



Brüssel, den 25. März 2019
(OR. en)

7434/19

JAI 331
COSI 57
FRONT 120
ASIM 38
DAPIX 117
ENFOPOL 122
SIRIS 57
VISA 70
FAUXDOC 26
COPEN 128
CYBER 105
DATAPROTECT 108
CT 29
JAIEX 49
EF 124

ÜBERMITTLUNGSVERMERK

Absender: Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag des Generalsekretärs der Europäischen Kommission

Eingangsdatum: 21. März 2019

Empfänger: Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union

Nr. Komm.dok.: COM(2019) 145 final

Betr.: MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN EUROPÄISCHEN RAT UND DEN RAT
Auf dem Weg zu einer wirksamen und echten Sicherheitsunion -
Achtzehnter Fortschrittsbericht

Die Delegationen erhalten in der Anlage das Dokument COM(2019) 145 final.

Anl.: COM(2019) 145 final



Brüssel, den 20.3.2019
COM(2019) 145 final

**MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN
EUROPÄISCHEN RAT UND DEN RAT**

**Auf dem Weg zu einer wirksamen und echten Sicherheitsunion - Achtzehnter
Fortschrittsbericht**

{SWD(2019) 140 final}

I. EINLEITUNG

Dies ist der 18. Bericht über die Fortschritte auf dem Weg zu einer wirksamen und echten Sicherheitsunion. Er beleuchtet die Entwicklungen in zwei der wichtigsten Bereiche: „Bekämpfung des Terrorismus und der organisierten Kriminalität sowie der Instrumente zu ihrer Unterstützung“ und „Stärkung unserer Abwehrbereitschaft und Widerstandsfähigkeit gegen diese Bedrohungen“.

Im Vorfeld der Wahlen zum Europäischen Parlament im Mai 2019 wird in diesem Bericht die wichtige Arbeit hervorgehoben, die auf verschiedenen Ebenen geleistet wurde, um Cyberbedrohungen und Desinformation im Zusammenhang mit Wahlen zu bekämpfen und zu verhindern. Als Reaktion auf die Forderung des Europäischen Rates nach Maßnahmen zum Schutz der demokratischen Systeme der Union und zur Bekämpfung von Desinformation vor den bevorstehenden Wahlen hat die Union erhebliche Fortschritte hin zu stärker koordinierten Maßnahmen bezüglich der Resilienz bei Wahlen erzielt. Angesichts des Zeitdrucks, noch vor den Wahlen zum Europäischen Parlament im Mai 2019 dafür zu sorgen, dass die Union angemessen vorbereitet ist, fordert die Kommission alle beteiligten Akteure – staatliche Behörden, politische Parteien und insbesondere Online-Plattformen – auf, ihre Anstrengungen zu verstärken, um gegen Desinformation vorzugehen. Im Vorfeld der Tagung des Europäischen Rates am 21. und 22. März 2019, auf der die Fortschritte in diesem Bereich erörtert werden, fordert die Kommission ferner die Mitgliedstaaten auf, ihre Koordinierung zu intensivieren, um gegen Desinformation vorzugehen und den Schutz der Wahlen zum Europäischen Parlament sicherzustellen.

Die EU hat bei den Bemühungen um eine wirksame und echte Sicherheitsunion beträchtliche Fortschritte erzielt. Unter anderem wurden Einigungen über eine Reihe vorrangiger Gesetzgebungsinitiativen erzielt, die die Sicherheit für alle Bürger erhöhen werden. In den vergangenen Monaten¹ erzielten das Europäische Parlament und der Rat eine Einigung über die Interoperabilität der EU-Informationssysteme in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung sowie über neue EU-Vorschriften, die den Handlungsspielraum von Terroristen und anderen Straftätern einengen sollen, sodass ihnen der Zugang zu Ausgangsstoffen für Explosivstoffe, die Finanzierung ihrer Aktivitäten und unerkanntes Reisen erschwert werden. Über 15 von 22 Gesetzgebungsinitiativen, die die Kommission im Rahmen der Sicherheitsunion vorgelegt hat (siehe die Liste aller Initiativen im Rahmen der Sicherheitsunion in *Anhang I*), wurden Einigungen erzielt. Somit sorgt die EU für konkrete Fortschritte in diesem Bereich, der für das Europäische Parlament, den Rat und die Kommission eine gemeinsame Priorität darstellt.²

Weitere Anstrengungen sind jedoch erforderlich. Insbesondere müssen die beiden gesetzgebenden Organe in dieser Legislaturperiode gegen die akute Bedrohung durch terroristische Online-Inhalte vorgehen, indem sie eine Einigung über den Vorschlag der Kommission erzielen. Ebenso müssen das Europäische Parlament und der Rat eine Einigung über den Vorschlag der Kommission für einen Ausbau der Europäischen Grenz- und

¹ Diese Ergebnisse bauen auf den vorherigen Fortschritten bei den Arbeiten hin zu einer wirksamen und echten Sicherheitsunion auf. Eine vollständige Übersicht ist den vorherigen Fortschrittsberichten zur Sicherheitsunion zu entnehmen: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en.

² Siehe die Gemeinsame Erklärung zu den gesetzgeberischen Prioritäten der EU für den Zeitraum 2018-2019: https://ec.europa.eu/commission/sites/beta-political/files/joint-declaration-eu-legislative-priorities-2018-19_en.pdf.

Küstenwache erzielen, der die Sicherheit durch einen verbesserten Schutz der Außengrenzen der Union erhöhen soll.

Die tragischen Ereignisse in Christchurch (Neuseeland) vom 15. März 2019 zeigen, dass der Terrorismus – egal ob durch Rechtsextremismus oder andere extremistische Ideologien angetrieben – nach wie vor eine eindeutige und unmittelbare Gefahr darstellt. Die Schwierigkeiten bei dem Versuch, live gestreamte Inhalte von Internetplattformen zu entfernen und ihr erneutes Auftauchen zu verhindern, unterstreichen abermals, wie wichtig der Vorschlag der Kommission zu terroristischen Online-Inhalten ist. Die beiden gesetzgebenden Organe müssen dringend zu einer Einigung über die vorgeschlagenen Vorschriften zur Entfernung terroristischer Online-Inhalte gelangen. Von ebenso großer Bedeutung für die Bekämpfung des Terrorismus in all seinen Formen ist es, dass sämtliche Mitgliedstaaten die von der EU insbesondere als Reaktion auf Terroranschläge in Europa erlassenen Rechtsvorschriften vollständig umsetzen. Dabei handelt es sich vor allem um die Richtlinien zur Terrorismusbekämpfung und über die Kontrolle des Erwerbs und des Besitzes von Waffen, die den Handlungsspielraum von Terroristen einengen sollen. Im Rahmen der Bekämpfung von Extremismus ist die Kommission durch entsprechende Maßnahmen auch aktiv gegen illegale Hetze im Internet, Hass gegen Muslime und Antisemitismus vorgegangen.

Des Weiteren werden in diesem Bericht die Fortschritte bei der Umsetzung weiterer Prioritäten im Bereich der Sicherheit, insbesondere bei Maßnahmen für einen besseren Schutz des öffentlichen Raums, dargelegt. Die vollständige und korrekte Umsetzung der vereinbarten Maßnahmen hat oberste Priorität, damit die Vorteile einer wirksamen und echten Sicherheitsunion in vollem Umfang gewährleistet sind. Die Kommission unterstützt die Mitgliedstaaten aktiv, unter anderem durch die Bereitstellung von Finanzmitteln und die Erleichterung des Austauschs bewährter Verfahren. Wenn es erforderlich ist, macht die Kommission auch in vollem Umfang von ihren durch die Verträge verliehenen Befugnissen zur Durchsetzung des EU-Rechts Gebrauch, gegebenenfalls auch durch Vertragsverletzungsverfahren.

Den Hintergrund dieses Berichts bildet der 15. Europäische Gedenktag für die Opfer des Terrorismus, der am 11. März 2019, 15 Jahre nach den Bombenanschlägen von Madrid vom 11. März 2004 und drei Jahre nach den tödlichen Anschlägen in Brüssel und Zaventem vom 22. März 2016 begangen wurde. Die Unterstützung der Opfer von Terroranschlägen ist ein wichtiger Teil der Bemühungen um eine wirksame und echte Sicherheitsunion. Um diese Unterstützung weiter auszubauen, nahm die Kommission am 31. Januar 2019 einen Beschluss über die Finanzierung des Pilotprojekts „Einrichtung eines EU-Kompetenzzentrums für Terroropfer“³ an. Das EU-Kompetenzzentrum wird als Zentrum für Fachwissen und Plattform für Experten, die sich mit Terroropfern befassen, fungieren.

Die Kommission begrüßt den Bericht des Europäischen Parlaments über die Feststellungen und Empfehlungen des Sonderausschusses Terrorismus⁴ als wertvollen Beitrag zur gemeinsamen Arbeit auf dem Weg zu einer wirksamen und echten Sicherheitsunion.

II. FORTSCHRITTE BEI DEN GESETZGEBERISCHEN PRIORITÄTEN

³ C(2019) 636 vom 31.1.2019.

⁴ Entschließung des Europäischen Parlaments vom 12. Dezember 2018 zu den Feststellungen und Empfehlungen des Sonderausschusses Terrorismus (2018/2044(INI)).

1. Solidere und intelligentere Informationssysteme in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung

Informationsaustausch ist ein zentraler Aspekt der Unterstützung, die die EU den nationalen Behörden bei der Bekämpfung von Terrorismus und schwerer Kriminalität leistet. Vor diesem Hintergrund bedeutet die Interoperabilität EU-weiter Informationssysteme eine wesentliche Änderung der Art und Weise, in der den nationalen Behörden Daten zur Verfügung gestellt werden; sie garantiert, dass die Daten richtig und vollständig sind. Die beiden gesetzgebenden Organe haben eine politische Einigung über die betreffenden vorrangigen Legislativvorschläge erzielt, mit denen die **Interoperabilität der EU-Informationssysteme** in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung erreicht werden soll.⁵ Die vorgeschlagenen Maßnahmen werden dafür sorgen, dass die EU-Informationssysteme intelligenter und gezielter zusammenarbeiten und die Grundrechte zugleich in vollem Umfang gewahrt bleiben. Dank der bestmöglichen Nutzung der vorhandenen Daten werden durch die Interoperabilität Informationslücken geschlossen, indem sie dazu beiträgt, Mehrfachidentitäten zu erkennen und Identitätsbetrug zu bekämpfen. Sobald die beiden gesetzgebenden Organe die neuen Vorschriften förmlich angenommen haben, wird die Kommission die Mitgliedstaaten bei ihrer Umsetzung unterstützen. Es bedarf einer engen Zusammenarbeit mit den EU-Agenturen und allen Mitgliedstaaten sowie den assoziierten Schengen-Ländern, um das ehrgeizige Ziel der vollständigen Interoperabilität der EU-Informationssysteme in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung bis 2020 zu erreichen. Zur Vorbereitung dieser Zusammenarbeit fand am 5. März 2019 ein erster Workshop mit Sachverständigen der Mitgliedstaaten statt, mit dem ein Prozess der wirksamen Koordinierung eingeleitet wurde.

