Rat der
Europäischen Union

Brüssel, den 18. Juni 2018
(OR. en)

10242/18

HYBRID 11	**ENER 242**
COPS 223	**EUMC 106**
PROCIV 40	**CIVCOM 120**
CSDP/PSDC 346	**TRANS 271**
CYBER 147	**COEST 126**
CFSP/PESC 583	**ESPACE 32**
JAI 668	**COTER 80**
ECOFIN 632	**CSC 200**
POLMIL 89	**IPCR 15**

ÜBERMITTLUNGSVERMERK

Absender:	Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag des Generalsekretärs der Europäischen Kommission
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	JOIN(2018) 16 final
Betr.:	GEMEINSAME MITTEILUNG AN DAS EUROPÄISCHE PARLAMENT, DEN EUROPÄISCHEN RAT UND DEN RAT Stärkung der Resilienz und Ausbau der Kapazitäten zur Abwehr hybrider Bedrohungen

Die Delegationen erhalten in der Anlage das Dokument JOIN(2018) 16 final.

Anl.: JOIN(2018) 16 final

EUROPÄISCHE
KOMMISSION

HOHE VERTRETERIN
DER UNION FÜR
AUSSEN- UND
SICHERHEITSPOLITIK

Brüssel, den 13.6.2018
JOIN(2018) 16 final

GEMEINSAME MITTEILUNG AN DAS EUROPÄISCHE PARLAMENT, DEN EUROPÄISCHEN RAT UND DEN RAT

Stärkung der Resilienz und Ausbau der Kapazitäten zur Abwehr hybrider Bedrohungen

1. EINLEITUNG

Hybride Aktivitäten staatlicher und nichtstaatlicher Akteure stellen weiterhin eine ernste und akute Bedrohung für die EU und ihre Mitgliedstaaten dar. Die Versuche, Länder zu destabilisieren, indem das Vertrauen der Öffentlichkeit in staatliche Institutionen untergraben und die zentralen Werte der Gesellschaften infrage gestellt werden, haben zugenommen. Unsere Gesellschaften sehen sich großen Herausforderung durch diejenigen gegenüber, die der EU und ihren Mitgliedstaaten schaden wollen, sei es durch Cyberangriffe auf die Wirtschaft und öffentliche Dienste, gezielte Desinformationskampagnen oder feindselige Militäraktionen.

Hybride Kampagnen sind multidimensional, kombinieren Zwangsausübung mit subversiven Maßnahmen und nutzen zur Destabilisierung des Gegners sowohl konventionelle als auch nicht konventionelle Mittel und Taktiken auf diplomatischer, militärischer, wirtschaftlicher und technologischer Ebene. Sie sind so konzipiert, dass sie schwer aufzudecken oder jemandem zuzuordnen sind und können sowohl von staatlichen als auch nichtstaatlichen Akteuren ausgehen. Der Nervengift-Anschlag von Salisbury im vergangenen März[1] hat einmal mehr verdeutlicht, wie vielfältig hybride Bedrohungen sein können und wie groß das Spektrum der verfügbaren Taktiken inzwischen ist. In seiner Reaktion auf diesen Vorfall unterstrich der Europäische Rat[2], dass die EU und ihre Mitgliedstaaten ihre Fähigkeiten zur Aufdeckung, Verhinderung und Abwehr hybrider Bedrohungen ausbauen müssen, unter anderem in den Bereichen Cyberfragen, strategische Kommunikation und Spionageabwehr. Zudem wies er darauf hin, dass die Abwehrfähigkeit gegen chemische, biologische, radiologische und nukleare (CBRN) Bedrohungen gestärkt werden muss.

Die von nichtkonventionellen Waffen ausgehenden Gefahren fallen wegen des potenziellen Ausmaßes der verursachten Schäden in eine eigene Kategorie. Sie sind nicht nur schwer aufzudecken und jemandem zuzuordnen, sondern auch ihre Bewältigung ist ein komplexes Unterfangen. Generellen Anlass zur Sorge geben der internationalen Gemeinschaft[3] auch chemische, biologische, radiologische und nukleare Bedrohungen, die noch massiver als hybride Bedrohungen sind und auch mit Terrorismus in Verbindung stehen können, wobei insbesondere das Risiko der geografischen Weiterverbreitung und die eventuelle Weitergabe an nichtstaatliche Akteure besorgniserregend sind.

Der Aufbau von Resilienz gegenüber diesen Bedrohungen und die Stärkung der Kapazitäten fallen in erster Linie in die Zuständigkeit der Mitgliedstaaten. Die EU-Organe haben jedoch bereits eine Reihe von Maßnahmen ergriffen, um die nationalen Anstrengungen zu verstärken. Dazu gehört auch die enge Zusammenarbeit mit anderen internationalen Akteuren, wie insbesondere der Nordatlantikvertrags-Organisation (NATO)[4]. Diese Arbeiten könnten ausgeweitet werden, um die Mitgliedstaaten in Bereichen wie Krisenreaktion zu unterstützen[5].

---

1 Bezüglich des Anschlags von Salisbury stimmte der Europäische Rat am 22. März 2018 „mit der Einschätzung der Regierung des Vereinigten Königreichs überein, wonach sehr wahrscheinlich die Russische Föderation für den Anschlag verantwortlich ist und es keine andere plausible Erklärung gibt."

2 Schlussfolgerungen des Europäischen Rates von März 2018.

3 So auch dem Sicherheitsrat der Vereinten Nationen, siehe Resolution S/RES/2325 (2016) vom 14. Dezember 2016.

4 Die Abwehr hybrider Bedrohungen ist einer der sieben Bereiche der Zusammenarbeit mit der Nordatlantikvertrags-Organisation gemäß der Gemeinsamen Erklärung, die vom Präsidenten des Europäischen Rates, dem Präsidenten der Europäischen Kommission und dem Generalsekretär der Nordatlantikvertrags-Organisation im Juli 2016 in Warschau unterzeichnet wurde.

