EUROPÄISCHE
KOMMISSION

HOHE VERTRETERIN
DER UNION FÜR
AUSSEN- UND
SICHERHEITSPOLITIK

Brüssel, den 6.4.2016
JOIN(2016) 18 final

GEMEINSAME MITTEILUNG AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

Gemeinsamer Rahmen für die Abwehr hybrider Bedrohungen -

eine Antwort der Europäischen Union

1. EINFÜHRUNG

In den letzten Jahren hat sich das Sicherheitsumfeld der Europäischen Union drastisch verändert. Die großen Herausforderungen hinsichtlich Frieden und Stabilität in den Ländern der östlichen und der südlichen Nachbarschaft der EU verdeutlichen nach wie vor, dass die Union ihre Kapazitäten als Sicherheitsgarant anpassen und ausbauen muss, wobei besonderes Augenmerk auf der engen Verbindung zwischen äußerer und innerer Sicherheit liegen muss. Viele der derzeitigen Herausforderungen, die Frieden, Sicherheit und Wohlstand in Frage stellen, sind durch die Instabilität in der unmittelbaren Nachbarschaft der EU und die sich wandelnden Bedrohungen bedingt. Der Präsident der Europäischen Kommission, Jean-Claude Juncker, betonte in seinen politischen Leitlinien von 2014, dass wir „in der Sicherheits- und Verteidigungspolitik ... an einem stärkeren Europa arbeiten" müssen und dass „nationale und europäische Instrumente wirksamer kombiniert [werden müssen], als dies in der Vergangenheit der Fall war". Im Anschluss an die Aufforderung des Rates „Auswärtige Angelegenheiten" vom 18. Mai 2015 hat die Hohe Vertreterin in enger Zusammenarbeit mit den Kommissionsdienststellen und der Europäischen Verteidigungsagentur (EDA) und in Abstimmung mit den EU-Mitgliedstaaten den vorliegenden Gemeinsamen Rahmen erstellt, der praktikable Vorschläge zur Unterstützung bei der Bewältigung hybrider Bedrohungen und zur Stärkung der Resilienz der EU und ihrer Mitgliedstaaten sowie der Partner enthält.[1] Im Juni 2015 erinnerte der Europäische Rat daran, dass EU-Instrumente mobilisiert werden müssen, um einen Beitrag zur Bewältigung hybrider Bedrohungen zu leisten.[2]

Auch wenn „hybride Bedrohungen" unterschiedlich definiert werden und dabei immer wieder neuen Entwicklungen Rechnung getragen werden muss, geht es grundsätzlich darum, die Mischung von Zwang und Unterwanderung und von konventionellen und unkonventionellen Methoden (diplomatischer, militärischer, wirtschaftlicher oder technologischer Natur) zu erfassen, auf die von staatlichen oder nichtstaatlichen Akteuren in koordinierter Weise zur Erreichung bestimmter Ziele zurückgegriffen werden kann, ohne dass jedoch die Schwelle eines offiziell erklärten Kriegs erreicht wird. Normalerweise liegt der Schwerpunkt auf der Ausnutzung von Verwundbarkeiten der Zielgemeinschaft und auf Verschleierungsstrategien zur Behinderung von Entscheidungsprozessen. Großangelegte Desinformationskampagnen und die Nutzung der sozialen Medien zur Beherrschung des politischen Diskurses oder zur Radikalisierung, Rekrutierung und Steuerung von Stellvertreterakteuren („proxy actors") können als Vehikel für hybride Bedrohungen dienen.

Soweit die Abwehr hybrider Bedrohungen die nationale Sicherheit und Verteidigung und die Aufrechterhaltung von Recht und Ordnung betrifft, liegt die Hauptverantwortung bei den Mitgliedstaaten, da die meisten nationalen Verwundbarkeiten länderspezifischer Natur sind. Allerdings sehen sich viele EU-Mitgliedstaaten gemeinsamen Bedrohungen ausgesetzt, die sich auch gegen länderübergreifende Netze oder Infrastrukturen richten

[1] Schlussfolgerungen des Rates zur Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) vom Mai 2015 [Consilium 8971/15].
[2] Schlussfolgerungen des Europäischen Rates vom Juni 2015 [EUCO 22/15].

können. Solchen Bedrohungen kann besser durch Koordinierung auf EU-Ebene begegnet werden, indem die politischen Konzepte und die Instrumente der EU genutzt werden, auf europäische Solidarität und gegenseitige Hilfe gesetzt wird und das Potenzial des Vertrags von Lissabon voll ausgeschöpft wird. Mit den politischen Konzepten und den Instrumenten der EU kann ein entscheidender Mehrwert für die Verbesserung des Bewusstseins für hybride Bedrohungen erzielt werden, was bis zu einem gewissen Grade bereits der Fall ist. Dies trägt zur Stärkung der Resilienz der Mitgliedstaaten bei, die so besser auf gemeinsame Bedrohungen reagieren können. Das auswärtige Handeln der Union, das im vorliegenden Rahmen vorgeschlagen wird, folgt den Grundsätzen des Artikels 21 des Vertrags über die Europäische Union (EUV), zu denen Demokratie, Rechtsstaatlichkeit, die universelle Gültigkeit und Unteilbarkeit der Menschenrechte sowie die Achtung der Grundsätze der Charta der Vereinten Nationen und des Völkerrechts gehören[3].

Mit dieser Gemeinsamen Mitteilung soll ein ganzheitlicher Ansatz gefördert werden, der es der EU ermöglicht, in Abstimmung mit den Mitgliedstaaten durch Schaffung von Synergien zwischen allen einschlägigen Instrumenten und durch Förderung einer engen Zusammenarbeit zwischen allen relevanten Akteuren speziell Bedrohungen hybrider Natur abzuwehren.[4] Die Maßnahmen stützen sich auf bestehende Strategien und sektorspezifische Maßnahmen, die der Erhöhung der Sicherheit dienen. Insbesondere die Europäische Sicherheitsagenda[5], die Globale EU-Strategie für die Außen- und Sicherheitspolitik und der Europäische Aktionsplan im Verteidigungsbereich[6], die Cybersicherheitsstrategie der EU[7], die Strategie für eine sichere Energieversorgung[8] und die Strategie der Europäischen Union für maritime Sicherheit[9] können ebenfalls zur Abwehr hybrider Bedrohungen beitragen.

Da die Abwehr hybrider Bedrohungen auch ein Anliegen der NATO ist und der Rat „Auswärtige Angelegenheiten“ die Intensivierung der Zusammenarbeit und der Koordinierung in diesem Bereich vorgeschlagen hat, zielen einige der Vorschläge auf den Ausbau der Zusammenarbeit zwischen der EU und der NATO bei der Abwehr hybrider Bedrohungen.

Die vorgeschlagene Strategie konzentriert sich auf die folgenden Elemente: Verbesserung des Bewusstseins für hybride Bedrohungen, Stärkung der Resilienz sowie Prävention, Krisenreaktion und Rückkehr zur Normalität.

---

[3] Die Charta der Grundrechte der EU ist für die EU-Institutionen und die Mitgliedstaaten bei der Ausführung der Unionsvorschriften rechtsverbindlich.

[4] Für etwaige Legislativvorschläge gelten die Rechtssetzungsvorgaben der Kommission gemäß den Leitlinien der Kommission für eine bessere Rechtsetzung, SWD(2015) 111.

[5] COM(2015) 185 final.

[6] Soll 2016 vorgelegt werden.

[7] EU-Politikrahmen für die Cyberabwehr [Consilium 15585/14] und Gemeinsame Mitteilung „Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum“ vom Februar 2013, JOIN(2013) 1.

[8] Mitteilung „Strategie für eine sichere europäische Energieversorgung“ vom Mai 2014, SWD(2014) 330.

[9] Gemeinsame Mitteilung „Für einen offenen und sicheren globalen maritimen Bereich: Elemente einer Strategie der Europäischen Union für maritime Sicherheit“, JOIN(2014) 9 final vom 6.3.2014.