Nach derzeitigem Stand wird die künftige Architektur der interoperablen EU-Informationssysteme das verstärkte **Schengener Informationssystem**⁶, das bestehende **Visa-Informationssystem**⁷, die kürzlich vereinbarte Ausweitung des **Europäischen Strafregisterinformationssystems**⁸ auf Drittstaatsangehörige sowie das neu eingerichtete **Einreise-/Ausreisensystem der EU**⁹ und das **Europäische Reiseinformations- und -genehmigungssystem (ETIAS)**¹⁰ umfassen.

Im Rahmen der technischen Umsetzung des Europäischen Reiseinformations- und -genehmigungssystems legte die Kommission am 7. Januar 2019 einen Vorschlag mit technischen Änderungen der betreffenden Verordnung vor.¹¹ Die vorgeschlagenen Änderungen betreffen die Rechtsakte über diejenigen EU-Informationssysteme, in denen das Europäische Reiseinformations- und -genehmigungssystem Abfragen durchführen wird, um

⁵ COM(2017) 793 final vom 12.12.2017, COM(2017) 794 final vom 12.12.2017, COM(2018) 478 final vom 13.6.2018, COM(2018) 480 final vom 13.6.2018. Die am 5. Februar 2019 erzielte politische Einigung wurde am 13. Februar 2019 vom Ausschuss der Ständigen Vertreter des Rates und am 19. Februar 2019 vom Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments gebilligt.

⁶ Verordnung (EU) 2018/1860 vom 28.11.2018, Verordnung (EU) 2018/1861 vom 28.11.2018 und Verordnung (EU) 2018/1862 vom 28.11.2018.

⁷ Verordnung (EG) Nr. 767/2008 vom 9.7.2008.

⁸ Die beiden gesetzgebenden Organe erzielten am 11. Dezember 2018 eine politische Einigung über diesen vorrangigen Vorschlag (COM(2017) 344 final vom 29.6.2017). Der Ausschuss der Ständigen Vertreter des Rates billigte die Einigung am 19. Dezember 2018. Das Plenum des Europäischen Parlaments bestätigte die Einigung am 11. März 2019.

⁹ Verordnung (EU) 2017/2226 vom 30.11.2017.

¹⁰ Verordnung (EU) 2018/1240 vom 12.9.2018 und Verordnung (EU) 2018/1241 vom 12.9.2018.

¹¹ COM(2019) 4 final vom 7.1.2019.

Sicherheitsrisiken oder Risiken irregulärer Migration zu bewerten, die mit von der Visumpflicht befreiten Drittstaatsangehörigen verbunden sind, bevor diese in den Schengen-Raum einreisen. Für die vollständige Einrichtung des Europäischen Reiseinformations- und -genehmigungssystems sind diese vorgeschlagenen Änderungen erforderlich. Die Kommission fordert die beiden gesetzgebenden Organe auf, ihre Arbeit an den technischen Änderungen voranzutreiben, damit so bald wie möglich eine Einigung erzielt werden kann. Auf diese Weise würde eine rasche und fristgerechte Einrichtung des Europäischen Reiseinformations- und -genehmigungssystems möglich, sodass es Anfang 2021 seinen Betrieb aufnehmen könnte.

Im Mai 2018 legte die Kommission einen Vorschlag zur **Stärkung des bestehenden Visa-Informationssystems**¹² vor, der gründlichere Hintergrundüberprüfungen von Visumantragstellern und die Schließung von Informationslücken durch einen besseren Informationsaustausch zwischen den Mitgliedstaaten vorsieht. Der Rat nahm sein Verhandlungsmandat am 19. Dezember 2018 an, und am 13. März 2019 stimmte das Plenum des Europäischen Parlaments über seinen Bericht zu dem Vorschlag ab und schloss damit seine erste Lesung ab. Die Kommission fordert eine rasche Aufnahme der Verhandlungen zwischen den beiden gesetzgebenden Organen nach der Wahl des nächsten Europäischen Parlaments.

Im Mai 2016 schlug die Kommission vor, den Anwendungsbereich von **Eurodac**¹³ auszuweiten: Das System sollte dem Vorschlag zufolge nicht mehr nur zur Identifizierung von Asylbewerbern, sondern auch von illegal aufhältigen Drittstaatsangehörigen und von Drittstaatsangehörigen, die irregulär in die EU einreisen, genutzt werden. Im Einklang mit den Schlussfolgerungen des Europäischen Rates vom Dezember 2018¹⁴ und der Mitteilung der Kommission vom 6. März 2019 über die Fortschritte bei der Umsetzung der Europäischen Migrationsagenda¹⁵ fordert die Kommission die beiden gesetzgebenden Organe auf, den Vorschlag unverzüglich anzunehmen. Durch die Annahme dieses Legislativvorschlags kann Eurodac Teil der künftigen Architektur interoperabler EU-Informationssysteme werden, sodass die wichtigsten Daten von illegal aufhältigen Drittstaatsangehörigen und Personen, die irregulär in die EU eingereist sind, integriert werden.

Zur Stärkung der EU-Informationssysteme in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung fordert die Kommission das Europäische Parlament und den Rat auf,

- den Legislativvorschlag über **Eurodac**, über den eine Einigung zum Greifen nah ist, vor den Wahlen zum Europäischen Parlament anzunehmen; (*Priorität der Gemeinsamen Erklärung*)
- auf eine rasche Einigung über die vorgeschlagenen technischen Änderungen hinzuwirken, die für die Einrichtung des **Europäischen Reiseinformations- und -genehmigungssystems** erforderlich sind.

2. Mehr Sicherheit durch ein verbessertes Außengrenzenmanagement

¹² COM(2018) 302 final vom 16.5.2018.

¹³ COM(2016) 272 final vom 4.5.2016.

¹⁴ <https://www.consilium.europa.eu/de/press/press-releases/2018/12/14/european-council-conclusions-13-14-december-2018/>

¹⁵ COM(2019) 126 final vom 6.3.2019.

Ein starker Schutz der Außengrenzen ist für die Sicherheit im Raum der Freizügigkeit ohne Kontrollen an den Binnengrenzen unverzichtbar. Dieser Schutz ist eine Aufgabe der Mitgliedstaaten, die das Management ihrer Außengrenzen in ihrem eigenen Interesse und im gemeinsamen Interesse aller (Mitgliedstaaten) mit Unterstützung der **Europäischen Grenz- und Küstenwache** sicherstellen müssen. Als Reaktion auf die Schlussfolgerungen des Europäischen Rates vom Juni 2018¹⁶ schlug die Kommission im September 2018 vor, die Kapazitäten der Europäischen Grenz- und Küstenwache auszubauen.¹⁷ Dadurch würde die Agentur auf eine neue operative Ebene gehoben und mit einer ständigen Reserve von 10 000 Grenzschutzbeamten mit Exekutivbefugnissen und eigener Ausrüstung ausgestattet, wobei die Grundrechte und die Souveränität der Mitgliedstaaten zugleich in vollem Umfang gewahrt blieben.

Die gesetzgeberischen Arbeiten an dem Vorschlag kommen gut voran, und die Verhandlungen zwischen den beiden gesetzgebenden Organen sind in die entscheidende Phase eingetreten. Das Europäische Parlament nahm sein Verhandlungsmandat am 11. Februar 2019 an, während der Rat sein Mandat am 20. Februar 2019 erhielt. Am 27. Februar 2019 und am 12. März 2019 fanden zwei Trilogsitzungen statt. Die Kommission begrüßt und unterstützt die bei diesem vorrangigen Dossier erzielten Fortschritte, die deutlich machen, dass sich alle Organe dafür einsetzen, dass dieser Vorschlag vor den Wahlen zum Europäischen Parlament 2019 verabschiedet wird.

Damit die Sicherheit durch ein verbessertes Management der Außengrenzen erhöht wird, fordert die Kommission das Europäische Parlament und den Rat auf,

- während der laufenden Legislaturperiode des Europäischen Parlaments den Legislativvorschlag zur Stärkung der **Europäischen Grenz- und Küstenwache** anzunehmen. (*Initiative im Rahmen der Lage der Union 2018*)

3. Radikalisierung verhindern

Das Vorgehen gegen terroristische Inhalte im Internet ist weiterhin eine der größten Herausforderungen im Kampf gegen den Terrorismus und bei der Radikalisierungsprävention. Diese Inhalte spielten bei den meisten Angriffen, die in den letzten beiden Jahren auf europäischem Boden stattfanden, eine Rolle, sei es in Form der Anstiftung zu einem Anschlag, von Anleitungen für dessen Durchführung oder der Verherrlichung der tödlichen Folgen. Um der eindeutigen und unmittelbaren Gefahr, die von solchen Inhalten ausgeht, entgegenzuwirken, wurde die Rede zur Lage der Union 2018 von Präsident Juncker durch einen Vorschlag¹⁸ für eine Verordnung zu **terroristischen Online-Inhalten** flankiert, mit der ein Rechtsrahmen zur Verhinderung des Missbrauchs von Hosting-Dienstleistern für die Verbreitung terroristischer Online-Propaganda festgelegt wird. Die künftigen Vorschriften gewährleisten die uneingeschränkte Achtung der freien Meinungsäußerung und anderer Grundrechte, müssen aber auch unbedingt wirksame Maßnahmen vorsehen, um terroristische Online-Inhalte so schnell wie möglich zu entfernen, da der potenzielle Schaden, der durch solche Inhalte verursacht wird, mit jeder Stunde, die sie online verfügbar bleiben, zunimmt.