5 Auf dem G7-Gipfel im Juni 2018 in Charlevoix wurde zudem vereinbart, einen G7-Schnellreaktionsmechanismus zu entwickeln, um Bedrohungen für Demokratien abzuwehren:

Mit dieser gemeinsamen Mitteilung wird auch der Aufforderung des Europäischen Rates nachgekommen, diese Arbeiten voranzutreiben. Sie ist Teil eines umfassenderen Pakets, zu dem auch der jüngste Fortschrittsbericht zur Sicherheitsunion[6] gehört, der eine Bilanz der Umsetzung des CBRN-Aktionsplans vom Oktober 2017[7] (Abwehr chemischer, biologischer, radiologischer und nuklearer Risiken) sowie einen Ausblick auf das weitere Vorgehen zu dessen Umsetzung enthält. Zu dem Paket gehört ferner der zweite Fortschrittsbericht[8] über die Durchführung der 22 Maßnahmen des „Gemeinsamen Rahmens für die Abwehr hybrider Bedrohungen – eine Antwort der Europäischen Union“[9].

2. DIE ANTWORT DER EU

Die Kommission und die Hohe Vertreterin haben konsequente Anstrengungen unternommen, um die Fähigkeiten der EU auszubauen und die Mitgliedstaaten wirksam bei der Abwehr sowohl hybrider als auch chemischer, biologischer, radiologischer und nuklearer Bedrohungen zu unterstützen. In Bereichen wie strategische Kommunikation, Lageerfassung, Stärkung der Abwehrbereitschaft und Resilienz sowie Stärkung der Krisenreaktionskapazitäten wurden bereits greifbare Ergebnisse erzielt.

Die im Anschluss an den Europäischen Rat vom März 2015 eingerichtete East StratCom Task Force hat bei den Arbeiten zur Antizipierung, Rückverfolgung und Bekämpfung von Desinformationen aus ausländischen Quellen eine Führungsrolle übernommen. Die Analysen und die Informationsarbeit[10] der Experten der Task Force haben das Bewusstsein für die Auswirkungen russischer Desinformationen erheblich geschärft. In den letzten zwei Jahren hat die Task Force über 4000 Fälle von Desinformation aufgedeckt, von denen viele gezielt gegen Europa gerichtet waren. Ein weiterer Schwerpunkt der Arbeit der East StratCom Task Force ist die verbesserte Bereitstellung positiver Informationen mit dem Ziel einer größeren Breitenwirkung in der östlichen Nachbarschaft. Aufgrund dieses Erfolgs wurden zwei weitere Task Forces mit anderer geografischer Ausrichtung eingerichtet: eine Task Force für den Westbalkan und eine Task Force für die arabischsprachige Welt.

Es wurden wichtige Schritte unternommen, um die nötigen Strukturen für eine verbesserte Lageerfassung und zur Unterstützung der Entscheidungsfindung aufzubauen. 2016 wurde innerhalb des EU-Zentrums für Informationsgewinnung und -analyse des Europäischen Auswärtigen Dienstes die EU-Analyseeinheit für hybride Bedrohungen eingerichtet. Sie nimmt von verschiedenen Interessenträgern stammende, sowohl als geheim eingestufte als auch frei zugängliche Informationen über hybride Bedrohungen entgegen und wertet sie aus. Bislang wurden über 100 Bewertungen und Briefings vorgelegt, die an die EU-Institutionen und die Mitgliedstaaten als Informationsgrundlage für die Entscheidungsfindung der EU weitergegeben wurden. Die EU-Analyseeinheit für hybride Bedrohungen arbeitet eng mit dem Europäischen Zentrum zur Bewältigung hybrider Bedrohungen in Helsinki zusammen. Das Zentrum wurde im April 2017 eingerichtet, um den strategischen Dialog zu fördern und Forschungsarbeiten und Analysen zu hybriden

---

https://g7.gc.ca/en/official-documents/charlevoix-commitment-defending-democracy-from-foreign-threats/

6 Fünfzehnter Fortschrittsbericht „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion“, COM(2018) 470 final.

7 COM(2017) 610 final.

8 Gemeinsamer Bericht über die Umsetzung des Gemeinsamen Rahmens für die Abwehr hybrider Bedrohungen (Juli 2017 bis Juli 2018), JOIN(2018) 14.

9 JOIN(2016) 18 final.

10 Siehe www.euvsdisinfo.eu

Bedrohungen durchzuführen. Mittlerweile sind 16 Länder[11] Mitglied des Zentrums, das kontinuierliche Unterstützung durch die EU erhält.

Auch zur Stärkung der Abwehrbereitschaft und der Resilienz wurden wichtige Schritte unternommen, insbesondere was chemische, biologische, radiologische und nukleare Bedrohungen anbelangt. In den letzten sechs Monaten wurde viel getan, um Defizite bei der Abwehrbereitschaft gegenüber chemischen, biologischen, radiologischen und nuklearen Sicherheitsvorfällen zu ermitteln, vor allem in Bezug auf die Detektionsfähigkeiten zur Verhütung chemischer, biologischer, radiologischer und nuklearer Angriffe. Auf Initiative der Kommission führte ein Konsortium nationaler Experten für verschiedene chemische, biologische, radiologische und nukleare Szenarien eine Analyse der Defizite bei der Detektionsausrüstung durch. Der Bericht über diese Defizitanalyse wurde den Mitgliedstaaten übermittelt, damit sie fundierte Entscheidungen über Detektionsstrategien treffen und operative Maßnahmen ergreifen können, um die festgestellten Defizite zu beheben.

Diese Arbeiten wurden durch Übungen zur Prüfung der erzielten Fortschritte untermauert. Bei der 2017 veranstalteten parallelen und koordinierten Übung (PACE17) mit der Nordatlantikvertrags-Organisation wurde die Reaktionsfähigkeit der EU im Fall einer hybriden Krise großen Maßstabs eingehend geprüft. Bei dieser größten bislang durchgeführten Übung wurden nicht nur das EU-Einsatzprotokoll für die Abwehr hybrider Bedrohungen („EU Hybrid Playbook“) und die verschiedenen EU-Reaktionsmechanismen und deren Fähigkeit zur effizienten Interaktion getestet, sondern auch die Interaktion der EU-Reaktion auf hybride Bedrohungen mit den Maßnahmen der Nordatlantikvertrags-Organisation. Eine Übung für 2018 befindet sich in der Planungsphase mit dem Ziel, diese Art von Übung als jährliche Praxis zu etablieren und die Mitgliedstaaten bei der Stärkung ihre Reaktionsfähigkeiten auf hybride Krisen zu unterstützen.

