Rat der
Europäischen Union

Brüssel, den 26. Juli 2019
(OR. en)

11501/19

JAI 845
COSI 159
FRONT 237
ASIM 89
DAPIX 248
ENFOPOL 354
SIRIS 120
VISA 164
FAUXDOC 55
COPEN 322
CYBER 232
DATAPROTECT 189
CT 79
JAIEX 113
EF 249

ÜBERMITTLUNGSVERMERK

Absender:	Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag des Generalsekretärs der Europäischen Kommission
Eingangsdatum:	25. Juli 2019
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2019) 353 final
Betr.:	MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN EUROPÄISCHEN RAT UND DEN RAT Auf dem Weg zu einer wirksamen und echten Sicherheitsunion - Neunzehnter Fortschrittsbericht

Die Delegationen erhalten in der Anlage das Dokument COM(2019) 353 final.

Anl.: COM(2019) 353 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 24.7.2019
COM(2019) 353 final

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

Auf dem Weg zu einer wirksamen und echten Sicherheitsunion - Neunzehnter Fortschrittsbericht

I. EINLEITUNG

Dies ist der neunzehnte Bericht über die weiteren 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 der Abwehrbereitschaft und Widerstandsfähigkeit gegen diese Bedrohungen“.

Die Bürgerinnen und Bürger Europas erwarten zu Recht, dass die Union für ihre Sicherheit sorgt. Für die Juncker-Kommission hat die Sicherheit seit dem ersten Tag oberste Priorität. In „Eine neue Strategische Agenda 2019-2024“, die vom Europäischen Rat beschlossen wurde, wird der „Schutz der Bürgerinnen und Bürger und der Freiheiten“ unter den vier Hauptprioritäten der Union an erster Stelle genannt.[1] Der Europäische Rat hat ferner angekündigt, dass er die Anstrengungen der Union im Kampf gegen Terrorismus und grenzüberschreitende Kriminalität ausweiten und verstärken wird, unter anderem durch Verbesserung der Zusammenarbeit und des Informationsaustauschs und Weiterentwicklung gemeinsamer Instrumente.

Dank der engen Zusammenarbeit zwischen dem Europäischen Parlament, dem Rat und der Kommission kommt die EU bei der gemeinsamen Arbeit auf dem Weg zu einer wirksamen und echten Sicherheitsunion sehr gut voran; zur Unterstützung der Mitgliedstaaten und zur Erhöhung der Sicherheit für alle Bürgerinnen und Bürger hat sie eine Reihe vorrangiger Gesetzgebungsinitiativen ergriffen und setzt ein breites Spektrum nichtlegislativer Maßnahmen um.[2] Die Union hat entschlossen gehandelt, um Terroristen und anderen Straftätern keinen Handlungsspielraum mehr zu lassen und Terroristen handlungsunfähig zu machen, indem sie den Erwerb und die Verwendung bestimmter Feuerwaffen und Explosivstoffe verboten und den Zugang zu Finanzmitteln eingeschränkt hat. Darüber hinaus hat die EU den Informationsaustausch zwischen den Mitgliedstaaten verbessert, Informationslücken geschlossen und noch offene Fragen geklärt, sowie gleichzeitig der Radikalisierung entgegengewirkt, die Europäerinnen und Europäer im Internet geschützt, Cyberbedrohungen und durch den Cyberspace ermöglichte Bedrohungen bekämpft, das Management der Außengrenzen der Union gestärkt und die internationale Zusammenarbeit im Bereich der Sicherheit intensiviert.

Zudem muss eine Reihe vorrangiger Initiativen im Rahmen der Sicherheitsunion erst noch von den beiden gesetzgebenden Organen angenommen werden. Nachdem sich das Europäische Parlament am 2. Juli 2019 für seine neunte Wahlperiode konstituiert hat, wird in diesem Bericht

- dargelegt, wo für die beiden gesetzgebenden Organe Handlungsbedarf besteht, um gegen unmittelbare Bedrohungen vorzugehen. Besonders dringend ist die **Bekämpfung von terroristischer Propaganda und Radikalisierung im Internet**;
- aufgeführt, bei welchen noch nicht angenommenen vorrangigen Initiativen im Rahmen der Sicherheitsunion die beiden gesetzgebenden Organe handeln müssen, um die **Cybersicherheit** zu erhöhen und den Zugang zu **elektronischen Beweismitteln**

[1] https://www.consilium.europa.eu/media/39914/a-new-strategic-agenda-2019-2024.pdf

[2] Einen Überblick bieten das Factsheet „Sicherheitsunion – Ein Europa, das schützt“ (https://ec.europa.eu/commission/sites/beta-political/files/euco-sibiu-security-union_1.pdf) und die Mitteilung „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Achtzehnter Fortschrittsbericht“ (COM(2019) 145 final vom 20.3.2019).

zu erleichtern und um die Arbeiten an solideren und intelligenteren Informationssystemen in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung abzuschließen;

- der Stand der dringenden gemeinsamen Arbeiten mitgeteilt, die im März 2019 eingeleitet wurden, um ausgehend von den bis zum 15. Juli 2019 vorgelegten nationalen Risikobewertungen der Mitgliedstaaten die **Sicherheit der 5G-Netze** zu bewerten und zu erhöhen;
- ein von der Kommission am 24. Juli 2019 angenommenes Paket von vier Berichten über die **Bekämpfung der Geldwäsche** behandelt, in denen die derzeitigen Risiken und Schwachstellen im Bereich der Geldwäsche analysiert werden und die Anwendung des einschlägigen EU-Rechtsrahmens im privaten und im öffentlichen Sektor bewertet wird;
- über die Fortschritte informiert, die seit März 2019[3] bei der Umsetzung legislativer Maßnahmen im Rahmen der Sicherheitsunion erzielt wurden, wobei die Interoperabilität der Informationssysteme zu den obersten Prioritäten für eine zügige und vollständige Umsetzung durch die Mitgliedstaaten zählt;
- eine Bestandsaufnahme der laufenden Arbeiten zur Bekämpfung von Desinformation und zum Schutz von Wahlen vor Cyberbedrohungen, der Anstrengungen zur Verbesserung der Abwehrbereitschaft und des Schutzes gegenüber Sicherheitsbedrohungen sowie der Zusammenarbeit mit internationalen Partnern in Sicherheitsfragen vorgenommen.

II. FORTSCHRITTE BEI DEN GESETZGEBERISCHEN PRIORITÄTEN

1. Radikalisierungsprävention im Internet und in den Gemeinschaften

Die Radikalisierungsprävention sowohl im Internet als auch in den Gemeinschaften steht im Mittelpunkt der Reaktion der EU auf den Terrorismus.

Der entsetzliche Anschlag, der am 15. März 2019 im neuseeländischen Christchurch verübt wurde, war eine schreckliche Erinnerung daran, wie das Internet für die Zwecke des Terrorismus nutzbar gemacht werden kann, unabhängig davon, ob dieser von Dschihadismus, Rechtsextremismus oder einer anderen extremistischen Ideologie befeuert wird. Die Geschwindigkeit und der Umfang, in denen der Anschlag von Christchurch per Livestream über die Internetplattformen verbreitet wurde, haben gezeigt, wie wichtig es ist, dass Internetplattformen über geeignete Möglichkeiten verfügen, die rasche Ausbreitung solcher Inhalte einzudämmen.

Als Reaktion darauf unterstützten die Staats- und Regierungschefs einiger Mitgliedstaaten und Drittländer, Präsident Juncker und die Online-Plattformen am 15. Mai 2019 den „**Christchurch-Aufruf**“[4], in dem kollektive Maßnahmen zur Beseitigung terroristischer und gewaltverherrlichender extremistischer Online-Inhalte aufgeführt sind. Weitere

---

[3] Siehe die Mitteilung „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Achtzehnter Fortschrittsbericht“ (COM(2019) 145 final vom 20.3.2019).

[4] https://www.elysee.fr/emmanuel-macron/2019/05/15/the-christchurch-call-to-action-to-eliminate-terrorist-and-violent-extremist-content-online.en. Der französische Präsident Emmanuel Macron und die neuseeländische Premierministerin Jacinda Ardern hatten die politischen Entscheidungsträger und die Online-Plattformen für den 15. Mai 2019 nach Paris eingeladen, um diese Initiative auf den Weg zu bringen.

diesbezügliche Verpflichtungen wurden von der G7[5] und der G20[6] übernommen.

Die Kommission hat auf die von terroristischen Online-Inhalten ausgehende eindeutige und gegenwärtige Gefahr bereits mit dem von Präsident Juncker in seiner Rede zur Lage der Union 2018 angekündigten **Legislativvorschlag** reagiert und einen klaren, harmonisierten Rechtsrahmen zur Verhinderung des Missbrauchs von Hosting-Dienstleistern für die Verbreitung terroristischer Online-Propaganda vorgeschlagen.[7] Die vorgeschlagenen Maßnahmen schreiben vor, dass Internetplattformen terroristische Inhalte innerhalb einer Stunde aus dem Netz nehmen müssen, wenn sie von den zuständigen Behörden eines Mitgliedstaats eine Entfernungsanordnung erhalten. Zudem ist eine Plattform, wenn sie für die Verbreitung terroristischer Inhalte missbraucht wird, auf der Grundlage klarer Vorschriften und Garantien verpflichtet, proaktiv tätig werden, um den betreffenden Inhalt aufzuspüren und sein erneutes Auftauchen zu verhindern. Die Behörden der Mitgliedstaaten müssen dafür sorgen, dass besondere Strafverfolgungsstellen mit den notwendigen Mitteln ausgestattet sind, um terroristische Inhalte erkennen und entsprechende Entfernungsanordnungen erlassen zu können.

Auf diese Weise kann ein schnelles und wirksames unionsweites System mit soliden Garantien aufgebaut werden, einschließlich wirksamer Beschwerdeverfahren und gerichtlicher Rechtsbehelfe. Die vorgeschlagenen Maßnahmen werden dazu beitragen, das reibungslose Funktionieren des digitalen Binnenmarkts zu gewährleisten und gleichzeitig die Sicherheit zu erhöhen, das Vertrauen in das Internet zu stärken und die Garantien für die Freiheit der Meinungsäußerung und die Informationsfreiheit zu verbessern.

Im Dezember 2018 einigten sich die Ministerinnen und Minister für Justiz und Inneres im Rat auf eine allgemeine Ausrichtung zu dem Vorschlag. Das Europäische Parlament hat seinen Standpunkt im April 2019 in erster Lesung festgelegt. **Die Kommission fordert die beiden gesetzgebenden Organe auf, so bald wie möglich interinstitutionelle Verhandlungen über diese vorrangige Initiative für die Entfernung terroristischer Online-Inhalte aufzunehmen**, damit rasch eine Einigung über einen EU-Rechtsrahmen mit klaren Vorschriften und Garantien erzielt werden kann.