Während der Rat sein Verhandlungsmandat im Dezember 2018 annahm, dauern die Arbeiten im Europäischen Parlament noch an, sodass das Parlament sein Verhandlungsmandat

¹⁶ <https://www.consilium.europa.eu/media/35938/28-euco-final-conclusions-de.pdf>

¹⁷ COM(2018) 631 final vom 12.9.2018.

¹⁸ COM(2018) 640 final vom 12.9.2018.

hoffentlich im Laufe des Monats März 2019 annehmen kann.¹⁹ Da ein EU-Rechtsrahmen für die Entfernung terroristischer Online-Inhalte mit klaren Regeln und Schutzvorkehrungen dringend erforderlich ist, fordert die Kommission die beiden gesetzgebenden Organe auf, noch in der laufenden Legislaturperiode des Europäischen Parlaments eine Einigung über den vorgeschlagenen Rechtsakt zu erzielen.

Gleichzeitig unterstützt die Kommission die Mitgliedstaaten weiterhin bei ihren Bemühungen, **Radikalisierung zu verhindern**. Ein spezieller EU-Kooperationsmechanismus, der nationale Vertreter zusammenbringt, trägt dazu bei, dass die Unterstützung auf EU-Ebene den Bedürfnissen der Mitgliedstaaten entspricht.²⁰ Zu den jüngsten Beispielen zählt eine Konferenz zum Thema „EU-Städte gegen Radikalisierung“, die gemeinsam mit dem Ausschuss der Regionen am 26. Februar 2019 veranstaltet wurde. Am 13. März 2019 veranstaltete die Kommission ein Expertentreffen mit nationalen politischen Entscheidungsträgern, um praktische Schritte zur weiteren Unterstützung von Strafvollzug und Bewährungshilfe zu ermitteln. Die Ergebnisse dieser Arbeit werden in ein Handbuch einfließen, das das Aufklärungsnetzwerk gegen Radikalisierung zum Thema der Rehabilitation und Wiedereingliederung von terroristischen Straftätern, zurückkehrenden ausländischen terroristischen Kämpfern und im Gefängnis radikalisierten Personen erstellt (siehe auch Abschnitt IV.4 – Außenbeziehungen).

Um Radikalisierung zu verhindern, fordert die Kommission das Europäische Parlament auf,

- dringend sein Verhandlungsmandat für den Legislativvorschlag zur Verhinderung der Verbreitung **terroristischer Online-Inhalte** anzunehmen, damit die beiden gesetzgebenden Organe während der laufenden Legislaturperiode des Europäischen Parlaments eine Einigung über diese Rechtsvorschrift erzielen können. (*Initiative im Rahmen der Lage der Union 2018*)

4. Erhöhung der Cybersicherheit

Die klassischen Cyber-Bedrohungen für Systeme und Daten nehmen weiter zu, und die Zahl der Angriffe böswilliger Akteure auf verschiedene Ziele und Opfer ist im Jahr 2018 gestiegen. Die Bekämpfung der Cyberkriminalität und die Verbesserung der Cybersicherheit bleiben daher auch weiterhin eine Priorität bei EU-Maßnahmen. Durch die Umsetzung der in der Gemeinsamen Mitteilung „Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen“²¹ vom September 2017 dargelegten Maßnahmen hat die EU bei der Erhöhung der Cybersicherheit greifbare Fortschritte erzielt.

¹⁹ Der Ausschuss für Binnenmarkt und Verbraucherschutz des Europäischen Parlaments stimmte am 4. März 2019 über seine Stellungnahme ab. Der Ausschuss für Kultur und Bildung des Europäischen Parlaments stimmte am 11. März 2019 über seinen Bericht ab. Der Ausschuss des Europäischen Parlaments für bürgerliche Freiheiten, Justiz und Inneres wird voraussichtlich am 21. März 2019 über seinen Bericht abstimmen.

²⁰ Die Bedürfnisse der Mitgliedstaaten bei der Radikalisierungsprävention wurden erstmals in den sogenannten strategischen Leitlinien für Präventionsmaßnahmen der EU für das Jahr 2019 ermittelt. Die strategischen Leitlinien sind unter folgender Adresse abrufbar: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3626&news=1&mod_groups=1&month=08&year=2018.

²¹ JOIN(2017) 450 final vom 13.9.2017.

Am 12. März 2019 bestätigte das Plenum des Europäischen Parlaments die politische Einigung der beiden gesetzgebenden Organe über den **Rechtsakt zur Cybersicherheit**. Der Rechtsakt, der voraussichtlich im Mai 2019 in Kraft treten wird, wird die Kapazitäten für die Cybersicherheit und die Abwehrbereitschaft der Mitgliedstaaten und der Unternehmen erhöhen. Darüber hinaus wird damit ein EU-Rahmen für die Cybersicherheitszertifizierung von Produkten, Systemen und Dienstleistungen im Bereich der Informations- und Kommunikationstechnologie geschaffen. Dieser Rechtsakt wird zudem die Zusammenarbeit und Koordinierung zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU, insbesondere der umbenannten EU-Agentur für Cybersicherheit, verbessern.

Weitere Fortschritte sind jedoch in Bezug auf den Vorschlag der Kommission vom September 2018 über ein **Europäisches Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung und das Netz nationaler Koordinierungszentren**²² erforderlich. Mit dem Vorschlag sollen die technologischen und industriellen Kapazitäten im Bereich der Cybersicherheit unterstützt und die Wettbewerbsfähigkeit der Cybersicherheitsbranche in der Union gesteigert werden. Das Europäische Parlament und der Rat nahmen ihre Verhandlungsmandate am 13. März 2019 an. Die erste Trilogsitzung fand ebenfalls am 13. März 2019 statt. Die Kommission fordert die beiden gesetzgebenden Organe auf, zu einer raschen Einigung über die vorgeschlagene Rechtsvorschrift zu gelangen.

Die EU hat erhebliche Fortschritte erzielt bei der weiteren Verwirklichung der **gemeinsamen diplomatischen Reaktion der EU auf böswillige Cyberaktivitäten** (dem „Instrumentarium für die Cyberdiplomatie“) und reagierte damit auf die Forderung des Europäischen Rates²³, die Arbeit an der Fähigkeit, mit restriktiven Maßnahmen der EU auf Cyberangriffe zu reagieren und diese zu verhindern, voranzubringen. Am 8. März 2019 legten die Hohe Vertreterin der Union für Außen- und Sicherheitspolitik und die Kommission einen gemeinsamen Vorschlag für eine Verordnung des Rates über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen, vor. Die Kommission und die Hohe Vertreterin fordern die rasche Annahme dieses Vorschlags zur Stärkung der Widerstandsfähigkeit der Union gegen Cyberangriffe.

Zur Erhöhung der Cybersicherheit fordern die Kommission und die Hohe Vertreterin den Rat auf,

- die Verordnung des Rates über **restriktive Maßnahmen gegen Cyberangriffe**, die die Union oder ihre Mitgliedstaaten bedrohen, anzunehmen.

5. Terroristen den Handlungsspielraum nehmen

Die EU hat weitere Maßnahmen ergriffen, um Terroristen und Kriminelle handlungsunfähig zu machen, indem ihnen der Zugang zu Ausgangsstoffen für Explosivstoffe, die Finanzierung ihrer Aktivitäten und unerkanntes Reisen erschwert werden.

Das Europäische Parlament und der Rat erzielten am 14. Februar 2019 eine politische Einigung über die vorgeschlagene Verordnung über **Beschränkungen für die Vermarktung und Verwendung von Ausgangsstoffen für Explosivstoffe**²⁴. Sobald die Verordnung

²² COM(2018) 630 final vom 12.9.2018.

²³ Siehe die Schlussfolgerungen des Europäischen Rates vom Juni 2018 und Oktober 2018.

²⁴ COM(2018) 209 final vom 17.4.2018.

anwendbar ist, wird sie den derzeitigen Rechtsrahmen erheblich verbessern, indem sie den Zugang zu gefährlichen Ausgangsstoffen für Explosivstoffe, die unter Umständen zur Herstellung selbst gebauter Bomben missbraucht werden, beschränkt. Durch die Verordnung sollen Sicherheitslücken geschlossen werden. Zu diesem Zweck sieht sie Maßnahmen wie das Verbot weiterer Chemikalien, obligatorische Prüfungen der Strafregistereinträge von Personen, die eine Lizenz für den Erwerb beschränkter Stoffe beantragen, und eine Klarstellung, dass Vorschriften für Wirtschaftsteilnehmer ebenso für im Internet tätige Unternehmen gelten, vor.

Im Rahmen der Bemühungen zur Bekämpfung der Terrorismusfinanzierung erzielten die beiden gesetzgebenden Organe zudem eine Einigung über die vorgeschlagene Richtlinie zur **Erleichterung der Nutzung von Finanz- und sonstigen Informationen** für die Verhütung, Aufdeckung, Untersuchung oder Verfolgung schwerer Straftaten.²⁵ Sobald diese Richtlinie förmlich angenommen und umgesetzt ist, wird sie bestimmten Strafverfolgungsbehörden und Vermögensabschöpfungsstellen direkten Zugang zu Informationen über Bankkonten in zentralen nationalen Bankkontenregistern verschaffen. Ferner wird die Richtlinie die Zusammenarbeit zwischen den nationalen zentralen Meldestellen und den Strafverfolgungsbehörden verstärken und den Zugang von Europol zu Finanzinformationen erleichtern.

Auf dieser Grundlage wird die Kommission weitere Überlegungen über die Zusammenarbeit zwischen den zentralen Meldestellen verschiedener Mitgliedstaaten anstellen, unter anderem in dem gemäß der 5. Geldwäscherichtlinie vorgesehen anstehenden Bericht über die Zusammenarbeit zwischen den zentralen Meldestellen.²⁶ Darüber hinaus prüft die Kommission ebenfalls gemäß der 5. Geldwäscherichtlinie Aspekte, die mit der potenziellen Verknüpfung von nationalen zentralen Bankkontenregistern und Datenabfragesystemen in der EU verbunden sind. Außerdem untersucht die Kommission Einziehungsmaßnahmen ohne vorherige Verurteilung in der Union. Abschließend wird die Kommission – auch als Reaktion auf eine Aufforderung des Europäischen Parlaments²⁷ – weiterhin die Notwendigkeit, die technische Durchführbarkeit und die Verhältnismäßigkeit zusätzlicher Maßnahmen zur Aufdeckung der Finanzierungskanäle des Terrorismus in der EU bewerten.

