und äußere Sicherheit aus einem einschlägigen Blickwinkel noch tiefer verwurzelt sind.

Analyseeinheit für hybride Bedrohungen

Maßnahme 2: Einrichtung einer EU-Analyseeinheit für hybride Bedrohungen („EU Hybrid Fusion Cell“) innerhalb des bestehenden Zentrums der Europäischen Union für Informationsgewinnung

und -analyse, die sowohl als geheim eingestufte als auch frei zugängliche Informationen über hybride Bedrohungen entgegennehmen und auswerten kann. Die Mitgliedstaaten werden aufgefordert, nationale Kontaktstellen für hybride Bedrohungen einzurichten, um für die Zusammenarbeit und eine sichere Kommunikation mit der EU-Analyseeinheit für hybride Bedrohungen zu sorgen.

Die EU-Analyseeinheit für hybride Bedrohungen wurde innerhalb des EU-Zentrums für Informationsgewinnung und -analyse eingerichtet; sie soll von verschiedenen Interessenträgern übermittelte, geheime und offen zugängliche Informationen über hybride Bedrohungen entgegennehmen und analysieren. Die Analysen werden anschließend innerhalb der EU und zwischen den Mitgliedstaaten geteilt und fließen in die EU-Entscheidungsprozesse ein; dazu gehören auch Beiträge zu Sicherheitsrisiko-Bewertungen, die auf EU-Ebene durchgeführt werden. Die Abteilung Aufklärung des Militärstabs der EU trägt mit militärischen Analysen zur Arbeit der Analyseeinheit bei. Bisher wurden mehr als 50 Bewertungen und Briefings zur Hybrid-Thematik erarbeitet. Seit Januar 2017 hat die Analyseeinheit regelmäßig das „Hybrid Bulletin" erstellt, in dem aktuelle Bedrohungen und einschlägige Fragen analysiert und mit dem die Organe und Einrichtungen der EU sowie den nationalen Kontaktstellen[8] direkt informiert werden. Die Analyseeinheit erreichte wie geplant im Mai 2017 ihre volle Funktionsfähigkeit. Außerdem stehen die Mitarbeiter mit Kollegen der neu eingerichteten NATO-Analyseeinheit für hybride Bedrohungen in Kontakt, wobei sowohl bei der Einrichtung der Analyseeinheit gewonnene Erkenntnisse als auch Informationen (unter vollständiger Einhaltung der EU-Vorschriften für den Austausch als geheim eingestufter Informationen) weitergegeben werden. Die EU-Analyseeinheit für hybride Bedrohungen beschäftigt sich gegenwärtig mit weiteren Initiativen zum Ausbau der künftigen Zusammenarbeit und wird eine Schlüsselrolle bei den im Herbst 2017 geplanten parallelen Übungen von EU und NATO spielen, in deren Rahmen die Reaktionsbereitschaft der Analyseeinheit für hybride Bedrohungen getestet und die gewonnenen Erfahrungen berücksichtigt werden.

Strategische Kommunikation

Maßnahme 3: Die Hohe Vertreterin wird zusammen mit den Mitgliedstaaten sondieren, wie die Kapazitäten für eine vorausschauende strategische Kommunikation modernisiert und koordiniert werden können und wie der Einsatz von Medienbeobachtungs- und Sprachspezialisten optimiert werden kann.

In den vergangenen Monaten waren massive Desinformationskampagnen und die systematische Verbreitung von Falschmeldungen in sozialen Medien eine von vielen Maßnahmen zur Destabilisierung von Gegnern. Wenn soziale Medien bevorzugt als Plattformen genutzt werden, können verlässlich und legitim erscheinende Informationen die öffentliche Meinung zugunsten einzelner Personen, Organisationen oder Regierungen beeinflussen. Solche hybriden Taktiken zielen zudem darauf ab, in unseren Gesellschaften Verwirrung zu stiften und die Glaubwürdigkeit unserer demokratischen Regierungen sowie unserer Strukturen, Einrichtungen und Wahlen in Misskredit zu bringen. Falschmeldungen werden häufig über Online-Plattformen verbreitet (siehe auch Maßnahme 17). Die Kommission und die Hohe Vertreterin begrüßen die Schritte, die Online-Plattformen und

[8] Bislang haben 21 Mitgliedstaaten nationale Kontaktstellen benannt. Die diesen angehörenden Personen sind in den Hauptstädten der Mitgliedstaaten in ihren Positionen mit der Hybrid- und Resilienz-Thematik befasst.

Medienunternehmen zur Bekämpfung von Fehlinformationen in jüngster Zeit unternommen haben. Die Kommission wird derartige freiwillige Maßnahmen weiterhin unterstützen.

Die Hohe Vertreterin hat die East StratCom Task Force eingerichtet, die Fehlinformationen und damit geführte Kampagnen voraussieht bzw. darauf reagiert. Auf diese Weise wird die Kommunikation über die Politiken der Union in den Ländern der östlichen Nachbarschaft erheblich verbessert und ein Beitrag zur Medienlandschaft in diesen Ländern geleistet. Die Taskforce hat in den vergangenen beiden Jahren in über 3000 Einzelfällen Fehlinformationen in 18 Sprachen aufgedeckt. Wenn die neue Website „*#EUvsdisinformation*" mit einer Online-Suchfunktion in Kürze zur Verfügung steht, wird sich der Zugang für die Nutzer deutlich verbessern. Durch die Forschungs- und Analysetätigkeit wird allerdings belegt, dass es wesentlich mehr Kanäle zur Verbreitung von Fehlinformationen und über diese täglich veröffentlichte Meldungen gibt. Das aus dem Programm „Horizont 2020" finanzierte Projekt „EU-STRAT" dient zur Politik- und Medienanalyse in den Ländern der östlichen Nachbarschaft.

Die Hohe Vertreterin fordert die Mitgliedstaaten auf, die Arbeit der StratCom Task Forces zu fördern und damit effizienter gegen wachsende hybride Bedrohungen vorzugehen. Dadurch wird die Task Force South dabei unterstützt, die Kommunikation und die Information der Öffentlichkeit in der arabischen Welt – auch auf Arabisch – zu verbessern, mit Falschmeldungen aufzuräumen und über die Europäische Union und ihre Politik sachlich zu informieren. Durch die Kooperation mit Journalisten vor Ort wird dazu beigetragen, dass die produzierten Nachrichten für den Kulturkreis adäquat aufbereitet sind. Beide Taskforces werden von der EU-Analyseeinheit für hybride Bedrohungen unterstützt und sollen die diesbezüglichen Anstrengungen der Mitgliedstaaten fördern und ergänzen. Außerdem kofinanziert die Kommission das Europäische Netzwerk für strategische Kommunikation, ein 26 Mitgliedstaaten umfassendes Kooperationsnetzwerk, in dem Analysen, bewährte Verfahren und Ideen über den Einsatz strategischer Kommunikation für die Bekämpfung des gewalttätigen Extremismus sowie von Fehlinformationen ausgetauscht werden.

Kompetenzzentrum für die „Abwehr hybrider Bedrohungen"

***Maßnahme 4:* Die Mitgliedstaaten werden aufgefordert, die Einrichtung eines Kompetenzzentrums für die „Abwehr hybrider Bedrohungen" zu erwägen.**

Finnland hat auf den Aufruf zur Einrichtung eines Kompetenzzentrums im April 2017 reagiert und das Europäische Zentrum zur Bewältigung hybrider Bedrohungen eingerichtet. Zehn Mitgliedstaaten der EU[9], Norwegen und die USA sind Mitglieder, und sowohl die Europäische Union als auch die NATO wurden gebeten, den Lenkungsausschuss[10] zu unterstützen. Zu den Aufgaben des Zentrums gehört es, den strategischen Dialog in Gang zu bringen sowie zusammen mit Interessengemeinschaften Forschungsarbeiten und Analysen durchzuführen, um die Resilienz und Reaktionsfähigkeit als Beitrag zur Abwehr hybrider Bedrohungen zu verbessern. In dem Zentrum sollen künftig außerdem Übungen zur Hybrid-Thematik stattfinden. Das Zentrum steht bereits in engem Kontakt mit der EU-Analyseeinheit für hybride Bedrohungen und die Arbeit der beiden Organisationen sollte sich gegenseitig ergänzen. Die EU prüft gegenwärtig, wie sie das Zentrum konkret unterstützen kann.