Parallel dazu setzt die Kommission die Zusammenarbeit mit den Online-Plattformen im Rahmen des **EU-Internetforums**[8] fort. Wie von Präsident Juncker beim Pariser Treffen vom 15. Mai 2019 zum „Christchurch-Aufruf" angekündigt, hat die Kommission gemeinsam mit Europol begonnen, ein **EU-Krisenprotokoll** zu erarbeiten, das es Regierungen und Internetplattformen ermöglichen soll, rasch und koordiniert auf die Verbreitung terroristischer Online-Inhalte zu reagieren, zum Beispiel unmittelbar nach einem Terroranschlag. Diese Arbeiten sind Teil der Bemühungen auf internationaler Ebene, den „Christchurch-Aufruf" umzusetzen. Neben weiteren Gesprächen mit den Mitgliedstaaten und der Industrie und einer

---

5 https://www.elysee.fr/en/g7/2019/04/06/g7-interior-ministers-meeting-what-are-the-outcomes

6 Beim G20-Gipfel am 28./29. Juni 2019 in Osaka bekräftigten die politischen Entscheidungsträger ihre Zusage zu handeln, um die Bevölkerung davor zu schützen, dass Terrorismus und gewaltverherrlichender Extremismus, der den Terrorismus begünstigt, das Internet für ihre Zwecke nutzbar machen (https://g20.org/pdf/documents/en/FINAL_G20_Statement_on_Preventing_Terrorist_and_VECT.pdf).

7 COM(2018) 640 final vom 12.9.2018.

8 In dem 2015 gegründeten **EU-Internetforum** kommen die EU-Innenminister, die Internetbranche und andere Interessenträger zusammen, um in einer freiwilligen Partnerschaft gemeinsam gegen den Missbrauch des Internets durch terroristische Gruppierungen vorzugehen und die Bürgerinnen und Bürger zu schützen.

für September 2019 anberaumten Planübung zur Simulation einer Notlage wird die Kommission eine Ministertagung des EU-Internetforums für den 7. Oktober 2019 einberufen, auf der das EU-Krisenprotokoll gebilligt werden soll.

Darüber hinaus **unterstützt** die Kommission nach wie vor in ganz Europa **die Mitgliedstaaten und lokalen Akteure in ihren Bemühungen, vor Ort in den lokalen Gemeinschaften eine Radikalisierung zu verhindern und zu bekämpfen.** . Dies erfordert langfristige nachhaltige Bemühungen, in die alle relevanten Akteure auf lokaler, nationaler und EU-Ebene einbezogen werden. Der im August 2018 eingesetzte **Lenkungsausschuss für Maßnahmen der Union zur Prävention und Bekämpfung von Radikalisierung,** der die Kommission beraten soll, wie die politische Reaktion der EU in diesem Bereich verstärkt werden könnte, trat am 17. Juni 2019 zu seiner zweiten Sitzung zusammen, um weitere Maßnahmen in vorrangig anzugehenden Problembereichen wie Radikalisierung in Gefängnissen und Bekämpfung extremistischer Ideologien zu prüfen. Da vor Ort und an der Basis tätige Praktiker häufig am besten in der Lage sind, die Anzeichen für eine Radikalisierung frühzeitig zu erkennen und ihr entgegenzuwirken, unterstützt das von der EU finanzierte **Aufklärungsnetzwerk gegen Radikalisierung**[9] weiter die an vorderster Front stehenden Akteure; diesem Netz gehören rund 5000 Praktiker aus Zivilgesellschaft, Schule und Polizei sowie nationale Koordinatoren und politische Entscheidungsträger an.

Die jüngste Zusammenarbeit von vor Ort tätigen Praktikern im Rahmen des Netzwerks hat zu einem besseren Verständnis der vom Rechtsextremismus ausgehenden Herausforderungen geführt. In diesem Jahr wird das Aufklärungsnetzwerk gegen Radikalisierung Informationsblätter veröffentlichen, um politischen Entscheidungsträgern und Praktikern dabei zu helfen, die wichtigsten Formen und Ausprägungen des Rechtsextremismus und des islamistischen Extremismus zu erkennen; hierzu zählen zentrale Narrative, Sprache, Formen, Symbole, Typologien und Strategien. Da die lokalen Akteure und die **Städte** bei der Prävention und Bekämpfung von Radikalisierung besonders gefordert sind, unterstützt die Kommission außerdem von Städten geführte Initiativen gegen Radikalisierung. Im Anschluss an die Konferenz vom 26. Februar 2019 zum Thema „EU-Städte gegen Radikalisierung“ trat am 8. Juli 2019 auf Einladung des Bürgermeisters von Straßburg eine Pilotgruppe von rund 20 Städten zu einer ersten Sitzung zusammen, um den Austausch bewährter Methoden zu intensivieren und die Anstrengungen der Städte in diesem Bereich zu verstärken.

Parallel dazu wird die Unterstützung von Partnerländern bei der Bekämpfung von Radikalisierung, die zum Terrorismus führen kann fortgesetzt, unter anderem in Gefängnissen.

---

[9] Die Kommission hat 2011 das **Aufklärungsnetzwerk gegen Radikalisierung** eingerichtet, um vor Ort und an der Basis tätige Praktiker zusammenzubringen. Im Jahr 2015 hat die Kommission das Netzwerk durch die Gründung des Exzellenzzentrums des Aufklärungsnetzwerks gegen Radikalisierung gestärkt, um gezieltere Beratungs-, Unterstützungs- und Betreuungsdienste für die Interessenträger in den Mitgliedstaaten zu entwickeln und um das Fachwissen und die Kompetenzen der verschiedenen Akteure zu verbessern. Weitere Informationen zur Tätigkeit des Aufklärungsnetzwerks gegen Radikalisierung unter https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network_en.

Damit der von terroristischen Online-Inhalten ausgehenden Bedrohung entgegengewirkt werden kann, fordert die Kommission das Europäische Parlament und den Rat auf,

- Verhandlungen über den Legislativvorschlag zur Verhinderung der Verbreitung **terroristischer Online-Inhalte** aufzunehmen, um rasch eine Einigung über einen EU-Rechtsrahmen mit klaren Vorschriften und Garantien zu erzielen.

2. Erhöhung der Cybersicherheit

Cybersicherheit stellt nach wie vor eine zentrale Herausforderung für die Sicherheit dar. Wichtige Fortschritte[10] bei der Bekämpfung der „klassischen" Cyberbedrohungen für Systeme und Daten hat die EU durch Umsetzung der Maßnahmen erzielt, die in der Gemeinsamen Mitteilung „Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen"[11] vom September 2017 aufgeführt sind. Hierzu zählt unter anderem der EU-Rechtsakt zur Cybersicherheit[12], mit dem der Agentur der Europäischen Union für Cybersicherheit ein dauerhaftes Mandat erteilt, ihre Rolle gestärkt und ein EU-Rahmen für die Cybersicherheitszertifizierung geschaffen wird. Die Kommission hat sich auch mit sektorspezifischen Erfordernissen befasst, zum Beispiel in ihrer Empfehlung zur Cybersicherheit im Energiesektor vom 3. April 2019[13]. Die kontinuierliche Zunahme der Angriffe böswilliger Akteure auf verschiedene Ziele und Opfer bedeutet jedoch, dass den Anstrengungen zur Bekämpfung der Cyberkriminalität und zur Erhöhung der Cybersicherheit im Handeln der EU weiterhin Priorität zukommt.

Das Europäische Parlament und der Rat müssen noch eine Einigung über die vorrangige Initiative der Kommission für ein **Europäisches Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung und ein Netz nationaler Koordinierungszentren**[14] erzielen. Mit dem Vorschlag sollen die technologischen und industriellen Kapazitäten im Bereich der Cybersicherheit unterstützt und die Wettbewerbsfähigkeit der Cybersicherheitsbranche in der Union gesteigert werden. Beide gesetzgebenden Organe haben ihre Verhandlungsmandate im März 2019 angenommen. Da es nicht möglich war, die interinstitutionellen Verhandlungen vor Ende der letzten Wahlperiode des Europäischen Parlaments abzuschließen, hat dieses seinen Standpunkt in erster Lesung förmlich festgelegt. Inzwischen sind die Beratungen zwischen den Mitgliedstaaten im Rat, bei denen die Wechselwirkungen zwischen der vorgeschlagenen Verordnung zur Einrichtung des Kompetenzzentrums für Cybersicherheit und des Netzes einerseits und den Programmen „Horizont Europa" und „Digitales Europa" andererseits im Mittelpunkt stehen, fortgesetzt worden. **Die Kommission fordert die beiden gesetzgebenden Organe auf, die interinstitutionellen Verhandlungen über diese vorrangige Initiative zur Erhöhung der**

---

10 Weitere Informationen in der Broschüre „Eine hohe Cybersicherheit in der Europäischen Union: Abwehrfähigkeit, Abschreckung und Abwehr": https://ec.europa.eu/digital-single-market/en/news/building-strong-cybersecurity-european-union-resilience-deterence-defence.

11 JOIN(2017) 450 final vom 13.9.2017.

12 Mit dem EU-Rechtsakt zur Cybersicherheit (Verordnung (EU) 2019/881 vom 17.4.2019) werden erstmals EU-weite Vorschriften für die Cybersicherheitszertifizierung von Produkten, Prozessen und Diensten eingeführt. Ferner ist darin ein neues, dauerhaftes Mandat für die EU-Agentur für Cybersicherheit sowie eine Aufstockung der Mittel der Agentur vorgesehen, damit sie ihre Aufgaben erfüllen kann. Weitere Informationen zur Aufforderung zur Einreichung von Vorschlägen unter https://ec.europa.eu/digital-single-market/en/news/eu10-million-eu-funding-available-projects-stepping-eus-cybersecurity-capabilities-and-cross.

13 C(2019) 2400 final vom 3.4.2019 und SWD(2019) 1240 final vom 3.4.2019.

14 COM(2018) 630 final vom 12.9.2018.

Cybersicherheit wieder aufzunehmen und zügig abzuschließen.

In der Zwischenzeit leistet die Kommission weiter **Unterstützung für Forschung und Innovation** im Zusammenhang mit Cybersicherheit und stellt auf der Grundlage des derzeitigen mehrjährigen Finanzrahmens 135 Mio. EUR für Projekte in Bereichen wie Cybersicherheit in kritischen Infrastrukturen, intelligentes Sicherheits- und Datenschutzmanagement sowie eigens für Bürger und kleine und mittlere Unternehmen entwickelte Instrumente bereit.[15] Im Juli 2019 hat die Kommission im Rahmen der Fazilität „Connecting Europe" eine neue Aufforderung zur Einreichung von Vorschlägen veröffentlicht und 10 Mio. EUR an EU-Mitteln für die wichtigsten Akteure bereitgestellt, die in der Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie)[16] genannt sind, unter anderem europäische Computer-Notfallteams, Betreiber wesentlicher Dienste (z. B. Banken, Krankenhäuser, Versorgungsbetriebe, Eisenbahngesellschaften, Luftfahrtunternehmen und Domain-Namen-Anbieter) sowie verschiedene Behörden. Zum ersten Mal wurde auch den europäischen Behörden für Cybersicherheitszertifizierung die Teilnahme gestattet, damit sie den EU-Rechtsakt zur Cybersicherheit umsetzen können.

Am 17. Mai 2019 hat der Rat eine **Sanktionsregelung** eingeführt, die es der EU ermöglicht, zur Abschreckung vor Cyberangriffen und zur Reaktion auf solche Angriffe, die eine externe Bedrohung für die EU und ihre Mitgliedstaaten darstellen, gezielte restriktive Maßnahmen zu verhängen. Die neue Sanktionsregelung gehört zum **Instrumentarium der EU für die Cyberdiplomatie**[17], dem Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten[18], der es der EU ermöglicht, die ihr zu Gebote stehenden Maßnahmen der Gemeinsamen Außen- und Sicherheitspolitik in vollem Umfang zur Abschreckung und Reaktion im Zusammenhang mit böswilligen Cyberaktivitäten zu nutzen.

