



Rat der
Europäischen Union

Brüssel, den 31. Oktober 2019
(OR. en)

13682/19

JAI 1139
COSI 220
FRONT 299
ASIM 131
DAPIX 321
ENFOPOL 471
SIRIS 161
VISA 231
FAUXDOC 72
COPEN 417
CYBER 295
DATAPROTECT 265
CT 113
JAIEX 161
EF 319

ÜBERMITTLUNGSVERMERK

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

Eingangsdatum: 31. Oktober 2019

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

Nr. Komm.dok.: COM(2019) 552 final

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

Die Delegationen erhalten in der Anlage das Dokument COM(2019) 552 final.

Anl.: COM(2019) 552 final



Brüssel, den 30.10.2019
COM(2019) 552 final

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

**Auf dem Weg zu einer wirksamen und echten Sicherheitsunion –
Zwanzigster Fortschrittsbericht**

I. EINLEITUNG

Dies ist der zwanzigste 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“.

Für die Juncker-Kommission hat die Sicherheit seit dem ersten Tag oberste Priorität. Aufbauend auf der Europäischen Sicherheitsagenda vom April 2015¹ und der Mitteilung über die Weichenstellung für eine echte und wirksame Sicherheitsunion vom April 2016² reagierte die EU mit einem koordinierten Ansatz auf eine Reihe von Terroranschlägen und andere wachsende Sicherheitsherausforderungen, wobei mit Blick auf die Erhöhung unserer kollektiven Sicherheit erhebliche Verbesserungen erzielt wurden.³ In zunehmendem Maße wurde deutlich, dass die gegenwärtigen Sicherheitsherausforderungen – Terrorismus, organisierte Kriminalität, Cyberangriffe, Desinformation und andere aufkommende Cyberbedrohungen – gemeinsame Bedrohungen darstellen. Nur indem wir zusammenarbeiten, können wir das Niveau der kollektiven Sicherheit erreichen, das die Bürger zu Recht einfordern und erwarten. Dieses gemeinsame Verständnis bildete die Grundlage für die Fortschritte auf dem Weg zu einer wirksamen und echten Sicherheitsunion. Entsprechend den Erfordernissen der für die Sicherheit der Bürger zuständigen nationalen Behörden lag der Schwerpunkt der auf EU-Ebene geleisteten Unterstützung auf legislativen und operativen Maßnahmen in Bereichen, in denen gemeinsames Handeln Auswirkungen auf die Sicherheit in den Mitgliedstaaten haben kann. Diese Arbeit wurde in enger Abstimmung mit dem Europäischen Parlament und dem Rat sowie unter Gewährleistung vollständiger Transparenz gegenüber der breiten Öffentlichkeit durchgeführt. Im Mittelpunkt steht dabei die uneingeschränkte Achtung der Grundrechte, da die Sicherheit der Union nur gewährleistet werden kann, wenn die Bürger darauf vertrauen, dass ihre Grundrechte in vollem Umfang gewahrt bleiben.

Im Rahmen ihrer Maßnahmen zur **Terrorismusbekämpfung** hat die EU neue Vorschriften erlassen, die Terroristen Handlungsmöglichkeiten nehmen sollen, indem ihnen der Zugang zu Explosivstoffen, Feuerwaffen und Finanzmitteln erschwert und ihre Bewegungsfreiheit eingeschränkt wird. Die EU hat den **Informationsaustausch** intensiviert, um sicherzustellen, dass die an vorderster Front tätigen Fachkräfte, wie Polizei- und Grenzschutzbeamte, wirksamen Zugang zu präzisen und vollständigen Daten haben, um die vorhandenen Informationen bestmöglich zu nutzen, Lücken zu schließen und offene Fragen zu klären. Ein starker Schutz der Außengrenzen ist für die Sicherheit im Raum der Freizügigkeit ohne Kontrollen an den Binnengrenzen unverzichtbar. Im März 2019 erzielten das Europäische Parlament und der Rat eine Einigung über eine gestärkte und voll ausgerüstete **Europäische Grenz- und Küstenwache**; die neue Verordnung soll Anfang Dezember 2019 in Kraft treten. Für die in den lokalen Gemeinschaften tätigen Akteure hat die EU eine Plattform und Finanzierungsmöglichkeiten für den Austausch bewährter Verfahren zur **Bekämpfung von Radikalisierung und zur Prävention von gewaltbarem Extremismus** geschaffen; zudem wurden neue Vorschriften über die wirksame Entfernung terroristischer Online-Inhalte

¹ COM(2015) 185 final vom 28.4.2015.

² COM(2016) 230 final vom 20.4.2016.

³ Die vorangegangenen Berichte über die Fortschritte auf dem Weg zu einer wirksamen und echten Sicherheitsunion sind verfügbar unter: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en.

vorgeschlagen. Mit den Aktionsplänen für einen besseren Schutz des öffentlichen Raums und für eine gesteigerte Abwehrbereitschaft gegen chemische, biologische, radiologische und nukleare Sicherheitsrisiken leistete die EU einen Beitrag zur **Stärkung der Widerstandsfähigkeit der Städte** gegen Anschläge. Mit Blick auf die **Cybersicherheit und durch den Cyberspace ermöglichte Bedrohungen** legte die EU eine neue Cybersicherheitsstrategie fest, verabschiedete einschlägige Rechtsvorschriften und ergriff Maßnahmen zur Bekämpfung von **Desinformation**, um in der EU durchgeführte Wahlen besser zu schützen. Die Maßnahmen zur Erhöhung der Sicherheit unserer **kritischen digitalen Infrastrukturen**, einschließlich einer verstärkten Zusammenarbeit bei der **Cybersicherheit von 5G-Netzen** in ganz Europa, werden fortgeführt.