Diese konkreten Maßnahmen verdeutlichen, dass die von der EU eingeführten Politikrahmen Früchte tragen: In den letzten beiden Jahren wurde eine Reihe weiterer Rahmen entwickelt, um die Arbeiten der EU zu lenken und zu fokussieren.

In dem im April 2016 vorgelegten *Gemeinsamen Rahmen für die Abwehr hybrider Bedrohungen – eine Antwort der Europäischen Union*[12] wird ein ressortübergreifender Ansatz, der sich auf 22 Maßnahmenbereiche erstreckt, zur Abwehr **hybrider Bedrohungen** und zur Stärkung der Resilienz der EU und ihrer Mitgliedstaaten sowie der internationalen Partner unterstützt. Die meisten der im Gemeinsamen Rahmen festgelegten Maßnahmen konzentrieren sich auf die Verbesserung der Lageerfassung und die Stärkung der Resilienz, um die Reaktionsfähigkeit zu verbessern. Sie reichen von der Steigerung der EU-Kapazität für Informationsanalysen über den besseren Schutz kritischer Infrastrukturen und der Cybersicherheit bis hin zur Bekämpfung von Radikalisierung und gewaltbereitem Extremismus. Cyberbedrohungen und Cyberangriffe sind ebenfalls wesentliche Schwerpunkte des Gemeinsamen Rahmens. Aus dem zweiten Fortschrittsbericht über die Umsetzung des Gemeinsamen Rahmens, der parallel zu dieser Gemeinsamen Mitteilung angenommen wird, geht hervor, dass bei diesen Maßnahmen

[11] 14 der derzeit 16 Mitglieder sind EU-Mitgliedstaaten: Dänemark, Deutschland, Estland, Finnland, Frankreich, Italien, Lettland, Litauen, die Niederlande, Polen, Spanien, Schweden, die Tschechische Republik, das Vereinigte Königreich. Seine Einrichtung geht auf den Gemeinsamen Rahmen für die Abwehr hybrider Bedrohungen zurück. Das Zentrum wird auch aktiv von der EU und der Nordatlantikvertrags-Organisation im Rahmen ihrer Zusammenarbeit unterstützt.

greifbare Fortschritten erzielt wurden. Er bestätigt zudem, dass die EU-Maßnahmen zur Abwehr hybrider Bedrohungen ausgebaut und vertieft wurden[13].

Im Bereich der **Cybersicherheit** war der 9. Mai 2018 ein wichtiger Meilenstein, denn bis zu diesem Tag mussten alle EU-Mitgliedstaaten die Umsetzung des ersten EU-weit verbindlichen Regelwerks auf dem Gebiet der Cybersicherheit, der Richtlinie zur Netz- und Informationssicherheit, in nationales Recht abgeschlossen haben. Dies ist ein wichtiger Bestandteil des umfassenden Ansatzes, der in der *Gemeinsamen Mitteilung „Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen*[14] vom September 2017 dargelegt wurde. Der Ansatz umfasst ein breites Spektrum konkreter Maßnahmen, um die Cybersicherheitsstrukturen und -fähigkeiten der EU deutlich zu stärken. Im Mittelpunkt stehen dabei die Stärkung der Resilienz der EU gegenüber Cyberangriffen und der Ausbau der Cybersicherheitskapazitäten der EU, die Schaffung besserer Möglichkeiten der strafrechtlichen Verfolgung und die Stärkung der globalen Stabilität durch internationale Zusammenarbeit. Die Mitteilung wurde zusammen mit einem Vorschlag für einen Rechtsakt zur Cybersicherheit vorgelegt, um mehr Rückhalt auf EU-Ebene[15] zu erreichen, und wurde durch eine Reihe von Vorschlägen untermauert, die nun zur Umsetzungsreife gebracht werden müssen (siehe unten).

Desinformation schadet unseren Demokratien, da sie die Fähigkeit der Bürgerinnen und Bürger beeinträchtigt, fundierte Entscheidungen zu treffen und am demokratischen Prozess teilzuhaben. Durch das Internet hat sich das Nachrichtenangebot für die Öffentlichkeit vom Volumen und der Vielfalt her enorm erhöht. Allerdings können neue Technologien auch dafür eingesetzt werden, um in bislang ungekanntem Maß äußerst gezielt und schnell Desinformationen zu verbreiten, mit dem Ziel, Misstrauen zu säen und gesellschaftliche Spannungen zu erzeugen. In der Mitteilung der Kommission *Bekämpfung von Desinformation im Internet – ein europäisches Konzept*[16] wird als Antwort auf das Problem der Desinformation ein europäisches Konzept entwickelt, bei dem verschiedene Interessenträger – insbesondere Online-Plattformen, aber auch Medienunternehmen – aufgefordert werden, bestimmte Maßnahmen zu ergreifen. Diese Maßnahmen decken ein breites Spektrum relevanter Bereiche ab, darunter mehr Transparenz, Vertrauenswürdigkeit und Rechenschaftspflicht von Online-Plattformen, sichere und stabile Wahlprozesse, Förderung von Bildung und Medienkompetenz, Unterstützung von Qualitätsjournalismus und Bekämpfung der Desinformation durch strategische Kommunikation. Zu den ersten konkreten Maßnahmen zählen ein Verhaltenskodex für den Bereich der Desinformation, der von einem Multi-Stakeholder-Forum zur Desinformation entwickelt werden soll, und ein Netz von Faktenprüfern, das noch vor dem Sommer eingerichtet sein soll. Anlässlich der ersten Sitzung des Multi-Stakeholder-Forums zur Desinformation am 29. Mai 2018 wurde vereinbart, welche Schritte im Hinblick auf die Annahme des Verhaltenskodex im Juli 2018 unternommen werden müssen. Die Kommission wird bis Ende 2018 prüfen, welche Fortschritte bei der Lösung des Problems erzielt wurden, und entscheiden, ob zusätzliche Maßnahmen in diesem Bereich erforderlich sind. Die vorgesehenen Maßnahmen werden mit denjenigen der East Stratcom Task Force im Einklang stehen und diese ergänzen.

In Bezug auf **chemische, biologische, radiologische und nukleare** Risiken werden im *Aktionsplan*[17] der Kommission vom Oktober 2017 23 praktische Aktionen und Maßnahmen vorgeschlagen, die Bürger und Infrastrukturen besser vor diesen

13 Erster Umsetzungsbericht (Juli 2017): JOIN(2017) 30 final.
14 JOIN(2017) 450 final.
15 COM(2017) 477 final, siehe unten.
16 COM(2018) 236 final.
17 COM(2017) 610 final.