Die Kommission trifft nicht nur Maßnahmen zur Bekämpfung von Cyberbedrohungen für Systeme und Daten, sondern auch zur Bewältigung der komplexen und vielschichtigen Herausforderungen, die mit **hybriden Bedrohungen** verbunden sind.[19] Der Europäische Rat hat in seinen Schlussfolgerungen vom 21. Juni 2019[20] hervorgehoben, dass „*[d]ie EU ... für eine koordinierte Reaktion auf hybride Bedrohungen und Cyberbedrohungen sorgen und ihre Zusammenarbeit mit einschlägigen internationalen Akteuren verstärken [muss]*." Die Kommission begrüßt, dass die Abwehr hybrider Bedrohungen auch zu den Prioritäten des finnischen Ratsvorsitzes gehört und dass auf der informellen Tagung der Ministerinnen und Minister für Justiz und Inneres vom 18./19. Juli 2019 in Helsinki eine auf konkreten

---

15 https://ec.europa.eu/programmes/horizon2020/en/h2020-section/cross-cutting-activities-focus-areas

16 Richtlinie (EU) 2016/1148 vom 6.7.2016.

17 http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/de/pdf

18 Hierzu zählen unter anderem Cyberangriffe sowie versuchte Cyberangriffe mit potenziell erheblichen Auswirkungen, z. B. Zugang zu Informationssystemen oder Abfangen von Daten über digitale Infrastrukturen wie 5G-Netze (siehe auch Abschnitt III „Erhöhung der Sicherheit digitaler Infrastrukturen").

19 Siehe *Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats* [Bericht über die Umsetzung des Gemeinsamen Rahmens für die Bekämpfung hybrider Bedrohungen (2016) und der Gemeinsamen Mitteilung „Stärkung der Resilienz und Ausbau der Kapazitäten zur Abwehr hybrider Bedrohungen" (2018)] (SWD(2019) 200 final vom 28.5.2019). Siehe auch den Legislativvorschlag vom September 2016 für eine Verordnung über eine Unionsregelung für die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung, der technischen Unterstützung und der Durchfuhr betreffend Güter mit doppeltem Verwendungszweck (Neufassung) (COM(2016) 616 final vom 28.9.2016).

20 https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-de.pdf

Szenarien beruhende Orientierungsaussprache über hybride Bedrohungen abgehalten wurde. Die für Verteidigungspolitik zuständigen Direktoren und die politischen Direktoren der EU haben am 7./8. bzw. 9./10. Juli 2019 ähnliche auf Szenarien gestützte Diskussionen geführt, über deren Ergebnisse den Außen- und Verteidigungsministern am 29./30. August 2019 in einer gemeinsamen informellen Sitzung Bericht erstattet wird.

Damit die Cybersicherheit erhöht werden kann, fordert die Kommission das Europäische Parlament und den Rat auf,

- rasch eine Einigung über den Legislativvorschlag für ein **Europäisches Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung und ein Netz nationaler Koordinierungszentren** zu erzielen.

3. Verbesserung des Zugangs der Strafverfolgungsbehörden zu elektronischen Beweismitteln

Die EU hat weitere Maßnahmen getroffen, um Terroristen und Kriminelle handlungsunfähig zu machen, indem ihnen der Zugang zu Ausgangsstoffen für Explosivstoffe[21], die Finanzierung ihrer Aktivitäten[22] und unerkanntes Reisen[23] erschwert werden.

Die Verhandlungen über die Vorschläge der Kommission vom April 2018 für die Verbesserung des **Zugangs** der Strafverfolgungsbehörden **zu elektronischen Beweismitteln** sollten so rasch wie möglich abgeschlossen werden – bei mehr als der Hälfte aller strafrechtlichen Ermittlungen wird heute ein grenzüberschreitender Antrag auf Zugang zu elektronischen Beweismitteln gestellt.[24] Der Rat hat seine Position für die Verhandlungen über die Vorschläge für eine Verordnung zur Verbesserung des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln in Strafsachen[25] und für eine Richtlinie zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren[26] festgelegt. Angesichts der entscheidenden Bedeutung eines effizienten Zugangs zu elektronischen Beweismitteln für die Untersuchung und Verfolgung grenzüberschreitender Straftaten wie Terrorismus oder Cyberkriminalität fordert die Kommission das Europäische Parlament nachdrücklich auf, diesen Vorschlag voranzubringen, damit die beiden gesetzgebenden Organe ihn rasch annehmen können.

Parallel dazu arbeitet die Kommission im Einklang mit den vom Rat auf der Tagung des Rates (Justiz und Inneres) vom 6./7. Juni 2019 erteilten Verhandlungsmandaten daran, in den

---

21 Verordnung (EU) 2019/1148 vom 20. Juni 2019 über die Vermarktung und Verwendung von Ausgangsstoffen für Explosivstoffe.

22 Richtlinie (EU) 2019/1153 vom 11. Juli 2019 zur Festlegung von Vorschriften zur Erleichterung der Nutzung von Finanz- und sonstigen Informationen für die Verhütung, Aufdeckung, Untersuchung oder Verfolgung bestimmter Straftaten.

23 Verordnung (EU) 2019/1157 vom 20. Juni 2019 zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern und der Aufenthaltsdokumente, die Unionsbürgern und deren Familienangehörigen ausgestellt werden, die ihr Recht auf Freizügigkeit ausüben.

24 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).

25 COM(2018) 225 final vom 17.4.2018. Der Rat hat sein Verhandlungsmandat für die vorgeschlagene Verordnung auf der Tagung des Rates (Justiz und Inneres) vom 7. Dezember 2018 angenommen.

26 COM(2018) 226 final vom 17.4.2018. Der Rat hat seine Verhandlungsposition zu der vorgeschlagenen Richtlinie auf der Tagung des Rates (Justiz und Inneres) vom 8. März 2019 angenommen.

laufenden Verhandlungen zum einen über ein Zweites Zusatzprotokoll zum Budapester Übereinkommen des Europarats über Computerkriminalität sowie zum anderen mit den Vereinigten Staaten die für den **internationalen Austausch elektronischer Beweismittel** erforderlichen Garantien zu verbessern und zu sichern.[27] Die Kommission hat vom 9. bis zum 11. Juli 2019 an der jüngsten Runde der Verhandlungen über ein Zweites Zusatzprotokoll zum Budapester Übereinkommen des Europarats über Computerkriminalität teilgenommen. Die Kommission und die Behörden der Vereinigten Staaten bereiten zurzeit auf fachlicher Ebene die förmliche Aufnahme der Verhandlungen über ein Abkommen zwischen der EU und den USA über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln vor.

Damit der Zugang der Strafverfolgungsbehörden zu elektronischen Beweismitteln verbessert werden kann, fordert die Kommission das Europäische Parlament auf,

- sein Verhandlungsmandat für die Legislativvorschläge zu **elektronischen Beweismitteln** anzunehmen, damit die Trilog-Gespräche mit dem Rat rasch aufgenommen werden können. *(Priorität der Gemeinsamen Erklärung)*

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

Nach dem Erlass der Vorschriften über die **Interoperabilität der Informationssysteme**[28], die bei der Aufdeckung von Mehrfachidentitäten und der Bekämpfung von Identitätsbetrug helfen, sodass Informationslücken geschlossen und noch offene Fragen geklärt werden, hat die Kommission zügig eine Reihe von Initiativen auf den Weg gebracht, um die Mitgliedstaaten unter anderem mit Workshops zur Erleichterung des Austauschs von Fachwissen und bewährten Methoden sowie bei Bedarf auch mit Finanzmitteln bei der Umsetzung zu unterstützen. Eine enge Zusammenarbeit zwischen den EU-Agenturen, sämtlichen Mitgliedstaaten und den assoziierten Schengen-Ländern ist von größter Bedeutung, um das ehrgeizige Ziel einer vollständigen Interoperabilität der EU-Informationssysteme in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung bis 2020 zu erreichen.

Dieses Ziel erfordert auch eine zügige vollständige Umsetzung der unlängst verabschiedeten Rechtsvorschriften zur Einrichtung neuer Informationssysteme – -des EU-Einreise-/Ausreisesystems[29] und des Europäischen Reiseinformations- und -genehmigungssystems[30] – sowie zur Stärkung des Schengener Informationssystems[31] und zur Einbeziehung von Drittstaatsangehörigen in das Europäische Strafregisterinformationssystem[32]. Die neue Architektur für solidere und intelligentere Informationssysteme in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung wird vor Ort nur dann etwas bewirken, wenn alle Komponenten nach dem vereinbarten Zeitplan auf Unionsebene und in jedem Mitgliedstaat vollständig umgesetzt werden.

---

27 https://www.consilium.europa.eu/de/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/

28 Verordnung (EU) 2019/817 vom 20. Mai 2019 und Verordnung (EU) 2019/818 vom 20. Mai 2019.

29 Verordnung (EU) 2017/2226 vom 30. November 2017.

30 Verordnung (EU) 2018/1240 vom 12. September 2018 und Verordnung (EU) 2018/1241 vom 12. September 2018.

31 Verordnung (EU) 2018/1860 vom 28. November 2018, Verordnung (EU) 2018/1861 vom 28. November 2018 und Verordnung (EU) 2018/1862 vom 28. November 2018.

32 Verordnung (EU) 2019/816 vom 17. April 2019.

Gleichzeitig besteht für die beiden gesetzgebenden Organe noch Handlungsbedarf, um die Arbeiten an solideren und intelligenteren Informationssystemen in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung abzuschließen.
Im Rahmen der technischen Umsetzung des **Europäischen Reiseinformations- und -genehmigungssystems** hat die Kommission am 7. Januar 2019 zwei Vorschläge mit technischen Änderungen der betreffenden Verordnung[33] vorgelegt, die für die vollständige Einrichtung des Systems erforderlich sind. Die Kommission fordert die beiden gesetzgebenden Organe auf, ihre Arbeiten an diesen technischen Änderungen voranzutreiben, damit so bald wie möglich eine Einigung erzielt werden kann, die eine rasche und fristgerechte Einrichtung des Europäischen Reiseinformations- und -genehmigungssystems ermöglichen würde, sodass es Anfang 2021 seinen Betrieb aufnehmen könnte.

Im Mai 2018 hat die Kommission einen Vorschlag zur **Stärkung des bestehenden Visa-Informationssystems**[34] vorgelegt, der eine gründlichere Prüfung des Hintergrunds von Antragstellern und die Schließung von Informationslücken durch einen besseren Informationsaustausch zwischen den Mitgliedstaaten vorsieht.
Der Rat hat am 19. Dezember 2018 sein Verhandlungsmandat angenommen, und das Plenum des Europäischen Parlaments hat am 13. März 2019 über seinen Bericht zu dem Vorschlag abgestimmt und damit seine erste Lesung abgeschlossen. Die Kommission fordert die beiden gesetzgebenden Organen auf, die Verhandlungen nach der Konstituierung des neuen Europäischen Parlaments rasch aufzunehmen.