Ungeachtet dessen bleibt noch viel zu tun. Der live gestreamte Anschlag auf eine Synagoge in Halle, bei dem am 9. Oktober 2019 zwei Personen getötet wurden, erinnerte auf schockierende Weise an die von gewaltbereitem Rechtsextremismus und Antisemitismus ausgehende Bedrohung. Zudem warf er erneut ein Schlaglicht auf den Missbrauch des Internets für die Zwecke terroristischer Propaganda und damit auf die **Notwendigkeit EU-weiter Vorschriften über die Entfernung terroristischer Online-Inhalte**. Auf seiner Tagung vom 7. und 8. Oktober 2019 betonte der Rat (Justiz und Inneres) im Rahmen der Erörterung des Themas gewaltbereiter Rechtsextremismus und Terrorismus die Notwendigkeit weiterer Anstrengungen, u. a. mit Blick auf das Vorgehen gegen die Verbreitung illegaler rechtsgerichteter extremistischer Inhalte online und offline. Zugleich machte die Ermordung von drei Polizeibeamten und eines weiteren Bediensteten im Pariser Polizeipräsidium am 3. Oktober 2019 deutlich, dass die Bedrohung durch den dschihadistischen Terrorismus nach wie vor real ist und die laufenden Anstrengungen zur Unterstützung der Mitgliedstaaten bei der Bewältigung dieser Bedrohung fortgesetzt werden müssen. Die Flucht inhaftierter Anhänger des ISIS/Da'esh im Zusammenhang mit den jüngsten Ereignissen in Nordsyrien könnte schwerwiegende Auswirkungen auf die Sicherheit in Europa haben. Es ist wichtig, dass die Mitgliedstaaten die vorhandenen Informationssysteme umfassend nutzen, um ausländische terroristische Kämpfer beim Überschreiten der Außengrenzen zu erkennen und zu identifizieren. Darüber hinaus wird weiter an der Verwendung von Informationen aus Kampfgebieten für die strafrechtliche Verfolgung ausländischer terroristischer Kämpfer gearbeitet.

In diesem Bericht werden die jüngsten Fortschritte bei den Bemühungen um eine wirksame und echte Sicherheitsunion erläutert und die Bereiche beleuchtet, in denen weitere Maßnahmen erforderlich sind. Er enthält aktuelle Informationen über die Umsetzung der vereinbarten Maßnahmen zur **Cybersicherheit von 5G-Netzen**, insbesondere über den am 9. Oktober 2019 veröffentlichten **Bericht über die EU-weite Risikobewertung und die Bekämpfung von Desinformation**.

Ein Schwerpunkt dieses Berichts liegt insbesondere auf der **externen Dimension** der Zusammenarbeit in der Sicherheitsunion, wie etwa der Unterzeichnung zweier bilateraler **Vereinbarungen zur Terrorismusbekämpfung** mit Albanien und der Republik Nordmazedonien und den im Rahmen der Zusammenarbeit mit Drittländern beim Austausch von **Fluggastdatensätzen** erzielten Fortschritten. Des Weiteren hat die Kommission gemeinsam mit diesem Bericht eine Empfehlung für einen Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen über ein Abkommen zwischen der EU und **Neuseeland** über den Austausch personenbezogener Daten zur Bekämpfung von schwerer Kriminalität und Terrorismus angenommen.

II. FORTSCHRITTE BEI DEN GESETZGEBERISCHEN PRIORITÄTEN

1. Radikalisierungsprävention im Internet und in den Gemeinschaften

Die **Prävention der Radikalisierung** ist ein Eckpfeiler der Reaktion der Union auf die Bedrohungen durch den Terrorismus. Im 21. Jahrhundert stellt in diesem Zusammenhang das Internet den wichtigsten Schauplatz für die Aktivitäten von Terroristen dar. Bereiche, in denen radikalisierte Personen Inhalte verbreiten und teilen können, ermöglichen die Entwicklung und das Wachstum weltweiter Netze sowohl dschihadistischer als auch rechtsgerichteter gewaltbereiter Extremisten. Aus diesem Grund verfolgt die Kommission weiterhin ihren zweigleisigen Ansatz gegen die Radikalisierung im Internet, bei dem die von ihr vorgelegten Vorschläge für Vorschriften über die Entfernung illegaler terroristischer Online-Inhalte die freiwillige Partnerschaft mit Online-Plattformen verstärken sollen.

Von wesentlicher Bedeutung ist in diesem Zusammenhang der **Legislativvorschlag zur Verhinderung der Verbreitung terroristischer Online-Inhalte**; dieser beinhaltet klare Vorschriften und Schutzvorkehrungen, nach denen Internetplattformen verpflichtet sind, terroristische Inhalte innerhalb einer Stunde nach Eingang einer begründeten Aufforderung der zuständigen Behörden zu entfernen und proaktive Maßnahmen zu ergreifen, die im Verhältnis zu dem Umfang stehen, in dem die Diensteanbieter terroristischem Material ausgesetzt sind.⁴ Die diesbezüglichen interinstitutionellen Verhandlungen zwischen dem Europäischen Parlament und dem Rat wurden am 17. Oktober 2019 mit einer ersten Trilogsitzung aufgenommen. Angesichts der von terroristischen Online-Inhalten ausgehenden Bedrohung fordert die Kommission die gesetzgebenden Organe auf, bis Ende 2019 eine Einigung über den vorgeschlagenen Rechtsakt zu erzielen.