2. ERKENNUNG DER HYBRIDEN NATUR EINER BEDROHUNG

Mit hybriden Bedrohungen sollen die Verwundbarkeiten eines Landes ausgenutzt und häufig grundlegende demokratische Werte und Freiheiten unterminiert werden. Als erster Schritt werden die Hohe Vertreterin und die Kommission gemeinsam mit den Mitgliedstaaten an der Verbesserung des Lagebewusstseins durch Überwachung und Bewertung der Bedrohungen arbeiten, die an den Schwachstellen der EU ansetzen könnten. Die Kommission entwickelt derzeit Methoden zur Bewertung von Sicherheitsrisiken, um zur besseren Information der Entscheidungsträger beizutragen und in Bereichen wie Luftsicherheit, Terrorismusfinanzierung oder Geldwäsche eine Politikgestaltung zu fördern, die den Risiken Rechnung trägt. Außerdem wäre es nützlich, wenn die Mitgliedstaaten untersuchen würden, welche Bereiche für hybride Bedrohungen anfällig sind. Das Ziel bestünde darin, dass sie Indikatoren für hybride Bedrohungen entwickeln, in Frühwarn- und bestehende Risikobewertungsmechanismen einbeziehen und gegebenenfalls auch weitergeben.

Maßnahme 1: ***Die Mitgliedstaaten werden aufgefordert, gegebenenfalls mit Unterstützung der Kommission und der Hohen Vertreterin eine Untersuchung über hybride Risiken zwecks Ermittlung zentraler Verwundbarkeiten – und spezifischer Indikatoren für hybride Bedrohungen – einzuleiten, von denen die nationalen und gesamteuropäischen Strukturen und Netze betroffen sein könnten.***

3. GESTALTUNG DER ANTWORT DER EU: VERBESSERUNG DES BEWUSSTSEINS FÜR HYBRIDE BEDROHUNGEN

3.1. EU-Analyseeinheit für hybride Bedrohungen (EU Hybrid Fusion Cell)

Die EU sollte unbedingt in Abstimmung mit ihren Mitgliedstaaten für ein ausreichendes Lagebewusstsein sorgen, damit jede Änderung der Sicherheitslage aufgrund hybrider Aktivitäten staatlicher und/oder nichtstaatlicher Akteure erkannt wird. Zur wirksamen Abwehr hybrider Bedrohungen ist wichtig, dass der Informationsaustausch verbessert wird und relevante nachrichtendienstliche Erkenntnisse bereichsübergreifend weitergegeben und zwischen der Europäischen Union, ihren Mitgliedstaaten und Partnern ausgetauscht werden.

Daher wird eine EU-Analyseeinheit für hybride Bedrohungen (EU Hybrid Fusion Cell) im EU-Zentrum für Informationsgewinnung und -analyse (EU INTCEN) des Europäischen Auswärtigen Dienstes (EAD) als zentrale Anlaufstelle eingerichtet. Diese Analyseeinheit soll sowohl als geheim eingestufte als auch offen zugängliche Informationen speziell über hybride Bedrohungen aufgrund von Indikatoren und Warnhinweisen verschiedener Interessenträger innerhalb des EAD (einschließlich der EU-Delegationen), der Kommission (und der EU-Agenturen[10]) und der Mitgliedstaaten entgegennehmen, auswerten und weiterleiten. In Zusammenarbeit mit bereits

[10] Im Rahmen ihres jeweiligen Mandats.

bestehenden ähnlichen Gremien auf EU-Ebene[11] und auf nationaler Ebene soll die Analyseeinheit externe Aspekte hybrider Bedrohungen für die EU und ihre Nachbarschaft untersuchen, um eine rasche Auswertung einschlägiger Vorfälle und eine fundierte strategische Entscheidungsfindung der EU zu ermöglichen, unter anderem indem sie Input für die Bewertung der Sicherheitsrisiken auf EU-Ebene liefert. Die Ergebnisse der Analyseeinheit werden gemäß den Vorschriften der Europäischen Union für den Datenschutz und den Umgang mit Verschlusssachen[12] behandelt und verarbeitet. Die Analyseeinheit sollte in Kontakt mit bestehenden Einrichtungen auf EU- und auf nationaler Ebene stehen. Die Mitgliedstaaten sollten nationale Kontaktstellen einrichten, die mit der EU-Analyseeinheit in Verbindung stehen. Das Personal innerhalb und außerhalb der EU (einschließlich der Angehörigen der Delegationen, Operationen und Missionen der EU) und in den Mitgliedstaaten sollte zudem für die Erkennung früher Anzeichen von hybriden Bedrohungen geschult werden.

<u>Maßnahme 2:</u> Einrichtung einer EU-Analyseeinheit für hybride Bedrohungen (EU Hybrid Fusion Cell) innerhalb des bestehenden EU INTCEN, 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 zu sorgen.

3.2. Strategische Kommunikation

Urheber hybrider Bedrohungen können systematisch Fehlinformationen streuen, unter anderem durch gezielte Kampagnen in sozialen Medien, mit denen sie die Radikalisierung von Individuen, die Destabilisierung der Gesellschaft und die Kontrolle über den politischen Diskurs anstreben. Die Fähigkeit zur Reaktion auf hybride Bedrohungen mit Hilfe einer fundierten Strategie für **strategische Kommunikation** ist von grundlegender Bedeutung. Eine rasche Information über die Fakten sowie die Sensibilisierung der Öffentlichkeit für hybride Bedrohungen sind entscheidende Faktoren für die Stärkung der Resilienz einer Gesellschaft.

Die strategische Kommunikation sollte die sozialen Medien wie auch die traditionellen Medien wie Hörfunk und Fernsehen und Onlinemedien in vollem Umfang nutzen. Der EAD sollte – gestützt auf die Tätigkeit der beiden Taskforces für strategische Kommunikation (Osten und arabischer Raum) – den Einsatz von Spezialisten für einschlägige Nicht-EU-Sprachen und für soziale Medien optimieren, die Informationen von außerhalb der EU verfolgen und dafür sorgen, dass auf Fehlinformationen mit gezielter Kommunikation reagiert wird. Darüber hinaus sollten die Mitgliedstaaten Mechanismen für eine koordinierte strategische Kommunikation entwickeln, um dazu

[11] Beispielsweise mit dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität und dem Europäischen Zentrum zur Terrorismusbekämpfung von Europol, Frontex oder dem IT-Notfallteam der EU (Computer Emergency Response Team – CERT-EU).
[12] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995.

beizutragen, dass die Urheber ermittelt werden und gegen Fehlinformationen vorgegangen wird, damit hybride Bedrohungen bloßgelegt werden.

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

3.3. Kompetenzzentrum für die „Abwehr hybrider Bedrohungen“

Aufbauend auf den Erfahrungen einiger Mitgliedstaaten und Partnerorganisationen[13] könnte eine multinationale Einrichtung oder ein Netz solcher Einrichtungen als Kompetenzzentrum für die Bewältigung hybrider Bedrohungen fungieren. Ein solches Zentrum könnte vorrangig erforschen, wie hybride Strategien eingesetzt werden, und könnte die Entwicklung neuer Konzepte und Technologien durch Privatwirtschaft und Industrie fördern, um zur Stärkung der Resilienz der Mitgliedstaaten beizutragen. Die Forschungsarbeit könnte außerdem einen Beitrag dazu leisten, dass die Politik, die Strategien und die Konzepte der EU und der Mitgliedstaaten besser aufeinander abgestimmt werden und dass bei der Entscheidungsfindung die mit hybriden Bedrohungen verbundene Komplexität und Mehrdeutigkeit berücksichtigt werden kann. Ein solches Zentrum sollte Programme zur Vorantreibung der Forschung und Übungen konzipieren, damit praktische Lösungen für die Herausforderungen im Zusammenhang mit hybriden Bedrohungen gefunden werden können. Die Stärke eines solchen Zentrums läge in der Fachkompetenz, die ein multinationales, interdisziplinäres Team mit Teilnehmern aus dem zivilen und dem militärischen Bereich, aus Privatsektor und Wissenschaft in sich vereint.

Ein solches Zentrum könnte eng mit den bestehenden Kompetenzzentren der EU[14] und der NATO[15] zusammenarbeiten, um von den Erkenntnissen über hybride Bedrohungen zu profitieren, die bereits in den Bereichen Cyberabwehr, strategische Kommunikation, zivil-militärische Zusammenarbeit, Energie und Krisenreaktion gewonnen wurden.

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

4. GESTALTUNG DER ANTWORT DER EU: STÄRKUNG DER RESILIENZ

Resilienz ist die Fähigkeit, Belastungen standzuhalten und gestärkt daraus hervorzugehen. Um hybriden Bedrohungen wirksam zu begegnen, müssen die potenziellen Verwundbarkeiten der wichtigsten Infrastrukturen, der Versorgungsketten und der Gesellschaft angegangen werden. Durch Rückgriff auf die Instrumente und Strategien der EU kann die Resilienz der Infrastrukturen auf der EU-Ebene erhöht werden.