[9] Finnland, Frankreich, Deutschland, Lettland, Litauen, Polen, Schweden, Vereinigtes Königreich, Estland, Spanien.
[10] Weitere EU-Mitgliedstaaten und NATO-Verbündete können sich am Zentrum beteiligen.

b. AUFBAU VON RESILIENZ

Im Gemeinsamen Rahmen wird die Resilienz (z. B. in den Bereichen Verkehr, Kommunikation, Energie, Finanzen oder regionale Sicherheitsinfrastrukturen) in den Mittelpunkt des Handelns der EU gerückt, um Propaganda und Informationskampagnen, Versuchen der Untergrabung von Geschäftstätigkeiten, Gesellschaften und Wirtschaftsströmen sowie Angriffen auf Informationstechnologie und Cyber-Infrastrukturen zu begegnen. Die Stärkung der Resilienz wird als Vorbeugungs- und Abschreckungsmaßnahme angesehen, mit der Gesellschaften gestärkt und die Eskalation von Krisen sowohl innerhalb als auch außerhalb der EU verhindert werden können. Die EU bringt einen Mehrwert, indem sie die Mitgliedstaaten und Partner beim Aufbau ihrer Resilienz, für den auf eine Vielzahl bestehender Instrumente und Programme zurückgegriffen wird, unterstützt. Was die Maßnahmen zur Stärkung der Resilienz in Bereichen wie Cybersicherheit, kritische Infrastrukturen, Schutz des Finanzsystems vor illegaler Nutzung und Bekämpfung von gewalttätigem Extremismus und Radikalisierung betrifft, so wurden erhebliche Fortschritte erzielt.

Schutz kritischer Infrastrukturen

Maßnahme 5: Die Kommission wird in Zusammenarbeit mit den Mitgliedstaaten und Interessenträgern gemeinsame Instrumente, einschließlich entsprechender Indikatoren, zur Verbesserung des Schutzes und der Resilienz kritischer Infrastrukturen gegenüber hybriden Bedrohungen in relevanten Bereichen ermitteln.

Im Zusammenhang mit dem Europäischen Programm für den Schutz kritischer Infrastrukturen (EPSKI) brachte die Kommission die Erarbeitung gemeinsamer Instrumente, unter anderem von Indikatoren für die Verwundbarkeit, voran, um in relevanten Bereichen die Resilienz kritischer Infrastrukturen gegenüber hybriden Bedrohungen zu verbessern. Im Mai 2017 veranstaltete die Kommission einen Workshop über hybride Bedrohungen für kritische Infrastrukturen, an dem Vertreter aus beinahe allen Mitgliedstaaten, Betreiber kritischer Infrastrukturen, die EU-Analyseeinheit für hybride Bedrohungen und die NATO als Beobachter teilnahmen. Man verständigte sich auf einen gemeinsamen Fahrplan und Schritte für die künftigen Arbeiten. Grundlage dafür ist ein Fragebogen, der an die nationalen Behörden der Mitgliedstaaten verschickt wurde. Die Kommission wird im Herbst die Konsultation der Interessenträger fortsetzen, um bis Ende 2017 eine Einigung über die Indikatoren zu erzielen.

Die Europäische Verteidigungsagentur arbeitet daran, häufig auftretende Fähigkeiten- und Forschungsmängel zu ermitteln, die sich aus der engen Verknüpfung zwischen Energieinfrastrukturen und Verteidigungskapazitäten ergeben. Die Europäische Verteidigungsagentur wird im Herbst 2017 ein Konzeptpapier ausarbeiten und Pilotmaßnahmen für ganzheitliche Methoden entwickeln.

Verbesserung der Energieversorgungssicherheit der EU

Maßnahme 6: Die Kommission wird in Zusammenarbeit mit den Mitgliedstaaten Bemühungen zur Diversifizierung der Energieträger unterstützen und Standards für Sicherheit und Gefahrenabwehr zwecks Erhöhung der Resilienz der nuklearen Infrastrukturen fördern.

Die Kommission legte im Dezember 2016 mit dem Paket zur Versorgungssicherheit konkrete Vorschläge vor, und im April 2017 erzielten der Rat und das Europäische Parlament eine

Einigung über die neue Verordnung zur Gasversorgungssicherheit, mit der Krisen bei der Gasversorgung vorgebeugt werden soll. Die neuen Bestimmungen sorgen für einen gemeinsamen, regional koordinierten Ansatz der Mitgliedstaaten zur Sicherung der Gasversorgung. Dadurch kann sich die EU besser auf Störungen der Gasversorgung im Krisenfall oder auf einen hybriden Angriff einstellen und mit diesen Situationen umgehen. Erstmals gilt dabei auch das Solidaritätsprinzip: Die Mitgliedstaaten werden in der Lage sein, Nachbarn bei einer schweren Krise oder einem Angriff zu unterstützen, sodass europäische Haushalte und Unternehmen vor Ausfällen verschont bleiben.

Die EU erzielte auch bei der Entwicklung zentraler Projekte zur Diversifizierung der Energieversorgungswege und -quellen im Einklang mit der Rahmenstrategie für die Energieunion und der Europäischen Strategie für Energieversorgungssicherheit Fortschritte. Beispielsweise finden am südlichen Gastransportkorridor Bauarbeiten für alle wichtigen Rohrleitungsprojekte statt: Erweiterung der Süd-Kaukasus-Pipeline, der Transanatolischen und der Transadriatischen Pipeline, der Pipeline oberhalb des Shah-Denis-Gasfelds sowie Ausweitung des südlichen Gastransportkorridors nach Zentralasien, insbesondere nach Turkmenistan. Die Flüssiggaseinfuhren nach Europa nehmen zu und stammen von neuen Lieferanten, wie zum Beispiel den USA. Das Beispiel des Terminals in Litauen zeigt, wie die Abhängigkeit von einem einzigen Lieferanten durch Diversifizierungsprojekte verringert werden kann. Verstärkte Anstrengungen im Energiebereich und eine bessere Nutzung der einheimischen – und insbesondere erneuerbaren – Energiequellen tragen ebenfalls zur Diversifizierung der Energieversorgungswege und -quellen bei.

Bei der nuklearen Sicherheit unterstützt die Kommission – vor allem im Rahmen von Workshops mit nationalen Stellen und Regulierungsbehörden – aktiv eine einheitliche und wirksame Durchführung der beiden Richtlinien über nukleare Sicherheit und grundlegende Sicherheitsnormen, die die Mitgliedstaaten bis Ende 2017 bzw. 2018 umsetzen müssen. Überdies wird durch das Euratom-Programm für Forschung und Ausbildung ein Beitrag zur Verbesserung der nuklearen Sicherheit geleistet.

Verkehr und Lieferketten

Maßnahme 7: Die Kommission wird neue Bedrohungen im Verkehrssektor überwachen und die Rechtsvorschriften erforderlichenfalls aktualisieren. Bei der Durchführung der EU-Strategie für maritime Sicherheit und der Strategie und der Aktionspläne der EU für das Zollrisikomanagement werden die Kommission und die Hohe Vertreterin (im Rahmen ihrer jeweiligen Zuständigkeiten) in Abstimmung mit den Mitgliedstaaten prüfen, wie hybriden Bedrohungen, insbesondere in Bezug auf kritische Verkehrsinfrastrukturen, begegnet werden kann.

Im Einklang mit der Mitteilung zur Sicherheitsunion liefert die Kommission mit den Mitgliedstaaten, dem Zentrum der Europäischen Union für Informationsgewinnung und -analyse und einschlägigen Agenturen Bewertungen der Sicherheitsrisiken auf EU-Ebene, um Bedrohungen für die Sicherheit der Verkehrssysteme zu identifizieren und die Entwicklung wirksamer und angemessener Risikominderungsmaßnahmen zu fördern. Der Abschuss einer Maschine der Malaysia Airlines (Flugnummer MH17) über der Ostukraine im Jahr 2014 machte die Risiken des Überflugs von Konfliktgebieten deutlich: Die Kommission hat gemäß den Empfehlungen der Europäischen Hochrangigen Taskforce zu Krisengebieten[11] mit

[11] https://www.easa.europa.eu/system/files/dfu/208599_EASA_CONFLICT_ZONE_CHAIRMAN_REPORT_no_B_update.pdf

Unterstützung nationaler Luftverkehrs- und Sicherheitsfachleute und des EAD eine Methode für die „gemeinsame EU-Risikobewertung“ entwickelt, mit der als geheim eingestufte Informationen ausgetauscht und ein gemeinsames Risikoszenario definiert werden können. Im März 2017 gab die Europäische Agentur für Flugsicherheit (EASA) auf der Grundlage der Ergebnisse dieser gemeinsamen EU-Risikobewertung das erste Informationsblatt zu Konfliktzonen (Conflict Zone Information Bulletin)[12] heraus. Die Kommission erwägt eine Ausweitung der Risikobewertungstätigkeiten, die im Bereich der Flugsicherheit durchgeführt werden, auf andere Verkehrsträger (z. B. Schienenverkehr, Seeverkehr) und wird 2018 diesbezügliche Vorschläge unterbreiten. Im Juni 2017 brachten die Kommission, der EAD und die Mitgliedstaaten ein Risikobewertungsprojekt zum Thema Sicherheit des Eisenbahnverkehrs auf den Weg, mit dem Lücken und etwaige Maßnahmen zur Gefahreneindämmung ermittelt werden sollen.