Der vorgeschlagene Rechtsakt ergänzt die freiwillige Partnerschaft mit der Internetbranche und anderen Interessenträgern im Rahmen des **EU-Internetforums**. Seit seiner Einrichtung im Jahr 2015 setzt dieses Forum Anreize für Internetunternehmen, bei der Erkennung und Entfernung terroristischer Online-Inhalte proaktiv vorzugehen; zudem ebnete es den Weg für die Brancheninitiative der „gemeinsamen Hash-Datenbank“⁵ sowie die Schaffung des *Global Internet Forum to Counter Terrorism* [Globales Internetforum zur Bekämpfung des Terrorismus]. Die bei der EU-Strafverfolgungsbehörde Europol angesiedelte EU-Meldestelle für Internetinhalte hat maßgeblich dazu beigetragen, die Zusammenarbeit mit Internetunternehmen zu intensivieren und die allgemeinen Zielsetzungen des EU-Internetforums zu erreichen. Auf der jüngsten Ministertagung des EU-Internetforums vom 7. Oktober 2019 verpflichteten sich die EU-Mitgliedstaaten und führende Vertreter von Internetunternehmen, im Rahmen des sogenannten **EU-Krisenprotokolls** zusammenzuarbeiten. Im EU-Krisenprotokoll werden Schwellenwerte für eine verstärkte Zusammenarbeit festgelegt und neue Wege für die Verbesserung der Krisenreaktion abgesteckt. Dies ist Teil der auf internationaler Ebene unternommenen Bemühungen um die Umsetzung des „Christchurch-Aufrufs“;⁶ Ziel ist es, eine koordinierte und rasche Reaktion zu

⁴ COM(2018) 640 final vom 12.9.2018.

⁵ Hierbei handelt es sich um ein von einem Unternehmenskonsortium eingerichtetes Tool, das die Zusammenarbeit erleichtert, um die Verbreitung terroristischer Inhalte über verschiedene Plattformen zu verhindern.

⁶ Als Reaktion auf die Anschläge im neuseeländischen Christchurch vom 15. März 2019 hatten der französische Präsident Emmanuel Macron und die neuseeländische Premierministerin Jacinda Ardern Staats- und Regierungschefs sowie Vertreter von Online-Plattformen für den 15. Mai 2019 nach Paris

gewährleisten und die virale Verbreitung terroristischer oder gewaltverherrlichender extremistischer Online-Inhalte einzudämmen.

Neben diesen Maßnahmen zur Bekämpfung der Radikalisierung im Internet unterstützt die Kommission weiterhin die auf nationaler und lokaler Ebene unternommenen Bemühungen, **Radikalisierung vor Ort zu verhindern und zu bekämpfen**. Aufbauend auf dem im Rahmen des Aufklärungsnetzwerks gegen Radikalisierung erworbenen reichen Erfahrungs- und Wissensschatz bietet die EU lokalen Akteuren, darunter auch den Städten,⁷ gezielte Unterstützung und Möglichkeiten für einen Austausch zwischen Fachleuten, Wissenschaftlern und politischen Entscheidungsträgern. So hat das Netzwerk beispielsweise spezifische Leitlinien herausgegeben und Workshops organisiert, um die zuständigen Behörden beim Umgang mit Kindern aus Konfliktgebieten zu unterstützen.⁸ Um die kontinuierliche Fortführung der im Aufklärungsnetzwerk gegen Radikalisierung begonnenen Tätigkeiten zu gewährleisten, hat die Kommission ein Verfahren für die Vergabe eines neuen Rahmenvertrags im Wert von schätzungsweise 61 Mio. EUR mit einer Laufzeit von vier Jahren ab 2020 eingeleitet.⁹

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

- die Verhandlungen über den Legislativvorschlag zur Verhinderung der Verbreitung **terroristischer Online-Inhalte** vor Ablauf des Jahres zum Abschluss zu bringen.

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

Die Intensivierung des Informationsaustauschs durch die EU ermöglichte eine vereinfachte Aufdeckung von Identitätsbetrug,¹⁰ verbesserte Grenzkontrollen,¹¹ die Modernisierung der

eingeladen, um den „Christchurch-Aufruf“ auf den Weg zu bringen. Präsident Juncker unterstützte den Aufruf und kündigte die Entwicklung eines EU-Krisenprotokolls an.

⁷ Zur Zusammenarbeit mit den Städten im Bereich der Sicherheit siehe auch Abschnitt V.2 zum Thema Abwehrbereitschaft und Schutz, insbesondere zum Schutz des öffentlichen Raums.

⁸ https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/ran-papers/docs/issue_paper_child_returnees_from_conflict_zones_112016_de.pdf

⁹ Der Rahmenvertrag ist in zwei Lose aufgeteilt: 29 000 000 EUR zur Unterstützung der Aktivitäten des Aufklärungsnetzwerks gegen Radikalisierung in den nächsten vier Jahren sowie 32 000 000 EUR für die Verbesserung der Fähigkeiten der Mitgliedstaaten, der nationalen, regionalen und lokalen Behörden und der vorrangigen Drittländer zur wirksamen Bekämpfung der Radikalisierung, insbesondere durch die Bereitstellung von Vernetzungsmöglichkeiten, gezielten und bedarfsorientierten Dienstleistungen sowie Forschung und Analyse.

¹⁰ 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.