[13] NATO-Kompetenzzentren.
[14] Z. B. EU-Institut für Sicherheitsstudien (EUISS), thematische EU-Kompetenzzentren im CBRN-Bereich.
[15] http://www.nato.int/cps/en/natohq/topics_68372.htm

4.1. Schutz kritischer Infrastrukturen

Es ist wichtig, kritische Infrastrukturen (z. B. für Energieversorgung oder Verkehr) zu schützen, da ein unkonventioneller Angriff durch Urheber hybrider Bedrohungen auf ein „weiches Ziel“ zu gravierenden Störungen in Wirtschaft und Gesellschaft führen könnte. Zum Schutz kritischer Infrastrukturen sieht das Europäische Programm für den Schutz kritischer Infrastrukturen[16] (EPSKI) einen alle Gefahrentypen berücksichtigenden sektorübergreifenden Systemansatz vor, der auf die Ermittlung von Abhängigkeiten und die Durchführung von Maßnahmen in den Bereichen Prävention, Abwehrbereitschaft und Reaktionsfähigkeit abzielt. Die Richtlinie über europäische kritische Infrastrukturen[17] sieht ein Verfahren zur Ermittlung und Ausweisung europäischer kritischer Infrastrukturen (EKI) und einen gemeinsamen Ansatz für die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, vor. Insbesondere sollten im Rahmen der Richtlinie die Arbeiten zur Verbesserung der Resilienz kritischer Verkehrsinfrastrukturen (z. B. der wichtigsten Flughäfen und Handelshäfen der EU) wiederaufgenommen werden. Die Kommission wird prüfen, ob gemeinsame Instrumente, einschließlich entsprechender Indikatoren, entwickelt werden sollten, um die Resilienz kritischer Infrastrukturen gegenüber hybriden Bedrohungen in allen maßgeblichen Bereichen zu erhöhen.

<u>Maßnahme 5:</u> 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.

4.1.1. Energienetze

Eine reibungslose Stromerzeugung und -versorgung ist für die EU von entscheidender Bedeutung und größere Stromausfälle könnten Schaden anrichten. Wesentlich für die Abwehr hybrider Bedrohungen ist die weitere Diversifizierung der Energiequellen, Lieferanten und Versorgungswege der EU, um eine sicherere und krisenfestere Energieversorgung zu gewährleisten. Die Kommission führt auch Risiko- und Sicherheitsbewertungen („Stresstests“) von Kraftwerken in der EU durch. Zur Diversifizierung der Energieversorgung werden derzeit die Bemühungen im Rahmen der Strategie für die Energieunion intensiviert: So kann beispielsweise Erdgas aus dem kaspischen Raum über den südlichen Gaskorridor nach Europa gelangen und in Nordeuropa werden Flüssiggas-Hubs, die aus verschiedenen Quellen beliefert werden, aufgebaut. Diesem Beispiel sollte man in Mittel- und Osteuropa sowie im

[16] Mitteilung der Kommission über ein Europäisches Programm für den Schutz kritischer Infrastrukturen, KOM(2006) 786 endg. vom 12.12.2006.

[17] Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern (ABl. L 345 vom 23.12.2008).

Mittelmeerraum (wo derzeit ein Gas-Hub entsteht) folgen.[18] Die Entwicklung des Marktes für Flüssigerdgas wird hierzu ebenfalls einen positiven Beitrag leisten.

Was Kernmaterial und kerntechnische Anlagen angeht, so unterstützt die Kommission die Entwicklung und Festlegung der höchsten Sicherheitsstandards und stärkt auf diese Weise die Resilienz. Die Kommission fördert die kohärente Umsetzung und Anwendung der Richtlinie über nukleare Sicherheit[19], die Vorschriften für die Verhütung von Unfällen und die Abmilderung von Unfallfolgen enthält, sowie der Bestimmungen der Richtlinie über die grundlegenden Sicherheitsnormen[20], die die internationale Zusammenarbeit im Bereich Notfallvorsorge und -reaktion vor allem zwischen benachbarten Mitgliedstaaten und mit angrenzenden Ländern betreffen.

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

4.1.2 Verkehr und Lieferketten

Der Verkehrsbereich ist für das Funktionieren der Union von grundlegender Bedeutung. Hybride Anschläge auf Verkehrsinfrastrukturen (wie Flughäfen, Straßen- und Eisenbahninfrastrukturen oder Häfen) können schwerwiegende Folgen haben, was zu Störungen des Reiseverkehrs und der Lieferketten führen kann. Was die Anwendung der Rechtsvorschriften über die Sicherheit im Luft- und Seeverkehr[21] angeht, so nimmt die Kommission regelmäßige Inspektionen vor[22], und bei ihren Maßnahmen im Bereich der Sicherheit des Landverkehrs berücksichtigt sie etwaige hybride Bedrohungen. In diesem Zusammenhang wird derzeit über einen EU-Rahmen auf der Grundlage der überarbeiteten Sicherheitsvorschriften für die Luftfahrt[23] als Teil der

[18] Zu den bisherigen Fortschritten siehe den Bericht zur Lage der Energieunion 2015, COM(2015) 572 final.

[19] Richtlinie 2009/71/Euratom des Rates vom 25. Juni 2009 über einen Gemeinschaftsrahmen für die nukleare Sicherheit kerntechnischer Anlagen, geändert durch die Richtlinie 2014/87/Euratom vom 8. Juli 2014.

[20] Richtlinie 2013/59/Euratom des Rates vom 5. Dezember 2013 zur Festlegung grundlegender Sicherheitsnormen für den Schutz vor den Gefahren einer Exposition gegenüber ionisierender Strahlung und zur Aufhebung der Richtlinien 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom und 2003/122/Euratom.

[21] Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates vom 11. März 2008 über gemeinsame Vorschriften für die Sicherheit in der Zivilluftfahrt und zur Aufhebung der Verordnung (EG) Nr. 2320/2002; Durchführungsverordnung (EU) 2015/1998 der Kommission vom 5. November 2015 zur Festlegung detaillierter Maßnahmen für die Durchführung der gemeinsamen Grundstandards für die Luftsicherheit; Richtlinie 2005/65/EG des Europäischen Parlaments und des Rates vom 26. Oktober 2005 zur Erhöhung der Gefahrenabwehr in Häfen; Verordnung (EG) Nr. 725/2004 des Europäischen Parlaments und des Rates vom 31. März 2004 zur Erhöhung der Gefahrenabwehr auf Schiffen und in Hafenanlagen.

[22] Das EU-Recht sieht Inspektionen durch die Kommission vor, mit denen sichergestellt werden soll, dass die Mitgliedstaaten die Bestimmungen über die Sicherheit im Luft- und Seeverkehr korrekt anwenden. Dazu gehören Inspektionen bei der zuständigen Behörde des Mitgliedstaats sowie Inspektionen von Flughäfen, Häfen, Luftfahrtunternehmen, Schiffen und Stellen, die Sicherheitsmaßnahmen durchführen. Die Inspektionen der Kommission sollen sicherstellen, dass die EU-Standards von den Mitgliedstaaten vollständig umgesetzt werden.

[23] Verordnung (EU) 2016/4 der Kommission vom 5. Januar 2016 zur Änderung der Verordnung (EG) Nr. 216/2008 des Europäischen Parlaments und des Rates hinsichtlich grundlegender

Luftverkehrsstrategie für Europa[24] diskutiert. Bedrohungen der maritimen Sicherheit werden in der Strategie der Europäischen Union für maritime Sicherheit und dem dazugehörigen Aktionsplan[25] behandelt. Letzterer ermöglicht es der EU und ihren Mitgliedstaaten, Fragen der maritimen Sicherheit – auch die Abwehr hybrider Bedrohungen – durch eine sektorübergreifende Zusammenarbeit zwischen zivilen und militärischen Akteuren umfassend anzugehen, um kritische maritime Infrastrukturen, die globale Lieferkette, den Seehandel sowie die natürlichen Ressourcen und die Energiequellen im Meer zu schützen. Die Sicherheit der internationalen Lieferkette ist auch Gegenstand der Strategie der Europäischen Union für das Zollrisikomanagement und des entsprechenden Aktionsplans[26].