Im Rahmen der Arbeit zur Bekämpfung des Dokumentenbetrugs erzielten die beiden gesetzgebenden Organe am 19. Februar 2019 eine vorläufige Einigung über die vorgeschlagene Verordnung zur Erhöhung der **Sicherheit der Personalausweise von Unionsbürgern und der Aufenthaltstitel**²⁸, damit diese Dokumente von Kriminellen und Terroristen nicht in betrügerischer Weise verwendet werden können. Der Ausschuss des

²⁵ Die beiden gesetzgebenden Organe erzielten am 12. Februar 2019 eine politische Einigung über den Vorschlag der Kommission (COM(2018) 213 final vom 17.4.2018). Diese wurde am 20. Februar 2019 vom Ausschuss der Ständigen Vertreter des Rates und am 26. Februar 2019 vom Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments gebilligt.

²⁶ Nach Artikel 65 Absatz 2 der Richtlinie (EU) 2018/843 vom 19. Juni 2018 muss die Kommission bis zum 1. Juni 2019 die Rahmenbedingungen für die Zusammenarbeit der zentralen Meldestellen mit Drittländern sowie Hindernisse und Möglichkeiten zur Verbesserung der Zusammenarbeit zwischen den zentralen Meldestellen in der Union, einschließlich der Möglichkeit, einen Koordinierungs- und Unterstützungsmechanismus einzurichten, bewerten.

²⁷ In seinem im Dezember 2018 angenommenen Abschlussbericht forderte der Sonderausschuss Terrorismus des Europäischen Parlaments die Einrichtung eines EU-Systems zur Nachverfolgung der Terrorismusfinanzierung für Transaktionen von Personen, die Verbindungen zum Terrorismus und zur Terrorismusfinanzierung im einheitlichen Euro-Zahlungsverkehrsraum haben.

²⁸ COM(2018) 212 final vom 17.4.2018.

Europäischen Parlaments für bürgerliche Freiheiten, Justiz und Inneres bestätigte die Einigung am 11. März 2019. Mit der Annahme der Verordnung werden Mindestsicherheitsmerkmale für Personalausweise, unter anderem biometrische Identifikatoren (ein Gesichtsbild und zwei Fingerabdrücke), auf einem kontaktlosen Chip eingeführt. Dies wird die Sicherheit nationaler Personalausweise und Aufenthaltstitel erheblich verbessern und es Terroristen und anderen Straftätern erschweren, solche Dokumente zu missbrauchen oder zu fälschen, um in die EU einzureisen oder sich innerhalb der EU zu bewegen. Sicherere Ausweisdokumente werden zur Stärkung des Managements der Außengrenzen der EU beitragen und gleichzeitig den Bürgerinnen und Bürgern der EU die Ausübung ihres Rechts auf Freizügigkeit erleichtern.

Weitere Fortschritte sind allerdings in Bezug auf die Vorschläge der Kommission vom April 2018 über den **Zugang zu elektronischen Beweismitteln** erforderlich, da bei mehr als der Hälfte aller strafrechtlichen Ermittlungen heute ein grenzüberschreitender Antrag auf Zugang zu elektronischen Beweismitteln gestellt wird.²⁹ Der Rat nahm sein Verhandlungsmandat über die Vorschläge für eine Verordnung³⁰ zur Verbesserung des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln in Strafsachen und für eine Richtlinie³¹ zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren an. Im Europäischen Parlament wurden jedoch seit der Annahme dieser Vorschläge durch die Kommission im April 2018 diesbezüglich nur sehr begrenzte Fortschritte erzielt. Angesichts der entscheidenden Bedeutung eines effizienten Zugangs zu elektronischen Beweismitteln für die Verfolgung von grenzüberschreitenden Straftaten wie Terrorismus und Cyberkriminalität fordert die Kommission das Europäische Parlament nachdrücklich auf, diesen Vorschlag voranzubringen.

Parallel dazu arbeitet die Kommission im Kontext der Verhandlungen über ein Zweites Zusatzprotokoll zum Budapester Übereinkommen des Europarates über Computerkriminalität und gemeinsam mit den USA an **internationalen Initiativen zum Zugang zu elektronischen Beweismitteln**. Daher nahm die Kommission am 5. Februar 2019 Empfehlungen³² für Verhandlungsmandate für diese beiden internationalen Initiativen an. Der Rat erörtert derzeit die Entwürfe der Mandate, unter anderem auf der Tagung des Rates „Justiz und Inneres“ am 7. und 8. März 2019. Die Kommission ersucht den Rat, den Beschluss zur Genehmigung der Teilnahme an Verhandlungen über ein Zweites Zusatzprotokoll zum Budapester Übereinkommen des Europarates über Computerkriminalität sowie den Beschluss über die Ermächtigung zur Aufnahme von Verhandlungen über ein Abkommen zwischen der EU und den USA über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln anzunehmen. Die Verhandlungen müssen rasch aufgenommen werden, damit die internationale Zusammenarbeit beim Austausch elektronischer Beweismittel vorankommt und gleichzeitig die Vereinbarkeit mit dem EU-Recht und den Verpflichtungen der Mitgliedstaaten im Rahmen dieser Zusammenarbeit gewahrt bleibt, wobei auch künftige Entwicklungen im EU-Recht zu berücksichtigen sind.

²⁹ In rund 85 % der strafrechtlichen Ermittlungen werden elektronische Beweismittel benötigt, und in zwei Dritteln dieser Ermittlungen müssen Beweismittel bei Online-Diensteanbietern mit Sitz in einem anderen Land beschafft werden. Siehe die Folgenabschätzung zum Legislativvorschlag (SWD(2018) 118 final vom 17.4.2018).

³⁰ COM(2018) 225 final vom 17.4.2018. Der Rat nahm sein Verhandlungsmandat für die vorgeschlagene Verordnung auf der Tagung des Rates „Justiz und Inneres“ am 7. Dezember 2018 an.

³¹ COM(2018) 226 final vom 17.4.2018. Der Rat nahm sein Verhandlungsmandat für die vorgeschlagene Richtlinie auf der Tagung des Rates „Justiz und Inneres“ am 8. März 2019 an.

³² COM(2019) 70 final vom 5.2.2019 und COM(2019) 71 final vom 5.2.2019.

Um Terroristen keinen Handlungsspielraum mehr zu lassen, fordert die Kommission

- das **Europäische Parlament** auf, dringend sein Verhandlungsmandat für die Legislativvorschläge zu **elektronischen Beweismitteln** anzunehmen, damit die Trilog-Gespräche mit dem Rat unverzüglich aufgenommen werden können; (*Priorität der Gemeinsamen Erklärung*)
- den **Rat** auf, die Beschlüsse zur Genehmigung der Teilnahme an Verhandlungen über ein **Zweites Zusatzprotokoll zum Budapester Übereinkommen des Europarats über Computerkriminalität** sowie über die Ermächtigung zur Aufnahme von **Verhandlungen über ein Abkommen zwischen der EU und den USA** über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln anzunehmen.

III. BEKÄMPFUNG VON DESINFORMATION UND SCHUTZ VON WAHLEN VOR ANDEREN CYBERBEDROHUNGEN

Die Gefahr, dass Außenstehende und Insider in öffentliche Debatten eingreifen und Wahlen manipulieren können, ist realer als je zuvor und könnte mit den anstehenden Wahlen zum Europäischen Parlament noch weiter zunehmen. Die möglichen Folgen – Unterminierung oder Delegitimierung demokratischer Institutionen – stellen eine schwere strategische und wachsende Bedrohung dar. Sie machen einen wesentlichen Teil der Herausforderungen für die Sicherheit aus, mit denen die EU heute über nationale Grenzen hinweg konfrontiert ist, und erfordern eine gemeinsame grenzübergreifende Reaktion.

Der Wahlkampf im Vorfeld der Wahlen zum Europäischen Parlament wird im März beginnen. Im Vorfeld der Tagung des Europäischen Rates am 21. und 22. März 2019 fordert die Kommission die Mitgliedstaaten auf, ihre Koordinierung und ihren Informationsaustausch zu intensivieren, um gegen Desinformation vorzugehen und Wahlen vor Cyberbedrohungen zu schützen. Die Mitgliedstaaten sollten die von der EU bereitgestellten Instrumente und Informationskanäle, insbesondere das neu eingerichtete Schnellwarnsystem, in vollem Umfang nutzen.³³ Aufgrund der Besorgnis über die derzeitige Lage fordert die Kommission außerdem Online-Plattformen nachdrücklich auf, ihre Bemühungen in allen Mitgliedstaaten zu beschleunigen, um dazu beizutragen, die Integrität der Wahlen zum Europäischen Parlament im Mai 2019 zu gewährleisten.

Um diese Bemühungen zu unterstützen, werden die Kommission und die Hohe Vertreterin weiterhin Maßnahmen in den beiden sich ergänzenden Bereichen Bekämpfung von Desinformation und Stärkung der demokratischen Resilienz bei Wahlen ergreifen, um gegen Cyber-Bedrohungen vorzugehen.

1. Maßnahmen zur Bekämpfung von Desinformation

Groß angelegte Kampagnen zur Desinformation der Bürger, einschließlich irreführender oder völlig falscher Informationen, können sich als eine weitere ernste Art der durch den Cyberspace möglichen Bedrohungen entpuppen und sind eine große Herausforderung im Hinblick auf die bevorstehenden Europawahlen. Die Kommission verfolgt aufmerksam die

³³ Als Teil des von der Kommission und der Hohen Vertreterin im Dezember 2018 vorgelegten Aktionsplans gegen Desinformation (siehe unten) wird das Schnellwarnsystem ein Forum für die Mitgliedstaaten, die EU-Institutionen und die beteiligten Partner bieten, in dem sie Informationen über laufende Desinformationskampagnen austauschen und ihre Reaktion koordinieren können. Das System wird ausschließlich auf frei zugänglichen, nicht vertraulichen Informationen beruhen.

Umsetzung der in ihrer **Mitteilung vom April 2018 festgelegten Maßnahmen zur Bekämpfung von Desinformation im Internet**.³⁴

Darüber hinaus werden auch die Fortschritte bei der Umsetzung des **Verhaltenskodex zur Bekämpfung von Desinformation**, den Vertreter von Online-Plattformen, führende soziale Netzwerke, Werbetreibende und Vertreter der Werbebranche im Oktober 2018 unterzeichnet haben, von der Kommission aufmerksam verfolgt (siehe unten). Nach Ablauf der ersten zwölf Monate des Kodex wird die Kommission eine umfassende Bewertung vornehmen. Erweisen sich Umsetzung oder Wirkung des Verhaltenskodex als unzureichend, so könnte die Kommission erforderlichenfalls weitere Maßnahmen vorschlagen, darunter auch legislative.