Bedrohungen schützen sollen, auch durch eine engere Zusammenarbeit zwischen der EU und ihren Mitgliedstaaten sowie mit der Nordatlantikvertrags-Organisation. Als Teil der Maßnahmen im Rahmen der Sicherheitsunion zur Verbesserung des Schutzes und der Resilienz gegen Terrorismus wurde dabei ein präventiver Ansatz zugrunde gelegt, ausgehend von der Annahme, dass chemische, biologische, radiologische und nukleare Risiken zwar eine geringe Eintrittswahrscheinlichkeit, im Ernstfall jedoch schwerwiegende und dauerhafte Folgen haben. Seither haben der Anschlag von Salisbury und die zunehmende Sorge angesichts des Interesses von Terroristen an chemischen, biologischen, radiologischen oder nuklearen Materialien und der Fähigkeit von Terroristen, diese sowohl innerhalb als auch außerhalb der EU[18] zu nutzen, gezeigt, dass von chemischen, biologischen, radiologischen und nuklearen Stoffen eine reale Bedrohung ausgeht. Auch deshalb ist es dringend geboten, den Aktionsplan vollständig umzusetzen. Er beruht auf einem gefahrenübergreifenden Konzept und konzentriert sich auf vier Ziele: Verringerung der Verfügbarkeit von chemischen, biologischen, radiologischen und nuklearen Materialien, Gewährleistung einer robusteren Abwehrbereitschaft und Reaktion gegenüber chemischen, biologischen, radiologischen und nuklearen Sicherheitsvorfällen, Ausbau der internen und externen Kontakte im Bereich der chemischen, biologischen, radiologischen und nuklearen Sicherheit mit wichtigen regionalen und internationalen Partnern der EU und Verbesserung der Kenntnisse über chemische, biologische, radiologische und nukleare Risiken. Detaillierte Informationen über die konkreten Fortschritte bei der Umsetzung des Aktionsplans sind dem jüngsten Fortschrittsbericht zur Sicherheitsunion zu entnehmen, der parallel zu dieser Gemeinsamen Mitteilung angenommen wurde.

Um die Wirksamkeit der Maßnahmen zur Abwehr hybrider Bedrohungen zu erhöhen und die geschlossene Haltung der EU-Mitgliedstaaten und der Verbündeten der Nordatlantikvertrags-Organisation (NATO) deutlich zum Ausdruck zu bringen, wurde die Zusammenarbeit bei der Abwehr hybrider Bedrohungen in der *Gemeinsamen Erklärung von Warschau*[19] im Juli 2016 zu einem Schlüsselbereich der **Zusammenarbeit zwischen der EU und der NATO** erklärt. Fast ein Drittel aller derzeitigen gemeinsamen Vorschläge für die Zusammenarbeit konzentrieren sich auf hybride Bedrohungen[20]. Anknüpfend an die oben genannten Übungen und das EU-Einsatzprotokoll[21] wird die Zusammenarbeit in diesem Jahr weiter vertieft.

3. VERSTÄRKUNG DER REAKTION AUF DIE SICH WANDELNDEN BEDROHUNGEN

3.1. Lageerfassung – Ausbau der Kapazitäten zur Aufdeckung hybrider Bedrohungen

Voraussetzung für die Abwehr hybrider Bedrohungen und die Reaktion darauf ist die Fähigkeit, böswillige hybride Aktivitäten und ihre internen oder externen Urheber zu einem möglichst frühen Zeitpunkt zuerkennen und mögliche Zusammenhänge zwischen scheinbar unabhängigen Ereignissen zu verstehen. Zu diesem Zweck ist es unerlässlich, alle verfügbaren Datenströme zu nutzen, auch im Rahmen der Informationsgewinnung aus frei zugänglichen Quellen.

---

18 Europol, Tendenz- und Lagebericht über den Terrorismus (TE-SAT) 2017, S. 16, abrufbar unter: www.europol.europa.eu/sites/default/files/documents/tesat2017.pdf. Siehe auch die Erklärungen des Generaldirektors der OVCW: www.globaltimes.cn/content/1044644.shtml.

19 Die von Präsident Juncker, Präsident Tusk und NATO-Generalsekretär Stoltenberg unterzeichnete Erklärung bildet die derzeitige Grundlage für die Zusammenarbeit zwischen der EU und der NATO.

20 15283/16 und 14802/17.

21 SWD(2016) 227 final.

Die im Europäischen Auswärtigen Dienst eingerichtete EU-Analyseeinheit für hybride Bedrohungen ist als zentrale und einzige EU-Anlaufstelle bereits eine wichtige Errungenschaft. Sie benötigt jedoch noch mehr Fachkompetenzen, um das gesamte Spektrum hybrider Bedrohungen bearbeiten zu können, auch auf dem Gebiet der chemischen, biologischen, radiologischen und nuklearen Sicherheit sowie im Bereich der Spionageabwehr. Dank einer Erweiterung der Fachkompetenzen könnten künftige Krisenreaktionsmaßnahmen der EU besser unterstützt werden, indem in diesen spezifischen Bereichen umfassendere zivile und militärische Produkte der Informationsgewinnung zur Verfügung gestellt werden. Dies könnte durch Maßnahmen der Mitgliedstaaten ergänzt werden, die darauf abzielen, dass ihre nationalen Dienste mehr Erkenntnisse aus der Informationsgewinnung an die EU-Analyseeinheit für hybride Bedrohungen weitergeben. Außerdem sollten die Mitgliedstaaten dafür sorgen, dass das bestehende Netzwerk nationaler Kontaktstellen der EU-Analyseeinheit zunehmend in die Lage versetzt wird, zeitkritische Informationen bereitzustellen und auszuwerten. In einem weiteren Schritt sollten sich die Mitgliedstaaten darum bemühen, mehr einschlägige Erkenntnisse ihrer nationalen Dienste an das EU-Zentrum für Informationsgewinnung und -analyse (EU INTCEN) weiterzugeben, um eine eingehendere Analyse potenzieller Bedrohungen zu ermöglichen.