Maßnahme 7: ***Die Kommission wird die Bedrohungslage im Verkehrssektor überwachen und die Rechtsvorschriften erforderlichenfalls aktualisieren. Bei der Durchführung der EU-Strategie für maritime Sicherheit und der Strategie und des Aktionsplans 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.***

4.1.3 Raumfahrt

Hybride Bedrohungen könnten sich gegen Infrastrukturen im Weltraum richten. Dies hätte Folgen in den verschiedensten Bereichen. Die EU hat einen Rahmen zur Unterstützung der Beobachtung und Verfolgung von Objekten im Weltraum[27] konzipiert, um derartige Ressourcen, die Mitgliedstaaten gehören, zu vernetzen, damit für bestimmte Nutzer (Mitgliedstaaten, EU-Institutionen, Raumfahrzeugeigentümer und -betreiber und Katastrophenschutzbehörden) Dienste zur Beobachtung und Verfolgung von Objekten im Weltraum[28] erbracht werden können. Im Kontext der angekündigten Weltraumstrategie für Europa wird die Kommission prüfen, wie darin die Überwachung hybrider Bedrohungen für Infrastrukturen im Weltraum berücksichtigt werden kann.

Die Satellitenkommunikation (SatCom) ist von zentraler Bedeutung für das Krisenmanagement, den Katastrophenschutz, die Tätigkeit der Polizei, den Grenzschutz

---

Umweltschutzanforderungen; Verordnung (EG) Nr. 216/2008 des Europäischen Parlaments und des Rates vom 20. Februar 2008 zur Festlegung gemeinsamer Vorschriften für die Zivilluftfahrt und zur Errichtung einer Europäischen Agentur für Flugsicherheit.

[24] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Eine Luftfahrtstrategie für Europa“, COM(2015) 598 final vom 7.12.2015.

[25] Im Dezember 2014 nahm der Rat einen Aktionsplan zur Umsetzung der Strategie der Europäischen Union für maritime Sicherheit an: http://ec.europa.eu/maritimeaffairs/policy/maritime-security/doc/20141216-action-plan_en.pdf

[26] Mitteilung der Kommission an das Europäische Parlament, den Rat und den Europäischen Wirtschafts- und Sozialausschuss über die Strategie und den Aktionsplan der EU für das Zollrisikomanagement: Umgang mit Risiken, Erhöhung der Sicherheit der Lieferkette und Vereinfachung des Handels, COM(2014) 527 final.

[27] Siehe Beschluss Nr. 541/2014/EU des Europäischen Parlaments und des Rates.

[28] Beispielsweise Alarmsystem zur Verhinderung von Kollisionen in der Erdumlaufbahn, Warnmeldungen bei Auseinanderbrechen oder Kollisionen und riskanten Wiedereintritten von Weltraumobjekten in die Erdatmosphäre.

und die Küstenüberwachung. Sie bildet das Rückgrat großräumiger Infrastrukturen, etwa in den Bereichen Verkehr, Raumfahrt oder ferngesteuerte Flugsysteme. Im Einklang mit der Aufforderung des Europäischen Rates, Vorbereitungen für die nächste Generation staatlicher Satellitenkommunikation (GovSatCom) zu treffen, prüft die Kommission derzeit in Zusammenarbeit mit der Europäischen Verteidigungsagentur die Möglichkeiten zur Bündelung der Nachfrage im Rahmen der Weltraumstrategie und des Europäischen Aktionsplans im Verteidigungsbereich, die in Vorbereitung sind.

Viele kritische Infrastrukturen erfordern präzise zeitliche Informationen für die Synchronisierung ihrer Netze (z. B. Energie und Telekommunikation) oder für Zeitstempelverfahren (z. B. Finanzmärkte). Die Abhängigkeit vom Zeitsynchronisierungssignal eines einzigen globalen Satellitennavigationssystems bietet nicht die erforderliche Resilienz gegenüber hybriden Bedrohungen. Galileo, das europäische globale Satellitennavigationssystem, wäre eine zweite zuverlässige Zeitquelle.

Maßnahme 8: ***Im Rahmen der Weltraumstrategie und des Europäischen Aktionsplans im Verteidigungsbereich, die in Vorbereitung sind, wird die Kommission vorschlagen, die Resilienz der Weltrauminfrastrukturen gegenüber hybriden Bedrohungen zu stärken, insbesondere durch eine mögliche Einbeziehung hybrider Bedrohungen in den Anwendungsbereich der Beobachtung und Verfolgung von Objekten im Weltraum, durch Vorbereitung der nächsten Generation der staatlichen Satellitenkommunikation auf europäischer Ebene und durch Einsatz von Galileo für kritische Infrastrukturen, die von zeitlicher Synchronisierung abhängen.***

4.2. Verteidigungsfähigkeiten

Die Verteidigungsfähigkeiten müssen gestärkt werden, um die Resilienz der EU gegenüber hybriden Bedrohungen zu verbessern. Eine wichtige Aufgabe besteht darin, die wesentlichen Bereiche, in denen solche Fähigkeiten benötigt werden, z. B. Überwachung und Aufklärung, zu ermitteln. Die Europäische Verteidigungsagentur könnte als Katalysator für die Entwicklung militärischer Fähigkeiten im Zusammenhang mit hybriden Bedrohungen dienen (z. B. durch Verkürzung von Entwicklungszyklen im Bereich der Verteidigungsfähigkeiten, durch Investitionen in Technologien, Systeme und Prototypen oder durch Öffnung der Rüstungsindustrie für innovative kommerzielle Technologien). Potenzielle Maßnahmen könnten im Rahmen des angekündigten Europäischen Aktionsplans im Verteidigungsbereich geprüft werden.

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.***

4.3. Schutz der öffentlichen Gesundheit und Ernährungssicherheit

Die Gesundheit der Bevölkerung könnte durch die vorsätzliche Verbreitung übertragbarer Krankheiten oder die Verseuchung von Lebensmitteln, des Bodens, der Luft und des Trinkwassers durch chemische, biologische, radiologische und nukleare Stoffe (CBRN-Stoffe) gefährdet werden. Darüber hinaus kann die vorsätzliche Verbreitung von Tier- und Pflanzenkrankheiten die Ernährungssicherheit in der Union ernsthaft beeinträchtigen und zu erheblichen wirtschaftlichen und sozialen Auswirkungen auf die Schlüsselbereiche der Lebensmittelkette in der EU führen. Die bestehenden EU-Strukturen für den Schutz der öffentlichen Gesundheit, der Umwelt und der Lebensmittelsicherheit können genutzt werden, um auf derartige hybride Bedrohungen zu reagieren.

Die EU-Rechtsvorschriften über grenzüberschreitende Gesundheitsgefahren[29] sehen Mechanismen für die Koordinierung der Bereitschaftsplanung im Hinblick auf schwerwiegende grenzüberschreitende Gesundheitsgefahren vor. Dabei arbeiten die Mitgliedstaaten, EU-Agenturen und die Wissenschaftlichen Ausschüsse[30] im Rahmen des Frühwarn- und Reaktionssystems zusammen. Der Gesundheitssicherheitsausschuss, der die Maßnahmen der Mitgliedstaaten im Falle von Bedrohungen koordiniert, kann als zentrale Anlaufstelle für den Umgang mit Verwundbarkeiten im Bereich der öffentlichen Gesundheit dienen[31] und darauf hinwirken, dass hybride Bedrohungen (insbesondere Bioterrorismus) in Leitlinien für die Krisenkommunikation und bei Krisensimulationsübungen mit den Mitgliedstaaten berücksichtigt werden. Im Bereich der Lebensmittelsicherheit tauschen die Behörden über das Schnellwarnsystem für Lebens- und Futtermittel (RASFF) und das gemeinsame Risikomanagementsystem für den Zoll (CRMS) Informationen zur Risikoanalyse aus, um von kontaminierten Lebensmitteln ausgehende Gesundheitsgefahren zu erkennen. Was die Tier- und die Pflanzengesundheit betrifft, wird das vorhandene Instrumentarium[32] im Zuge der Überarbeitung des EU-Rechtsrahmens[33] durch neue Elemente ergänzt werden, um auch den Schutz vor hybriden Bedrohungen zu verbessern.

<u>Maßnahme 10:</u> Die Kommission wird in Zusammenarbeit mit den Mitgliedstaaten das Bewusstsein für und die Resilienz gegenüber hybriden Bedrohungen im Rahmen der

[29] Beschluss Nr. 1082/2013/EU des Europäischen Parlaments und des Rates vom 22. Oktober 2013 zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren und zur Aufhebung der Entscheidung Nr. 2119/98/EG (ABl. L 293 vom 5.11.2013, S. 1).