Auf dieser Grundlage und als Reaktion auf die Forderung der politischen Führungsspitzen im Rahmen des Europäischen Rates vom Juni 2018 nach Maßnahmen zum Schutz der demokratischen Systeme der Union legte die Kommission gemeinsam mit der Hohen Vertreterin im Dezember 2018 einen **Gemeinsamen Aktionsplan gegen Desinformation**³⁵ vor. Der Aktionsplan unterstreicht, dass der **EU-Analyseeinheit für hybride Bedrohungen** zufolge die Desinformationskampagnen der Russischen Föderation die größte Bedrohung für die EU darstellen. Diese Kampagnen haben System, sind gut mit Ressourcen ausgestattet und daher mit den Kampagnen anderer Länder kaum vergleichbar. Um gegen die Bedrohungen durch Desinformationskampagnen vorzugehen, ist in dem Aktionsplan eine Aufstockung der Ressourcen für die Bekämpfung der Desinformation, genauer gesagt der **Task Forces für strategische Kommunikation** des Europäischen Auswärtigen Dienstes, darunter der East StratCom Task Force, vorgesehen.³⁶ Der Aktionsplan sieht ferner eine Aufstockung der Ressourcen für diesen Bereich vor und fordert eine Verstärkung in den nächsten zwei Jahren.

Mit dem Aktionsplan werden konkrete Maßnahmen zur Bekämpfung von Desinformation, darunter die Schaffung eines **Frühwarnsystems**, festgelegt. Das Frühwarnsystem wurde im März 2019 im Hinblick auf die Wahlen zum Europäischen Parlament gemeinsam von den EU-Institutionen und den Mitgliedstaaten geschaffen, um den Datenaustausch und die Auswertung von Desinformationskampagnen zu vereinfachen und Warnmeldungen über Desinformationsfälle zu verbreiten.

Der Aktionsplan sieht eine strenge Überwachung der Umsetzung des vorgenannten Verhaltenskodex vor, zu dem sich die Online-Plattformen verpflichtet haben. Am 29. Januar 2019 veröffentlichte die Kommission die **von den Unterzeichnern des Verhaltenskodex – Google, Facebook, Twitter, Mozilla und Berufsverbände der Werbebranche – vorgelegten Berichte**. Wenngleich die Kommission die Fortschritte begrüßte, forderte sie die Unterzeichner auf, ihre Anstrengungen im Vorfeld der Wahlen zum Europäischen Parlament 2019 zu intensivieren.³⁷

Die Europäische Kommission hat am 28. Februar 2019 **Berichte von Facebook, Google und Twitter** über die Fortschritte veröffentlicht, die diese im Januar 2019 im Hinblick auf ihre Verpflichtungen zur Bekämpfung von Desinformation erzielt haben. Aus diesen Berichten geht jedoch nicht ausreichend hervor, dass neue Strategien und Instrumente in allen EU-

³⁴ COM(2018) 236 final vom 26.4.2018, mit einem anschließenden Bericht über die Umsetzung COM(2018) 794 final vom 5.12.2018.

³⁵ JOIN(2018) 36 final vom 5.12.2018.

³⁶ Die East StratCom Task Force hat seit ihrer Einrichtung 2015 fast 5000 Beispiele für Desinformation durch die Russische Föderation erfasst, analysiert und ans Licht gebracht; so wurden unzählige Desinformationsnarrative aufgedeckt, das Bewusstsein dafür geschärft und Instrumente, Techniken und Absichten von Desinformationskampagnen enthüllt.

³⁷ Nähere Einzelheiten dazu siehe: http://europa.eu/rapid/press-release_IP-19-746_de.htm.

Mitgliedstaaten rechtzeitig umgesetzt und mit angemessenen Ressourcen ausgestattet werden. Daher gibt es bei allen Unterzeichnern noch Spielraum für Verbesserungen.³⁸ Ganz konkret ruft die Kommission die Plattformen auf, bis zum Beginn der Kampagne für die Europawahlen in allen EU-Mitgliedstaaten für die volle Transparenz der politischen Werbung zu sorgen, einen angemessenen Zugang zu den Daten der Plattformen zu Forschungszwecken zu ermöglichen und durch Kontaktstellen im Frühwarnsystem eine entsprechende Zusammenarbeit zwischen den Plattformen und den einzelnen Mitgliedstaaten zu gewährleisten.

Die Kommission wird am 20. März 2019 erneut über die Umsetzung des Verhaltenskodex Bericht erstatten.

2. Verbesserung der demokratischen Resilienz bei Wahlen

Die Kommission hat am 12. September 2018 ein an die Mitgliedstaaten und die europäischen nationalen politischen Parteien und Stiftungen gerichtetes Maßnahmenpaket angenommen, um die Resilienz unserer Wahlsysteme zu verbessern, darunter eine Empfehlung zu Wahlkooperationsnetzen, zu Online-Transparenz, zum Schutz vor Cybersicherheitsvorfällen und zur Bekämpfung von Desinformationskampagnen im Zusammenhang mit Wahlen zum Europäischen Parlament sowie einen Leitfaden der Kommission zur Anwendung des EU-Datenschutzrechts im Zusammenhang mit Wahlen³⁹ und eine legislative Änderung zur Verschärfung der Vorschriften über die Finanzierung europäischer politischer Parteien.

In seiner Entschließung vom 28. Oktober 2018 begrüßte das Europäische Parlament das Paket. Der Rat begrüßte das Paket in seinen Schlussfolgerungen vom 19. Februar 2019 über die Sicherstellung freier und fairer Europawahlen. Darin befürworteten alle Mitgliedstaaten einen koordinierten europäischen Ansatz zur Wahrung der Integrität der bevorstehenden Europawahlen. Der Rat „Justiz und Inneres“ erörterte den Sachstand am 7. März 2019.

Mit der Änderung der **Verordnung über das Statut und die Finanzierung von europäischen politischen Parteien und Stiftungen**⁴⁰ wird es möglich, Sanktionen aufzuerlegen, sollten personenbezogene Daten im Hinblick auf eine gezielte Einflussnahme auf das Ergebnis der Wahlen zum Europäischen Parlament illegal genutzt werden. Nach der politischen Einigung⁴¹ im Januar 2019 wurde der Wortlaut der Änderung am 12. März 2019 im Plenum des Europäischen Parlaments angenommen. Die Änderung soll noch vor den Wahlen zum Europäischen Parlament 2019 in Kraft treten.

Die Empfehlung zu **Wahlkooperationsnetzen, zu Online-Transparenz, zum Schutz vor Cybersicherheitsvorfällen und zur Bekämpfung von Desinformationskampagnen im Zusammenhang mit Wahlen zum Europäischen Parlament**⁴² richtet sich mit konkreten Maßnahmen für die einschlägigen Akteure in diesen Bereichen an die Mitgliedstaaten und die europäischen politischen Parteien und Stiftungen. Für die Umsetzung der Empfehlung haben nationale Wahlkooperationsnetze Kontaktstellen benannt, die sich an einem **europäischen Kooperationsnetz für Wahlen** beteiligen, um vor Bedrohungen zu warnen, bewährte

³⁸ Nähere Einzelheiten dazu siehe: http://europa.eu/rapid/press-release_STATEMENT-19-1379_de.htm.

³⁹ COM(2018) 638 final vom 12.9.2018.

⁴⁰ COM(2018) 636 final vom 12.9.2018.

⁴¹ Die beiden gesetzgebenden Organe erzielten am 16. Januar 2018 eine politische Einigung, die am 25. Januar 2019 vom Ausschuss der Ständigen Vertreter des Rates und am 29. Januar 2019 vom Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments gebilligt wurde.

⁴² C(2018) 5949 final vom 12.9.2018.

Vorgehensweisen zwischen den nationalen Netzen auszutauschen, gemeinsame Lösungen für ermittelte Herausforderungen zu erörtern und gemeinsame Projekte und Übungen der nationalen Netze zu fördern. Bei einer ersten Sitzung des Netzes am 21. Januar 2019 verständigten sich die Teilnehmer darauf, dass ein umfassendes Konzept unabdingbar ist, um die Integrität der Wahlen zu gewährleisten und einen offenen demokratischen Dialog und gleiche Ausgangsbedingungen für die Parteien aufrechtzuerhalten. Die zweite Sitzung des europäischen Kooperationsnetzes für Wahlen fand am 27. Februar 2019 statt und konzentrierte sich auf die Überwachung und Durchsetzung wesentlicher Aspekte im Zusammenhang mit den Wahlen, darunter Datenschutz, Medienregulierung, Rechtsdurchsetzung, Transparenz und soziale Medien, und das Engagement der verschiedenen Interessenträger bei der Maßnahmenüberwachung. Damit wurde der Grundstein für eine Übung zur Cyberabwehrfähigkeit gelegt, die im Anschluss an die nächste, für den 5. April 2019 anberaumte Sitzung stattfinden soll.

Ein **Workshop unter dem Motto „Enhancing cyber resilience of elections“** wurde am 19. Februar 2019 gemeinsam vom Europäischen Parlament und der Kommission organisiert, um die Sicherheit und die Resilienz der Wahlsysteme und der Infrastruktur gegenüber den sich ständig wandelnden Cyber-Bedrohungen zu verbessern. In diesem Rahmen erörterten nationale Behörden für Cybersicherheit aus den Mitgliedstaaten, die Agentur der Europäischen Union für Netz- und Informationssicherheit und Online-Plattformen Maßnahmen, die zur Gewährleistung der Integrität der Wahlen zum Europäischen Parlament 2019 dringlich und sinnvoll erscheinen.

Die EU-Institutionen und die Mitgliedstaaten arbeiten auch bei anderen **Sensibilisierungsmaßnahmen** eng zusammen, die darauf abzielen, die Integrität des Wahlverfahrens zu wahren und Akteure aus dem privaten und öffentlichen Sektor einzubeziehen, darunter Medien, Online-Plattformen und die Zivilgesellschaft.