Im Mai 2016 hat die Kommission vorgeschlagen, den Anwendungsbereich von **Eurodac**[35] zu erweitern: Das System soll nicht mehr nur zur Identifizierung von Asylbewerbern, sondern auch zur Identifizierung illegal aufhältiger und irregulär in die EU einreisender Drittstaatsangehöriger genutzt werden. Im Einklang mit den Schlussfolgerungen des Europäischen Rates vom Dezember 2018[36] und der Mitteilung der Kommission vom 6. März 2019 über die Fortschritte bei der Umsetzung der Europäischen Migrationsagenda[37] fordert die Kommission die beiden gesetzgebenden Organe auf, den Vorschlag anzunehmen. Die Annahme dieses Legislativvorschlags ist notwendig, damit Eurodac Teil der künftigen Architektur interoperabler EU-Informationssysteme wird, sodass die wichtigsten Daten von Drittstaatsangehörigen, die illegal aufhältig oder irregulär in die EU eingereist sind, integriert werden können.

Damit die EU-Informationssysteme in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung gestärkt werden können, fordert die Kommission das Europäische Parlament und den Rat auf,

- den Legislativvorschlag zu **Eurodac** anzunehmen *(Priorität der Gemeinsamen Erklärung)*;
- auf eine rasche Einigung über die vorgeschlagenen technischen Änderungen hinzuarbeiten, die für die Einrichtung des **Europäischen Reiseinformations- und -genehmigungssystems** erforderlich sind.

---

33 COM(2019) 3 final und COM(2019) 4 final vom 7.1.2019.
34 COM(2018) 302 final vom 16.5.2018.
35 COM(2016) 272 final vom 4.5.2016.
36 https://www.consilium.europa.eu/de/press/press-releases/2018/12/14/european-council-conclusions-13-14-december-2018/
37 COM(2019) 126 final vom 6.3.2019.

III. ERHÖHUNG DER SICHERHEIT DIGITALER INFRASTRUKTUREN

Die Resilienz unserer digitalen Infrastrukturen ist für die Behörden, die Wirtschaft, die Sicherheit unserer personenbezogenen Daten und das Funktionieren unserer demokratischen Institutionen von entscheidender Bedeutung. Die in den kommenden Jahren entstehenden **Netze der fünften Generation (5G-Netze)** werden das digitale Rückgrat unserer Gesellschaften und Volkswirtschaften bilden und Milliarden von Bürgern, Objekten und Systemen miteinander verbinden, auch in kritischen Sektoren wie Energie, Verkehr, Bank- und Gesundheitswesen; sie werden industrielle Steuerungssysteme ermöglichen, die sensible Informationen verarbeiten, und Sicherheitssysteme unterstützen.

Da die 5G-Technik angesichts weltweiter Umsätze, die im Jahr 2025 schätzungsweise 225 Mrd. EUR erreichen dürften, ein Schlüsselfaktor der europäischen Wettbewerbsfähigkeit auf dem Weltmarkt ist, **kommt der Sicherheit der 5G-Netze entscheidende Bedeutung für die Gewährleistung der strategischen Autonomie der Union zu**. Die Sicherstellung eines hohen Cybersicherheitsniveaus erfordert abgestimmte Maßnahmen sowohl auf nationaler als auch auf europäischer Ebene, da sich jede Schwachstelle in den 5G-Netzen eines Mitgliedstaats auf die Union als Ganzes auswirken würde.

Nachdem die Staats- und Regierungschefs auf der Tagung des Europäischen Rates vom März 2019 ihre Unterstützung bekundet hatten[38], hat die Kommission am 26. März 2019 eine **Empfehlung zur Cybersicherheit der 5G-Netze**[39] vorgelegt, in der Maßnahmen zur Bewertung der Cybersicherheitsrisiken von 5G-Netzen und zur Verstärkung von Präventivmaßnahmen dargelegt werden. Die Empfehlungen stützen sich auf koordinierte Risikobewertungs- und -managementmaßnahmen der EU, einen wirksamen Rahmen für Zusammenarbeit und Informationsaustausch sowie eine gemeinsame Lageeinschätzung auf EU-Ebene in Bezug auf kritische Kommunikationsnetze.

Als **erste Phase** des mit der Empfehlung eingeleiteten Prozesses haben alle Mitgliedstaaten bis zum 15. Juli 2019 ihre **nationale Risikobewertung** abgeschlossen und ihre Erkenntnisse der Kommission und der EU-Agentur für Cybersicherheit übermittelt oder angekündigt, dies in Kürze zu tun. Den nationalen Risikobewertungen lagen Leitlinien und eine gemeinsame Vorlage für die Berichterstattung zugrunde, auf die sich die Mitgliedstaaten und die Kommission geeinigt hatten, um die Kohärenz zu fördern und den Informationsaustausch über die nationalen Ergebnisse auf EU-Ebene zu erleichtern. Zu den Parametern, die von allen Mitgliedstaaten geprüft wurden, gehörten unter anderem:

- die wichtigsten Bedrohungen und Gefährdungsakteure im Zusammenhang mit 5G-Netzen,
- der Grad der Verwundbarkeit der 5G-Netzkomponenten und -funktionen sowie anderer Anlagen und
- verschiedene Arten von Schwachstellen, sowohl technischer als auch anderer Art, die möglicherweise in der 5G-Lieferkette entstehen können.

Darüber hinaus nahmen zahlreiche verantwortliche Akteure in den Mitgliedstaaten an den nationalen Risikobewertungen teil, darunter – je nach den nationalen Zuständigkeiten – Behörden für Cybersicherheit und Telekommunikation sowie Sicherheits- und

[38] https://data.consilium.europa.eu/doc/document/ST-1-2019-INIT/de/pdf
[39] C(2019) 2335 final vom 26.3.2019.

Nachrichtendienste, die ihre Zusammenarbeit und Koordinierung ebenfalls verstärken. Parallel dazu hat eine Reihe von Mitgliedstaaten mit Blick auf ihre nationalen Zeitpläne für die 5G-Einführung bereits Schritte unternommen, um die geltenden Sicherheitsanforderungen in diesem Bereich zu verschärfen, während mehrere andere Mitgliedstaaten ihre Absicht bekundet haben, in naher Zukunft neue Maßnahmen zu erwägen.

Auf der Grundlage der Ergebnisse der nationalen Risikobewertungen werden die Cybersicherheitsbehörden der Mitgliedstaaten in der Kooperationsgruppe für Netz- und Informationssysteme bis zum 1. Oktober 2019 eine **gemeinsame Überprüfung der Risiken auf EU-Ebene** vorbereiten[40], die die zweite Phase des mit der Empfehlung eingeleiteten Prozesses bilden wird. Darauf aufbauend wird die Kooperationsgruppe in einer dritten Phase bis zum 31. Dezember 2019 ein **gemeinsames Unionsinstrumentarium mit risikomindernden Maßnahmen** zur Bewältigung der festgestellten Risiken ausarbeiten. Die Kommission und die EU-Agentur für Cybersicherheit werden bei der Umsetzung der Empfehlung weiter Unterstützung leisten.

Die Arbeit der Kooperationsgruppe für Netz- und Informationssysteme wird von mehreren anderen Gremien unterstützt. Das Gremium Europäischer Regulierungsstellen für elektronische Kommunikation bereitet derzeit eine Umfrage zu allen bestehenden Sicherheitsmaßnahmen vor, die für die 5G-Netze von Belang sein könnten. Eine eigens eingesetzte Expertengruppe in der EU-Agentur für Cybersicherheit hat mit der Überprüfung der 5G-Bedrohungslage begonnen. Ferner werden die Kommission und die EU-Agentur für Cybersicherheit, nachdem der Rechtsakt zur Cybersicherheit am 27. Juni 2019 in Kraft getreten ist, alle notwendigen Schritte zur Einrichtung des EU-weiten Zertifizierungsrahmens einleiten. Die Mitgliedstaaten kamen im Juni 2019 auch im Normungsausschuss zusammen, um Cybersicherheit und Normung als Reaktion auf die Empfehlung zu erörtern, künftige Herausforderungen für die Normung im Bereich der Cybersicherheit, einschließlich der 5G-Netze, zu ermitteln und geeignete politische Initiativen auf EU-Ebene zu prüfen.

Die Sicherheit der 5G-Netze ist auch für die Union von strategischer Bedeutung. Ausländische Investitionen in strategischen Sektoren, der Erwerb kritischer Anlagen, Technologien und Infrastrukturen in der Union sowie die Versorgung mit kritischen Ausrüstungen können ebenfalls eine Gefahr für die Sicherheit der Union darstellen.

Der neue **EU-Rahmen für die Überprüfung ausländischer Direktinvestitionen**[41] ist am 10. April 2019 in Kraft getreten. In den kommenden 18 Monaten werden die Kommission und

---

[40] Die Kooperationsgruppe für Netz- und Informationssysteme wurde mit der Richtlinie (EU) 2016/1148 vom 6. Juli 2016 über die Sicherheit von Netz- und Informationssystemen eingesetzt. Wie in der Empfehlung vorgesehen, wurde innerhalb der Kooperationsgruppe für Netz- und Informationssysteme unter Federführung mehrerer Mitgliedstaaten ein eigener Arbeitsbereich dafür eingerichtet. Die Gruppe ist bereits dreimal – im April, Mai und Juli 2019 – zusammengetreten, um Informationen über die nationalen Ansätze auszutauschen und zu erörtern, wie die Vorbereitung der koordinierten Risikobewertung der EU erleichtert werden kann.

[41] Verordnung (EU) 2019/452 vom 19. März 2019 zur Schaffung eines Rahmens für die Überprüfung ausländischer Direktinvestitionen in der Union. Mit dem neuen Rahmen wird ein Kooperationsmechanismus geschaffen, der es den Mitgliedstaaten und der Kommission ermöglicht, Informationen auszutauschen und Bedenken in Bezug auf bestimmte Investitionen zu äußern. Ferner kann die Kommission Stellung nehmen, wenn eine Investition die Sicherheit oder die öffentliche Ordnung von mehr als einem Mitgliedstaat bedroht oder wenn eine Investition ein für die gesamte EU bedeutendes Projekt oder Programm beeinträchtigen könnte. Das letzte Wort darüber, wie die Investition zu behandeln ist, hat der Mitgliedstaat, in dem die Investition getätigt wird.

die Mitgliedstaaten die notwendigen Schritte unternehmen, um sicherzustellen, dass die EU die Verordnung zur Überprüfung von Investitionen ab dem 11. Oktober 2020 vollständig anwenden kann.

IV. BEKÄMPFUNG DER GELDWÄSCHE

Dank der Möglichkeit, innerhalb von Stunden Gelder von Bankkonto zu Bankkonto zu transferieren, können Kriminelle und Terroristen Terrorakte leichter vorbereiten oder die Erträge aus Straftaten illegal in verschiedenen Mitgliedstaaten waschen. Deshalb hat die Union einen soliden **Rechtsrahmen für die Bekämpfung der Geldwäsche und der Terrorismusfinanzierung** entwickelt, der den von der Arbeitsgruppe „Bekämpfung der Geldwäsche und der Terrorismusfinanzierung“ (*Financial Action Task Force* – FATF) festgelegten internationalen Standards entspricht.

Angesichts der Notwendigkeit, mit sich wandelnden Trends, technologischen Entwicklungen und dem Einfallsreichtum von Kriminellen bei der Ausnutzung von Lücken oder Schlupflöchern im System Schritt zu halten, hat die Kommission am 24. Juli 2019 ein **Paket von vier Berichten**[42] angenommen, in denen die derzeitigen Risiken und Schwachstellen im Zusammenhang mit der Geldwäsche analysiert werden und die Anwendung des Rahmens durch die einschlägigen Akteure im privaten und im öffentlichen Sektor bewertet wird.