[30] Beschluss C(2015) 5383 der Kommission vom 7.8.2015 zur Einsetzung Wissenschaftlicher Ausschüsse in den Bereichen öffentliche Gesundheit, Verbrauchersicherheit und Umwelt.

[31] Im Einklang mit dem Beschluss Nr. 1082/2013/EU des Europäischen Parlaments und des Rates vom 22. Oktober 2013 zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren und zur Aufhebung der Entscheidung Nr. 2119/98/EG (ABl. L 293 vom 5.11.2013, S. 1).

[32] Z.B. EU-Impfstoffbanken, komplexe elektronische Tierseuchennachrichtensysteme, verschärfte Bestimmungen für Labors und andere Einrichtungen, die mit Krankheitserregern zu tun haben.

[33] Verordnung (EU) 2016/429 des Europäischen Parlaments und des Rates vom 9. März 2016 zu Tierseuchen und zur Änderung und Aufhebung einiger Rechtsakte im Bereich der Tiergesundheit („Tiergesundheitsrecht“) (ABl. L 84 vom 31.3.2016, S. 1). Was die Verordnung des Europäischen Parlaments und des Rates über Maßnahmen zum Schutz vor Pflanzenschädlingen („Pflanzengesundheitsrecht“) angeht, so haben das Europäische Parlament und der Rat am 16. Dezember 2015 eine politische Einigung über den Text erzielt.

bestehenden Bereitschafts- und Koordinierungsmechanismen, insbesondere des Gesundheitssicherheitsausschusses, verbessern.

4.4. Cybersicherheit

Die vernetzte und digitalisierte Gesellschaft bringt der EU große Vorteile. Jedoch könnten Cyberangriffe zu Störungen der digitalen Dienste in der gesamten EU führen und von Urhebern hybrider Bedrohungen gezielt eingesetzt werden. Daher ist es für den digitalen Binnenmarkt wichtig, die Resilienz der Kommunikations- und Informationssysteme in Europa zu stärken. Die Cybersicherheitsstrategie der EU und die Europäische Sicherheitsagenda liefern den allgemeinen strategischen Rahmen für Initiativen der EU zu Cybersicherheit und Cyberkriminalität. Die EU setzt sich im Rahmen der Cybersicherheitsstrategie aktiv für die Schaffung eines entsprechenden Bewusstseins und die Entwicklung von Kooperationsmechanismen und Gegenmaßnahmen ein. Insbesondere sollen mit der vorgeschlagenen Richtlinie über Netz- und Informationssicherheit[34] (NIS) die Risiken im Bereich der Cybersicherheit für ein breites Spektrum von Anbietern grundlegender Dienste in den Bereichen Energie, Verkehr, Finanzen und Gesundheit angegangen werden. Diese Anbieter sowie die Anbieter zentraler digitaler Dienste (z. B. Cloud-Computing) sollten angemessene Sicherheitsvorkehrungen treffen und gravierende Sicherheitsvorfälle unter Hinweis auf etwaige hybride Bedrohungen den zuständigen nationalen Behörden melden. Nach Verabschiedung durch das Europäische Parlament und den Rat dürften die Umsetzung und Anwendung der Richtlinie in allen Mitgliedsaaten deren Fähigkeiten zur Gewährleistung der Cybersicherheit verbessern und dazu führen, dass die Mitgliedstaaten im Bereich der Cybersicherheit durch Austausch von Informationen und von bewährten Methoden zur Abwehr hybrider Bedrohungen enger zusammenarbeiten. Insbesondere sieht die Richtlinie die Einrichtung eines Netzes aus 28 nationalen CSIRT (Computer Security Incident Response Teams, d. h. Reaktionsteams für Computersicherheitsverletzungen) und dem CERT-EU[35] für eine operative Zusammenarbeit auf freiwilliger Basis vor.

Zur Förderung der Zusammenarbeit zwischen öffentlichem und privatem Sektor und EU-weiter Ansätze zur Cybersicherheit hat die Kommission eine NIS-Plattform eingerichtet, über die bewährte Risikomanagementverfahren weitergegeben werden. Während die Mitgliedstaaten für die Festlegung der Sicherheitsanforderungen und der Modalitäten für die Meldung nationaler Vorfälle zuständig sind, sorgt die Kommission für eine möglichst große Kohärenz der Risikomanagementkonzepte, wobei insbesondere der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) eine wichtige Rolle zukommt.

[34] Vorschlag der Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union, COM(2013) 48 final vom 7.2.2013. Der Rat der EU und das Europäische Parlament haben über diesen Richtlinienvorschlag eine politische Einigung erzielt, so dass die Richtlinie demnächst offiziell verabschiedet werden dürfte.

[35] IT-Notfallteam (Computer Emergency Response Team – CERT-EU) für die EU-Institutionen.

<u>Maßnahme 11:</u> Die Kommission legt den Mitgliedstaaten nahe, vorrangig dafür zu sorgen, dass ein Netz der 28 CSIRT und des CERT-EU und ein Rahmen für die strategische Zusammenarbeit geschaffen und voll genutzt werden. 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 in der NIS-Richtlinie vorgesehenen sektorübergreifenden Kapazitäten für die Bündelung von Informationen und Fachkompetenz und die Koordinierung der raschen Reaktion auf Vorfälle kompatibel sind.

4.4.1. Industrie

Der verstärkte Rückgriff auf Cloud-Computing und Big Data hat die Verwundbarkeit durch hybride Bedrohungen erhöht. Die EU-Strategie für einen digitalen Binnenmarkt sieht eine vertragliche öffentlich-private Partnerschaft für Cybersicherheit[36] vor, deren Schwerpunkt auf Forschung und Innovation liegen und die dazu beitragen soll, dass die Union in diesem Bereich ein hohes Maß an technologischer Kapazität bewahrt. Die vertragliche öffentlich-private Partnerschaft wird dem Aufbau von Vertrauen zwischen den verschiedenen Marktakteuren dienen und Synergien zwischen der Angebots- und der Nachfrageseite schaffen. Zwar werden im Mittelpunkt der vertraglichen öffentlich-privaten Partnerschaft und der Begleitmaßnahmen zivile Cybersicherheitsprodukte und -dienste stehen, doch dürften diese Initiativen für die Technologieanwender auch einen besseren Schutz vor hybriden Bedrohungen mit sich bringen.

<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 Nutzer und Infrastrukturen besser vor den Cyberaspekten hybrider Bedrohungen zu schützen.

4.4.2. Energie

Das Aufkommen intelligenter Häuser und Geräte und die Entwicklung intelligenter Netze, die eine immer stärkere Digitalisierung der Energieversorgung nach sich ziehen, haben auch eine größere Verwundbarkeit durch Cyberangriffe zur Folge. Die Strategie für eine sichere europäische Energieversorgung[37] und die Strategie für die Energieunion[38] zielen auf einen alle Gefahren abdeckenden Ansatz ab, der auch die Frage der Resilienz gegenüber hybriden Bedrohungen berücksichtigt. Das Thematische Netz für den Schutz kritischer Energieinfrastrukturen (Thematic Network on Critical Energy Infrastructure Protection) fördert die Zusammenarbeit zwischen Akteuren im Energiebereich (Erdöl, Erdgas und Strom). Die Kommission hat eine webbasierte

[36] Die Mitte 2016 auf den Weg gebracht werden soll.
[37] Mitteilung der Kommission an das Europäische Parlament und den Rat „Strategie für eine sichere europäische Energieversorgung“, COM(2014) 330 final.
[38] Mitteilung „Rahmenstrategie für eine krisenfeste Energieunion mit einer zukunftsorientierten Klimaschutzstrategie“, COM(2015) 80 final.

Plattform[39] für die Analyse und den Austausch von Informationen über Bedrohungen und Vorfälle eingerichtet. Sie arbeitet auch gemeinsam mit Interessenträgern[40] an einer umfassenden Cybersicherheitsstrategie für den Energiesektor, um die Verwundbarkeiten beim Betrieb intelligenter Netze zu reduzieren. Trotz zunehmender Integration der Strommärkte sind die Vorschriften und Verfahren für den Umgang mit Krisensituationen weiterhin Sache der einzelnen Länder. Wir müssen sicherstellen, dass die Regierungen bei der Vorsorge, der Prävention und der Minderung der Risiken zusammenarbeiten und sich alle relevanten Akteure auf ein gemeinsames Regelwerk stützen.