Künftige Schritte

- Die Hohe Vertreterin wird dafür sorgen, dass die EU-Analyseeinheit für hybride Bedrohungen mit zusätzlichen Analysekomponenten für chemische, biologische, radiologische und nukleare Bedrohungen sowie für Spionageabwehr und Cybersicherheit ausgestattet wird. Die Mitgliedstaaten werden aufgefordert, Erkenntnisse aus der Informationsgewinnung verstärkt für die Analyse bestehender und sich abzeichnender hybrider Bedrohungen zur Verfügung zu stellen.

- Die Kommission wird in Abstimmung mit der Hohen Vertreterin die Arbeiten für die Festlegung von Indikatoren für die Verwundbarkeit abschließen, damit die Mitgliedstaaten das Potenzial hybrider Bedrohungen in verschiedenen Sektoren besser einschätzen können. Diese Arbeiten sollen auch die von der EU durchgeführten Trendanalysen im Bereich hybrider Bedrohungen unterstützen.

3.2. **Verstärkte Maßnahmen gegen chemische, biologische, radiologische und nukleare Bedrohungen**

Der Aktionsplan gegen chemische, biologische, radiologische und nukleare Sicherheitsrisiken vom Oktober 2017 bildet den Rahmen für die Maßnahmen zur Steigerung der Abwehrbereitschaft, Resilienz und Koordinierung auf EU-Ebene. Darin sind eine Reihe von Maßnahmen zur Unterstützung der Mitgliedstaaten vorgesehen wie die Bündelung von Fachwissen und gemeinsamer Kapazitätsaufbau, der Austausch von Wissen und bewährten Verfahren und die Intensivierung der operativen Zusammenarbeit. Die Mitgliedstaaten und die Kommission müssen den Aktionsplan so schnell wie möglich gemeinsam umsetzen. Darüber hinaus sollte die Union auf der Grundlage der bereits erzielten Fortschritte bei der Analyse der Defizite im Bereich der Detektionskapazitäten und beim Austausch bewährter Verfahren in der neu geschaffenen Beratenden Gruppe für chemische, biologische, radiologische und nukleare Sicherheit weitere Maßnahmen ergreifen, um gegen neue und sich wandelnde Bedrohungen vorzugehen. Dies gilt insbesondere für chemische Bedrohungen. Ähnlich wie bei den Arbeiten zur

Beschränkung des Zugangs zu Ausgangsstoffen für Explosivstoffe[22] muss die EU rasch operative Maßnahmen ergreifen, um den Zugang zu hochgefährlichen chemischen Materialien strenger zu kontrollieren und die Möglichkeiten für die Detektion solcher Materialien in einem möglichst frühen Stadium zu optimieren. Ferner sollten die Mitgliedstaaten in Betracht ziehen, weitere Defizitanalysen und Bestandsaufnahmen auf EU-Ebene durchzuführen, beispielsweise in Bezug auf die Resilienz gegenüber chemischen, biologischen, radiologischen und nuklearen Bedrohungen und die Ressourcen und Konzepte für die Dekontamination. Die Vorbereitung auf Angriffe mit chemischen, biologischen, radiologischen und nuklearen Materialien und die Bewältigung der Folgen solcher Angriffe erfordern eine verstärkte Zusammenarbeit und Koordinierung zwischen den Mitgliedstaaten, einschließlich der Katastrophenschutzbehörden. Das Katastrophenschutzverfahren der Union kann hierbei eine zentrale Rolle spielen, um Europa als Ganzes in die Lage zu versetzen, sich besser vorzubereiten und im Bedarfsfall zu handeln.

Die internationale Zusammenarbeit ist in diesem Zusammenhang ebenfalls von großer Bedeutung und die EU kann auf den Verbindungen zu den regionalen CBRN-Exzellenzzentren – einschließlich möglicher Synergien mit der Nordatlantikvertrags-Organisation – sowie den Präventions-, Vorsorge- und Bewältigungsprogrammen für Naturkatastrophen und vom Menschen verursachte Katastrophen in der südlichen und der östlichen Nachbarschaft[23] aufbauen.

---

22 Im Zusammenhang mit den Arbeiten im Rahmen der Sicherheitsunion, die darauf abzielen, Terroristen und Kriminellen ihren Handlungsspielraum zu nehmen, hat die Kommission dezidierte Maßnahmen ergriffen, um den Zugang zu Ausgangsstoffen für Explosivstoffe, die für die Herstellung selbstgemachter Explosivstoffe missbraucht werden können, einzuschränken. Im Oktober 2017 legte die Kommission eine Empfehlung für unverzügliche Maßnahmen zur Verhütung des Missbrauchs von Ausgangsstoffen für Explosivstoffe (Empfehlung C(2017) 6950 final) auf der Grundlage der bestehenden Vorschriften vor. Daraufhin nahm die Kommission im April 2018 einen Vorschlag zur Überarbeitung und zur Verschärfung der Bestimmungen der bisherigen Verordnung (EU) Nr. 98/2013 über die Vermarktung und Verwendung von Ausgangsstoffen für Explosivstoffe an (COM(2018) 209 final).

23 In der östlichen und der südlichen Nachbarschaft werden Katastrophenschutzschulungen und -übungen im Rahmen der regionalen Präventions-, Vorsorge- und Bewältigungsprogramme für Naturkatastrophen und vom Menschen verursachte Katastrophen organisiert.

Künftige Schritte

- Die EU sollte Maßnahmen prüfen, durch die die Achtung der internationalen Regeln und Normen zur Verhinderung des Einsatzes chemischer Waffen unterstützt werden kann, unter anderem spezifische EU-Sanktionen für chemische Waffen.

- Um den Aktionsplan für die chemische, biologische, radiologische und nukleare Sicherheit voranzubringen, wird die Kommission mit den Mitgliedstaaten zusammenarbeiten, um bis Ende 2018 Folgendes abzuschließen:
  - Aufstellung einer Liste von chemischen Stoffen, die eine besondere Bedrohung darstellen, als Grundlage für operative Maßnahmen zur Einschränkung des Zugangs zu ihnen;
  - Aufnahme eines Dialogs mit privaten Akteuren in der Lieferkette, um gemeinsam gegen die sich wandelnden Bedrohungen durch Chemikalien vorzugehen, die als Ausgangsstoffe verwendet werden können;
  - beschleunigte Überprüfung von Bedrohungsszenarien und Analyse bestehender Detektionsmethoden, um die Erkennung chemischer Bedrohungen zu verbessern, mit dem Ziel, operative Leitlinien für die Mitgliedstaaten zu entwickeln, damit sie ihre Detektionsfähigkeiten ausbauen können.