Bei den Sicherheitsforschungsprojekten, die Zuge des 7. Rahmenprogramms und von Horizont 2020 erfolgten, werden ebenfalls große Anstrengungen in den Bereichen Luftsicherheit und Flugverkehrsmanagement (ATM) unternommen. Im Bereich der zivilen Luftfahrt entwickelt die Kommission gemeinsam mit der Europäischen Agentur für Flugsicherheit und Interessenträgern derzeit zwei neue Initiativen zur Erhöhung der Cybersicherheit, die auch auf hybride Bedrohungen abzielen: die Einrichtung eines IT-Notfallteams für den Luftverkehr sowie einer Taskforce für Cybersicherheit im Rahmen des gemeinsamen Unternehmens zur Entwicklung des europäischen Flugverkehrsmanagementsystems der neuen Generation (Single European Sky Air Traffic Management Research – SESAR), das für das Verkehrsmanagement im einheitlichen europäischen Luftraum zuständig ist. Die Europäische Verteidigungsagentur liefert dem gemeinsamen Unternehmen SESAR militärische Informationen über Cybersicherheit im Luftverkehr, auch der Europäischen Agentur für Flugsicherheit werden über die „Europäische strategische Koordinierungsplattform für Cybersicherheit“, die auf Ersuchen der Mitgliedstaaten und der Industrie die Abstimmung aller Luftverkehrsaktivitäten auf EU-Ebene erleichtern wird, Informationen zur Verfügung gestellt. Im Einklang mit dem Fahrplan für die Cybersicherheit für den Luftverkehr analysierte die Europäische Agentur für Flugsicherheit 2016 die Lücken in den bestehenden Regelungen und nahm die notwendigen Festlegungen im Hinblick auf das Europäische Zentrum für Cybersicherheit im Luftverkehr und dessen Einrichtung vor; dieses Zentrum hat inzwischen seine Tätigkeit aufgenommen, erstellt in Kooperation mit dem IT-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der EU (CERT-EU) Bedrohungsanalysen für den Luftverkehr (das diesbezügliche Memorandum of Understanding wurde im Februar 2017 unterzeichnet) und kooperiert mit EUROCONTROL (Fahrplan für die Zusammenarbeit wurde angenommen); gleichzeitig wurde eine Website für die Verbreitung öffentlich zugänglicher Analysen entwickelt. Im Herbst 2017 werden ein Normungsprogramm und ein sicherer Informationsaustausch beschlossen.

Zollrisikomanagement

Im Bereich Zoll konzentriert sich die Kommission darauf, das System für die Analyse von Vorabinformationen für Frachtgut und das Zollrisikomanagementsystem entscheidend zu verbessern. Damit wird das gesamte Spektrum der Zollrisiken abgedeckt, auch was Bedrohungen für die Sicherheit und Integrität internationaler Lieferketten und einschlägiger

[12] https://ad.easa.europa.eu/czib-docs/page-1

kritischer Infrastrukturen betrifft (z. B. direkte von Einfuhren ausgehende Bedrohungen für Seehafenanlagen, Flughäfen und Landgrenzen). Mit den Systemverbesserungen soll sichergestellt werden, dass die Zollbehörden in der EU von den Händlern alle erforderlichen Informationen über den Warenverkehr erhalten; dass sie diese Informationen effizienter zwischen den Mitgliedstaaten austauschen können; dass sie sowohl gemeinsame als auch spezifische Risikovorschriften der Mitgliedstaaten anwenden und dass sie bei risikobehafteten Lieferungen gezielter eingreifen können, indem sie intensiver mit anderen Behörden, insbesondere mit sonstigen Strafverfolgungs- und Sicherheitsstellen, zusammenarbeiten. Die für diese Systemverbesserung durch die Kommission erforderlichen IT-Entwicklungen befinden sich in der Anfangsphase und die auf zentraler Ebene relevanten Investitionen werden in den kommenden Monaten anlaufen.

Weltraum

Maßnahme 8: Im Rahmen der Weltraumstrategie und des Europäischen Aktionsplans im Verteidigungsbereich wird die Kommission vorschlagen, die Resilienz der Weltrauminfrastrukturen gegen hybride Bedrohungen zu stärken, insbesondere durch eine mögliche Ausweitung des Anwendungsbereichs der Beobachtung und Verfolgung von Objekten im Weltraum auf hybride Bedrohungen, durch Vorbereitung der nächsten Generation der staatlichen Satellitenkommunikation auf europäischer Ebene und durch Einsatz von Galileo für kritische Infrastrukturen, die von zeitlicher Synchronisierung abhängen.

Die Kommission bezieht bei der Ausarbeitung des Regelungsrahmens für staatliche Satellitenkommunikation (GovSatCom) sowie bei der Beobachtung und Verfolgung von Objekten im Weltraum im Jahr 2018 Aspekte der Resilienz gegenüber hybriden Bedrohungen in ihre Bewertung ein. Im Einklang mit der Weltraumstrategie wird die Kommission im Zuge der Vorbereitungen zur Weiterentwicklung von Galileo und Copernicus prüfen, in welchem Umfang diese dazu beitragen, dass kritische Infrastrukturen weniger verwundbar werden. Der Evaluierungsbericht sollte im Herbst 2017 abgeschlossen sein, der Vorschlag für die nächste Generation von Copernicus und Galileo im Jahr 2018. Die Europäische Verteidigungsagentur arbeitet an kollaborativen Kapazitätsentwicklungsprojekten in den Bereichen satellitengestützte Kommunikation, Ortung, Navigation und Zeitbestimmung für das Militär sowie Erdbeobachtung. Bei allen Projekten werden Resilienz-Anforderungen angesichts gegenwärtiger und neu aufkommender hybrider Bedrohungen im Mittelpunkt stehen.

Verteidigungsfähigkeiten

Maßnahme 9: Die Hohe Vertreterin wird in Abstimmung mit der Kommission und gegebenenfalls mit Unterstützung der Mitgliedstaaten Projekte zu Möglichkeiten der Anpassung der Verteidigungsfähigkeiten und zur Entwicklung von Verteidigungsfähigkeiten mit EU-Relevanz vorschlagen, insbesondere zur Abwehr hybrider Bedrohungen eines oder mehrerer Mitgliedstaaten.

Die Europäische Verteidigungsagentur führte 2016 und 2017 drei Planübungen mit Szenarien hybrider Bedrohung durch, an denen sich auch die Kommission, der EAD und Sachverständige aus den Mitgliedstaaten beteiligten. Die Ergebnisse werden in den überarbeiteten Plan zur Fähigkeitenentwicklung einfließen, sodass die sich daraus ergebenden zentralen Fähigkeitenentwicklungen, die zur Abwehr hybrider Bedrohungen erforderlich sind, künftig Teil der neuen EU-Prioritäten zur Fähigkeitenentwicklung sein werden. Bei der Überarbeitung des Bedarfskatalogs 2005 wird die Dimension der hybriden Bedrohung berücksichtigt werden. Im April 2017 schloss die Europäische Verteidigungsagentur die Erstellung eines Analyseberichts über militärische Aspekte ab, die sich aus hybriden

Angriffen auf kritische Hafeninfrastruktur ergeben, der im Oktober 2017 bei einem Workshop mit Seefahrtexperten erörtert wird. Für 2018 ist eine weitere spezifische Analyse der militärischen Aspekte im Zusammenhang mit der Abwehr von Minidrohnen geplant. Außerdem könnten Prioritäten bei Fähigkeiten zur Stärkung der Resilienz gegenüber hybriden Bedrohungen, die von den Mitgliedstaaten ermittelt wurden, ebenfalls für eine Unterstützung im Rahmen des Europäischen Verteidigungsfonds ab 2019 infrage kommen. Die Kommission appelliert an die Mitgesetzgeber, eine reibungslose Annahme zu gewährleisten, und ersucht die Mitgliedstaaten, Vorschläge für Fähigkeitenprojekte zur Verbesserung der Resilienz der EU gegenüber hybriden Bedrohungen zu unterbreiten.