Maßnahme 13: ***Die Kommission wird Leitlinien für Eigentümer intelligenter Netze erstellen, wie sie die Cybersicherheit ihrer Anlagen verbessern können. 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.***

4.4.3. Gewährleistung eines soliden Finanzsystems

Damit die Wirtschaft der EU funktionieren kann, braucht sie ein sicheres Finanz- und Zahlungssystem. Der Schutz des Finanzsystems einschließlich seiner Infrastruktur vor Cyberangriffen ist von wesentlicher Bedeutung, unabhängig davon, warum bzw. von wem es angegriffen wird. Um hybride Bedrohungen von Finanzdienstleistungen in der EU abzuwenden, muss die Branche die Gefahr verstehen, Abwehrmechanismen erprobt haben und über Technologien verfügen, um sich vor Angriffen schützen zu können. Daher ist der Austausch von Informationen über Bedrohungen zwischen den Finanzmarktteilnehmern untereinander sowie mit den zuständigen Behörden, einschlägigen Dienstleistern und Kunden entscheidend. Doch muss dieser Austausch auch gesichert sein und den Anforderungen des Datenschutzes gerecht werden. Im Einklang mit den entsprechenden Bemühungen im Rahmen internationaler Foren wie der G7 beabsichtigt die Kommission, die Faktoren zu ermitteln, die den Austausch von Informationen über Bedrohungen behindern, und Lösungen vorzuschlagen. Die Verfahrensabläufe zum Schutz der Wirtschaftstätigkeit und relevanter Infrastrukturen sollten unbedingt regelmäßig getestet und laufend weiterentwickelt werden, auch durch kontinuierliche Verbesserung der Sicherheitstechnologien.

Maßnahme 14: ***Die Kommission wird in Zusammenarbeit mit der ENISA[41], den Mitgliedstaaten, zuständigen internationalen, europäischen und nationalen Behörden und Finanzinstituten Plattformen und Netze für den Informationsaustausch über Bedrohungen fördern und Faktoren angehen, die den Austausch solcher Informationen behindern.***

[39] Incident and Threat Information Sharing EU Centre (ITIS-EUC).
[40] Über die Plattform EECSP (Energy Expert CyberSecurity Platform).
[41] Europäische Agentur für Netz- und Informationssicherheit.

4.4.4. Verkehr

Die modernen Verkehrssysteme (Schienen-, Straßen-, Luft- und Seeverkehr) stützen sich auf Informationssysteme, die für Cyberangriffe anfällig sind. Angesichts der grenzüberschreitenden Dimension kommt der EU hier eine besondere Rolle zu. Die Kommission wird in Abstimmung mit den Mitgliedstaaten weiterhin Cyberbedrohungen und Risiken im Zusammenhang mit unrechtmäßigen Eingriffen in den Verkehrsbereich analysieren. Derzeit erstellt die Kommission in Zusammenarbeit mit der Europäischen Agentur für Flugsicherheit (EASA)[42] einen Fahrplan für die Cybersicherheit im Luftverkehr. Cyberbedrohungen der maritimen Sicherheit werden zudem in der Strategie der Europäischen Union für maritime Sicherheit und dem dazugehörigen Aktionsplan behandelt.

<u>Maßnahme 15:</u> 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.

4.5. Bekämpfung der Finanzierung hybrider Bedrohungen

Die Verursachung hybrider Bedrohungen muss auch finanziert werden. So können mit Geld terroristische Gruppen unterstützt oder subtilere Formen der Destabilisierung gefördert werden, etwa indem Interessengruppen oder Parteien am politischen Rand unterstützt werden. Die EU hat ihre Anstrengungen zur Bekämpfung der organisierten Kriminalität und Terrorismusfinanzierung intensiviert, wie aus der Europäischen Sicherheitsagenda und insbesondere dem dazugehörigen Aktionsplan[43] hervorgeht. So werden insbesondere mit den neuen EU-Vorschriften zur Bekämpfung der Geldwäsche die Maßnahmen gegen Terrorismusfinanzierung und Geldwäsche verschärft; die Ermittlung und Verfolgung verdächtiger Geldtransfers und Informationsströme durch die nationalen Zentralstellen für Verdachtsmeldungen (FIU) werden erleichtert und die Rückverfolgbarkeit von Geldtransfers in der Europäischen Union wird sichergestellt. Dies könnte auch zur Abwehr hybrider Bedrohungen beitragen. Im Bereich der GASP-Instrumente könnten ebenfalls maßgeschneiderte, wirksame restriktive Maßnahmen zur Abwehr hybrider Bedrohungen ins Auge gefasst werden.

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

---

[42] Die von der Kommission im Dezember 2015 vorgeschlagene neue EASA-Verordnung ist derzeit Gegenstand von Beratungen zwischen dem Europäischen Parlament und dem Rat. Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung gemeinsamer Vorschriften für die Zivilluftfahrt und zur Errichtung einer Agentur der Europäischen Union für Flugsicherheit sowie zur Aufhebung der Verordnung (EG) Nr. 216/2008 des Europäischen Parlaments und des Rates, COM(2015) 613 final, 2015/0277(COD).

[43] Mitteilung der Kommission an das Europäische Parlament und den Rat „Ein Aktionsplan für ein intensiveres Vorgehen gegen Terrorismusfinanzierung“, COM(2016) 50 final.

4.6. Stärkung der Resilienz gegen Radikalisierung und gewalttätigen Extremismus

Zwar sind Terroranschläge und gewalttätiger Extremismus nicht per se hybrider Natur, doch können Urheber hybrider Bedrohungen anfällige Mitglieder einer Gesellschaft gezielt ansprechen und rekrutieren und sie über die modernen Kommunikationskanäle (z. B. die sozialen Medien und Proxy-Gruppen) und durch Propaganda radikalisieren.

Um gegen extremistische Inhalte im Internet vorzugehen, analysiert die Kommission derzeit im Rahmen der Strategie für einen digitalen Binnenmarkt den Bedarf an etwaigen neuen Maßnahmen, wobei deren Auswirkungen auf die Grundrechte der Meinungs- und Informationsfreiheit gebührend berücksichtigt werden. Dazu könnten auch strikte Verfahren zur Entfernung illegaler Inhalte („Melde- und Abhilfeverfahren“) gehören, ohne dass rechtmäßige Inhalte vom Netz genommen werden, sowie eine größere Verantwortung und Sorgfaltspflicht von Mittlern bei der Verwaltung ihrer Netze und Systeme. Dies würde den bereits praktizierten freiwilligen Ansatz ergänzen, bei dem Internetunternehmen und soziale Medien (insbesondere im Rahmen des EU-Internetforums) in Zusammenarbeit mit der bei Europol angesiedelten EU-Meldestelle für Internetinhalte terroristische Propaganda zügig entfernen.

Im Kontext der Europäischen Sicherheitsagenda wird Radikalisierung durch den Austausch von Erfahrungen und die Entwicklung einer guten Praxis bekämpft, unter anderem durch Zusammenarbeit in Drittländern. Das Beratungsteam für strategische Kommunikation in Bezug auf Syrien (SSCAT) hat die Aufgabe, die Entwicklung und Verbreitung alternativer Botschaften zu fördern, um terroristischer Propaganda entgegenzuwirken. Das Aufklärungsnetzwerk gegen Radikalisierung (RAN) unterstützt sowohl die Mitgliedstaaten als auch Praktiker, die in ihrer Arbeit mit radikalisierten Personen (wie ausländischen terroristischen Kämpfern) oder solchen, die als radikalisierungsgefährdet gelten, zu tun haben. Das Angebot des Aufklärungsnetzwerks gegen Radikalisierung umfasst Schulungen und Beratung sowie Unterstützung für bestimmte Drittländer, wenn diese zu einem entsprechenden Engagement bereit sind. Darüber hinaus fördert die Kommission die justizielle Zusammenarbeit zwischen den Akteuren der Strafrechtspflege, einschließlich Eurojust, bei der Bekämpfung von Terrorismus und Radikalisierung in allen Mitgliedstaaten, auch was den Umgang mit ausländischen terroristischen Kämpfern und Rückkehrern anbelangt.

Ergänzend zu den genannten Ansätzen trägt die EU im Rahmen des **auswärtigen Handelns** zur Bekämpfung von gewalttätigem Extremismus bei, unter anderem durch Engagement und Aufklärungsmaßnahmen in Drittländern, Prävention (Bekämpfung von Radikalisierung und Terrorismusfinanzierung) sowie Maßnahmen, um gegen die ursächlichen wirtschaftlichen, politischen und gesellschaftlichen Faktoren vorzugehen, die den Nährboden für terroristische Aktivitäten bilden.