Um Desinformation zu bekämpfen und die Resilienz der Wahlen zu gewährleisten, fordern die Kommission und die Hohe Vertreterin die Mitgliedstaaten dazu auf,

- die Maßnahmen des **gemeinsamen Aktionsplans gegen Desinformation** vom Dezember 2018 rasch und entschieden umzusetzen.

IV. UMSETZUNG WEITERER VORRANGIGER DOSSIERS IM SICHERHEITSBEREICH

1. Umsetzung legislativer Maßnahmen in der Sicherheitsunion

Die vollständige und korrekte Umsetzung der vereinbarten Maßnahmen hat oberste Priorität, damit die Vorteile einer wirksamen und echten Sicherheitsunion in vollem Umfang gewährleistet sind. Die Kommission unterstützt die Mitgliedstaaten aktiv, unter anderem durch die Bereitstellung von Finanzmitteln und die Erleichterung des Austauschs bewährter Verfahren. Wenn es erforderlich ist, macht die Kommission auch in vollem Umfang von ihren durch die Verträge verliehenen Befugnissen zur Durchsetzung des EU-Rechts Gebrauch, gegebenenfalls auch durch Vertragsverletzungsverfahren.

Was die Umsetzung der **EU-Richtlinie über Fluggastdatensätze**⁴³ anbelangt, hat die Kommission am 19. Juli 2018 Vertragsverletzungsverfahren gegen 14 Mitgliedstaaten

⁴³ Richtlinie (EU) 2016/681 vom 27.4.2016.

eingeleitet, weil sie die Verabschiedung nationaler Rechtsvorschriften zur vollständigen Umsetzung der Richtlinie⁴⁴ – einem wichtigen Instrument im Kampf gegen Terrorismus und andere schwere Straftaten – nicht mitgeteilt haben. Neun dieser Mitgliedstaaten haben zwischenzeitlich die vollständige Umsetzung notifiziert.⁴⁵ Den Mitgliedstaaten, die ihre Umsetzung nach wie vor nicht mitgeteilt haben, wurde eine mit Gründen versehene Stellungnahme übermittelt (Spanien am 24. Januar 2019, den Niederlanden und Finnland am 7. März 2019). Parallel dazu unterstützt die Kommission weiterhin alle Mitgliedstaaten bei ihren Bemühungen, die Entwicklung ihrer Systeme zur Erfassung von Fluggastdatensätzen zu vervollständigen, indem sie unter anderem den Austausch von Informationen und bewährten Verfahren ermöglicht.

Die Frist für die Umsetzung der **Richtlinie zur Terrorismusbekämpfung** endete am 8. September 2018.⁴⁶ Daher leitete die Kommission am 22. November 2018 Vertragsverletzungsverfahren gegen 16 Mitgliedstaaten ein, weil sie die Verabschiedung nationaler Rechtsvorschriften zur vollständigen Umsetzung der Richtlinie nicht mitgeteilt hatten. Neun dieser Mitgliedstaaten haben zwischenzeitlich die vollständige Umsetzung mitgeteilt.⁴⁷ Die Kommission fordert die verbleibenden sieben Mitgliedstaaten auf, die notwendigen Maßnahmen unverzüglich zu ergreifen.⁴⁸

Die Frist für die Umsetzung der **Richtlinie über die Kontrolle des Erwerbs und des Besitzes von Waffen**⁴⁹ endete am 14. September 2018. Bislang haben sechs Mitgliedstaaten die vollständige Umsetzung⁵⁰ und fünf Mitgliedstaaten die teilweise Umsetzung⁵¹ mitgeteilt. Die Kommission schickte 22 Mitgliedstaaten⁵², darunter auch jenen, die eine teilweise Umsetzung mitgeteilt hatten, am 22. November 2018 ein Aufforderungsschreiben.

Was die Umsetzung der **Richtlinie zum Datenschutz bei der Strafverfolgung**⁵³ anbelangt, hat die Kommission am 19. Juli 2018 Vertragsverletzungsverfahren gegen 19 Mitgliedstaaten eingeleitet, weil sie die Verabschiedung nationaler Rechtsvorschriften zur vollständigen Umsetzung der Richtlinie nicht mitgeteilt hatten.⁵⁴ Derzeit haben 17 Mitgliedstaaten die vollständige Umsetzung und fünf

⁴⁴ Bulgarien, die Tschechische Republik, Estland, Griechenland, Spanien, Frankreich, Zypern, Luxemburg, die Niederlande, Österreich, Portugal, Rumänien, Slowenien und Finnland.

⁴⁵ Bulgarien, Estland, Griechenland, Frankreich, Zypern, Luxemburg, Österreich, Portugal, Rumänien (Stand: 11. März 2019).

⁴⁶ Richtlinie (EU) 2017/541 vom 15.3.2017.

⁴⁷ Bulgarien, die Tschechische Republik, Deutschland, Estland, Spanien, Frankreich, Kroatien, Italien, Lettland, Litauen, Ungarn, Malta, die Niederlande, Österreich, Portugal, die Slowakei, Finnland und Schweden haben die Umsetzung mitgeteilt (Stand: 11. März 2019).

⁴⁸ Belgien, Polen, Rumänien und Slowenien haben eine teilweise Umsetzung gemeldet. Von Griechenland, Zypern und Luxemburg liegt noch keine Mitteilung vor (Stand: 11. März 2019).

⁴⁹ Richtlinie (EU) 2017/853 vom 17.5.2017.

⁵⁰ Dänemark, Frankreich, Kroatien, Italien, Malta und Österreich (Stand: 11. März 2019).

⁵¹ Die Tschechische Republik, Estland, Litauen, Portugal und das Vereinigte Königreich (Stand: 11. März 2019).

⁵² Belgien, Bulgarien, die Tschechische Republik, Deutschland, Estland, Irland, Griechenland, Spanien, Zypern, Lettland, Litauen, Luxemburg, Ungarn, die Niederlande, Polen, Portugal, Rumänien, Slowenien, die Slowakei, Finnland, Schweden und das Vereinigte Königreich (Stand: 11. März 2019).

⁵³ Richtlinie (EU) 2016/680 vom 27.4.2016.

⁵⁴ Belgien, Bulgarien, Tschechische Republik, Estland, Griechenland, Spanien, Frankreich, Kroatien, Zypern, Lettland, Litauen, Luxemburg, Ungarn, die Niederlande, Polen, Portugal, Rumänien, Slowenien und Finnland. Die Kommission erhält Antworten der Mitgliedstaaten einschließlich Notifizierungen zu den betreffenden Rechtsvorschriften, die derzeit geprüft werden (Stand: 11. März 2019).

Mitgliedstaaten die teilweise Umsetzung⁵⁵ mitgeteilt. Zum jetzigen Zeitpunkt sind die Verfahren gegen sechs Mitgliedstaaten abgeschlossen⁵⁶, während neun Mitgliedstaaten am 25. Januar 2019 eine mit Gründen versehene Stellungnahme⁵⁷ erhalten haben.

Die Kommission soll bis 9. Mai 2019 über die Kohärenz der Ermittlung der Betreiber wesentlicher Dienste Bericht erstatten. Anhand der Notifizierungen der Mitgliedstaaten konnte festgestellt werden, dass 25 Mitgliedstaaten die **Richtlinie über die Sicherheit von Netz- und Informationssystemen**⁵⁸ vollständig umgesetzt haben und ein Mitgliedstaat sie teilweise umgesetzt hat.⁵⁹ Die Kommission hat im Januar 2019 die Vertragsverletzungsverfahren gegen sechs Mitgliedstaaten wegen Nichtmitteilung der Umsetzungsmaßnahmen abgeschlossen.⁶⁰ Gegen neun Mitgliedstaaten⁶¹ laufen Vertragsverletzungsverfahren wegen Nichtmitteilung der vollständigen Umsetzung der Richtlinie. Im Zuge der Umsetzung der Richtlinie über die Sicherheit von Netz- und Informationssystemen mussten die Mitgliedstaaten der Kommission bis zum 9. November 2018 über die Ermittlung von Betreibern wesentlicher Dienste in ihrem Hoheitsgebiet Bericht erstatten. Die Kommission prüft derzeit die von den Mitgliedstaaten eingegangenen Informationen.⁶²

Darüber hinaus prüft die Kommission derzeit die Umsetzung der **Vierten Geldwäscherichtlinie**⁶³ und auch die Anwendung der Vorschriften durch die Mitgliedstaaten. Die Kommission hat Vertragsverletzungsverfahren gegen alle 28 Mitgliedstaaten eingeleitet, da sie der Auffassung ist, dass die von den Mitgliedstaaten vorgelegten Mitteilungen keine vollständige Umsetzung der Richtlinie darstellen.⁶⁴ Sie wird ihre Befugnisse bei Bedarf auch weiterhin nutzen, um die vollständige Umsetzung dieser Richtlinie sicherzustellen.

Die Kommission fordert die Mitgliedstaaten auf, dringend die erforderlichen Maßnahmen zu ergreifen, um die folgenden Richtlinien vollständig in nationales Recht umzusetzen und dies der Kommission mitzuteilen:

⁵⁵ Belgien, Deutschland, Estland, Irland, Frankreich, Kroatien, Italien, Litauen, Luxemburg, Ungarn, Malta, Österreich, Polen, Rumänien, die Slowakei, Schweden und das Vereinigte Königreich haben die vollständige Umsetzung gemeldet. Die Tschechische Republik, Portugal, Finnland, Slowenien und die Niederlande haben die teilweise Umsetzung mitgeteilt. Des Weiteren hat Dänemark die Umsetzung abgeschlossen (Stand: 11. März 2019).

⁵⁶ Belgien, Frankreich, Kroatien, Litauen, Luxemburg, Ungarn (Stand: 11. März 2019).
Griechenland, Zypern, Spanien, Slowenien, Portugal, die Tschechische Republik, Bulgarien, Lettland und die Niederlande (Stand: 11. März 2019).

⁵⁸ Richtlinie (EU) 2016/1148 vom 27.4.2016.

⁵⁹ Bulgarien, die Tschechische Republik, Dänemark, Deutschland, Griechenland, Estland, Irland, Spanien, Frankreich, Kroatien, Italien, Zypern, Lettland, Litauen, Malta, die Niederlande, Österreich, Polen, Portugal, Rumänien, Slowenien, die Slowakei, Finnland, Schweden und das Vereinigte Königreich meldeten die vollständige Umsetzung. Ungarn teilte die teilweise Umsetzung mit. Belgien und Luxemburg haben der Kommission keine Umsetzungsmaßnahmen gemeldet (Stand: 11. März 2019).