Das Paket enthält eine **Bewertung der potenziellen Vernetzung von nationalen zentralen Bankkontenregistern und Datenabrufsystemen** in der EU. Solche nationalen zentralen Systeme ermöglichen die Ermittlung natürlicher oder juristischer Personen, die Zahlungskonten, Bankkonten und Schließfächer innehaben oder kontrollieren; diese Informationen sind für die zuständigen Behörden bei der Bekämpfung der Geldwäsche und der Terrorismusfinanzierung häufig von entscheidender Bedeutung. Nach der 5. Geldwäscherichtlinie[43] sind die Mitgliedstaaten verpflichtet, solche nationalen zentralen Systeme einzurichten und ihren nationalen zentralen Meldestellen direkten Zugang dazu zu gewähren. Die unlängst erlassenen Vorschriften zur Erleichterung der Nutzung von Finanzinformationen für die Bekämpfung schwerer Straftaten[44] verschaffen den benannten Strafverfolgungsbehörden und Vermögensabschöpfungsstellen direkten Zugang zu ihren jeweiligen nationalen zentralen Bankkontenregistern. Darauf aufbauend werden in dem Bericht, wie in der Geldwäscherichtlinie vorgeschrieben, verschiedene bereits in Betrieb oder in der Entwicklung befindliche IT-Lösungen auf EU-Ebene bewertet, die als Modell für eine mögliche Vernetzung der nationalen zentralen Systeme dienen könnten. Da eine künftige EU-

---

42 *Report on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities* [Bericht über die Bewertung des Risikos von Geldwäsche und Terrorismusfinanzierung im Binnenmarkt und in Bezug auf grenzüberschreitende Tätigkeiten] (COM(2019) 370 final vom 24.7.2019), *Report on the interconnection of national centralised automated mechanisms (central registries or central electronic data retrieval systems) of the Member States on bank accounts* [Bericht über die Vernetzung von nationalen zentralen automatischen Mechanismen (zentrale Register oder zentrale elektronische Datenabfragesysteme) der Mitgliedstaaten für Bankkonten] (COM(2019) 372 final vom 24.7.2019), *Report on the assessment of recent alleged money laundering cases involving EU credit institutions* [Bericht über die Bewertung aktueller Fälle von mutmaßlicher Geldwäsche unter Beteiligung von Kreditinstituten in der EU] (COM(2019) 373 final vom 24.7.2019), *Report assessing the framework for cooperation between Financial Intelligence Units* [Bericht zur Bewertung der Rahmenbedingungen für die Zusammenarbeit zwischen den zentralen Meldestellen] (COM(2019) 371 final vom 24.7.2019).

43 Richtlinie (EU) 2015/849 vom 20.5.2015.

44 Richtlinie (EU) 2019/1153 vom 20.6.2019.

weite Vernetzung der zentralen Mechanismen den Zugang zu Finanzinformationen beschleunigen und die grenzüberschreitende Zusammenarbeit zwischen den zuständigen Behörden erleichtern würde, beabsichtigt die Kommission, sich weiter mit den relevanten Interessenträgern, den Regierungen sowie den zentralen Meldestellen, den Strafverfolgungsbehörden und den Vermögensabschöpfungsstellen als den potenziellen „Endnutzern" eines möglichen Vernetzungssystems zu beraten.

Im Rahmen der Überlegungen der Kommission zur Arbeit der zentralen Meldestellen wird in einem Bericht zur Bewertung der **Zusammenarbeit zwischen den zentralen Meldestellen** sowohl die Zusammenarbeit innerhalb der Union als auch die Zusammenarbeit mit Drittländern näher beleuchtet.[45] Es wurden bestimmte Mängel festgestellt, die bestehen bleiben dürften, bis die Aufgaben der zentralen Meldestellen und ihre Pflichten bei der grenzüberschreitenden Zusammenarbeit im EU-Rechtsrahmen für die Bekämpfung der Geldwäsche und der Terrorismusfinanzierung deutlicher ausformuliert werden. Aus der Bewertung geht ferner hervor, dass es eines stärkeren Mechanismus für die Koordinierung und Unterstützung der grenzüberschreitenden Zusammenarbeit und Analyse bedarf.

Neben den laufenden Arbeiten zur Bekämpfung der Geldwäsche und der Terrorismusfinanzierung wird die Kommission – auch als Reaktion auf eine Aufforderung des Europäischen Parlaments[46] – weiterhin die Notwendigkeit, die technische Durchführbarkeit und die Verhältnismäßigkeit zusätzlicher Maßnahmen zur Aufdeckung der Finanzierungskanäle des Terrorismus in der EU bewerten.[47]

V. UMSETZUNG WEITERER PRIORITÄTEN IM BEREICH DER SICHERHEIT

1. Umsetzung legislativer Maßnahmen im Rahmen der Sicherheitsunion

Selbst wenn über Maßnahmen im Rahmen der Sicherheitsunion eine Einigung erzielt wurde, ist der Prozess damit noch nicht zu Ende – es kommt entscheidend darauf an, dass sie anschließend von den Mitgliedstaaten zügig und vollständig umgesetzt werden, damit sie ihre Wirkung voll entfalten können. Zu diesem Zweck unterstützt die Kommission die Mitgliedstaaten aktiv, unter anderem durch die Bereitstellung von Finanzmitteln und die Erleichterung des Austauschs bewährter Methoden. Nötigenfalls ist die Kommission jedoch auch bereit, von den ihr durch die Verträge verliehenen Befugnissen zur Durchsetzung des EU-Rechts in vollem Umfang Gebrauch zu machen, gegebenenfalls auch durch Vertragsverletzungsverfahren.

Die Frist für die Umsetzung der **EU-Richtlinie über Fluggastdatensätze**[48] ist am 25. Mai 2018 abgelaufen. Bislang haben 25 Mitgliedstaaten der Kommission die vollständige Umsetzung mitgeteilt.[49] In zwei Mitgliedstaaten wurde die Richtlinie trotz der am 19. Juli

---

45 Diese Bewertung ist in Artikel 65 Absatz 2 der 5. Geldwäscherichtlinie (EU) 2018/843 vom 30. Mai 2018 vorgeschrieben.

46 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.

47 Siehe die Mitteilung „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Achtzehnter Fortschrittsbericht" (COM(2019) 145 final vom 20.3.2019).

48 Richtlinie (EU) 2016/681 vom 27. April 2016.

49 Die Angaben zur Mitteilung der vollständigen Umsetzung beruhen auf den Erklärungen der Mitgliedstaaten und berühren nicht die Prüfung der Umsetzung durch die Kommissionsdienststellen.

2018 eingeleiteten Vertragsverletzungsverfahren noch nicht vollständig umgesetzt.[50] Parallel dazu unterstützt die Kommission weiterhin alle Mitgliedstaaten bei ihren Bemühungen, die Entwicklung ihrer Systeme zur Erfassung von Fluggastdatensätzen abzuschließen, indem sie unter anderem den Austausch von Informationen und bewährten Verfahren erleichtert.

Die Frist für die Umsetzung der **Richtlinie zur Terrorismusbekämpfung**[51] ist am 8. September 2018 abgelaufen. Bislang haben 22 Mitgliedstaaten der Kommission die vollständige Umsetzung mitgeteilt. Drei Mitgliedstaaten haben trotz der am 22. November 2018 eingeleiteten Vertragsverletzungsverfahren noch nicht die Verabschiedung nationaler Rechtsvorschriften mitgeteilt, mit denen die Richtlinie vollständig umgesetzt wird.[52]

Die Frist für die Umsetzung der **Richtlinie über die Kontrolle des Erwerbs und des Besitzes von Waffen**[53] ist am 14. September 2018 abgelaufen. Bislang haben 8 Mitgliedstaaten der Kommission die vollständige Umsetzung mitgeteilt. 20 Mitgliedstaaten haben trotz der am 22. November 2018 eingeleiteten Vertragsverletzungsverfahren noch nicht die Verabschiedung nationaler Maßnahmen mitgeteilt, mit denen die Richtlinie vollständig umgesetzt wird.[54]

In Bezug auf die Umsetzung der **Richtlinie zum Datenschutz bei der Strafverfolgung**[55] in nationales Recht ist die Frist am 6. Mai 2018 abgelaufen. Bislang haben 20 Mitgliedstaaten der Kommission die vollständige Umsetzung mitgeteilt.[56] 7 Mitgliedstaaten haben trotz der Vertragsverletzungsverfahren, die die Kommission am 19. Juli 2018 eingeleitet hat, noch nicht die Verabschiedung nationaler Maßnahmen mitgeteilt, mit denen die Richtlinie vollständig umgesetzt wird.[57]

Die Mitgliedstaaten hatten bis zum 9. Mai 2018 Zeit, die **Richtlinie über die Sicherheit von Netz- und Informationssystemen**[58] in nationales Recht umzusetzen. Bislang haben 26 Mitgliedstaaten der Kommission die vollständige Umsetzung mitgeteilt, 2 Mitgliedstaaten haben die Richtlinie teilweise umgesetzt.[59] Zudem waren die Mitgliedstaaten nach der Richtlinie verpflichtet, bis zum 9. November 2018 die Betreiber wesentlicher Dienste zu ermitteln. Bis zum 9. Mai 2019 hätte die Kommission dem Europäischen Parlament und dem Rat einen Bericht vorlegen müssen, in dem die Kohärenz der Ansätze der Mitgliedstaaten für die Ermittlung der Betreiber wesentlicher Dienste in ihrem Hoheitsgebiet bewertet wird. Da jedoch eine Reihe von Mitgliedstaaten noch keine vollständigen Informationen über das

---

50 Slowenien hat eine teilweise Umsetzung mitgeteilt. Spanien hat noch nicht mitgeteilt, dass es die Richtlinie umgesetzt hat (Stand: 24. Juli 2019).

51 Richtlinie (EU) 2017/541 vom 15. März 2017.

52 Polen hat eine teilweise Umsetzung mitgeteilt. Griechenland und Luxemburg haben noch nicht mitgeteilt, dass sie die Richtlinie umgesetzt haben (Stand: 24. Juli 2019).

53 Richtlinie (EU) 2017/853 vom 17. Mai 2017.

54 Belgien, Tschechien, Estland, Litauen, Polen, Portugal, Schweden und das Vereinigte Königreich haben eine teilweise Umsetzung mitgeteilt. Deutschland, Irland, Griechenland, Spanien, Zypern, Luxemburg, Ungarn, die Niederlande, Rumänien, Slowenien, die Slowakei und Finnland haben noch nicht mitgeteilt, dass sie die Richtlinie umgesetzt haben (Stand: 24. Juli 2019).

55 Richtlinie (EU) 2016/680 vom 27. April 2016.

56 20 Mitgliedstaaten haben die Umsetzung abgeschlossen (Stand: 24. Juli 2019).

57 Lettland, Portugal, Slowenien und Finnland haben eine teilweise Umsetzung mitgeteilt. Griechenland und Spanien haben noch nicht mitgeteilt, dass sie die Richtlinie umgesetzt haben. Deutschland hat zwar die vollständige Umsetzung mitgeteilt, die Kommission sieht diese Umsetzung jedoch nicht als vollständig an (Stand: 24. Juli 2019).

58 Richtlinie (EU) 2016/1148 vom 27. April 2016.

59 Belgien und Ungarn haben die Richtlinie teilweise umgesetzt (Stand: 24. Juli 2019).

Ermittlungsverfahren vorgelegt hatte, musste die Kommission ihren Bericht verschieben.