***Maßnahme 10*: Die Kommission wird in Zusammenarbeit mit den Mitgliedstaaten das Bewusstsein für und die Resilienz gegenüber hybriden Bedrohungen im Rahmen der bestehenden Bereitschafts- und Koordinierungsmechanismen, insbesondere des Gesundheitssicherheitsausschusses, verbessern.**

Zur Verbesserung von Vorsorge und Resilienz angesichts hybrider Bedrohungen und im Interesse des Kapazitätsaufbaus innerhalb von Gesundheits- und Lebensmittelversorgungssystemen unterstützt die Kommission die Mitgliedstaaten durch Schulungen und Simulationsübungen sowie durch die Förderung des Austauschs von auf Erfahrungen beruhenden Leitlinien und die Finanzierung gemeinsamer Aktionen. Dies geschieht insbesondere auf der Grundlage des EU-Rahmens für Gesundheitssicherheit im Fall schwerwiegender grenzüberschreitender Gesundheitsgefahren und des Gesundheitsprogramms zur Umsetzung der internationalen Gesundheitsvorschriften, einer für 196 Länder (darunter die Mitgliedstaaten) verbindlichen Rechtsgrundlage, mit der weltweit akuten und grenzübergreifenden Risiken für die öffentliche Gesundheit vorgebeugt und auf diese reagiert werden soll. Die Dienststellen der Kommission werden im Herbst 2017 eine Übung zu komplexen und multidimensionalen hybriden Bedrohungen durchführen, um die sektorübergreifende Vorsorge und Reaktion im Gesundheitswesen zu testen. Die Kommission und die Mitgliedstaaten bereiten im Hinblick auf eine Verbesserung der Impfstoffversorgung und der Gesundheitssicherheit auf EU-Ebene (2018-2020) eine gemeinsame Maßnahme zur Impfung vor, die auch die Vorhersage von Angebot und Nachfrage bei Impfstoffen sowie Forschungsarbeiten über innovative Verfahren zur Herstellung von Impfstoffen umfasst. Die Kommission arbeitet ferner mit der Europäischen Behörde für Lebensmittelsicherheit und dem Europäischen Zentrum für die Prävention und die Kontrolle von Krankheiten zusammen, um sich auf fortschrittliche wissenschaftliche Untersuchungsmethoden einzustellen, um Gesundheitsgefahren und deren Ursachen genauer zu ermitteln und damit Ausbrüche im Zusammenhang mit der Lebensmittelsicherheit rasch in den Griff zu bekommen. Mit der „Globalen Forschungszusammenarbeit für die Handlungsbereitschaft gegenüber Infektionskrankheiten“ hat die Kommission ein Förderungsnetzwerk eingerichtet, damit die Forschung im Falle eines signifikanten Ausbruchs innerhalb von 48 Stunden koordiniert reagieren kann.

***Maßnahme 11*: Die Kommission legt den Mitgliedstaaten nahe, vorrangig für die Schaffung und uneingeschränkte Nutzung eines Netzes der 28 CSIRT und des CERT-EU (IT-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der EU) und eines Rahmens für die strategische Zusammenarbeit zu sorgen. Die Kommission sollte in Abstimmung mit den Mitgliedstaaten sicherstellen, dass sektorspezifische Initiativen gegen Cyberbedrohungen (z. B. in den Bereichen Luftverkehr, Energie und Seeverkehr) mit den unter die NIS-Richtlinie fallenden sektorübergreifenden Kapazitäten für die Bündelung von Informationen und Fachwissen und die Koordinierung der raschen Reaktion auf Vorfälle kompatibel sind.**

Der jüngsten weltweiten Cyberangriffe, bei denen mit Ransomware und Schadsoftware Tausende Computersysteme lahmgelegt wurden, haben erneut deutlich gemacht, dass die Resilienz gegenüber Cyberangriffen und die Sicherheitsmaßnahmen der EU dringend verstärkt werden müssen. Wie in der Halbzeitbewertung zum digitalen Binnenmarkt angekündigt, überprüfen die Kommission und die Hohe Vertreterin nun die Cybersicherheitsstrategie der EU aus dem Jahr 2013, und zwar im Wege der Annahme eines Pakets, das im September 2017 vorgelegt werden soll. Damit wird angestrebt, diesen Bedrohungen wirksamere sektorübergreifende Reaktionen entgegenzusetzen und auf diese Weise das Vertrauen in die digitale Gesellschaft und Wirtschaft zu erhöhen. Ferner wird das Mandat der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) überarbeitet werden, um ihre Rolle im veränderten „Ökosystem der Cybersicherheit" zu definieren. Der Europäische Rat[13] hat das Vorhaben der Kommission begrüßt, die Cybersicherheitsstrategie zu überarbeiten.

Die Annahme der Richtlinie zur Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie)[14] im Juli 2016 war ein wichtiger Schritt, der uns der angestrebten Resilienz gegenüber Cyberangriffen auf europäischer Ebene ein Stück näher bringt. Mit der Richtlinie werden erstmals EU-weite Regelungen für die Cybersicherheit festgelegt, die Fähigkeiten zur Gewährleistung der Cybersicherheit verbessert und die Zusammenarbeit zwischen den Mitgliedstaaten verstärkt. Unter anderen werden damit Unternehmen in kritischen Sektoren verpflichtet, geeignete Sicherheitsmaßnahmen zu ergreifen und jeden ernsten Cybervorfall an die zuständige nationale Behörde zu melden. Zu den betroffenen Sektoren gehören die Bereiche Energie, Verkehr, Wasserversorgung, das Gesundheits- und das Bankwesen sowie die Finanzmarktinfrastrukturen. Im Fall von digitalen Marktplätzen, Cloud-Computing-Diensten und Suchmaschinen müssen ähnliche Schritte unternommen werden. Die (von der Kommission 2016 eingesetzte) Kooperationsgruppe für Netz- und Informationssicherheit, deren Auftrag in der Verhinderung einer Marktfragmentierung besteht, wird grenz- und sektorübergreifend für eine kohärente Umsetzung sorgen. In diesem Zusammenhang bildet die Richtlinie über Netz- und Informationssicherheit den Bezugsrahmen für alle sektoralen Initiativen im Bereich der Cybersicherheit. Ferner wird mit der Richtlinie das Netzwerk von Computer-Notfallteams (CSIRT) eingerichtet, das alle einschlägigen Interessenträger vereint. Gleichzeitig überwachen die Kommission und CERT-EU aktiv die Cyberbedrohungslage und gewährleisten durch den Informationsaustausch mit nationalen Behörden die Sicherheit der IT-Systeme der EU-Organe und ihre Resilienz gegenüber Cyberangriffen. Im Mai 2017 bot der Vorfall um die Ransomware „WannaCry" die erste Gelegenheit, bei der dieses Netzwerk den Informationsaustausch und die Zusammenarbeit im Wege einer entsprechenden Beratungstätigkeit in der Praxis erproben konnte. Das IT-Notfallteam der EU stand in engem Kontakt mit dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3) bei Europol, den Reaktionsteams für Computersicherheitsverletzungen (Computer Security Incident Response Teams – CSIRT) der betroffenen Länder, Einrichtungen zur Bekämpfung der Cyberkriminalität und maßgeblichen Partnern aus der Industrie, um die Bedrohung einzudämmen und die Opfer zu unterstützen. Durch den Austausch nationaler Lageberichte entstand ein gemeinsames Lagebewusstsein innerhalb der EU. Aufgrund dieser Erfahrung war das Netzwerk besser für die nächsten Zwischenfälle (z. B. „NonPetya") gerüstet. Man stieß auch auf mehrere Herausforderungen, an deren Bewältigung gearbeitet wird.

[13] Schlussfolgerungen des Europäischen Rates vom 22. und 23. Juni 2017.

[14] 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).

<u>Maßnahme 12</u>: Die Kommission wird in Abstimmung mit den Mitgliedstaaten gemeinsam mit der Industrie im Rahmen einer vertraglichen öffentlich-privaten Partnerschaft für Cybersicherheit die Entwicklung und Erprobung von Technologien vorantreiben, um die Nutzer und die Infrastrukturen besser vor den Cyberaspekten hybrider Bedrohungen zu schützen.

Im Juli 2016 unterzeichnete die Kommission in Abstimmung mit den Mitgliedstaaten mit der Industrie eine vertragliche öffentlich-private Partnerschaft für Cybersicherheit zur Entwicklung und Erprobung von Technologien, in die sie bis zu 450 Mio. EUR aus dem Rahmenprogramm für Forschung und Innovation „Horizont 2020" investiert, um die Nutzer und die Infrastrukturen besser vor Cyberbedrohungen und Bedrohungen hybrider Natur zu schützen. Die Partnerschaft mündete in die erste europaweite strategische Forschungsagenda, die auf eine größere Resilienz kritischer Infrastrukturen sowie den Schutz der Bürgerinnen und Bürger vor Cyberangriffen ausgerichtet ist. Die Partnerschaft führte zu einer besseren Abstimmung unter den Interessenträgern, was mehr Effizienz und Wirksamkeit bei der Finanzierung der Cybersicherheit im Rahmen von Horizont 2020 brachte. Die Partnerschaft arbeitet gleichzeitig an Fragen der Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnologien und an Möglichkeiten zur Beseitigung des auf dem Markt herrschenden akuten Mangels an qualifizierten Fachkräften für Cybersicherheit. Da dringend zivile Forschung betrieben werden muss und hohe Resilienz im Bereich Verteidigung erforderlich ist, leistet die Cyberforschungs- und Technologiegruppe der Europäischen Verteidigungsagentur Beiträge zu den von der Europäischen Cybersicherheitsorganisation in ihrer Agenda für strategische Forschung und Innovation ermittelten Forschungsbereichen.