¹¹ Einführung systematischer Kontrollen aller Bürger an den Außengrenzen mithilfe des Schengener Informationssystems. Alle Schengen-Staaten sowie Rumänien, Bulgarien, Kroatien und Zypern nehmen entsprechend den im April 2017 erlassenen Vorschriften an den Außengrenzen einen systematischen Abgleich mit den einschlägigen Datenbanken vor. Nach diesen Vorschriften können an den Land- oder Seegrenzen vorübergehende Ausnahmeregelungen Anwendung finden, um unverhältnismäßige Auswirkungen auf den Verkehrsfluss zu vermeiden; dies gilt jedoch ausschließlich mit Blick auf EU-

europaweiten Strafverfolgungsdatenbanken,¹² die Schließung von Informationslücken¹³ und die Stärkung der EU-Strafverfolgungsbehörde Europol¹⁴. Von zentraler Bedeutung ist diesbezüglich die **Interoperabilität der EU-Informationssysteme**,¹⁵ die es erlaubt, die vorhandenen Informationen bestmöglich zu nutzen und offene Fragen zu klären. Entsprechend den Bedürfnissen der in den Bereichen Strafverfolgung, Grenzschutz und Migration an vorderster Front tätigen Beamten wird die Interoperabilität diesen einen schnelleren und systematischeren Zugang zu Informationen ermöglichen und damit zu einer Erhöhung der inneren Sicherheit und des Grenzmanagements beitragen.

Die Interoperabilität und alle damit verbundenen Innovationen werden jedoch mit Blick auf Sicherheit, Grenzmanagement und Migrationssteuerung nur dann konkret Wirkung zeigen, wenn jeder Mitgliedstaat die einschlägigen Rechtsvorschriften vollständig umsetzt. Daher wird der **Umsetzung** der Interoperabilität in der Sicherheitsunion sowohl auf politischer als auch auf technischer Ebene höchste Priorität eingeräumt. Die Kommission und die Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA) unterstützen die Mitgliedstaaten mit Fachwissen sowie durch den Austausch bewährter Verfahren über ein Netzwerk nationaler Koordinatoren; zudem wird ein Scorecard entwickelt, um wirksame Überwachungs- und Koordinierungsvorkehrungen zu ermöglichen. 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.

Indessen müssen das Europäische Parlament und der Rat die diesbezügliche **gesetzgeberische Arbeit zum Abschluss bringen**. Eine zügige Einigung über alle anhängigen Legislativvorschläge ist von entscheidender Bedeutung für die Gewährleistung der vollständigen und zeitnahen Umsetzung der Interoperabilität. Erstens sind im Rahmen der technischen Umsetzung des **Europäischen Reiseinformations- und -genehmigungssystems**

Bürger. Gegenwärtig haben sechs Mitgliedstaaten/assoziierte Schengen-Länder (Kroatien, Finnland, Ungarn, Lettland, Norwegen und Slowenien) solche Ausnahmeregelungen mitgeteilt. Was die Luftgrenzen betrifft, so sind seit April 2019 keine von den Vorschriften über systematische Kontrollen abweichenden Ausnahmeregelungen mehr zulässig.

¹² Das verstärkte Schengener Informationssystem (Verordnung (EU) 2018/1860 vom 28. November 2018, Verordnung (EU) 2018/1861 vom 28. November 2018, Verordnung (EU) 2018/1862 vom 28. November 2018) und das auf Drittstaatsangehörige erweiterte Europäische Strafregisterinformationssystem (Verordnung (EU) 2019/816 vom 17. April 2019). Die Verstärkung des Schengener Informationssystems wurde unter anderem durch eine allgemeine Verpflichtung erreicht, Ausschreibungen mit Terrorismusbezug in das System einzugeben.

¹³ Das Einreise-/Ausreisesystem der EU (Verordnung (EU) 2017/2226 vom 30. November 2017) und das Europäische Reiseinformations- und -genehmigungssystem (Verordnung (EU) 2018/1240 vom 12. September 2018 und Verordnung (EU) 2018/1241 vom 12. September 2018).

¹⁴ In den letzten Jahren wurde die Rolle von Europol erheblich erweitert und vertieft. Die Stärkung der Agentur erfolgte mit der Annahme der Europol-Verordnung im Jahr 2016 (Verordnung (EU) 2016/794 vom 11. Mai 2016). Die Mitgliedstaaten tauschen mittlerweile deutlich mehr Informationen mit und über Europol aus. Mit der Errichtung des Europäischen Zentrums zur Terrorismusbekämpfung (ECTC) wurden die Analysekapazitäten von Europol in Fällen von Terrorismus verbessert. Die Haushaltsmittel von Europol wurden in den letzten Jahren kontinuierlich erhöht und stiegen von 82 Mio. EUR im Jahr 2014 auf 138 Mio. EUR im Jahr 2019. Die Verhandlungen über den Haushaltsplan 2020 sind noch nicht abgeschlossen.

¹⁵ Verordnung (EU) 2019/817 vom 20. Mai 2019 und Verordnung (EU) 2019/818 vom 20. Mai 2019.

technische Änderungen der einschlägigen Verordnungen¹⁶ erforderlich, um die vollständige Einrichtung des Systems zu ermöglichen. Die Kommission fordert das Europäische Parlament auf, seine Tätigkeiten bezüglich dieser technischen Änderungen zügiger voranzutreiben, sodass die interinstitutionellen Verhandlungen so bald wie möglich aufgenommen werden können. Zweitens sind die interinstitutionellen Verhandlungen über den im Mai 2018 vorgelegten Vorschlag für die Stärkung und den Ausbau des bestehenden **Visa-Informationssystem**¹⁷ noch nicht abgeschlossen. Unter Hinweis auf die erste Trilogsitzung vom 22. Oktober 2019 fordert die Kommission die beiden gesetzgebenden Organe auf, die Verhandlungen zeitnah zum Abschluss zu bringen. Drittens wurde noch immer keine Einigung über den im Mai 2016 vorgelegten Vorschlag der Kommission erzielt, den Geltungsbereich von **Eurodac**¹⁸ auszuweiten und die Fingerabdrücke und einschlägigen Daten nicht nur von Asylbewerbern und beim irregulären Überschreiten der Außengrenze aufgegriffenen Personen zu speichern, sondern auch von illegal aufhältigen Drittstaatsangehörigen. Mit den vorgeschlagenen Änderungen würde auch die Aufbewahrungsfrist für die Fingerabdrücke und einschlägigen Daten von Personen verlängert, die irregulär in die EU einreisen. Die Kommission fordert die gesetzgebenden Organe auf, den Vorschlag anzunehmen.