Die Kommission prüft zurzeit die Umsetzung der **4. Geldwäscherichtlinie**[60] sowie die Anwendung der Vorschriften durch die Mitgliedstaaten. Die Kommission hat Vertragsverletzungsverfahren gegen 24 Mitgliedstaaten eingeleitet, da sie der Auffassung ist, dass aus den von den Mitgliedstaaten vorgelegten Mittteilungen keine vollständige Umsetzung dieser Richtlinie hervorgeht.[61]

Die Kommission fordert die Mitgliedstaaten auf, dringend die notwendigen Maßnahmen zu treffen, um die folgenden Richtlinien vollständig in nationales Recht umzusetzen, und sie der Kommission mitzuteilen:

- die **EU-Richtlinie über Fluggastdatensätze**: 1 Mitgliedstaat muss noch die Umsetzung in nationales Recht mitteilen, und 1 Mitgliedstaat muss die Mitteilung der Umsetzung vervollständigen;[62]
- die **Richtlinie zur Terrorismusbekämpfung**: 2 Mitgliedstaaten müssen noch die Umsetzung in nationales Recht mitteilen, und 1 Mitgliedstaat muss die Mitteilung der Umsetzung vervollständigen;[63]
- die **Richtlinie über die Kontrolle des Erwerbs und des Besitzes von Waffen**: 12 Mitgliedstaaten müssen noch die Umsetzung in nationales Recht mitteilen, und 8 Mitgliedstaaten müssen die Mitteilung der Umsetzung vervollständigen;[64]
- die **Richtlinie zum Datenschutz bei der Strafverfolgung**: 2 Mitgliedstaaten müssen noch die Umsetzung in nationales Recht mitteilen, und 5 Mitgliedstaaten müssen die Mitteilung der Umsetzung vervollständigen;[65]
- die **Richtlinie über die Sicherheit von Netz- und Informationssystemen**: 2 Mitgliedstaaten müssen noch die Mitteilung der Umsetzung vervollständigen;[66]
- die **4. Geldwäscherichtlinie**: 24 Mitgliedstaaten müssen noch die Mitteilung der Umsetzung vervollständigen.[67]

2. Bekämpfung von Desinformation und Schutz von Wahlen vor anderen Cyberbedrohungen

60 Richtlinie (EU) 2015/849 vom 20. Mai 2015.

61 Belgien, Bulgarien, Tschechien, Dänemark, Deutschland, Estland, Irland, Spanien, Frankreich, Italien, Zypern, Lettland, Litauen, Ungarn, die Niederlande, Österreich, Polen, Portugal, Rumänien, Slowenien, die Slowakei, Finnland, Schweden und das Vereinigte Königreich (Stand: 24. Juli 2019).

62 Slowenien hat eine teilweise Umsetzung mitgeteilt. Spanien hat noch nicht mitgeteilt, dass es die Richtlinie umgesetzt hat (Stand: 24. Juli 2019).

63 Polen hat eine teilweise Umsetzung mitgeteilt. Griechenland und Luxemburg haben noch nicht mitgeteilt, dass sie die Richtlinie umgesetzt haben (Stand: 24. Juli 2019).

64 Belgien, Tschechien, Estland, Litauen, Polen, Portugal, Schweden und das Vereinigte Königreich haben eine teilweise Umsetzung mitgeteilt. Deutschland, Irland, Griechenland, Spanien, Zypern, Luxemburg, Ungarn, die Niederlande, Rumänien, Slowenien, die Slowakei und Finnland haben noch nicht mitgeteilt, dass sie die Richtlinie umgesetzt haben (Stand: 24. Juli 2019).

65 Lettland, Portugal, Slowenien und Finnland haben eine teilweise Umsetzung mitgeteilt. Griechenland und Spanien haben noch nicht mitgeteilt, dass sie die Richtlinie umgesetzt haben. Deutschland hat zwar die vollständige Umsetzung mitgeteilt, die Kommission sieht diese Umsetzung jedoch nicht als vollständig an (Stand: 24. Juli 2019).

66 Belgien und Ungarn haben die Richtlinie teilweise umgesetzt (Stand: 24. Juli 2019).

67 Belgien, Bulgarien, Tschechien, Dänemark, Deutschland, Estland, Irland, Spanien, Frankreich, Italien, Zypern, Lettland, Litauen, Ungarn, die Niederlande, Österreich, Polen, Portugal, Rumänien, Slowenien, die Slowakei, Finnland, Schweden und das Vereinigte Königreich (Stand: 24. Juli 2019).

Der Schutz demokratischer Prozesse und Institutionen vor Desinformation und der damit verbundenen Einflussnahme ist weltweit eine große Herausforderung für die Gesellschaft. Um dieses Problem anzugehen, hat die EU einen **soliden Rahmen für ein koordiniertes Vorgehen gegen Desinformation** unter voller Achtung der europäischen Werte und Grundrechte geschaffen.[68] Wie in der Gemeinsamen Mitteilung vom 14. Juni 2019 über die Umsetzung des Aktionsplans gegen Desinformation[69] dargelegt, hat die Arbeit in mehreren einander ergänzenden Bereichen dazu beigetragen, Desinformation keinen Raum mehr zu geben und die Integrität der Wahlen zum Europäischen Parlament zu wahren.

Der Europäische Rat begrüßte in seinen Schlussfolgerungen vom 21. Juni 2019[70] die Absicht der Kommission, eine gründliche Beurteilung der Umsetzung der Verpflichtungen vorzunehmen, die Online-Plattformen und andere Unterzeichner im Rahmen des **Verhaltenskodex gegen Desinformation**[71] eingegangen sind; er forderte die Kommission und die Hohe Vertreterin der Union für Außen- und Sicherheitspolitik auf, „*[d]ie sich wandelnde Art der Bedrohungen und die zunehmende Gefahr von böswilligen Eingriffen und Online-Manipulation, die mit der Entwicklung von künstlicher Intelligenz und Datenerhebungstechniken einhergehen*“, kontinuierlich zu bewerten und angemessen zu reagieren.

Die Kommission und die Hohe Vertreterin werden ihre Arbeit in diesem Bereich im Einklang mit den Schlussfolgerungen des Europäischen Rates vorantreiben. Im März 2019 richteten die Kommission und die Hohe Vertreterin ein **Schnellwarnsystem** der EU-Organe und der Mitgliedstaaten ein, um den Austausch von Erkenntnissen im Zusammenhang mit Desinformationskampagnen zu erleichtern und Abwehrmaßnahmen koordinieren zu können. Das erste Treffen der Kontaktstellen der Mitgliedstaaten nach den Wahlen zum Europäischen Parlament fand am 3./4. Juni 2019 in Tallinn statt. Zur weiteren Stärkung des Schnellwarnsystems werden die Hohe Vertreterin und die Kommission im Herbst 2019 in enger Zusammenarbeit mit den Mitgliedstaaten die Funktionsweise des Systems überprüfen. Ferner werden sie gemeinsame Methoden für die Analyse und Aufdeckung von Desinformationskampagnen sowie stärkere Partnerschaften mit internationalen Partnern wie G7 und NATO entwickeln.

Auch die Arbeit im **Europäischen Kooperationsnetz für Wahlen**[72] wird fortgesetzt. Das Netz hat am 7. Juni 2019 eine erste Sitzung abgehalten, um eine Bestandsaufnahme der

---

68 Siehe den Aktionsplan gegen Desinformation (JOIN(2018) 36 final vom 5.12.2018).

69 JOIN(2019) 12 final vom 14.6.2019.

70 https://www.consilium.europa.eu/de/press/press-releases/2019/06/20/european-council-conclusions-final-20-june-2019/. Die Aufforderung des Europäischen Rates stützt sich auf Beiträge des rumänischen Ratsvorsitzes sowie der Kommission und der Hohen Vertreterin für Außen- und Sicherheitspolitik über die gewonnenen Erkenntnisse zu Desinformation und Gewährleistung freier und fairer Wahlen, einschließlich der Gemeinsamen Mitteilung über die Umsetzung des Aktionsplans gegen Desinformation.

71 Der Verhaltenskodex, der im Oktober 2018 von den Online-Plattformen Facebook, Google und Twitter, von Mozilla sowie von Werbetreibenden und der Werbebranche unterzeichnet wurde, enthält Selbstregulierungsstandards zur Bekämpfung von Desinformation. Der Kodex dient dazu, die in der Mitteilung der Kommission vom April 2018 über die Bekämpfung von Desinformation im Internet (COM(2018) 236 final vom 26.4.2018) festgelegten Ziele mithilfe eines breiten Spektrums von Verpflichtungen zu verwirklichen, die von der Transparenz politischer Werbung über die Schließung von Scheinkonten bis zur Demonetisierung der Verbreiter von Desinformation reichen.

72 Das Europäische Kooperationsnetz für Wahlen verbindet die Kontaktstellen der nationalen Wahlkooperationsnetze von Behörden, die für Wahlfragen und für die Überwachung und Durchsetzung von Vorschriften im Zusammenhang mit wahlrelevanten Online-Aktivitäten zuständig sind. Das

Wahlen zum Europäischen Parlament vorzunehmen. Diese Überlegungen und weitere Beiträge von zuständigen nationalen Behörden, politischen Parteien und Online-Plattformen werden in den umfassenden Bericht der Kommission über die Wahlen zum Europäischen Parlament einfließen, der im Oktober 2019 angenommen werden soll. Die Mitgliedstaaten haben auch bei anderen Wahlen als denen zum Europäischen Parlament von dem Netz Gebrauch gemacht. Dies zeigt, dass es für die Gewährleistung der Integrität der Demokratie in der EU generell von Nutzen ist.

Die Kommission wird weiterhin die Erfüllung der Verpflichtungen überwachen und fördern, die die Plattformen im Rahmen des **Verhaltenskodex gegen Desinformation** eingegangen sind. Aus den von Google, Twitter und Facebook nach dem Verhaltenskodex vorgelegten Berichten geht hervor, dass alle Plattformen vor den Wahlen zum Europäischen Parlament tätig geworden sind, um politische Werbung zu kennzeichnen und über Anzeigenbibliotheken mit Suchfunktion öffentlich zugänglich zu machen. Gleichzeitig gibt es noch Raum für Verbesserungen, wie die Gruppe europäischer Regulierungsstellen für audiovisuelle Mediendienste[73] festgestellt hat. Insbesondere fehlt nach wie vor ein Zugang zu den detaillierten Rohdaten, die für eine umfassende Überwachung erforderlich sind. Und schließlich sollten die Plattformen Forschern unter Beachtung der Vorschriften über den Schutz personenbezogener Daten einen zweckdienlichen Zugang zu Daten gewähren. Noch in diesem Jahr wird die Kommission eine umfassende Bewertung der Erfüllung aller im Rahmen des Verhaltenskodex eingegangenen Verpflichtungen in den ersten 12 Monaten seines Bestehens vornehmen. Auf dieser Grundlage könnte die Kommission dann weitere Maßnahmen, auch regulatorischer Art, in Erwägung ziehen, um die langfristige Reaktion der EU auf Desinformation zu verbessern.