<u>Maßnahme 13</u>: Die Kommission wird Leitlinien für Eigentümer intelligenter Netze herausgeben, um die Cybersicherheit ihrer Anlagen zu verbessern. Im Rahmen der Initiative für die Neugestaltung des Strommarktes wird die Kommission erwägen, „Risikovorsorgepläne" und Verfahrensregeln für den Informationsaustausch und die Gewährleistung der Solidarität zwischen den Mitgliedstaaten im Krisenfall vorzuschlagen, einschließlich Vorschriften über die Verhinderung und Eindämmung von Cyberangriffen.

Im Energiesektor arbeitet die Kommission eine sektorale Strategie zur Cybersicherheit aus, die auch die Einrichtung einer Energieexperten-Plattform zur Cybersicherheit für eine bessere Umsetzung der NIS-Richtlinie vorsieht. Im Februar 2017 wurden zur Unterstützung dieser Plattform die besten verfügbaren Technologien zur Erhöhung des Niveaus der Cybersicherheit für intelligente Verbrauchserfassungssysteme in einer Studie ermittelt. Außerdem hat die Kommission die webbasierte Plattform „*Incident and Threat Information Sharing EU Centre*" (ITIS-EUC) eingerichtet, über die Informationen über Cyberbedrohungen und -vorfälle im Energiesektor analysiert und ausgetauscht werden.

<u>Verbesserung der Resilienz des Finanzsektors gegenüber hybriden Bedrohungen</u>

<u>Maßnahme 14</u>: Die Kommission wird in Zusammenarbeit mit der ENISA[15], den Mitgliedstaaten, zuständigen internationalen, europäischen und nationalen Behörden und Finanzinstitutionen Plattformen und Netze für den Informationsaustausch über Bedrohungen fördern und Faktoren angehen, die den Austausch solcher Informationen behindern.

[15] Agentur der Europäischen Union für Netz- und Informationssicherheit.

Nachdem die Kommission erkannt hatte, dass Cyberbedrohungen zu den größten Risiken für die finanzielle Stabilität zählen, überarbeitete sie den Regelungsrahmen für Zahlungsdienste in der Europäischen Union, der jetzt umgesetzt werden soll. Die überarbeitete Richtlinie über Zahlungsdienste[16] enthält neue Bestimmungen zur Erhöhung der Sicherheit von Zahlungsinstrumenten und über die starke Kundenauthentifizierung; sie soll Betrugshandlungen insbesondere bei Online-Zahlungen eindämmen. Der neue Rechtsrahmen wird ab Januar 2018 gelten. Derzeit entwickelt die Kommission mit Unterstützung der Europäischen Bankenaufsichtsbehörde und in Abstimmung mit Interessenträgern technische Regulierungsstandards, deren Veröffentlichung für Ende 2017 vorgesehen ist und die die starke Kundenauthentifizierung und sichere Kommunikation im Interesse der Sicherheit von Zahlungsvorgängen zum Gegenstand haben. Ferner hat die Kommission im internationalen Bereich eng mit den jeweiligen G7-Partnern an den im Oktober 2016 von den Finanzministern der G7 und den Vorsitzenden der Zentralbanken verabschiedeten G7-Grundsätzen zur Cyber-Sicherheit für den Finanzsektor (G7 fundamental principles of cyber security in the financial sector) zusammengearbeitet. Diese Grundsätze sind an (öffentliche und private) Unternehmen der Finanzbranche gerichtet und tragen innerhalb des Finanzsektors zu einem koordinierten Ansatz in Bezug auf Cybersicherheit bei, damit – auch immer gefährlichere und komplexere – Cyberbedrohungen gemeinsam angegangen werden können.

Verkehr

Maßnahme 15: Die Kommission und die Hohe Vertreterin werden (im Rahmen ihrer jeweiligen Zuständigkeiten) in Abstimmung mit den Mitgliedstaaten prüfen, wie auf hybride Bedrohungen reagiert werden kann, insbesondere im Zusammenhang mit Cyberangriffen im Verkehrssektor.

Die Umsetzung des Aktionsplans für die EU-Strategie für maritime Sicherheit[17] wird dazu beitragen, die Abschottungsmentalität beim Informationsaustausch und bei der gemeinsamen Nutzung von Vermögenswerten durch Zivil- und Militärbehörden abzubauen. Dank eines behördenübergreifenden Ansatzes arbeiten die einzelnen Akteure verstärkt zusammen. Bis Ende 2017 sollen die Arbeiten an einer gemeinsamen strategischen Agenda der Kommission und des EAD für zivile und militärische Forschung mit einem Workshop über den Schutz kritischer maritimer Infrastrukturen abgeschlossen werden. Diese Arbeiten könnten künftig auf die neu entstehende Bedrohung für Unterwasserrohrleitungen, Energietransfer sowie Glasfaser- und herkömmliche Kommunikationsnetze ausgeweitet werden, die von Störungen außerhalb der nationalen Hoheitsgewässer ausgeht.

In einer vor Kurzem durchgeführten Studie[18] wurde die Risikobewertungskapazität der nationalen Behörden bewertet, die Küstenschutzaufgaben wahrnehmen. Darin wurden die wichtigsten Hindernisse für die Zusammenarbeit ermittelt und praktische Empfehlungen zur Verbesserung der Zusammenarbeit zwischen Seebehörden auf EU- und nationaler Ebene in diesem spezifischen Bereich formuliert. Die Risikobewertung ist für die Abwehr von

[16] Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt (ABl. L 337 vom 23.12.2015, S. 35).

[17] https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf und der 2. Bericht über die Umsetzung des Aktionsplans für die EU-Strategie für maritime Sicherheit, der den Mitgliedstaaten am 21. Juni 2017 vorgestellt wurde.

[18] Studie zur Evaluierung der Risikobewertungskapazität auf Ebene der Behörden der Mitgliedsaaten, die Aufgaben der Küstenwache wahrnehmen („Evaluation of risk assessment capacity at the level of Member States' authorities performing coast guard functions"), 2017, https://ec.europa.eu/maritimeaffairs/documentation/studies

Bedrohungen für den Seeverkehr und in noch größerem Maße für die Evaluierung und Prävention hybrider Bedrohungen von großer Bedeutung, da dies zusätzliche und komplexere Erwägungen erfordert. Die Ergebnisse dieser Studie werden in verschiedenen Küstenschutz-Foren präsentiert, damit die vorgeschlagenen Empfehlungen bewertet und umgesetzt werden können, um die Zusammenarbeit in diesem Bereich zu verbessern; Vorsorge und Reaktion hinsichtlich hybrider Bedrohungen sind dabei die wichtigsten Ziele.

Bekämpfung der Terrorismusfinanzierung

Maßnahme 16: Die Kommission wird bei der Umsetzung des Aktionsplans gegen Terrorismusfinanzierung auch die Abwehr hybrider Bedrohungen berücksichtigen.

Die Urheber hybrider Bedrohungen und ihre Unterstützer sind für die Umsetzung ihrer Pläne auf Finanzmittel angewiesen. Die Anstrengungen der EU im Kampf gegen Verbrechen und Terrorismusfinanzierung im Rahmen der Europäischen Sicherheitsagenda sowie des Aktionsplans gegen Terrorismusfinanzierung können ebenfalls zur Abwehr hybrider Bedrohungen beitragen. Im Dezember 2016 legte die Kommission drei Legislativvorschläge vor, die strafrechtliche Sanktionen für Geldwäsche und unerlaubte Bargeld-Zahlungen sowie die Sicherstellung und die Einziehung von Vermögenswerten zum Gegenstand hatten[19].
Bis zum 26. Juni 2017 hatten die Mitgliedstaaten zur Umsetzung der 4. Geldwäscherichtlinie[20] Zeit, und im Juli 2016 legte die Kommission einen konkreten Legislativvorschlag vor, um die Richtlinie um zusätzliche Maßnahmen[21] zu ergänzen und damit zu verschärfen.

Am 26. Juni 2017 veröffentlichte die Kommission die in der 4. Geldwäscherichtlinie vorgesehene supranationale Risikobewertung. Außerdem brachte sie einen Vorschlag für eine Verordnung zur Verhinderung der Einfuhr und der Lagerung von unrechtmäßig aus einem Drittland ausgeführten Kulturgütern in der EU[22] auf den Weg. Im weiteren Jahresverlauf wird ein Bericht darüber folgen, wie die Kommission den Bedarf an zusätzlichen Maßnahmen zur Aufdeckung der Finanzierungskanäle des Terrorismus in der EU einschätzt. Ferner überprüft die Kommission die Rechtsvorschriften zur Betrugsbekämpfung und zu Betrug und Fälschung im bargeldlosen Zahlungsverkehr[23].