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

- auf eine rasche Einigung über die vorgeschlagenen technischen Änderungen hinzuarbeiten, die für die Einrichtung des **Europäischen Reiseinformations- und -genehmigungssystems** erforderlich sind;
- die Verhandlungen über den Vorschlag zur Stärkung des bestehenden **Visa-Informationssystem** zügig durchzuführen und abzuschließen;
- den Legislativvorschlag zu **Eurodac** anzunehmen (*Priorität der Gemeinsamen Erklärung*).

3. *Terroristen den Handlungsspielraum nehmen*

Die EU hat entschlossene Maßnahmen ergriffen, um Terroristen den Handlungsspielraum zu nehmen; dazu hat sie neue Vorschriften erlassen, die Terroristen und anderen Straftätern den Zugang zu Explosivstoffen,¹⁹ Feuerwaffen und Finanzmitteln²⁰ erschweren und ihre Bewegungsfreiheit einschränken²¹.

Um die justizielle Reaktion auf den Terrorismus zu verbessern, hat die EU-Agentur für justizielle Zusammenarbeit (Eurojust) am 1. September 2019 ein europäisches justizielles

¹⁶ Verordnung (EU) 2018/1240 vom 12. September 2018 und Verordnung (EU) 2018/1241 vom 12. September 2018.

¹⁷ COM(2018) 302 final vom 16.5.2018.

¹⁸ COM(2016) 272 final vom 4.5.2016.

¹⁹ Verordnung (EU) 2019/1148 vom 20. Juni 2019 über die Vermarktung und Verwendung von Ausgangsstoffen für Explosivstoffe. Die Verordnung trat am 31. Juli 2019 in Kraft und gilt nach Ablauf von 18 Monaten ab ihrem Inkrafttreten.

²⁰ 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.

²¹ Einführung systematischer Kontrollen aller Bürger an den Außengrenzen mithilfe des Schengener Informationssystems.

Terrorismusregister (**Judicial Counter-Terrorism Register**) eingerichtet. In diesem Register werden justizielle Informationen gesammelt, um Verbindungen zwischen Verfahren gegen Terrorverdächtige herzustellen und so bei potenziell grenzüberschreitenden Ermittlungen in Terrorismusfällen die Koordinierung zwischen den Staatsanwälten zu verbessern.

Es sind jedoch weitere Anstrengungen erforderlich, um die Ermittlungen in grenzüberschreitenden Fällen zu unterstützen und zu erleichtern; dies gilt insbesondere für den **Zugang** der Strafverfolgungsbehörden zu **elektronischen Beweismitteln**. Bezüglich der im April 2018 vorgelegten Legislativvorschläge zur Verbesserung des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln in strafrechtlichen Ermittlungen²² muss das Europäische Parlament zunächst seine Verhandlungsposition annehmen, bevor die gesetzgebenden Organe Verhandlungen aufnehmen können. Die Kommission fordert das Europäische Parlament nachdrücklich auf, diesen Legislativvorschlag voranzubringen, damit die gesetzgebenden Organe auf eine zeitnahe Annahme hinwirken können. Auf der Grundlage ihres Vorschlags über interne Vorschriften der EU führt die Kommission zudem **internationale Verhandlungen** über die Verbesserung des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln. Am 25. September 2019 nahmen die Kommission und die Behörden der Vereinigten Staaten die förmlichen Verhandlungen über ein **Abkommen zwischen der EU und den USA über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln** auf. Eine weitere Verhandlungsrunde ist für den 6. November 2019 geplant. Im Zusammenhang mit den laufenden Verhandlungen über ein **Zweites Zusatzprotokoll zum Budapester Übereinkommen des Europarats über Computerkriminalität** nahm die Kommission im Namen der Union im Juli, September und Oktober 2019 an drei Verhandlungsrunden teil. Zwar wurden bei diesen Verhandlungen gute Fortschritte erzielt, jedoch muss noch eine Reihe wichtiger Themen erörtert werden, die für die Union von erheblichem Interesse sind, wie beispielsweise Datenschutzgarantien. Die Verhandlungen über ein Zweites Zusatzprotokoll werden im November 2019 und im Laufe des Jahres 2020 fortgesetzt. In beiden Fällen müssen die Verhandlungen zügig vorangetrieben werden, damit die internationale Zusammenarbeit beim Austausch elektronischer Beweismittel vorankommt und zugleich die Vereinbarkeit mit dem EU-Recht und den daraus erwachsenden Verpflichtungen der Mitgliedstaaten gewährleistet ist, wobei auch künftige Entwicklungen des EU-Rechts zu berücksichtigen sind.

Angesichts der anhaltenden Bedenken bezüglich der Geldwäsche nahm das Europäische Parlament am 19. September 2019 eine **Entschließung zum Stand der Umsetzung der Rechtsvorschriften der Union zur Bekämpfung von Geldwäsche**²³ an, die dem vier Berichte über die Bekämpfung der Geldwäsche umfassenden Paket²⁴ Rechnung trägt, das von der Kommission am 24. Juli 2019 angenommen wurde. Das Europäische Parlament forderte die Mitgliedstaaten auf, für die ordnungsgemäße und zügige Umsetzung der Richtlinien zur Bekämpfung der Geldwäsche zu sorgen. Darüber hinaus forderte das Europäische Parlament

²² COM(2018) 225 final vom 17.4.2018 und COM(2018) 226 final vom 17.4.2018.