3. Abwehrbereitschaft und Schutz

Die Stärkung der Abwehrbereitschaft und der Widerstandsfähigkeit gegen Sicherheitsbedrohungen ist ein wichtiger Aspekt der Arbeit auf dem Weg zu einer wirksamen und echten Sicherheitsunion. Hierzu zählen auch die Unterstützung, die die Kommission den Mitgliedstaaten und deren lokalen Behörden für einen besseren **Schutz des öffentlichen Raums** gewährt[74], sowie die Unterstützung für die Mitgliedstaaten bei der Steigerung der

---

Europäische Kooperationsnetz für Wahlen dient dazu, vor Bedrohungen zu warnen, bewährte Methoden zwischen den nationalen Netzen auszutauschen, gemeinsame Lösungen für die ermittelten Herausforderungen zu erörtern und gemeinsame Projekte und Übungen der nationalen Netze zu fördern.

73 In der Gruppe europäischer Regulierungsstellen für audiovisuelle Mediendienste kommen die Leiter oder hochrangige Vertreter nationaler unabhängiger Regulierungsstellen im Bereich der audiovisuellen Dienste zusammen, um die Kommission bei der Umsetzung der EU-Richtlinie über audiovisuelle Mediendienste (Richtlinie 2010/13/EU vom 10. März 2010) zu beraten. In ihrer jüngsten Sitzung vom 20./21. Juni 2019 in Bratislava stellte die Gruppe die Ergebnisse der bisherigen Arbeit zum Thema Desinformation vor, bei denen die Wahlen zum Europäischen Parlament 2019 und die damit verbundenen Bereiche politischer und themenbezogener Werbung im Mittelpunkt standen.

74 Siehe den Abschnitt „Bewährte Verfahren für Behörden und private Betreiber für einen besseren Schutz des öffentlichen Raums“ in der Mitteilung „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Achtzehnter Fortschrittsbericht“ (COM(2019) 145 final vom 20.3.2019). Grundlage hierfür ist der Aktionsplan vom Oktober 2017 für einen besseren Schutz des öffentlichen Raums (COM(2017) 612 final vom 18.10.2017). Am 5. Juni 2019 fand im Rahmen des EU-Forums zum Schutz des öffentlichen Raums das dritte Treffen des Forums der Betreiber statt. Unter den Teilnehmern waren Vertreter der EU-Mitgliedstaaten und private Betreiber öffentlicher Räume, die durch 14 europäische Verbände vertreten wurden, aus den Bereichen Gastgewerbe, Live-Veranstaltungen, Musik und Unterhaltung, Freizeitparks und Attraktionen, Luftverkehr, Schienenverkehr, Einkaufszentren und Telekommunikation sowie private Sicherheitsdienste und Hersteller von Sicherheitsausrüstung.

Abwehrbereitschaft gegen **chemische, biologische, radiologische und nukleare Sicherheitsrisiken**[75], bei der Umsetzung der beiden Aktionspläne in diesem Bereich sowie bei der Bedarfsanalyse für die entsprechenden Abwehrkapazitäten, die im Rahmen von rescEU aufzubauen sind[76]. Angesichts der sich wandelnden chemischen Bedrohungen[77] hat die Kommission in Zusammenarbeit mit den Mitgliedstaaten und nach Rücksprache mit den internationalen Partnern eine Liste von Chemikalien aufgestellt, die hinsichtlich eines möglichen Missbrauchs für terroristische Zwecke am meisten Anlass zur Besorgnis geben. Die EU-Liste dient als Grundlage für die weitere Arbeit zur Beschränkung des Zugangs zu diesen Chemikalien und zur Zusammenarbeit mit den Herstellern bei der Verbesserung der Detektionsfähigkeiten.

Technisch gesehen bieten unbemannte Luftfahrzeuge eine große Vielfalt von Betriebsmöglichkeiten. Infolge des in den letzten Jahren zu beobachtenden raschen Wachstums des Marktes für unbemannte Luftfahrzeugsysteme für militärische, zivile gewerbliche und Freizeitzwecke bieten **Drohnen** jedoch nicht nur neue Möglichkeiten, sondern stellen auch eine zunehmende Bedrohung für die Sicherheit von kritischen Infrastrukturen (einschließlich des Luftverkehrs), öffentlichen Räumen und Veranstaltungen, sensiblen Bereichen und Menschen dar. In Europa sind Drohnen schon eingesetzt worden, um den Luftverkehr und Strafverfolgungsmaßnahmen zu stören, kritische Infrastrukturen auszuforschen und Schmuggelware in Gefängnisse und über Grenzen zu bringen.

Die Kommission unterstützt die Mitgliedstaaten bei der Bekämpfung der wachsenden Bedrohung für Bürger und kritische Funktionsbereiche der Gesellschaft, die von Drohnen ausgeht, ohne deren Nutzen, z. B. bei Notfalleinsätzen, zu negieren. Um das Risiko ihrer böswilligen Verwendung zu mindern, hat die Kommission unlängst **gemeinsame EU-weite Vorschriften für den sicheren Betrieb von Drohnen**[78] erlassen, die unter anderem die Betreiber zur Registrierung verpflichten und die Fernidentifizierung ermöglichen. Zudem unterstützt die Kommission die Mitgliedstaaten, indem sie Trends bei der Entwicklung der von Drohnen ausgehenden Bedrohung beobachtet, einschlägige Forschungsprojekte und Maßnahmen zum Kapazitätsaufbau finanziert und den Austausch zwischen den Mitgliedstaaten und anderen Interessenträgern erleichtert. Um diese Unterstützung zu verstärken, wird die Kommission am 17. Oktober 2019 eine hochrangige internationale Konferenz zur Abwehr der von Drohnen ausgehenden Gefahren veranstalten.

Als Reaktion auf die Notwendigkeit eines weit gefassten Ansatzes für die EU-Politik zum **Schutz kritischer Infrastrukturen**[79] hat die Kommission am 23. Juli 2019 eine Evaluierung

---

75 Insbesondere durch Umsetzung des Aktionsplans vom Oktober 2017 für eine gesteigerte Abwehrbereitschaft gegen chemische, biologische, radiologische und nukleare Sicherheitsrisiken (COM(2017) 610 final vom 18.10.2017).

76 Siehe Artikel 12 Absatz 2 des Beschlusses Nr. 1313/2013/EU vom 17. Dezember 2013 über ein Katastrophenschutzverfahren der Union in der Fassung des Beschlusses (EU) 2019/420 vom 13. März 2019.

77 Siehe den Abschnitt „Verstärkte Maßnahmen gegen chemische Bedrohungen“ in der Mitteilung „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Fünfzehnter Fortschrittsbericht“ (COM(2018) 470 final vom 13.6.2018).

78 Durchführungsverordnung (EU) 2019/947 der Kommission vom 24. Mai 2019 über die Vorschriften und Verfahren für den Betrieb unbemannter Luftfahrzeuge (ABl. L 152 vom 11.6.2019).

79 In „*Comprehensive Assessment of EU Security Policy*“ [Umfassende Bewertung der EU-Sicherheitspolitik] aus dem Jahr 2017 (SWD(2017) 278 final vom 26.7.2017) wurde darauf hingewiesen, dass für die EU-Politik zum Schutz kritischer Infrastrukturen ein weit gefasster Ansatz notwendig ist.

der Richtlinie über europäische kritische Infrastrukturen[80] vorgelegt. Diese Richtlinie ist der Rechtsrahmen für die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern. Bei ihrer Evaluierung wurde festgestellt, dass sich der Kontext, in dem kritische Infrastrukturen in Europa betrieben werden, seit Inkrafttreten der Richtlinie erheblich verändert hat, unter anderem durch die Weiterentwicklung der Rechtsvorschriften in den Sektoren, auf die die Richtlinie vor allem ausgerichtet ist, etwa im Energiesektor[81], und dass die Bestimmungen der Richtlinie aufgrund der veränderten Rahmenbedingungen zum Teil überholt sind. Gleichzeitig wird eine Politik der EU zum Schutz kritischer Infrastrukturen, die die Subsidiarität wahrt und mit einem zusätzlichen Nutzen verbunden ist, von den Mitgliedstaaten nach wie vor unterstützt.

4. Externe Dimension

Angesichts des grenzübergreifenden, globalen Charakters der meisten Sicherheitsbedrohungen, denen sich die Union gegenübersieht, ist die Zusammenarbeit mit internationalen Organisationen und Partnerländern außerhalb der EU ein notwendiger Bestandteil der Arbeit auf dem Weg zu einer wirksamen und echten Sicherheitsunion.

Die Nutzung der Vorteile multilateraler Zusammenarbeit ist ein fester Bestandteil dieser Bemühungen; dies gilt auch für die Zusammenarbeit zwischen der EU und den Vereinten Nationen, die unlängst mit der Unterzeichnung des **Rahmens der Vereinten Nationen und der Europäischen Union für die Terrorismusbekämpfung**[82] anlässlich des zweiten hochrangigen politischen Dialogs zwischen den Vereinten Nationen und der EU über die Terrorismusbekämpfung am 24. April 2019 in New York verstärkt wurde. Der Rahmen fördert die Zusammenarbeit beim Kapazitätsaufbau für die Bekämpfung des Terrorismus und für die Prävention und Bekämpfung des gewaltverherrlichenden Extremismus in Afrika, dem Nahen Osten und Asien. In dem Rahmen sind die Bereiche der Zusammenarbeit zwischen der EU und den Vereinten Nationen und die Prioritäten bis 2020 festgelegt.

Die **Zusammenarbeit mit dem westlichen Balkan im Bereich der Sicherheit** stellt eine besondere regionale Priorität dar, in deren Rahmen eine Reihe sicherheitsrelevanter vorrangiger Maßnahmen umgesetzt wird, die in der Strategie für den westlichen Balkan von 2018[83] festgelegt wurden. Zu diesem Zweck organisierte die Kommission am 4. April 2019 das erste Treffen der „Agenturenübergreifenden Taskforce für den westlichen Balkan“, bei dem Vertreter von sieben EU-Agenturen ihre Erfahrungen austauschten und die operative Zusammenarbeit mit Partnern in der Region, unter anderem zur Bekämpfung von organisierter Kriminalität, Terrorismus, Feuerwaffen, Drogen, Schleuserkriminalität und Menschenhandel, intensivierten. Gemeinsam mit allen sechs Westbalkanländern wurden Erhebungen über hybride Risiken in die Wege geleitet. Ein weiteres konkretes Beispiel für die Zusammenarbeit mit der Region ist die Statusvereinbarung für die Europäische Grenz- und Küstenwache zwischen der EU und Albanien, die am 1. Mai 2019 in Kraft trat und auf deren Grundlage kurz danach Teams der Europäischen Agentur für die Grenz- und Küstenwache an

---

80 Mit der Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, soll der Schutz kritischer Infrastrukturen in der Europäischen Union verbessert werden.

81 Insbesondere durch die Verordnung (EU) 2017/1938 vom 25. Oktober 2017 über Maßnahmen zur Gewährleistung der sicheren Gasversorgung und die Verordnung (EU) 2019/941 vom 5. Juni 2019 über die Risikovorsorge im Elektrizitätssektor.

82 https://eeas.europa.eu/sites/eeas/files/2019042019_un-eu_framework_on_counter-terrorism.pdf

83 COM(2018) 65 final vom 6.2.2018.

die Grenze zu Griechenland entsandt wurden. Hierbei handelt es sich um das erste Abkommen dieser Art mit einem Drittland und die erste Entsendung in ein Drittland. Ähnliche Abkommen sollten bald mit anderen Ländern der Region unterzeichnet werden.