- Die Mitgliedstaaten sollten Bestandsaufnahmen der vorhandenen wesentlichen medizinischen Gegenmittel sowie der Labor-, Behandlungs- und sonstigen Kapazitäten erstellen. Die Kommission wird mit den Mitgliedstaaten zusammenarbeiten, um die Verfügbarkeit dieser Bestände in der gesamten EU regelmäßig zu erfassen, damit sie im Falle von Angriffen besser zugänglich und rasch einsetzbar sind.

3.3. **Strategische Kommunikation – kohärente Informationsverbreitung**

Eine große Herausforderung im Zusammenhang mit hybriden Bedrohungen besteht darin, die breite Öffentlichkeit für den Unterschied zwischen Information und Desinformation zu sensibilisieren und zu schulen. Aufbauend auf den Erfahrungen mit der East StratCom Task Force, der EU-Analyseeinheit für hybride Bedrohungen und dem Europäischen Zentrum zur Bewältigung hybrider Bedrohungen sowie auf anderen Bemühungen der Kommission[24] werden die Kommission und die Hohe Vertreterin die strategischen Kommunikationsfähigkeiten der EU weiter ausbauen und professionalisieren, indem eine systematische Interaktion und Kohärenz zwischen den bestehenden Strukturen gewährleistet werden. Andere EU-Institutionen und die Mitgliedstaaten werden ebenfalls einbezogen, unter anderem über die angekündigte sichere Online-Plattform gegen Desinformation.

Bei der strategischen Kommunikation zwischen den EU-Institutionen, mit den Mitgliedstaaten sowie mit Partnern und internationalen Organisationen wird eine verbesserte Koordinierung und Zusammenarbeit von grundlegender Bedeutung sein und Vorbereitungen und Praxis erfordern, bevor in Echtzeit auf Krisen reagiert werden kann.

[24] Die Vertretungen der Kommission sind beispielsweise auch im Bereich Faktenchecks und Entlarvung von Mythen tätig. Einige von ihnen haben an die jeweiligen Länder angepasste Tools entwickelt, z. B. *Les Décodeurs de l'Europe* in Frankreich, *UE Vero Falso* in Italien, der öffentliche *EU-Mythbuster-Karikaturwettbewerb* in Österreich, eine ähnliche Karikatur-Serie in Rumänien und *Euromyths A-Z* von der Vertretung des Vereinigten Königreichs. Weitere derartige Projekte sind in Vorbereitung.

Wahlen haben sich als besonders strategisches und sensibles Ziel für Angriffe im Cyberspace und die Online-Umgehung konventioneller („Offline"-) Schutzmaßnahmen und Regeln erwiesen, wie z. B. des zulässigen Zeitraums der Wahlwerbung, transparenter Finanzierungsregeln und der Gleichbehandlung der Kandidaten. Dazu gehören Angriffe auf Wahlinfrastrukturen und für den Wahlkampf genutzte IT-Systeme sowie politisch motivierte Massendesinformationskampagnen im Internet und Cyberangriffe von Drittländern mit dem Ziel, demokratische Wahlen zu diskreditieren und zu delegitimieren. Auf EU-Ebene wird in verschiedener Hinsicht darauf hingearbeitet, in den Mitgliedstaaten das Bewusstsein für die Vorbereitung und die Reaktion auf diese neuen Bedrohungen zu schärfen. Im Rat werden die für die Cybersicherheit zuständigen Behörden der Mitgliedstaaten[25] freiwillige Leitlinien und gemeinsame bewährte Verfahren festlegen, um die Cybersicherheit der für Wahlen eingesetzten Technologie während des gesamten Wahlprozesses zu gewährleisten. Dies umfasst Informationssysteme und IKT-Lösungen für die Registrierung der Wähler und Kandidaten, die Sammlung und Zählung der Stimmen und die Verbreitung der Ergebnisse sowie Hilfssysteme, die in unmittelbarem Zusammenhang mit der Rechtmäßigkeit der Wahlergebnisse stehen.

Im Falle hybrider Angriffe muss auch eine rasche, zuverlässige und stimmige Information der breiten Öffentlichkeit gewährleistet sein. Bei einem auf chemische, biologische, radiologische und nukleare Materialien zurückgehenden Vorfall oder Ereignis mit ähnlichen Auswirkungen ist mit einer heftigen Reaktion der Öffentlichkeit zu rechnen, denn die Bürgerinnen und Bürger wollen rasche Antworten. Eine strategische Nachrichtenpolitik ist von zentraler Bedeutung, auch zwischen internationalen Organisationen, die ihre Reaktionspläne getrennt voneinander umsetzen.

Künftige Schritte

- Der Europäische Auswärtige Dienst und die Kommission werden im Rahmen ihrer jeweiligen Zuständigkeiten zusammenarbeiten, um zu einer strukturierteren Zusammenarbeit im Bereich der strategischen Kommunikation mit dem Ziel zu gelangen, gegen die von Quellen innerhalb und außerhalb der EU ausgehende Desinformation vorzugehen und ausländische Regierungen von der Verbreitung feindseliger Desinformation und von hybrider Einmischung abzuschrecken.

- Die Kommission wird im Herbst mit den Mitgliedstaaten und einschlägigen Interessenträgern hochrangige Veranstaltungen abhalten, darunter das dem Thema Demokratie gewidmete Grundrechtekolloquium, um bewährte Verfahren und Leitlinien zu fördern, wie durch den Cyberspace ermöglichte und auf gezielter Desinformation beruhende Bedrohungen für Wahlen verhindert oder eingedämmt werden können und wie darauf reagiert werden kann.

- Die Hohe Vertreterin und die Kommission werden prüfen, wie die Arbeit der drei StratCom Task Forces hinsichtlich der Instrumente und Ressourcen besser unterstützt werden kann, um sicherzustellen, dass die EU ausreichende Anstrengungen unternimmt, die der Komplexität der Desinformationskampagnen feindlicher Akteure gerecht werden.

[25] Unter der Schirmherrschaft der mit der Richtlinie über die Sicherheit von Netz- und Informationssystemen eingesetzten Kooperationsgruppe.