Der Achte Bericht über **Fortschritte auf dem Weg zu einer wirksamen und echten Sicherheitsunion** enthält weitere Einzelheiten über die Fortschritte bei der Umsetzung des Aktionsplans zur Bekämpfung der Terrorismusfinanzierung.

[19] Dritter Fortschrittsbericht „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion“, COM(2016) 831 final.
[20] Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission (Text von Bedeutung für den EWR, ABl. L 141 vom 5.6.2015, S. 73).
[21] Einzelheiten sind dem Dritten Fortschrittsbericht „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion“ (COM(2016) 831 final) und dem Achten Fortschrittsbericht „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion“ (COM(2017) 354 final) zu entnehmen.
[22] COM(2017) vom 26.6.2017, COM(2017) 340 final, SWD(2017) 275 final 0.
[23] Achter Fortschrittsbericht „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion“, COM(2017) 354 final.

Förderung gemeinsamer Werte der EU sowie inklusiver, offener und resilienter Gesellschaften

Stärkung der Resilienz gegen Radikalisierung und gewalttätigen Extremismus

Eine religiöse und ideologische Radikalisierung, ethnische Auseinandersetzungen und Minderheitenkonflikte können von externen Akteuren durch die Unterstützung bestimmter Gruppierungen oder durch die Anstachelung von Konflikten zwischen einzelnen Gruppen ausgelöst werden. Es sind weitere Herausforderungen hinzugekommen, etwa die Bedrohung durch Einzeltäter, neue Wege der Radikalisierung, möglicherweise auch im Zusammenhang mit der Flüchtlingskrise, sowie der Aufschwung des Rechtsextremismus (der mit Gewalt gegen Migranten einhergeht) und Polarisierungsrisiken. Die Arbeit zur Bekämpfung der Radikalisierung wird im Kontext der Sicherheitsunion vorangetrieben und könnte bezüglich der hybriden Bedrohungen auch insofern indirekt relevant sein, als für eine Radikalisierung empfängliche Personen durch Urheber hybrider Bedrohungen manipuliert werden könnten.

Maßnahme 17: ***Die Kommission führt die in der Europäischen Sicherheitsagenda genannten Maßnahmen gegen Radikalisierung durch und prüft die Notwendigkeit, die Verfahren zur Entfernung illegaler Inhalte auszubauen; gleichzeitig appelliert sie an die Sorgfaltspflicht der Mittler bei der Verwaltung der Netze und Systeme.***

Radikalisierungsprävention

Die Kommission setzt ihre vielfältigen Maßnahmen zur Bekämpfung der Radikalisierung weiter um, wie in der im Juni 2016 vorgestellten Mitteilung zur Unterstützung der Prävention von Radikalisierung, die zu extremistisch motivierter Gewalt führt[24], dargelegt wird, in der wichtige Maßnahmen vorgesehen sind: inklusive Bildung und gemeinsame europäischen Werte sollen gefördert und Online-Propaganda mit extremistischen Inhalten und Radikalisierung in Haftanstalten bekämpft werden, daneben soll die Zusammenarbeit mit Drittländern verstärkt und die Forschung intensiviert werden, um das sich ständig verändernde Phänomen der Radikalisierung besser zu verstehen und eine bessere Grundlage für strategische Antworten zu erhalten. Das Aufklärungsnetzwerk gegen Radikalisierung (RAN) hat maßgeblich zu den Bemühungen der Kommission beitragen, die Mitgliedstaaten auf diesem Gebiet durch die Zusammenarbeit mit Praktikern vor Ort auf der Ebene der Gemeinschaften zu unterstützen. Weitere Einzelheiten enthält der Achte Fortschrittsbericht „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion“[25].

Radikalisierung im Internet und Hetze

Die Kommission setzt sich im Einklang mit der Europäischen Sicherheitsagenda[26] dafür ein, dass weniger illegale Inhalte im Internet abrufbar sind und kooperiert hierfür vor allem mit der EU-Meldestelle für Internetinhalte bei Europol und dem EU-Internetforum.[27] Auch dank

[24] http://ec.europa.eu/dgs/education_culture/repository/education/library/publications/2016/communication-preventing-radicalisation_en.pdf

[25] COM(2017) 354 final.

[26] Weitere Einzelheiten enthält der Achte Fortschrittsbericht „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion“, COM(2017) 354 final.

[27] Weitere Einzelheiten enthält der Achte Fortschrittsbericht „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion“, COM(2017) 354 final.

des Verhaltenskodex zur Bekämpfung illegaler Online-Hetze[28] wurden erhebliche Fortschritte erzielt. Weitere Einzelheiten enthält der Achte Fortschrittsbericht „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion“[29]. Diese Maßnahmen werden – auch im Lichte der Schlussfolgerungen des Europäischen Rates[30] sowie des G7-Gipfels[31] und des G20-Gipfels in Hamburg[32] – verstärkt werden.

Online-Plattformen spielen eine entscheidende Rolle bei der Bekämpfung illegaler oder potenziell schädlicher Inhalte. Wie in der Halbzeitüberprüfung der Strategie für einen digitalen Binnenmarkt[33] dargestellt, wird die Kommission für eine bessere Koordinierung von Dialogen mit Plattformen sorgen, und dabei die Mechanismen und technischen Lösungen für die Entfernung illegaler Inhalte in den Mittelpunkt stellen. Gegebenenfalls sollten diese durch Vorgaben zu einzelnen Aspekten, etwa der Meldung und Entfernung illegaler Inhalte, untermauert werden. Ferner wird die Kommission im Bereich Haftungsregeln Orientierung geben.

Intensivierung der Zusammenarbeit mit Drittländern

***Maßnahme 18:** Die Hohe Vertreterin wird in Abstimmung mit der Kommission eine Untersuchung der hybriden Risiken in benachbarten Regionen auf den Weg bringen. Die Hohe Vertreterin, die Kommission und die Mitgliedstaaten werden die ihnen jeweils zur Verfügung stehenden Instrumente nutzen, um die Kapazitäten der Partner aufzubauen und deren Resilienz gegenüber hybriden Bedrohungen zu stärken. GSVP-Missionen könnten als eigene Maßnahme oder ergänzend zu anderen EU-Instrumenten entsandt werden, um Partner bei der Verbesserung ihrer Kapazitäten zu unterstützen*.

Die EU konzentriert sich verstärkt darauf, Fähigkeiten und Resilienz im Sicherheitssektor in Partnerländern aufzubauen. Dafür stützt sie sich unter anderem auf den engen Zusammenhang zwischen Sicherheit und Entwicklung, entwickelt die sicherheitspolitische Dimension der überarbeiteten Europäischen Nachbarschaftspolitik weiter und tritt mit den Mittelmeeranrainerstaaten in einen Dialog zu den Themen Terrorismusbekämpfung und Sicherheit ein. In diesem Zusammenhang wurde in Kooperation mit der Republik Moldau ein Pilotprojekt zur Risikobewertung auf den Weg gebracht. Dabei soll ermittelt werden, wo die zentralen Verwundbarkeiten des Landes liegen, damit sichergestellt ist, dass sie durch die Unterstützung der EU gezielt beseitigt werden. Die Ergebnisse des Pilotprojekts zeigten, dass die Bewertung an sich als nützlich erachtet wurde. Die Kommission und der EAD werden auf der Grundlage der dabei gewonnenen Erfahrungen Empfehlungen abgeben, damit Maßnahmen in den Bereichen Wirksamkeitssteigerung, strategische Kommunikation, Schutz kritischer Infrastrukturen und Cybersicherheit Vorrang eingeräumt wird.

Künftig könnten weitere an die EU angrenzende Länder von der Untersuchung profitieren und auf dieser ersten Erfahrung aufbauen, wobei die Konzepte auf die unterschiedlichen

[28] „Code of Conduct on illegal online hate speech“, 31. Mai 2016, http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf.
[29] Weitere Einzelheiten enthält der Achte Fortschrittsbericht „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion“, COM(2017) 354 final.
[30] Schlussfolgerungen des Rates vom 22. und 23. Juni 2017.
[31] G7-Gipfel in Taormina, Italien, 26.-27.5.2017.
[32] G20-Gipfel in Hamburg, Deutschland, 7.-8.7.2017.
[33] Siehe Mitteilung der Kommission COM(2017) 228 final.

nationalen Gegebenheiten vor Ort zugeschnitten und spezifische Bedrohungen berücksichtigen würden, sodass Überschneidungen mit den über die Themen Terrorismusbekämpfung und Sicherheit geführten Dialogen vermieden würden. Die Kommission und die Hohe Vertreterin der Union für Außen- und Sicherheitspolitik haben am 7. Juni 2017 eine allgemeine Gemeinsame Mitteilung mit dem Titel „Ein strategisches Konzept für Resilienz im Rahmen des auswärtigen Handelns der EU“[34] angenommen. Damit sollen Partnerländer dabei unterstützt werden, mehr Resilienz gegenüber den aktuellen globalen Herausforderungen zu entwickeln. In der Mitteilung wird das Erfordernis anerkannt, von der Kriseneindämmung zu einem eher strukturell ausgerichteten, langfristigen Ansatz für Verwundbarkeiten überzugehen, wobei ein besonderer Schwerpunkt auf der Antizipation, Prävention und Vorsorge liegen soll.