<u>Maßnahme 17:</u> 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.

4.7. Intensivierung der Zusammenarbeit mit Drittländern

Wie in der Europäischen Sicherheitsagenda hervorgehoben wurde, konzentriert sich die EU verstärkt auf den Aufbau von Kapazitäten in ***Partnerländern*** im Sicherheitssektor, unter anderem indem sie auf den engen Zusammenhang von Sicherheit und Entwicklung setzt und die sicherheitspolitische Dimension der überarbeiteten Europäischen Nachbarschaftspolitik[44] ausbaut. Diese Maßnahmen können auch die Resilienz der Partner gegenüber hybriden Aktivitäten stärken.

Die Kommission beabsichtigt, den Austausch operativer und strategischer Informationen mit den Erweiterungsländern sowie im Rahmen der Östlichen Partnerschaft und der Südlichen Nachbarschaft weiter zu intensivieren, wenn dies zur Bekämpfung der organisierten Kriminalität, des Terrorismus, der irregulären Migration und des illegalen Kleinwaffenhandels beiträgt. Im Bereich der Terrorismusbekämpfung verstärkt die EU ihre Zusammenarbeit mit Drittländern durch Ausbau des Sicherheitsdialogs und durch Aktionspläne.

Die Finanzierungsinstrumente der EU im Außenbereich zielen auf den Aufbau funktionierender und rechenschaftspflichtiger Institutionen in Drittländern ab[45] – eine Voraussetzung, um wirksam auf Sicherheitsbedrohungen reagieren und die Resilienz verbessern zu können. In diesem Zusammenhang sind die Reform des Sicherheitssektors und der Kapazitätsaufbau zur Förderung von Sicherheit und Entwicklung[46] wesentliche Instrumente. Im Rahmen des Instruments, das zu Stabilität und Frieden beiträgt[47], hat die Kommission Maßnahmen zur Stärkung der Resilienz gegenüber Cyberangriffen entwickelt und die Fähigkeiten von Partnern zur Erkennung und Bekämpfung von Cyberangriffen und Cyberkriminalität verbessert, damit hybride Bedrohungen in Drittländern abgewehrt werden können. Außerdem finanziert die EU Maßnahmen zum Aufbau von Kapazitäten in Partnerländern zur Reduzierung von CBRN-Sicherheitsrisiken[48].

---

[44] Gemeinsame Mitteilung an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Überprüfung der Europäischen Nachbarschaftspolitik“, JOIN(2015) 50 final vom 18.11.2015.

[45] Ebenda; Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Erweiterungsstrategie der EU“, COM(2015) 611 final vom 10.11.2015. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Für eine EU-Entwicklungspolitik mit größerer Wirkung: Agenda für den Wandel“, KOM(2011) 637 endg. vom 13.10.2011.

[46] Gemeinsame Mitteilung „Kapazitätsaufbau zur Förderung von Sicherheit und Entwicklung – Befähigung unserer Partner zur Krisenprävention und -bewältigung“, JOIN(2015) 17 final.

[47] Verordnung (EU) Nr. 230/2014 des Europäischen Parlaments und des Rates vom 11. März 2014 zur Schaffung eines Instruments, das zu Stabilität und Frieden beiträgt (ABl. L 77 vom 15.3.2014, S. 1).

[48] Die Maßnahmen erstrecken sich unter anderem auf die Bereiche Grenzüberwachung, Krisenmanagement, Ersthilfe, illegaler Handel, Kontrolle der Ausfuhr von Gütern mit doppeltem Verwendungszweck, Seuchenüberwachung und -bekämpfung, Nuklearforensik, Rückkehr zur Normalität

Ferner könnten die Mitgliedstaaten angesichts des angestrebten umfassenden Konzepts für das Krisenmanagement auf Instrumente und Missionen der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) zurückgreifen, die sie für sich genommen oder in Ergänzung zu anderen EU-Instrumenten einsetzen könnten, um Partner beim Ausbau ihrer Kapazitäten zu unterstützen. Folgende Maßnahmen könnten in Frage kommen: i) Unterstützung im Bereich strategische Kommunikation, ii) Beratung von Schlüsselministerien, deren Ressorts durch hybride Bedrohungen besonders gefährdet sind, iii) zusätzliche Unterstützung beim Grenzmanagement in Notsituationen. Darüber hinaus könnte geprüft werden, ob weitere Synergien zwischen den GSVP-Instrumenten und den Akteuren der Bereiche Sicherheit, Zoll und Justiz, einschließlich der einschlägigen EU-Agenturen[49], Interpol und der Europäischen Gendarmerietruppe (im Rahmen ihrer jeweiligen Mandate) möglich sind.

<u>Maßnahme 18:</u> 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 eigenständige Maßnahme oder ergänzend zu anderen EU-Instrumenten entsandt werden, um Partner bei der Verbesserung ihrer Kapazitäten zu unterstützen.

5. PRÄVENTION, KRISENREAKTION UND RÜCKKEHR ZUR NORMALITÄT

Wie in Abschnitt 3.1 dargelegt, soll die vorgeschlagene EU-Analyseeinheit für hybride Bedrohungen (EU Hybrid Fusion Cell) relevante Indikatoren prüfen, damit hybriden Bedrohungen vorgebeugt und darauf reagiert werden kann und die Entscheidungsträger der EU über einschlägige Informationen verfügen. Zwar können Schwachstellen durch langfristige Maßnahmen auf nationaler und EU-Ebene abgebaut werden, doch kurzfristig kommt es weiterhin darauf an, dass die Fähigkeit der Mitgliedstaaten und der Union gestärkt wird, rasch und koordiniert zu handeln, wenn es darum geht, hybriden Bedrohungen vorzubeugen, darauf zu reagieren und sich davon zu erholen.

Eine rasche Reaktion auf Ereignisse, die durch hybride Bedrohungen ausgelöst sind, ist von grundlegender Bedeutung. In diesem Zusammenhang könnte die Förderung nationaler Katastrophenschutzmaßnahmen und -kapazitäten durch das Europäische Zentrum für die Koordination von Notfallmaßnahmen[50] ein geeignetes Instrument für die Reaktion auf Aspekte hybrider Bedrohungen sein, die Katastrophenschutzmaßnahmen erforderlich machen. Dies könnte in Abstimmung mit anderen Krisenreaktionsmechanismen und Frühwarnsystemen der EU erfolgen, insbesondere mit

---

nach einem Vorfall und Schutz stark gefährdeter Einrichtungen. Methoden, die sich im Zusammenhang mit den im Rahmen des CBRN-Aktionsplans der EU entwickelten Instrumenten bewährt haben, wie die Tätigkeit des Europäischen Ausbildungszentrums für Gefahrenabwehr im Nuklearbereich und die Teilnahme der EU an der internationalen Arbeitsgruppe für Fragen der Grenzüberwachung, können auch an Drittländer weitergeben werden.

[49] Europol, Frontex, CEPOL, Eurojust.

[50] http://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en

dem EAD-Lagezentrum, wenn es um die äußere Sicherheit geht, und dem Zentrum für strategische Analyse und Reaktion im Bereich der inneren Sicherheit.

Die Solidaritätsklausel (Artikel 222 AEUV) ermöglicht ein gemeinsames Handeln der Union und der Mitgliedstaaten, wenn ein Mitgliedstaat von einem Terroranschlag, einer Naturkatastrophe oder einer vom Menschen verursachten Katastrophe betroffen ist. Die Unterstützung der Mitgliedstaaten durch die Union ist im Beschluss 2014/415/EU des Rates[51] geregelt. Die Vorkehrungen für die Koordinierung im Rat sollten sich auf die Integrierte EU-Regelung für die politische Reaktion auf Krisen[52] stützen. Demnach nennen die Kommission und die Hohe Vertreterin (in ihren jeweiligen Zuständigkeitsbereichen) die einschlägigen Instrumente der Union und unterbreiten dem Rat Vorschläge für Beschlüsse über Sondermaßnahmen.

Artikel 222 AEUV gilt auch für Situationen, in denen ein Mitgliedstaat von einem Terroranschlag oder einer Katastrophe betroffen ist und direkte Unterstützung durch einen oder mehrere Mitgliedstaaten erhält. In diesem Fall findet der Beschluss 2014/415/EU des Rates keine Anwendung. Wenn ein EU-Mitgliedstaat mit erheblichen hybriden Bedrohungen konfrontiert ist, sollten die Kommission und die Hohe Vertreterin (in ihren jeweiligen Zuständigkeitsbereichen) in Anbetracht der häufig unklaren Sachlage im Zusammenhang mit hybriden Handlungen jeweils bewerten, ob als letztes Mittel auf die Solidaritätsklausel zurückgegriffen werden sollte.