3.4. **Resilienz und Abschreckung im Bereich Cybersicherheit**

Cybersicherheit ist sowohl für unseren Wohlstand als auch für unsere Sicherheit von entscheidender Bedeutung. Da unser tägliches Leben und unsere Wirtschaft in zunehmendem Maße von digitalen Technologien bestimmt werden, sind wir den damit verbundenen Gefahren immer stärker ausgesetzt.

Eine wirksame Cybersicherheit wird in der EU durch unzureichende Investitionen und mangelnde Koordinierung behindert. Um hier Abhilfe zu schaffen, bemüht sich die EU um Aufbau von Kapazitäten durch Unterstützungsmaßnahmen, eine stärkere Koordinierung und neue Strukturen zur Förderung der Entwicklung und Verbreitung von Cybersicherheitstechnologien[26]. Mit der Richtlinie über die Sicherheit von Netz- und Informationssystemen[27] wurde ein unionsweites Mindestsicherheitsniveau für solche Systeme eingeführt. Die vollständige Umsetzung der Richtlinie durch alle Mitgliedstaaten ist von entscheidender Bedeutung für die Steigerung der Cyberresilienz: Dies ist ein erster wichtiger Schritt. Mit der Datenschutz-Grundverordnung wird eine Verpflichtung zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde eingeführt. Andere wichtige Maßnahmen sind die Stärkung und Modernisierung der EU-Cybersicherheitsagentur und die Schaffung eines EU-Zertifizierungsrahmen für IKT-Produkte und -Dienste[28], um das Vertrauen der Verbraucher zu stärken. Außerdem laufen Bemühungen zur Unterstützung des Netzwerks der Kompetenzzentren der Mitgliedstaaten, um die Entwicklung und Verbreitung von Cybersicherheitslösungen zu fördern und den Aufbau von Kapazitäten in diesem Bereich auf EU-Ebene und auf nationaler Ebene zu ergänzen. Dies erfolgt in Anlehnung an die Arbeiten im Zusammenhang mit dem von der Kommission am 6. Juni vorgelegten Programm „Digitales Europa“[29], durch das EU-Investitionen in die Cybersicherheit neue Priorität erhalten.

Gleichzeitig wurde in einer Empfehlung für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen („Konzeptentwurf“)[30] dargelegt, wie die Zusammenarbeit zwischen den Mitgliedstaaten und verschiedenen EU-Akteuren im Falle großer grenzüberschreitenden Cyberangriffe funktionieren sollte. Darin wird die entscheidende Rolle der Lageerfassung für eine wirksame Koordinierung auf technischer, operativer und strategischer/politischer Ebene hervorgehoben. Die mit der Richtlinie über die Sicherheit von Netz- und Informationssystemen eingesetzte Kooperationsgruppe arbeitet außerdem an der Verbesserung des Austauschs von Informationen zwischen den beteiligten Parteien und ihrer gemeinsamen Nutzung und entwickelt eine gemeinsame Systematik zur Beschreibung von Vorfällen. Dieser Ansatz wird bei künftigen Übungen getestet. Die Analyseeinheit für hybride Bedrohungen ist für die strategische Analyse von aktuellen und sich abzeichnenden Cyberbedrohungen auf der Grundlage der Beiträge der Nachrichtendienste der Mitgliedstaaten zuständig.

Der „Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten“, der das Instrumentarium für die Cyberdiplomatie („Cyber Diplomacy Toolbox“) liefert, stellt in operativer Hinsicht einen großen Fortschritt dar. Darin werden

---

[26] Im Kontext der Stärkung von Innovationen in den europäischen Regionen wurde im Dezember 2017 eine neue interregionale Pilotmaßnahme zur Intensivierung der Arbeiten im Bereich der Cybersicherheit auf den Weg gebracht.

[27] 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.

[28] COM(2017) 477.

[29] Vorschlag für eine Verordnung zur Aufstellung des Programms „Digitales Europa“ für den Zeitraum 2021-2027, COM(2018) 434.

[30] C(2017) 6100.

die der Gemeinsamen Außen- und Sicherheitspolitik zuzurechnenden – auch restriktiven – Maßnahmen dargelegt, die zur Verstärkung der Reaktion der EU auf Aktivitäten, die ihren politischen, sicherheitsbezogenen und wirtschaftlichen Interessen schaden, eingesetzt werden können. Je mehr die Mitgliedstaaten dieses Instrumentarium nutzen, desto größer wird seine abschreckende Wirkung sein. Im April nahm der Rat „Auswärtige Angelegenheiten“ Schlussfolgerungen zu böswilligen Cyberaktivitäten an, in denen er den böswilligen Einsatz von Informations- und Kommunikationstechnologien wie im Falle der Angriffe mit Wannacry und NotPetya entschieden verurteilte, die in der EU und darüber hinaus erheblichen Schaden und wirtschaftliche Verluste verursacht haben.

Die EU und ihre Mitgliedstaaten müssen ihre Fähigkeit zur Zuordnung von Cyberangriffen verbessern, nicht zuletzt durch einen besseren Austausch von Erkenntnissen. Die Zuordnung der Angriffe würde potenzielle Aggressoren abschrecken und die Wahrscheinlichkeit erhöhen, dass die Verantwortlichen ordnungsgemäß zur Rechenschaft gezogen werden. Eine zunehmende Abschreckung ist ein zentrales Ziel des strategischen Ansatzes der Kommission zur Verbesserung der Cybersicherheit. Die jüngsten Vorschläge der Kommission zur Verbesserung der grenzüberschreitenden Sammlung elektronischer Beweismittel für Strafverfahren würde auch die Fähigkeit der Strafverfolgungsbehörden, Cyberstraftaten zu untersuchen und zu verfolgen, erheblich verbessern.

Für eine wirksame Cyberresilienz bedarf es eines umfassenden gemeinsamen Ansatzes. Das erfordert solidere und wirksamere Strukturen zur Förderung der Cybersicherheit und zur Reaktion auf Cyberangriffe in den Mitgliedstaaten und auch in den Organen, Einrichtungen und Delegationen der EU sowie bei EU-Missionen und -Operationen: Das Fehlen eines gemeinsamen sicheren Kommunikationsnetzes zwischen allen EU-Institutionen ist ein entscheidender Schwachpunkt. Das Bewusstsein für die Cybersicherheit seitens der EU-Institutionen und ihrer Mitarbeiter sollte durch eine verbesserte Sicherheitskultur und intensivere Schulungsmaßnahmen erhöht werden.