²³ https://www.europarl.europa.eu/doceo/document/TA-9-2019-0022_DE.html

²⁴ Bericht über die Bewertung der mit grenzüberschreitenden Tätigkeiten im Zusammenhang stehenden Risiken der Geldwäsche und der Terrorismusfinanzierung für den Binnenmarkt (COM(2019) 370 final vom 24.7.2019), Bericht über die Vernetzung der zentralen automatischen Mechanismen (zentrale Register oder zentrale elektronische Datenabrufsysteme) der Mitgliedstaaten für Bankkonten (COM(2019) 372 final vom 24.7.2019), Bericht über die Bewertung aktueller Fälle von mutmaßlicher Geldwäsche unter Beteiligung von Kreditinstituten aus der EU (COM(2019) 373 final vom 24.7.2019), Bericht über die Bewertung des Rahmens für die Zusammenarbeit zwischen den zentralen Meldestellen für Geldwäsche-Verdachtsanzeigen (FIU) (COM(2019) 371 final vom 24.7.2019).

die Kommission auf, der Frage nachzugehen, ob sich eine Verordnung zur Bekämpfung von Geldwäsche besser eignen würde als eine Richtlinie, und die Notwendigkeit eines Koordinierungs- und Unterstützungsmechanismus für die zentralen Meldestellen zu bewerten.

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

- rasch eine Einigung über die Legislativvorschläge zu **elektronischen Beweismitteln** zu erzielen (*Priorität der Gemeinsamen Erklärung*).

4. Erhöhung der Cybersicherheit

Die Erhöhung der Cybersicherheit ist nach wie vor ein zentraler Aspekt der Bemühungen um eine echte und wirksame Sicherheitsunion. Mit der Durchführung der Cybersicherheitsstrategie der EU aus dem Jahr 2017²⁵ hat die Union ihre Abwehrfähigkeit verbessert, indem sie dafür gesorgt hat, dass sie weniger angreifbar ist, sich schneller von Angriffen erholt und unter anderem dank des Rahmens für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten größere Chancen auf eine Ergreifung und Bestrafung der Angreifer bestehen, sodass eine wirksamere Abschreckung gewährleistet ist. Im Rahmen der Umsetzung des EU-Politikrahmens für die Cyberabwehr unterstützt die Union darüber hinaus die Mitgliedstaaten bei deren diesbezüglichen Maßnahmen.²⁶

Mit dem Inkrafttreten des Rechtsakts zur Cybersicherheit²⁷ im Juni 2019 nahm der **EU-Rahmen für die Cybersicherheitszertifizierung** Gestalt an. Die Zertifizierung spielt eine entscheidende Rolle, wenn es darum geht, das Vertrauen in Produkte und Dienstleistungen zu stärken und deren Sicherheit zu erhöhen – beides ist für den digitalen Binnenmarkt von zentraler Bedeutung. Der Zertifizierungsrahmen wird EU-weite Schemata für die Cybersicherheitszertifizierung in Form umfassender Pakete von Vorschriften, technischen Anforderungen, Normen und Verfahren bereitstellen. Es befassen sich zwei Sachverständigengruppen mit dem Zertifizierungsrahmen, namentlich die Europäische Gruppe für die Cybersicherheitszertifizierung, in der die Mitgliedstaaten vertreten sind, und die Gruppe der Interessenträger für die Cybersicherheitszertifizierung, die sich aus Branchenvertretern zusammensetzt. In der letztgenannten Gruppe werden die Nachfrage- und die Angebotsseite des Marktes für Produkte und Dienstleistungen der Informations- und Kommunikationstechnologie vertreten sein, darunter kleine und mittlere Unternehmen, Anbieter digitaler Dienste, europäische und internationale Normungsgremien, nationale Akkreditierungsstellen, Datenschutz-Aufsichtsbehörden und Konformitätsbewertungsstellen.

Indessen müssen das Europäische Parlament und der Rat noch eine Einigung über die Gesetzgebungsinitiative²⁸ für ein **Europäisches Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung** und ein **Netz nationaler Koordinierungszentren** erzielen. Der Vorschlag zielt darauf ab, die Cybersicherheitskapazitäten der Union durch die Förderung des technischen und industriellen Cybersicherheitsökosystems sowie die Koordinierung und Bündelung der entsprechenden Ressourcen zu stärken. Die Kommission fordert die beiden gesetzgebenden Organe auf, die interinstitutionellen Verhandlungen über

²⁵ JOIN(2017) 450 final vom 13.9.2017.

²⁶ EU-Politikrahmen für die Cyberabwehr (Aktualisierung 2018), vom Rat angenommen am 19. November 2018 (14413/18).

²⁷ Verordnung (EU) 2019/881 vom 17. April 2019.

²⁸ COM(2018) 630 final vom 12.9.2018.

diese vorrangige Initiative zur Erhöhung der Cybersicherheit wieder aufzunehmen und zügig abzuschließen.

Im Rahmen ihrer Bemühungen um die Erhöhung der Cybersicherheit leistet die EU sowohl auf nationaler als auch auf regionaler Ebene Unterstützung.²⁹