Ist hingegen ein EU-Mitgliedstaat multiplen ernsthaften hybriden Bedrohungen ausgesetzt, die einen bewaffneten Angriff darstellen, so könnte (statt Artikel 222 AEUV) Artikel 42 Absatz 7 EUV herangezogen werden, damit angemessen und zeitnah reagiert werden kann. Kommt es zu großangelegten, schwerwiegenden hybriden Bedrohungen, so kann auch eine verstärkte Zusammenarbeit und Koordinierung mit der NATO erforderlich sein.

Die Mitgliedstaaten sollten ihre Einsatzkräfte auch für potenzielle hybride Bedrohungen wappnen. Damit sie im Falle eines hybriden Angriffs rasch und wirksam Entscheidungen treffen können, müssen sie regelmäßige Übungen – auf Arbeits- und auf politischer Ebene – abhalten, um die Funktionsfähigkeit der nationalen und multinationalen Entscheidungsprozesse zu testen. Ziel wäre ein gemeinsames Protokoll der Mitgliedstaaten, der Kommission und der Hohen Vertreterin für das operative Vorgehen im Ernstfall mit konkreten Verfahren, die bei einer hybriden Bedrohung – von der ersten Phase der Identifizierung der Bedrohung bis zur Endphase eines Angriffs – zu befolgen sind, und mit der Zuordnung der Aufgaben jeder EU-Institution und jedes Akteurs in dem Prozess.

Im Rahmen der GSVP könnte folgender wichtiger Beitrag geleistet werden: a) zivile und militärische Ausbildung, b) Beratungsmissionen zur Verbesserung der Kapazitäten eines

[51] Beschluss 2014/415/EU des Rates über die Vorkehrungen für die Anwendung der Solidaritätsklausel durch die Union (ABl. L 192 vom 1.7.2014, S. 53).
[52] http://www.consilium.europa.eu/de/documents-publications/publications/2014/eu-ipcr/

bedrohten Staats im Bereich Sicherheit und Verteidigung, c) Notfallplan zur Erkennung von Anzeichen für hybride Bedrohungen und zur Stärkung der Frühwarnkapazitäten, d) Unterstützung beim Grenzkontrollmanagement in Notsituationen, e) Unterstützung in Spezialbereichen wie Eindämmung der CBRN-Risiken und Evakuierung von nicht am Kampfeinsatz beteiligten Personen.

Maßnahme 19: ***Die Hohe Vertreterin und die Kommission werden in Abstimmung mit den Mitgliedstaaten für die Erstellung eines gemeinsamen Protokolls für das operative Vorgehen 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.***

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.***

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.***

6. INTENSIVIERUNG DER ZUSAMMENARBEIT MIT DER NATO

Hybride Bedrohungen sind nicht nur für die EU eine Herausforderung, sondern auch für andere große Partnerorganisationen wie die Vereinten Nationen (UN), die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) und insbesondere die NATO. Damit wirksam reagiert werden kann, sind Dialog und Koordinierung zwischen den Organisationen sowohl auf politischer als auch auf operativer Ebene erforderlich. Eine engere Zusammenarbeit zwischen der EU und der NATO würde beide Organisationen besser in die Lage versetzen, sich auf hybride Bedrohungen in geeigneter Weise vorzubereiten und darauf zu reagieren. Dabei würden sie sich – gestützt auf einen inklusiven Ansatz – ergänzen und gegenseitig unterstützen und gleichzeitig die Beschlussfassungsautonomie und die Datenschutzvorschriften beider Organisationen achten.

Die beiden Organisationen teilen die gleichen Werte und stehen vor ähnlichen Herausforderungen. Die EU-Mitgliedstaaten und die NATO-Verbündeten erwarten von ihnen, dass sie sie unterstützen und im Falle einer Krise rasch, entschlossen und koordiniert handeln bzw. im Idealfall die Krise verhindern. Verschiedene Bereiche wurden ermittelt, in denen die Zusammenarbeit und die Koordinierung zwischen der EU und der NATO ausgebaut werden können, darunter Lagebewusstsein, strategische Kommunikation, Cybersicherheit und Krisenprävention und -reaktion. Der derzeitige informelle Dialog zwischen der EU und der NATO über hybride Bedrohungen sollte

intensiviert werden, um die Tätigkeit der beiden Organisationen in diesem Bereich aufeinander abzustimmen.

Damit EU und NATO in komplementärer Weise auf Bedrohungen reagieren können, ist es wichtig, dass sie vor und während einer Krise die Lage in gleicher Weise beurteilen. Dies ließe sich durch einen regelmäßigen Austausch von Analysen und Erfahrungen erreichen, aber auch durch unmittelbare Kontakte zwischen der EU-Analyseeinheit und der entsprechenden Stelle bei der NATO. Ebenso wichtig ist eine bessere gegenseitige Kenntnis der Krisenmanagementverfahren, damit bei Bedarf rasch und wirksam gehandelt werden kann. Die Resilienz könnte gestärkt werden, indem bei der Festlegung von Benchmarks für kritische Komponenten der Infrastrukturen für Komplementarität gesorgt und im Bereich der strategischen Kommunikation und der Cyberabwehr eng zusammenarbeitet wird. Gemeinsame Übungen auf politischer und Arbeitsebene unter Einschluss aller Beteiligten würden die Fähigkeit beider Organisationen zu einer fundierten Entscheidungsfindung verbessern. Die Sondierung weiterer Optionen für Ausbildungs- und Schulungsmaßnahmen würde dazu beitragen, dass in einschlägigen Bereichen ein vergleichbares Maß an Fachwissen vorhanden ist.

<u>Maßnahme 22:</u> 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 ein inklusiver Ansatz verfolgt und die Beschlussfassungsautonomie jeder Organisation geachtet wird.

7. SCHLUSSFOLGERUNGEN

Diese Gemeinsame Mitteilung enthält Maßnahmen, die dazu beitragen sollen, hybride Bedrohungen abzuwehren und die Resilienz auf EU- und nationaler Ebene sowie der Partner zu stärken. Da der Schwerpunkt auf der **Verbesserung des Bewusstseins** für hybride Bedrohungen liegt, wird vorgeschlagen, spezielle Mechanismen für den Informationsaustausch mit den Mitgliedstaaten zu schaffen und die Kapazitäten der EU für strategische Kommunikation zu koordinieren. Außerdem werden Maßnahmen zur **Stärkung der Resilienz** in Bereichen wie Cybersicherheit, kritische Infrastrukturen, Schutz des Finanzsystems vor illegaler Nutzung und Bekämpfung von gewalttätigem Extremismus und Radikalisierung umrissen. In jedem dieser Bereiche wird die Durchführung der von der EU und den Mitgliedstaaten vereinbarten Strategien sowie die vollständige Umsetzung der vorhandenen Rechtsvorschriften durch die Mitgliedstaaten ein erster wichtiger Schritt sein. Außerdem werden einige konkretere Maßnahmen vorgeschlagen, mit denen diese Bemühungen untermauert werden sollen.

Was die **Prävention, die Abwehr und die Erholung von hybriden Bedrohungen** angeht, so wird vorgeschlagen zu prüfen, inwieweit bei großangelegten, schweren hybriden Angriffen auf die Solidaritätsklausel des Artikels 222 AEUV (gemäß den Vorkehrungen des dazugehörigen Beschlusses) und auf Artikel 42 Absatz 7 EUV zurückgegriffen werden kann. Die Fähigkeit zur strategischen Entscheidungsfindung

könnte durch Einführung eines gemeinsamen Protokolls für das operative Vorgehen verbessert werden.

Schließlich wird eine **Intensivierung der Zusammenarbeit und Koordinierung zwischen der EU und der NATO** bei der gemeinsamen Abwehr hybrider Bedrohungen vorgeschlagen.

Für die Durchführung dieses Gemeinsamen Rahmens werden die Hohe Vertreterin und die Kommission die ihnen zur Verfügung stehenden zweckdienlichen EU-Instrumente mobilisieren. Es ist dringend geboten, dass die EU gemeinsam mit den Mitgliedstaaten für die Verringerung der Risiken sorgt, die mit potenziellen hybriden Bedrohungen durch staatliche und nichtstaatliche Akteure verbunden sind.