Künftige Schritte

- Das Europäische Parlament und der Rat sollten beschleunigt darauf hinarbeiten, die Verhandlungen über die Vorschläge zur Cybersicherheit bis zum Jahresende einvernehmlich abzuschließen und sich zügig über die vorgeschlagenen Rechtsvorschriften für die Sammlung elektronischer Beweismittel zu einigen.

- Die Kommission und die Hohe Vertreterin werden eng mit den Mitgliedstaaten zusammenarbeiten, um die Cyberaspekte der EU-weiten Krisenbewältigungs- und -reaktionsmechanismen voranzubringen. Die Mitgliedstaaten werden aufgefordert, ihre Arbeiten zur Zuordnung von Cyberangriffen und zur konkreten Nutzung des Instrumentariums für die Cyberdiplomatie fortzusetzen, um die politische Antwort auf Cyberangriffe zu verstärken.

- Angesichts der Notwendigkeit, unsere Cyberabwehrfähigkeiten auszubauen, wird eine eigene Aus- und Fortbildungsplattform eingerichtet, damit die von den Mitgliedstaaten angebotenen Cyberabwehr-Ausbildungsmöglichkeiten besser koordiniert werden können. Es werden Synergien mit ähnlichen Maßnahmen der Nordatlantikvertrags-Organisation angestrebt.

3.5. **Resilienz gegenüber feindseligen nachrichtendienstlichen Aktivitäten**

Die Bekämpfung feindseliger nachrichtendienstlicher Aktivitäten erfordert in erster Linie eine verstärkte, wirksame Koordinierung zwischen den Mitgliedstaaten im Einklang mit den einschlägigen EU- und nationalen Vorschriften und Regelungen. Allerdings müssen dazu unbedingt die Fähigkeiten der EU-Institutionen ausgebaut werden, damit sie der wachsenden Bedrohung durch Aktivitäten begegnen können, die speziell gegen die Institutionen gerichtet sind, und – untermauert von entsprechenden Schulungen und Verbesserungen bei der physischen Sicherheit – eine Kultur des Sicherheitsbewusstseins schaffen können. Die Institutionen könnten auch mit den Mitgliedstaaten zusammenarbeiten, um ein solideres EU-Akkreditierungssystem einzuführen. Ein solches System würde es dank einer proaktiven Meldepraxis besser ermöglichen, die Mitgliedstaaten und Institutionen auf etwaige feindselige Akteure aufmerksam zu machen, vor allem wenn diese von Mitgliedstaaten bereits als solche ermittelt wurden.

Die Koordinierung zwischen den Mitgliedstaaten sowie zwischen den Mitgliedstaaten und anderen einschlägigen internationalen Organisationen, insbesondere der Nordatlantikvertrags-Organisation, würde dazu beitragen, die Spionageabwehr zum Schutz vor feindseligen Aktivitäten in der EU zu verbessern. Ein Beispiel für einen Bereich, der von einer verstärkten Koordinierung zwischen den Mitgliedstaaten profitieren würde, ist die Überprüfung von Investitionen auf der Grundlage der von der Kommission im September 2017 vorgeschlagenen Verordnung[31] zur Überprüfung ausländischer Direktinvestitionen durch die Mitgliedstaaten aus Gründen der Sicherheit oder öffentlichen Ordnung. Eine verstärkte Koordinierung zwischen den Mitgliedstaaten wäre zudem für die Prüfung von Finanztransaktionen wichtig, da gegnerische Nachrichtendienste ihre gegen die EU gerichteten Maßnahmen zunehmend mithilfe ausgeklügelter Systeme finanzieren.

Künftige Schritte

- Der Europäische Auswärtige Dienst und die Kommission werden verbesserte, praktische Maßnahmen ergreifen, um die Fähigkeit der EU zur Interaktion mit den Mitgliedstaaten bei der Abwehr von feindseligen nachrichtendienstlichen Aktivitäten, die speziell gegen die Institutionen gerichtet sind, zu unterstützen und auszubauen.

- Die EU-Analyseeinheit für hybride Bedrohungen wird durch Fachkompetenzen im Bereich Spionageabwehr verstärkt, sodass detaillierte Analysen und Briefings über wahrscheinliche feindselige nachrichtendienstliche Aktivitäten gegen Einzelpersonen oder die Institutionen erstellt werden können.

- Das Europäische Parlament und der Rat sollten beschleunigt darauf hinarbeiten, die Verhandlungen über den Vorschlag zur Überprüfung von Investitionen bis zum Jahresende abzuschließen.

[31] Vorschlag der Kommission für eine Verordnung des Europäischen Parlaments und des Rates zur Schaffung eines Rahmens für die Überprüfung ausländischer Direktinvestitionen in der Europäischen Union, COM(2017) 487.

4. FAZIT

Die EU widmet dem Thema hybride sowie chemische, biologische, radiologische und nukleare Bedrohungen große Aufmerksamkeit. Der Vorfall im März im Vereinigten Königreich hat verdeutlicht, wie breit das Spektrum der hybriden Kriegsführung ist und dass insbesondere eine größere Resilienz gegenüber chemischen, biologischen, radiologischen und nuklearen Bedrohungen unerlässlich ist.

Die Kommission und die Hohe Vertreterin haben eine Reihe von Initiativen zur Bewältigung der Herausforderungen im Zusammenhang mit hybriden Bedrohungen angenommen und vorgeschlagen. Die Kommission erhöht auch das Tempo bei der Umsetzung des Aktionsplans von 2017 für eine gesteigerte Abwehrbereitschaft gegen chemische, biologische, radiologische und nukleare Sicherheitsrisiken.

Diese Gemeinsame Mitteilung dient dazu, den Europäischen Rat über die bereits laufenden Arbeiten zu informieren und Bereiche zu ermitteln, in denen die Maßnahmen intensiviert werden sollten, um den wichtigen Beitrag der EU zur Bewältigung dieser Bedrohungen weiter zu vertiefen und auszubauen. Die Mitgliedstaaten, die Kommission und die Hohe Vertreterin müssen diese Arbeiten nun zügig weiter vorantreiben.