Die EU befasst sich auch weiterhin nicht nur mit der Bekämpfung von Cyberbedrohungen für Systeme und Daten, sondern auch mit der Bewältigung der komplexen und vielschichtigen Herausforderungen, die mit **hybriden Bedrohungen** verbunden sind. Beim Rat wurde eine horizontale Arbeitsgruppe für die Abwehr hybrider Bedrohungen eingesetzt, die sich mit der Verbesserung der Widerstandsfähigkeit der EU und ihrer Mitgliedstaaten gegen hybride Bedrohungen und der Unterstützung von Maßnahmen zur Stärkung der Krisenfestigkeit von Gesellschaften befasst. Die Kommission und der Europäische Auswärtige Dienst unterstützen diese Bemühungen mit ihrem Gemeinsamen Rahmen für die Bekämpfung hybrider Bedrohungen³⁰ aus dem Jahr 2016 und der Gemeinsamen Mitteilung³¹ über die Stärkung der Resilienz und den Ausbau der Kapazitäten zur Abwehr hybrider Bedrohungen aus dem Jahr 2018. Des Weiteren erarbeitet die Gemeinsame Forschungsstelle einen Rahmen für ein „konzeptionelles Modell“ zur Charakterisierung hybrider Bedrohungen, um die Mitgliedstaaten und ihre zuständigen Behörden bei der Ermittlung der Art möglicher hybrider Angriffe zu unterstützen. Mit diesem Modell wird untersucht, in welcher Weise ein (staatlicher oder nichtstaatlicher) Akteur in verschiedenen Bereichen (Wirtschaft, Militär, Gesellschaft, Politik) eine Reihe von Instrumenten (von Desinformation über Spionage bis hin zu physischen Aktionen) einsetzt, um ein bestimmtes Zielobjekt zu treffen und damit eine Reihe von Zielsetzungen zu erreichen.

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.

III. ERHÖHUNG DER SICHERHEIT DIGITALER INFRASTRUKTUREN

Netze der fünften Generation (5G-Netze) sind das künftige Rückgrat unserer zunehmend digitalisierten Volkswirtschaften und Gesellschaften. Sie werden Milliarden von Objekten und Systemen miteinander verbinden, u. a. in kritischen Sektoren wie Energie, Verkehr, Bank- und Gesundheitswesen, aber auch in industriellen Steuerungssystemen, die sensible Informationen verarbeiten und Sicherheitssysteme unterstützen. Die Gewährleistung der Sicherheit und Widerstandsfähigkeit der 5G-Netze ist daher von größter Bedeutung.

Im Rahmen eines koordinierten Konzepts veröffentlichten die Mitgliedstaaten mit Unterstützung der Kommission und der Agentur der Europäischen Union für Cybersicherheit am 9. Oktober 2019 einen Bericht über die **EU-weit koordinierte Risikobewertung der**

²⁹ So fördert die Kommission beispielsweise eine interregionale Innovationspartnerschaft zur Cybersicherheit, in deren Rahmen die Bretagne, Kastilien und León, Nordrhein-Westfalen, Mittelfinnland und Estland eine europäische Wertschöpfungskette im Bereich der Cybersicherheit entwickeln, wobei der Schwerpunkt auf den Aspekten Kommerzialisierung und Ausbau liegt.

³⁰ JOIN(2016) 18 final (6.4.2016).

³¹ JOIN(2018) 16 final vom 13.6.2018.

Cybersicherheit in 5G-Netzen.³² Dieser wichtige Schritt ist Teil der Umsetzung der von der Europäischen Kommission im März 2019 vorgelegten Empfehlung zur Gewährleistung eines hohen Cybersicherheitsniveaus der 5G-Netze in der gesamten EU.³³ Der Bericht beruht auf den Ergebnissen der nationalen Risikobewertungen, die alle Mitgliedstaaten in Bezug auf ihre Cybersicherheit durchgeführt haben. Darin werden die gravierendsten Bedrohungen und ihre Verursacher, die anfälligsten Anlagen und Einrichtungen, die wichtigsten Schwachstellen (technischer und anderer Art) und eine Reihe strategischer Risiken aufgezeigt. Diese Bewertung bildet die Grundlage für die Ermittlung von Risikominderungsmaßnahmen, die auf nationaler und europäischer Ebene ergriffen werden können.

In dem Bericht wird eine Reihe wichtiger **Probleme im Bereich der Cybersicherheit** genannt, die aller Wahrscheinlichkeit nach in den 5G-Netzen in Erscheinung treten oder an Bedeutung gewinnen werden. Diese Sicherheitsprobleme stehen in erster Linie in Zusammenhang mit zentralen *Innovationen* der 5G-Technik, insbesondere mit der großen Bedeutung von Software, dem breiten Spektrum der Dienste und Anwendungen, die durch 5G-Technik ermöglicht werden, der Rolle der *Anbieter* beim Aufbau und Betrieb von 5G-Netzen und dem Grad der Abhängigkeit von einzelnen Anbietern. Das bedeutet, dass die Produkte, Dienstleistungen und Betriebstätigkeiten der Anbieter zunehmend Teil der „Angriffsfläche“ der 5G-Netze werden. Zudem wird auch das Risikoprofil der einzelnen Anbieter von besonderer Bedeutung sein, darunter auch die Wahrscheinlichkeit, dass ein Nicht-EU-Land Einfluss auf einen Anbieter ausübt.

Das in der im März 2019 vorgelegten Empfehlung der Kommission festgelegte Verfahren sieht vor, dass die Mitgliedstaaten bis zum 31. Dezember 2019 ein **Instrumentarium mit Risikominderungsmaßnahmen** zur Bewältigung der auf nationaler und Unionsebene ermittelten Cybersicherheitsrisiken vereinbaren. Zudem werden sich die Kommission und der Europäische Auswärtige Dienst weiterhin mit gleich gesinnten Partnern über die Cybersicherheit und Widerstandsfähigkeit von 5G-Netzen austauschen. Die Kommission steht bezüglich der EU-weit koordinierten Risikobewertung der Cybersicherheit in 5G-Netzen in Kontakt mit der NATO.

³² Die EU-weit koordinierte Risikobewertung der Cybersicherheit in 5G-Netzen wurde von der durch die Richtlinie zur Netz- und Informationssicherheit (Richtlinie (EU) 2016/1148 vom 6. Juli 2016) eingesetzte Kooperationsgruppe der zuständigen Behörden mit Unterstützung der Kommission und der Agentur der Europäischen Union für Cybersicherheit vorgenommen: <https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security>.