Zudem wurde im Juli 2019 ein Europol-Verbindungsbeamter nach Albanien entsandt, um die albanischen Behörden weiter in ihren Anstrengungen zur Prävention und Bekämpfung der organisierten Kriminalität zu unterstützen. Zur Verstärkung des Kampfs gegen den illegalen Handel mit Feuerwaffen legte die Kommission am 27. Juni 2019 eine Bewertung des Aktionsplans zur **Bekämpfung des unerlaubten Handels mit Feuerwaffen** zwischen der EU und dem südosteuropäischen Raum (2015-2019)[84] vor. In der Bewertung wird der Mehrwert der Zusammenarbeit dargelegt, gleichzeitig jedoch hervorgehoben, dass weitere Anstrengungen erforderlich sind, z. B. die Einrichtung effizienter nationaler Koordinierungszentren für Feuerwaffen oder die Harmonisierung der Erhebung von Daten und der Berichterstattung über die Beschlagnahme von Feuerwaffen.

Die gleiche Priorität räumt die EU dem Ausbau der **Zusammenarbeit mit den Ländern des Nahen Ostens und Nordafrikas** im Bereich der Sicherheit ein. Mit Tunesien und Algerien hat die EU einen Sicherheitsdialog aufgenommen. Die EU und Tunesien führten am 12. Juni in Tunis ihren dritten Dialog über Sicherheit und Terrorismusbekämpfung, der zweite Dialog zwischen der EU und Algerien über Sicherheit und Terrorismusbekämpfung fand am 12. November 2018 in Algier statt. Ferner laufen Gespräche über die Aufnahme eines strukturierten Sicherheitsdialogs mit Marokko, die an die jüngste Tagung des Assoziationsrats vom 27. Juni anschließen, auf der die EU und Marokko die Bedeutung einer Vertiefung der Zusammenarbeit im Bereich der Sicherheit für die Bewältigung gemeinsamer Herausforderungen anerkannten. Parallel dazu wird über die Entwicklung eines strukturierten Sicherheitsdialogs mit Ägypten beraten; dies wurde auch beim jüngsten Treffen hoher Beamter der EU und Ägyptens am 10. Juli in Kairo wieder bestätigt.

Auf der Grundlage eines Mandats des Rates hat die Kommission informelle Gespräche mit den meisten Ländern des **Nahen Ostens und Nordafrikas** aufgenommen; Ziel ist es, förmliche Verhandlungen über eine internationale Übereinkunft über den Austausch personenbezogener Daten zwischen der Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (**Europol**) und den Behörden, die in den Ländern des **Nahen Ostens und Nordafrikas** für die Bekämpfung von schwerer Kriminalität und Terrorismus zuständig sind, einzuleiten. In diesem Zusammenhang fördert die Kommission auch den Abschluss direkter Arbeitsvereinbarungen zwischen Europol und den Partnerbehörden in den Ländern des **Nahen Ostens und Nordafrikas**, um einen förmlichen Rahmen für die regelmäßige Zusammenarbeit auf strategischer Ebene zu schaffen.

Die EU und die **Vereinigten Staaten** sind beim Umgang mit gemeinsamen Bedrohungen und bei der Erhöhung der Sicherheit enge strategische Partner. Auf der Tagung ihrer Justiz- und Innenminister vom 19. Juni 2019 bekräftigten die EU und die Vereinigten Staaten, dass die Bekämpfung des Terrorismus zu ihren obersten Prioritäten gehört. Beide Parteien bestätigten erneut die Bedeutung des Abkommens zwischen der EU und den USA über Fluggastdatensätze[85] und sagten zu, im September 2019 im Einklang mit den Bestimmungen des Abkommens mit einer gemeinsamen Evaluierung zur Bewertung seiner Umsetzung zu

---

84 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190627_com-2019-293-commission-report_de.pdf

85 ABl. L 215 vom 11.8.2012, S. 5.

beginnen. Ferner verpflichteten sich beide Seiten, ihre gemeinsamen Anstrengungen zur Bekämpfung des Terrorismus zu intensivieren, auch durch einen vermehrten Austausch von Informationen aus Kampfgebieten für Ermittlungs- und Strafverfolgungszwecke.

Um diese Zusammenarbeit zu verstärken, hat die Kommission gemeinsam mit dem EU-Koordinator für die Terrorismusbekämpfung am 10. Juli 2019 in Brüssel einen hochrangig besetzten Workshop zu Informationen aus Kampfgebieten veranstaltet. In dem Workshop kamen hohe Beamte aus den Verteidigungs-, Innen- und Justizministerien der Mitgliedstaaten, aus den Vereinigten Staaten, von Europol und Eurojust sowie Vertreter internationaler Organisationen zusammen, um Meinungen über die Verwendung von Informationen aus Kampfgebieten auszutauschen und gemeinsame Überlegungen zu den verfahrenstechnischen, rechtlichen und operativen Herausforderungen anzustellen, vor denen sie derzeit stehen, wenn sie Terroristen identifizieren und vor Gericht bringen wollen. Ferner haben die EU und die Vereinigten Staaten am 14./15. Mai 2019 einen Dialog zum Kapazitätsaufbau für die Abwehr chemischer, biologischer, radiologischer und nuklearer Gefahren geführt, um die von Massenvernichtungswaffen ausgehenden Bedrohungen zu verringern und die chemische, biologische, radiologische und nukleare Sicherheit weltweit zu erhöhen.

Das seit 2010 bestehende **Abkommen zwischen der EU und den Vereinigten Staaten über das Programm zur Fahndung nach Finanzquellen des Terrorismus**[86] regelt die Übermittlung und Verarbeitung von Daten zum Zwecke der Identifizierung, Aufspürung und Verfolgung von Terroristen und ihren Netzen. Das Abkommen enthält Garantien zum Schutz der Daten von EU-Bürgern und sieht eine regelmäßige Überprüfung der „Garantien, Kontrollen und Reziprozitätsbestimmungen“ vor. In einem am 22. Juli 2019 veröffentlichten Evaluierungsbericht[87] stellt die Kommission fest, dass nach ihrer Überzeugung das Abkommen, einschließlich seiner wesentlichen Garantien und Kontrollen, ordnungsgemäß umgesetzt wird. Sie begrüßt die beständige Transparenz der Behörden der Vereinigten Staaten bei der Weitergabe von Informationen, die den Wert des Programms zur Fahndung nach Finanzquellen des Terrorismus für die gemeinsamen Anstrengungen zur Terrorismusbekämpfung verdeutlicht. Die nach dem Abkommen bereitgestellten Informationen haben entscheidend dazu beigetragen, die Untersuchung terroristischer Anschläge auf europäischem Boden, unter anderem der im Jahr 2017 in Stockholm, Barcelona und Turku verübten Anschläge, voranzubringen. Die Mitgliedstaaten und Europol haben das Programm zur Fahndung nach Finanzquellen des Terrorismus intensiver als bisher genutzt, und aus den in diesem Rahmen gesammelten Daten haben sich siebenmal so viele Ermittlungsansätze ergeben wie im vorangegangenen Berichtszeitraum. Die nächste gemeinsame Überprüfung des Abkommens soll 2021 stattfinden.

Im Bereich der internationalen Zusammenarbeit beim Austausch von **Fluggastdatensätzen für die Bekämpfung von Terrorismus und schwerer Kriminalität** haben die EU und Kanada bei ihrem 17. Gipfeltreffen am 17./18. Juli 2019 in Montreal den Abschluss ihrer Verhandlungen über ein neues Abkommen über Fluggastdatensätze begrüßt. Zwar wies Kanada darauf hin, das Abkommen noch rechtlich überprüfen zu müssen, die Vertragsparteien verpflichteten sich jedoch, es vorbehaltlich dieser Überprüfung so bald wie möglich zu schließen, wobei sie die entscheidende Rolle dieses Abkommens für die Erhöhung der Sicherheit bei gleichzeitiger Wahrung der Privatsphäre und des Schutzes

86 ABl. L 195 vom 27.7.2010, S. 5.
87 COM(2019) 342 final vom 22.7.2019.

personenbezogener Daten anerkannten. Das zwischen der EU und Australien bestehende Abkommen über Fluggastdatensätze[88] wird beim Besuch eines EU-Teams im August 2019 in Canberra gemeinsam überprüft und evaluiert.

Darüber hinaus arbeitet die Kommission mit den Mitgliedstaaten im Rat an einem Standpunkt der EU für die bevorstehende 40. Tagung der Versammlung der **Internationalen Zivilluftfahrt-Organisation**, die vom 24. September bis zum 4. Oktober 2019 stattfinden wird. Die Versammlung wird politische Leitlinien festlegen und dem Rat der Internationalen Zivilluftfahrt-Organisation Anweisungen zur fachlichen Arbeit an Normen der Internationalen Zivilluftfahrt-Organisation für die Verarbeitung von Fluggastdatensätzen erteilen. Der Rat billigte ein Informationspapier, das von der Kommission ausgearbeitet worden war, um den Standpunkt der Union zu den Grundprinzipien zu umreißen, die für alle künftigen globalen Normen für Fluggastdatensätze gelten sollten. Das Informationspapier wird dem Gremium für seine Mitglieder, die keine EU-Mitgliedstaaten sind, vorgelegt.

VI. FAZIT

Dank der engen Zusammenarbeit zwischen dem Europäischen Parlament, dem Rat, den Mitgliedstaaten und der Kommission hat die EU in den letzten Jahren erhebliche Fortschritte bei der gemeinsamen Arbeit für eine wirksame und echte Sicherheitsunion gemacht und eine Einigung über zahlreiche vorrangige Gesetzgebungsinitiativen erzielt. Mit Unterstützung der Kommission setzen die Mitgliedstaaten auch eine Vielzahl nichtlegislativer, operativer Maßnahmen um, die die Sicherheit für alle Bürgerinnen und Bürger erhöhen sollen. Gleichzeitig gibt es noch eine Reihe vorrangiger Initiativen im Rahmen der Sicherheitsunion, bei denen die beiden gesetzgebenden Organe tätig werden müssen, um gegen unmittelbare Bedrohungen vorzugehen. Die Kommission fordert das Europäische Parlament und den Rat auf, die notwendigen Schritte zu unternehmen, um rasch eine Einigung über die Legislativvorschläge zur Bekämpfung von terroristischer Propaganda und Radikalisierung im Internet zu erzielen, die Cybersicherheit zu erhöhen, den Zugang zu elektronischen Beweismitteln zu erleichtern und die Arbeiten an solideren und intelligenteren Informationssystemen in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung abzuschließen.

Die Kommission fordert die Mitgliedstaaten auf, alle im Rahmen der Sicherheitsunion erlassenen Rechtsvorschriften zügig und vollständig umzusetzen, damit sie ihre Wirkung voll entfalten können. Zudem fordert die Kommission die Mitgliedstaaten auf, die äußerst wichtige Arbeit an praktischen Maßnahmen zur Erhöhung der Sicherheit digitaler Infrastrukturen fortzusetzen und zu intensivieren, gegen Desinformation und andere Cyberbedrohungen vorzugehen, Abwehrbereitschaft und Schutz zu verstärken und bei der Bewältigung gemeinsamer Bedrohungen die Zusammenarbeit mit Partnern außerhalb der Union auszubauen. In ihrer Gesamtheit erhöhen diese Maßnahmen die Sicherheit aller Bürgerinnen und Bürger.

[88] ABl. L 186 vom 14.7.2012, S. 4.