Resilienz gegenüber Cyberangriffen im Entwicklungsbereich

Die EU unterstützt Länder außerhalb Europas dabei, die Resilienz ihrer Informationsnetze zu verbessern. Die ständig zunehmende Digitalisierung mit ihrer inhärenten Sicherheitsdimension geht mit besonderen Herausforderungen für die Resilienz der Informationsnetzsysteme weltweit einher, da Cyberangriffe nicht vor Grenzen haltmachen. Die EU unterstützt Drittländer dabei, ihre Fähigkeiten aufzubauen, um Fällen von unbeabsichtigtem Versagen und Cyberangriffen angemessen vorzubeugen und auf diese zu reagieren. Im Anschluss an ein Pilotprojekt zur Cybersicherheit, das in der ehemaligen jugoslawischen Republik Mazedonien, dem Kosovo[35] und der Republik Moldau im Jahr 2016 abgeschlossen wurde, wird die Kommission mit einem neuen Programm für den Zeitraum 2017-2020 die Resilienz gegenüber Cyberangriffen in Drittstaaten, hauptsächlich in Afrika und Asien, aber auch in der Ukraine stärken. Es zielt darauf ab, kritische Informationsinfrastrukturen und -netze in Drittländern auf der Grundlage eines ressortübergreifenden Ansatzes sicherer zu machen und besser auf Notfälle vorzubereiten sowie gleichzeitig die Einhaltung von Menschenrechten und Rechtsstaatlichkeit sicherzustellen.

Luftsicherheit

Die zivile Luftfahrt bildet weiterhin ein wichtiges und symbolträchtiges Ziel für Terroristen, könnte aber auch bei einer hybriden Kampagne ins Visier geraten. Die EU hat zwar einen soliden Sicherheitsrahmen für den Luftverkehr entwickelt, Flüge aus Drittländern könnten dennoch leichter angreifbar sein. Im Einklang mit der Resolution 2309 (2016) des Sicherheitsrates der VN verstärkt die Kommission ihre Bemühungen zum Ausbau von Fähigkeiten in Drittländern. Im Januar 2017 stellte die Kommission mit einer neuen integrierten Risikobewertung sicher, dass die Bemühungen zum Fähigkeitenausbau auf der Ebene der EU und der Mitgliedstaaten sowie mit internationalen Partnern Vorrang erhalten und koordiniert erfolgen. 2016 leitete die Kommission ein vierjähriges Projekt zur Sicherheit der zivilen Luftfahrt in Afrika und auf der arabischen Halbinsel ein, mit dem terroristische Bedrohungen für die zivile Luftfahrt abgewehrt werden sollen. Schwerpunkte dieses Projekts sind der Erfahrungsaustausch zwischen den Partnerstaaten und Sachverständigen der

[34] Gemeinsame Mitteilung an das Europäische Parlament und den Rat: Ein strategisches Konzept für Resilienz im Rahmen des auswärtigen Handelns der EU, JOIN(2017) 21 final.

[35] Diese Bezeichnung berührt nicht die Standpunkte zum Status und steht im Einklang mit der Resolution 1244 des VN-Sicherheitsrates und dem Gutachten des Internationalen Gerichtshofs zur Unabhängigkeitserklärung des Kosovos.

Mitgliedstaaten der Europäischen Zivilluftfahrtkonferenz, ferner Mentoring sowie Schulungs- und Coachingmaßnahmen. Diese Aktivitäten werden im Laufe des Jahres 2017 intensiviert.

c. 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. In weiterer Folge werden regelmäßige Bewertungen und Übungen stattfinden.

Maßnahme 19: ***Die Hohe Vertreterin und die Kommission werden in Abstimmung mit den Mitgliedstaaten für die Erstellung eines gemeinsamen Einsatzprotokolls und die Durchführung regelmäßiger Übungen zur Verbesserung der Fähigkeit zur strategischen Entscheidungsfindung im Falle komplexer hybrider Bedrohungen sorgen, wobei die Verfahren des Krisenmanagements und der Integrierten EU-Regelung für die politische Reaktion auf Krisen zugrunde gelegt werden.***

Im Gemeinsamen Rahmen wurde die Einrichtung eines Krisenreaktionsmechanismus für Ereignisse, die durch hybride Bedrohungen ausgelöst wurden, empfohlen, um den EU-Krisenreaktionsmechanismus[36] und Frühwarnsysteme aufeinander abzustimmen. Zu diesem Zweck haben die Dienststellen der Kommission und der EAD das EU-Einsatzprotokoll für die Abwehr hybrider Bedrohungen („EU Playbook“)[37] herausgegeben, in dem Modalitäten für jene Verfahren festgelegt werden, die für die Koordination, die Zusammenführung und Analyse von Informationen und die Gewinnung von Erkenntnissen für die politische Entscheidungsfindung sowie ferner für Übungen und Schulungen und die Zusammenarbeit mit Partnerorganisationen, insbesondere der NATO, im Falle einer hybriden Bedrohung maßgeblich sind. Die NATO hat analog dazu ein sogenanntes Playbook für ein verstärktes Zusammenspiel von NATO und EU bei der Prävention und Abwehr hybrider Bedrohungen in den Bereichen Cyberabwehr, strategische Kommunikation, Lagebewusstsein und Krisenbewältigung entwickelt. Das EU-Playbook wird im Herbst 2017 im Zuge der parallelen und koordinierten Übung, die auch das Zusammenspiel mit der NATO umfasst, getestet.

Maßnahme 20: ***Die Kommission und die Hohe Vertreterin werden (in ihren jeweiligen Zuständigkeitsbereichen) die Anwendbarkeit von Artikel 222 AEUV) und Artikel 42 Absatz 7 EUV und die praktischen Konsequenzen des Rückgriffs darauf, falls es zu einem großangelegten, schweren hybriden Angriff kommt, prüfen.***

Artikel 42 Absatz 7 EUV bezieht sich auf einen bewaffneten Angriff auf das Hoheitsgebiet eines Mitgliedstaats, Artikel 222 AEUV (Solidaritätsklausel) dagegen auf einen Terroranschlag, eine Naturkatastrophe oder eine vom Menschen verursachte Katastrophe im

[36] Die Integrierte EU-Regelung des Rates für die politische Reaktion auf Krisen (IPCR), das ARGUS-System der Kommission und Krisenbewältigung und -reaktion des EAD.
[37] Arbeitsunterlage der Kommissionsdienststellen SWD(2016) 227, angenommen am 7. Juli 2016.

Hoheitsgebiet eines Mitgliedstaats. Bei einem hybriden Angriff kommt eher der letztgenannte Artikel zur Anwendung, da in diesem Fall kriminelle /subversive Handlungen kombiniert werden. Durch die Berufung auf die Solidaritätsklausel werden eine Koordination auf der Ebene des Rates (IPCR-Regelung der EU), die Einbeziehung der zuständigen Organe, Agenturen und Einrichtungen der EU sowie ihre Unterstützungsprogramme und -mechanismen ausgelöst. Im Beschluss 2014/415/EU des Rates sind die Vorkehrungen für die Anwendung der Solidaritätsklausel durch die Union festgelegt. Diese Anwendungsmodalitäten gelten weiterhin und es besteht keine Notwendigkeit, den Beschluss des Rates zu überarbeiten. Wenn ein hybrider Angriff im Zuge eines bewaffneten Angriffs erfolgt, könnte auch Artikel 42 Absatz 7 geltend gemacht werden. In einem solchen Fall sollten sowohl die Mitgliedstaaten als auch die EU Hilfe und Unterstützung leisten. Die Kommission und die Hohe Vertreterin werden weiterhin die wirksamsten Methoden zur Abwehr solcher Angriffe prüfen.

Durch die Annahme des oben genannten EU-Protokolls wird diese Bewertung unmittelbar unterstützt und im Rahmen der parallelen und koordinierten Übung (PACE) der EU im Oktober 2017 getestet. Im Rahmen dieser Übung werden die verschiedenen Mechanismen der EU und die Interaktionsfähigkeit getestet, um die Entscheidungsfindung zu beschleunigen, wenn eine hybride Bedrohung Unklarheit verursacht und die Lage unübersichtlich wird.