⁶⁰ Irland, Spanien, Frankreich, Kroatien, die Niederlande und Portugal (Stand: 11. März 2019).

⁶¹ Bulgarien, Belgien, Dänemark, Lettland, Litauen, Luxemburg, Ungarn, Österreich und Rumänien (Stand: 11. März 2019).

⁶² Bulgarien, Zypern, die Tschechische Republik, Deutschland, Dänemark, Estland, Spanien, Finnland, Frankreich, Kroatien, Ungarn, Irland, Italien, Litauen, Malta, die Niederlande, Polen, Portugal, die Slowakei, Schweden und das Vereinigte Königreich (Stand: 11. März 2019).

⁶³ Richtlinie (EU) 2015/849 vom 20.5.2015.

⁶⁴ Die Kommission hat gegen alle Mitgliedstaaten Vertragsverletzungsverfahren wegen Nichtmitteilung der nationalen Rechtsvorschriften zur vollständigen Umsetzung der Richtlinie eingeleitet, da die Kommission bei ihrer Prüfung zu dem Schluss kam, dass einige Bestimmungen der Richtlinie nicht umgesetzt wurden.

- die **EU-Richtlinie über Fluggastdatensätze**; hier müssen drei Mitgliedstaaten noch die Umsetzung in nationales Recht mitteilen, zwei Mitgliedstaaten müssen noch die restlichen Umsetzungsmaßnahmen mitteilen;⁶⁵
- die **Richtlinie über die Sicherheit von Netz- und Informationssystemen**; hier müssen zwei Mitgliedstaaten noch die Umsetzung in nationales Recht mitteilen, ein Mitgliedstaat muss noch die restlichen Umsetzungsmaßnahmen mitteilen;⁶⁶
- die **Richtlinie zur Terrorismusbekämpfung**; hier müssen drei Mitgliedstaaten noch die Umsetzung in nationales Recht mitteilen, vier Mitgliedstaaten müssen noch die restlichen Umsetzungsmaßnahmen mitteilen;⁶⁷
- die **Richtlinie über die Kontrolle des Erwerbs und des Besitzes von Waffen**; hier müssen 17 Mitgliedstaaten die Umsetzung der Richtlinie in nationales Recht noch mitteilen und fünf müssen noch die restlichen Umsetzungsmaßnahmen mitteilen;⁶⁸
- die **Richtlinie zum Datenschutz bei der Strafverfolgung**; hier müssen fünf Mitgliedstaaten noch die Umsetzung in nationales Recht mitteilen und fünf Mitgliedstaaten noch die restlichen Umsetzungsmaßnahmen mitteilen;⁶⁹ und
- die **Vierte Geldwäscherichtlinie**; hier muss ein Mitgliedstaat noch die restlichen Umsetzungsmaßnahmen mitteilen.⁷⁰

2. Schutz des öffentlichen Raums: empfohlene bewährte Verfahren

Die Kommission unterstützt die Mitgliedstaaten und deren nationale Behörden im Rahmen ihrer praktischen Arbeiten für einen besseren Schutz und eine gesteigerte Resilienz gegen Terrorismus weiterhin beim **Schutz des öffentlichen Raums**. Im Rahmen der Umsetzung des

⁶⁵ Die Mitteilungen von Spanien, den Niederlanden und Finnland stehen noch aus. Die Tschechische Republik und Slowenien haben eine teilweise Umsetzung mitgeteilt, sie müssen noch die restlichen Umsetzungsmaßnahmen mitteilen (Stand: 11. März 2019). Die Verweise auf die Mitteilung der vollständigen Umsetzung tragen den Erklärungen der Mitgliedstaaten Rechnung und greifen der Umsetzungsprüfung durch die Kommissionsdienststellen nicht vor.

⁶⁶ Belgien und Luxemburg müssen ihre Umsetzungsmaßnahmen noch melden. Ungarn hat eine teilweise Umsetzung mitgeteilt und noch die restlichen Umsetzungsmaßnahmen mitteilen (Stand: 11. März 2019).

⁶⁷ Griechenland, Zypern und Luxemburg müssen ihre Umsetzungsmaßnahmen noch melden. Belgien, Polen, Rumänien und Slowenien haben eine teilweise Umsetzung mitgeteilt, sie müssen noch die restlichen Umsetzungsmaßnahmen mitteilen (Stand: 11. März 2019).

⁶⁸ Belgien, Bulgarien, Deutschland, Irland, Griechenland, Spanien, Zypern, Lettland, Luxemburg, Ungarn, die Niederlande, Polen, Rumänien, Slowenien, die Slowakei, Finnland und Schweden müssen die Umsetzung noch mitteilen. Die Tschechische Republik, Estland, Litauen, Portugal und das Vereinigte Königreich haben eine teilweise Umsetzung mitgeteilt, sie müssen noch die restlichen Umsetzungsmaßnahmen mitteilen (Stand: 11. März 2019). Der Verweis auf die Mitteilungen der vollständigen Umsetzung trägt den Erklärungen der Mitgliedstaaten Rechnung und ist unbeschadet der Umsetzungsprüfung durch die Kommissionsdienststellen.

⁶⁹ Die Mitteilung von Bulgarien, Griechenland, Spanien, Zypern und Lettland steht noch aus. Die Tschechische Republik, Portugal, die Niederlande, Finnland und Slowenien haben eine teilweise Umsetzung mitgeteilt, sie müssen noch die restlichen Umsetzungsmaßnahmen mitteilen (Stand: 11. März 2019).

⁷⁰ Rumänien hat eine teilweise Umsetzung mitgeteilt und muss daher noch die restlichen Umsetzungsmaßnahmen mitteilen. Alle anderen Mitgliedstaaten haben die vollständige Umsetzung mitgeteilt. Aus der Bewertung der Kommission geht dennoch hervor, dass nach wie vor einige Bestimmungen der Richtlinie nicht vollständig umgesetzt sind (Stand: 11. März 2019).

Aktionsplans für einen besseren Schutz des öffentlichen Raums⁷¹ vom Oktober 2017 konzentrieren sich die Maßnahmen auf die Ausarbeitung und Zusammenstellung von Leitlinien und bewährten Verfahren. Im Zuge der Zusammenarbeit mit Behörden und privaten Betreibern öffentlicher Räume im sogenannten Forum der Betreiber⁷² hat die Kommission in Bezug auf mehrere Maßnahmen bewährte Verfahren ermittelt, die alle Betreiber und Behörden zum Schutz der öffentlichen Räume umsetzen können, um die Sicherheit zu verstärken.⁷³ Sie bieten grundlegende Orientierungspunkte für künftige Arbeiten innerhalb aller einschlägigen Bereiche für den Schutz öffentlicher Räume (siehe nachfolgender Kasten).

Bewährte Verfahren für Behörden und private Betreiber für einen besseren Schutz des öffentlichen Raums

Bewertung und Planung

- Ausarbeitung und Durchführung von Schwachstellenbeurteilungen, um mögliche Schwachstellen für Angriffe von außen wie auch von innen zu ermitteln.
- Ausarbeitung und Umsetzung eines Sicherheitsplans für Einrichtungen oder Veranstaltungen, einschließlich Vorbereitungs-, Notfall und Wiederherstellungsmaßnahmen, und Ermittlung geeigneter Sicherheitsmaßnahmen für das Umfeld des Gebäudes oder der Veranstaltung. Die Sicherheitsmaßnahmen müssen wirksam, diskret, angemessen und auf die unterschiedlichen Umgebungen zugeschnitten sein und der jeweiligen konkreten Funktionsweise Rechnung tragen;
- Ernennung und Schulung einer für die Koordinierung und Umsetzung der im Sicherheitsplan aufgeführten Sicherheitsmaßnahmen zuständigen Person und
- Ausarbeitung und Umsetzung eines Krisenmanagementplans;

Sensibilisierung und Schulung

- Einführung öffentlicher Kampagnen zur Sensibilisierung im Hinblick auf die Meldung von verdächtigem Verhalten und zur Reaktion im Falle eines die Sicherheit gefährdenden Angriffs gegen eine Einrichtung oder eine Veranstaltung;
- Ausarbeitung und Umsetzung eines internen Sensibilisierungsprogramms zur Sicherheit für alle Angestellten;
- Ausarbeitung und Umsetzung eines internen Programms zur Sensibilisierung für innere Bedrohungen, das dem Schutz von Einrichtungen oder Veranstaltungen vor verschiedensten Bedrohungen von innen (wie Sabotage, gewerbsmäßiger Diebstahl oder Terroranschläge) dient;
- Ausarbeitung grundlegender Sicherheitsschulungsprogramme für das gesamte Personal und Durchführung konkreter Sicherheitsschulungen, um so zur Entwicklung einer Unternehmenssicherheitskultur beizutragen. Ausarbeitung von Maßnahmen, die das Personal motivieren, solide Sicherheitsvorschriften umzusetzen und ein hohes Maß an Wachsamkeit aufrechtzuerhalten; und
- Durchführung regelmäßiger Sicherheitsübungen, die dazu dienen, die Abwehr- und Reaktionsbereitschaft im Angriffsfall zu ermitteln;

⁷¹ COM(2017) 612 final vom 18.10.2017.

⁷² Das im Zuge des Aktionsplans vom Oktober 2017 für einen besseren Schutz des öffentlichen Raums eingerichtete öffentlich-private Betreiber-Forum führt die Entscheidungsträger der Mitgliedstaaten und Betreiber verschiedener Sektoren zusammen, darunter Großveranstaltungen und Entertainment, Gastgewerbe, Einkaufszentren, Sport- und Kulturveranstaltungen, Verkehrsknotenpunkte u. a. m.

⁷³ Weitere Einzelheiten zu den bewährten Verfahren sind der Arbeitsunterlage der Kommissionsdienststellen zu bewährten Verfahren für den Schutz des öffentlichen Raums zu entnehmen (SWD(2019) 140 vom 20.3.2019).