Maßnahme 21: ***Die Hohe Vertreterin wird in Abstimmung mit den Mitgliedstaaten für die Integration, Nutzung und Koordinierung der militärischen Fähigkeiten zur Abwehr hybrider Bedrohungen im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik sorgen.***

Als Reaktion auf den an die integrierten militärischen Fähigkeiten erteilten Auftrag zur Unterstützung der GASP/GSVP, im Anschluss an ein Seminar mit Militärexperten im Dezember 2016 sowie anknüpfend an die von der Arbeitsgruppe des EU-Militärausschusses im Mai 2017 formulierten Vorgaben wurde im Juli 2017 die militärische Beratung zum „militärischen Beitrag der EU zur Abwehr hybrider Bedrohungen im Rahmen der GSVP“ fertiggestellt, die im Rahmen des „Concept Development Implementation Plan“ weiterentwickelt wird.

d. ZUSAMMENARBEIT ZWISCHEN DER EU UND DER NATO

Maßnahme 22*: Die Hohe Vertreterin wird in Abstimmung mit der Kommission den informellen Dialog fortsetzen und die Zusammenarbeit und Koordinierung mit der NATO in den Bereichen Lagebewusstsein, strategische Kommunikation, Cybersicherheit und „Krisenprävention und -reaktion“ zur Abwehr hybrider Bedrohungen intensivieren, wobei die Grundsätze der gleichberechtigten Teilhabe und der Beschlussfassungsautonomie jeder Organisation zu achten sind.*

Auf der Grundlage der von den Präsidenten des Europäischen Rates und der Europäischen Kommission sowie vom Generalsekretär der NATO am 8. Juli 2016 in Warschau unterzeichneten gemeinsamen Erklärung haben die EU und die NATO gemeinsam 42 Umsetzungsvorschläge entwickelt, die in der Folge in einem gesonderten parallelen Verfahren am 6. Dezember 2016 von den Räten der EU und der NATO[38] befürwortet wurden. Im Juni 2017 haben die Hohe Vertreterin/Vizepräsidentin und der NATO-Generalsekretär einen Bericht über die Fortschritte veröffentlicht, die bei den 42 Maßnahmen der

[38] http://www.consilium.europa.eu/de/press/press-releases/2016/12/06-eu-nato-joint-declaration/

Gemeinsamen Erklärung erzielt wurden. Die Abwehr hybrider Bedrohungen ist einer der sieben in der Gemeinsamen Erklärung genannten Kooperationsbereiche, auf den wiederum zehn der 42 Maßnahmen entfallen. Wie der Bericht belegt, haben die gemeinsamen Bemühungen des vergangenen Jahres zu greifbaren Ergebnissen geführt. Viele der spezifischen Maßnahmen zur Abwehr hybrider Bedrohungen wurden bereits erwähnt, unter anderem das Europäische Kompetenzzentrum zur Bewältigung hybrider Bedrohungen, das verbesserte Lagebewusstsein, die Einrichtung der EU-Analyseeinheit für hybride Bedrohungen und ihr Zusammenspiel mit der neu geschaffenen NATO-Analyseeinheit für hybride Bedrohungen sowie die Zusammenarbeit zwischen den Teams für strategische Kommunikation. Erstmals werden Mitarbeiter der EU und der NATO gemeinsam üben, wie auf ein hybrides Szenario reagiert werden soll. Bei dieser Übung wird voraussichtlich die Umsetzung mehr als eines Drittels der gemeinsamen Vorschläge getestet. Die EU wird in diesem Jahr eine eigene parallele und koordinierte Übung durchführen und bereitet sich darauf vor, 2018 eine führende Rolle zu übernehmen.

Was die Resilienz-Thematik betrifft, so haben Mitarbeiter der EU und der NATO an gemeinsamen Briefings teilgenommen, die auch den EU-Mechanismus zur integrierten EU-Regelung für die politische Reaktion auf Krisen zum Gegenstand hatten. Dank regelmäßiger Kontakte zwischen Mitarbeitern von NATO und EU, unter anderem im Wege von Workshops und der Teilnahme der NATO am Lenkungsausschuss der Europäischen Verteidigungsagentur, konnten Informationen über die Mindestanforderungen der NATO in Bezug auf die Resilienz auf nationaler Ebene ausgetauscht werden. Für Herbst ist ein weiterer Austausch zwischen der Kommission und der NATO zum Thema Stärkung der Resilienz geplant. Im nächsten Fortschrittsbericht über die Zusammenarbeit zwischen EU und NATO werden Möglichkeiten für eine Ausweitung der Zusammenarbeit zwischen den beiden Organisationen vorgeschlagen.

3. SCHLUSSFOLGERUNG

In dem Gemeinsamen Rahmen werden Maßnahmen erläutert, die dazu beitragen sollen, hybride Bedrohungen abzuwehren und die Resilienz auf der Ebene der EU, der Mitgliedstaaten sowie der Partner zu stärken. Die Kommission und die Hohe Vertreterin erzielen in allen Bereichen in enger Abstimmung mit den Mitgliedstaaten und Partnern gute Ergebnisse. Zugleich kommt es darauf an, dass dieser Elan angesichts bestehender und sich ständig weiterentwickelnder hybrider Bedrohungen anhält. Die Mitgliedstaaten tragen die Hauptverantwortung für die Abwehr hybrider Bedrohungen, die mit der nationalen Sicherheit sowie mit der Aufrechterhaltung von Recht und Ordnung zusammenhängen. Resilienz auf nationaler Ebene und kollektive Bemühungen zum Schutz vor hybriden Bedrohungen müssen als einander verstärkende Elemente ein und derselben Gesamtanstrengung verstanden werden. Die Mitgliedstaaten werden daher aufgefordert, so rasch wie möglich Untersuchungen über hybride Risiken durchzuführen. Diese liefern nämlich wertvolle Informationen darüber, wie verwundbar Europa ist und in welchem Umfang vorgesorgt wurde. Das Potenzial der EU-Analyseeinheit für hybride Bedrohungen sollte – aufbauend auf den beträchtlichen Fortschritten im Bereich der Bewusstseinsbildung – optimiert werden. Die Hohe Vertreterin fordert die Mitgliedstaaten auf, die Arbeit der StratCom Task Forces zu fördern und damit effizienter gegen wachsende hybride Bedrohungen vorzugehen. Die EU wird das unter der Federführung Finnlands eingerichtete Europäische Zentrum zur Bewältigung hybrider Bedrohungen in vollem Umfang unterstützen.

Die einzigartige Stärke der EU liegt darin, den Mitgliedstaaten und Partnern beim Aufbau ihrer Resilienz zur Seite zu stehen und dabei auf eine breite Palette von Instrumenten und Programmen zurückgreifen zu können. Bei Maßnahmen zur Stärkung der Resilienz in Bereichen wie Verkehr, Energie, Cybersicherheit, kritische Infrastrukturen, Schutz des Finanzsystems vor illegaler Nutzung und Bekämpfung von gewalttätigem Extremismus und Radikalisierung wurden beträchtliche Fortschritte erzielt. Die EU wird sich auch künftig für die Stärkung der Resilienz einsetzen, da sich die Natur der hybriden Bedrohungen weiterentwickelt. Konkret wird die EU Indikatoren entwickeln, um den Schutz kritischer Infrastrukturen vor hybriden Bedrohungen und deren Resilienz ihnen gegenüber in relevanten Bereichen zu verbessern.

Aus dem Europäischen Verteidigungsfonds können – zusammen mit den Mitgliedstaaten – Prioritäten bei den Fähigkeiten zur Stärkung der Resilienz gegenüber hybriden Bedrohungen kofinanziert werden. Mit dem geplanten Cybersicherheitspaket sowie sektorübergreifenden Maßnahmen zur Umsetzung der Richtlinie zur Netz- und Informationssicherheit werden neue Plattformen zur EU-weiten Abwehr hybrider Bedrohungen entstehen.

Die Kommission und die Hohe Vertreterin rufen die Mitgliedstaaten und Interessenträger dazu auf, wenn immer dies nötig ist, rasch zu einer Einigung zu gelangen und für eine zügige und effiziente Umsetzung der zahlreichen, in dieser Mitteilung erläuterten Maßnahmen zur Stärkung der Resilienz zu sorgen. Die EU wird an ihre bereits fruchtbare Zusammenarbeit mit der NATO anknüpfen und diese vertiefen.

Die Union engagiert sich weiterhin für die Mobilisierung aller relevanten EU-Instrumente zur Abwehr komplexer Bedrohungen. Die EU wird auch in Zukunft die Mitgliedstaaten vorrangig in ihren Bemühungen unterstützen. Sie wird an der Seite ihrer wichtigsten Partner dabei als starker und noch rascher reagierender Sicherheitsgarant auftreten.