Physischer Schutz

- Bewertung der Sicherheit und der Aspekte des physischen Schutzes bereits ab der Planung eines neuen Gebäudes oder einer neuen Veranstaltung;
- Bewertung der erforderlichen Zugangskontrollen und -barrieren, ohne dabei neue Schwachstellen zu erschaffen. Zugangskontrollen und -barrieren sollten Risiken nicht verlagern und keine neuen Ziele schaffen;
- Bewertung der geeignetsten Technologien für das Aufspüren von Explosivstoffen, Schusswaffen, Stichwaffen sowie chemischen, biologischen, radiologischen und nuklearen Stoffen;

Zusammenarbeit

- Benennung von Kontaktstellen und Festlegung der jeweiligen Funktionen und Zuständigkeiten bei der öffentlich-privaten Zusammenarbeit in Sicherheitsfragen (z. B. zwischen Betreibern, privaten Sicherheitsdiensten und Strafverfolgungsbehörden) mit dem Ziel einer besseren Kommunikation und Kooperation auf regelmäßiger Basis;
- eine vertrauensvolle und zeitnahe Kommunikation und Kooperation zum Austausch von Informationen über konkrete Risiken und Bedrohungen zwischen zuständigen Behörden, lokalen Strafverfolgungsbehörden und dem privaten Sektor;
- Koordination der Arbeiten zum Schutz des öffentlichen Raums auf kommunaler, regionaler und nationaler Ebene und Kommunikation sowie Austausch bewährter Verfahren auf allen Ebenen, einschließlich der EU-Ebene;
- Behörden sollten gemeinsam mit Betreibern praktische Empfehlungen und Leitlinien zur Ermittlung und Minimierung von Sicherheitsbedrohungen sowie zur Reaktion darauf ausarbeiten und zur Verfügung stellen.

3. Schwachstellen digitaler Infrastrukturen

Wenn es darum geht, das weitere wirtschaftliche Umfeld unserer Regierungen, industrielle Forschung, geistiges Eigentum, Geschäftspläne, aber auch unsere Wahlen und demokratischen Institutionen sowie unsere eigenen personenbezogenen Daten zu schützen, kommt es entscheidend auf digitale Resilienz an. Ein Brennpunkt der Cybersicherheit in der öffentlichen Debatte in ganz Europa ist der Aspekt der fünften Generation von Kommunikationsnetzen (5G). Bei der jüngsten informellen Tagung des Ministerrates „Telekommunikation“ vom 1. März 2019 in Bukarest sprachen sich die Minister für einen koordinierten europäischen Ansatz aus, um die digitale Resilienz in der EU im Zusammenhang mit 5G-Netzen zu stärken. 5G-Netzinfrastrukturen bilden eine wichtige Grundlage für die digitale Wirtschaft. Die 5G-Technologie ist soll über die Verbraucherdienste hinaus unverzichtbare Dienste für vertikale Sektoren wie Mobilität, Energie und Gesundheitswesen erbringen. 5G ist ein weltweiter Standard; Ausrüstungen und Geräte dafür werden von einer Reihe weltweiter Anbieter vertrieben.

Die Einführung von 5G-Netzen in den kommenden Jahren ist ein Meilenstein gegenüber früheren Netzstandards. Die Datenspeicherung in der Cloud wird es ermöglichen, Milliarden von Geräten im Internet der Dinge zu vernetzen, sodass Innovationen im Bereich der künstlichen Intelligenz in Gang gebracht und neue Möglichkeiten für Bürger und Unternehmen geschaffen werden. Die Cybersicherheit hat daher einen ganz besonderen Stellenwert, da Schwachstellen ausgenutzt werden und sehr schweren Schaden anrichten könnten. Da das Internet keine Grenzen kennt, kann sich eine Verletzung der Sicherheit in einem Mitgliedstaat auf viele andere auswirken.

Um Schutz vor potenziellen schwerwiegenden Auswirkungen auf die Sicherheit kritischer digitaler Infrastrukturen zu garantieren, ist ein gemeinsamer Ansatz der EU hinsichtlich der Sicherheit von 5G-Netzen erforderlich. Zu diesem Zweck wird die Kommission im Anschluss an den Europäischen Rat vom 21./22. März 2019 eine Empfehlung für einen gemeinsamen EU-Ansatz im Hinblick auf Sicherheitsrisiken im Zusammenhang mit 5G-Netzen vorlegen; diese stützt sich auf eine gemeinsame EU-Risikobewertung und Risikomanagementmaßnahmen, einen wirksamen Rahmen für die Zusammenarbeit und den Informationsaustausch und eine gemeinsame Lageeinschätzung auf EU-Ebene, die kritische Kommunikationsnetze umfasst. Die Beratungen über mögliche Maßnahmen sollten den Einsatz von Quantentechnologien zur Gewährleistung der Netzsicherheit und des Schutzes der gespeicherten Daten berücksichtigen.⁷⁴

Das Europäische Parlament nahm am 12. März 2019 eine Entschließung zu Sicherheitsbedrohungen im Zusammenhang mit der wachsenden technologischen Präsenz Chinas in der EU und mögliche Maßnahmen auf EU-Ebene an, um diese einzudämmen.

4. Außenbeziehungen

Die Verhandlungen zwischen der EU und Kanada über ein **überarbeitetes Abkommen über Fluggastdatensätze** schreiten gut voran. Das am 11./12. April 2019 anstehende Gipfeltreffen EU-Kanada in Montreal könnte den Verhandlungen positive Impulse bescheren.

Die Kommission arbeitet gemeinsam mit den Behörden der Vereinigten Staaten zusammen, um die bevorstehende gemeinsame Evaluierung des **Abkommens zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über die Verwendung von Fluggastdatensätzen**⁷⁵ im Einklang mit den Bestimmungen des Abkommens vorzubereiten. Die Arbeiten für die fünfte gemeinsame Überarbeitung des **Abkommens zwischen der Europäischen Union und den Vereinigten Staaten über das Programm zum Aufspüren der Finanzierung des Terrorismus**⁷⁶ sind bereits im Gange. Die gemeinsame Überarbeitung der Garantien, Kontrollen und Reziprozitätsbestimmungen des Abkommens wird auch dazu dienen, den Wert des Programms als Instrument zur Terrorismusbekämpfung sowohl für die EU als auch die USA zu prüfen.

Die laufenden Entwicklungen in Syrien haben die Gespräche über **ausländische terroristische Kämpfer**, die sich derzeit in den Konfliktzonen aufhalten bzw. dort gefangen gehalten werden, stärker in den Fokus rücken lassen. Die EU kann die Mitgliedstaaten auf deren Wunsch hin unterstützen, insbesondere was Informationsaustausch und strafrechtliche Ermittlungen anbelangt, vor allem im Hinblick auf die Zusammenarbeit mit internationalen Partnern und über Europol sowie auf der Grundlage von Fachwissen und bewährten Verfahren über die Rehabilitation und Wiedereingliederung, die vom Aufklärungsnetzwerk gegen Radikalisierung ausgearbeitet wurden. Die EU kann auch den Aufbau von Kapazitäten unterstützen, um Drittstaaten, die ganz besonders von rückkehrenden ausländischen terroristischen Kämpfern betroffen sind, zur Seite zu stehen. Die Entscheidung über eine mögliche Repatriierung ausländischer terroristischer Kämpfer und deren Familien aus den Konfliktzonen ist von den jeweiligen Mitgliedstaaten zu treffen.

⁷⁴ Siehe Mitteilung zur Europäischen Cloud-Initiative - Aufbau einer wettbewerbsfähigen Daten- und Wissenswirtschaft in Europa (COM(2016) 178 final vom 19.4.2016).

⁷⁵ ABl. L 215 vom 11.8.2012, S. 5.

⁷⁶ ABl. L 195 vom 27.7.2010, S. 5.

Die Plenarsitzung der Arbeitsgruppe Ostafrika im Rahmen des **Globalen Forums „Terrorismusbekämpfung“**, bei dem die EU und Ägypten gemeinsam den Vorsitz führten und an dem zahlreiche Vertreter von Polizei- und Justizbehörden aus Somalia, Kenia, Sudan, Uganda, Djibouti, Äthiopien, Jemen und Tansania teilnahmen, fand am 20. Februar 2019 in Nairobi statt.

V. FAZIT

Die Kommission hat beträchtliche Fortschritte auf dem Weg hin zu einer wirksamen und echten Sicherheitsunion erzielt, wobei in den vergangenen Wochen und Monaten eine Reihe vorrangiger Rechtsetzungsinitiativen vom Europäischen Parlament und Rat angenommen wurde. Dennoch sind vor den bevorstehenden Wahlen zum Europäischen Parlament im Mai 2019 weitere Anstrengungen erforderlich, um dringenden Sicherheitsanforderungen gerecht zu werden. Insbesondere fordert die Kommission die gesetzgebenden Organe auf, Verhandlungen über die vorgeschlagenen Vorschriften über die Entfernung terroristischer Online-Inhalte aufzunehmen, sobald das Europäische Parlament sein Verhandlungsmandat angenommen hat, um noch in der laufenden Legislaturperiode des Europäischen Parlaments eine Einigung erzielen zu können. Die Verhandlungen über den Vorschlag zur Stärkung der Europäischen Agentur für die Grenz- und Küstenwache befinden sich bereits im Trilog; damit wird deutlich, dass alle Organe darauf hinarbeiten, dass dieser Vorschlag noch vor den Wahlen zum Europäischen Parlament angenommen wird. Die Kommission fordert die Mitgliedstaaten auf, alle in der Sicherheitsunion vereinbarten Maßnahmen vollständig umzusetzen, um für die umfassende Sicherheit aller Bürger Sorge zu tragen.

Angesichts des Zeitdrucks, noch vor den Wahlen zum Europäischen Parlament im Mai 2019 dafür zu sorgen, dass die Union angemessen vorbereitet ist, fordert die Kommission zudem alle beteiligten Akteure auf, ihre Anstrengungen für mehr demokratische Resilienz bei Wahlen und gegen Desinformation zu verstärken. Im Vorfeld der Tagung des Europäischen Rates am 21./22. März 2019 müssen die Mitgliedstaaten ihre Koordinierung und ihren Informationsaustausch intensivieren, um gegen Desinformation vorzugehen und Wahlen vor Cyberbedrohungen zu schützen. Dabei gilt es, die von der EU bereitgestellten Instrumente vollumfänglich zu nutzen. Zugleich müssen Online-Plattformen ihre Bemühungen in allen Mitgliedstaaten beschleunigen, um dazu beizutragen, die Integrität der Wahlen zum Europäischen Parlament im Mai 2019 zu gewährleisten. Die Kommission wird diese Arbeiten in den kommenden Wochen und Monaten weiterhin unterstützen und fördern, um die Integrität der Wahlen zum Europäischen Parlament zu wahren.