³³ C(2019) 2355 final vom 26.3.2019.

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

Die EU hat einen **Rahmen für ein koordiniertes Vorgehen gegen Desinformation** unter uneingeschränkter Achtung der europäischen Werte und Grundrechte geschaffen.³⁴ Im Zuge der Umsetzung des Aktionsplans gegen Desinformation³⁵ wird weiter daran gearbeitet, Desinformation keinen Raum mehr zu geben und damit unter anderem die Integrität von Wahlen zu schützen.

Im Mittelpunkt steht dabei die Zusammenarbeit mit der Industrie im Rahmen des **Verhaltenskodex zur Bekämpfung von Desinformation** für Online-Plattformen und die Werbebranche, der im Oktober 2018 eingeführt wurde.³⁶ Die Kommission hat die Wirksamkeit des Kodex nach Ablauf des ersten Jahres nach seinem Inkrafttreten auf der Grundlage der jährlichen Selbstbewertungsberichte untersucht, die von den Online-Plattformen und den übrigen Unterzeichnern des Kodex eingereicht und am 29. Oktober 2019 gemeinsam mit einer Erklärung der Kommission veröffentlicht wurden.³⁷ Insgesamt zeigen die Berichte, dass die Unterzeichner ernsthafte Anstrengungen unternehmen, um ihren Verpflichtungen nachzukommen.

Die von den Plattformen bezüglich der fünf Säulen des Kodex ergriffenen Maßnahmen unterscheiden sich in Tempo und Umfang. Insgesamt wurden bei den die Europawahl 2019 betreffenden Verpflichtungen größere Fortschritte erzielt, insbesondere mit Blick auf die Einschränkung von Werbung und finanziellen Anreizen für Desinformation (Säule 1), die Gewährleistung der Transparenz politischer und themenbezogener Werbung (Säule 2) und die Sicherstellung der Integrität der Dienste gegenüber Scheinkonten und fragwürdigem Verhalten (Säule 3). Weniger bzw. keine Fortschritte erzielten die Plattformen hingegen bezüglich ihrer Verpflichtungen zur Stärkung der Handlungskompetenz der Verbraucher (Säule 4) sowie zur Stärkung der Position der Forschungsgemeinschaft unter anderem durch die Bereitstellung eines angemessenen und datengeschützten Zugangs zu Datensätzen zu Forschungszwecken (Säule 5). Unterschiede bestehen zudem hinsichtlich des Umfangs der von den einzelnen Plattformen zur Gewährleistung der Umsetzung ihrer Verpflichtungen ergriffenen Maßnahmen sowie mit Blick auf die Durchführung der einzelnen Strategien in den Mitgliedstaaten. Die Kommission arbeitet weiterhin mit den Unterzeichnern des Kodex und anderen Interessenträgern zusammen, um die Maßnahmen zur Bekämpfung von Desinformation zu verstärken.

³⁴ Siehe den Aktionsplan gegen Desinformation (JOIN(2018) 36 final vom 5.12.2018).

³⁵ JOIN(2019) 12 final vom 14.6.2019.

³⁶ Im Rahmen des Kodex haben sich die Online-Plattformen Google, Facebook, Twitter und Microsoft verpflichtet, die manipulative Nutzung ihrer Dienste durch böswillige Akteure zu verhindern, die Transparenz und Offenlegung politischer Werbung sicherzustellen und weitere Maßnahmen zur Verbesserung der Transparenz, Rechenschaftspflicht und Vertrauenswürdigkeit des Internet-Ökosystems zu ergreifen. Zudem haben Berufsverbände der Werbebranche zugesagt, mit den Plattformen zusammenzuarbeiten, um die Kontrolle von Werbeplatzierungen zu verbessern sowie Tools zur Gewährleistung der Markensicherheit zu entwickeln und so der Platzierung von Werbung auf Websites entgegenzuwirken, über die Desinformation verbreitet wird.

³⁷ https://ec.europa.eu/commission/presscorner/detail/de/statement_19_6166 Neben Google, Facebook, Twitter und Microsoft zählen Mozilla, sieben europäische oder nationale Berufsverbände der Werbebranche sowie EDiMA, ein europäischer Verband von Plattformen und anderen im Online-Bereich tätigen Technologieunternehmen, zu den Unterzeichnern des Kodex.

Im Rahmen des Aktionsplans gegen Desinformation haben die Kommission und die Hohe Vertreterin gemeinsam mit den Mitgliedstaaten ein **Frühwarnsystem** eingerichtet, um gegen Desinformationskampagnen vorzugehen. Dank dieses Frühwarnsystems waren die Organe und Mitgliedstaaten der EU im Vorfeld der Wahlen zum Europäischen Parlament im Jahr 2019 in der Lage, Informationen und Analysen auszutauschen und ihre Abwehrmaßnahmen zu koordinieren. Nach den Wahlen wurde diese Zusammenarbeit weiter intensiviert, wobei auf Arbeitsebene ein täglicher Austausch erfolgt und in verschiedenen Mitgliedstaaten drei Treffen der Kontaktstellen des Frühwarnsystems stattfanden.

Eine weitere praktische Maßnahme zur Ermittlung von Desinformation ist die Tätigkeit des **Teams für strategische Kommunikation** („StratComms“) und insbesondere der East StratCom Task Force, die im Rahmen des Projekts „EUvsDisinfo“ kremlfreundliche Desinformation überwacht, analysiert und abwehrt.³⁸ Mit seiner Mittelausstattung in Höhe von 3 Mio. EUR gelang es dem Team im Jahr 2019, seine Tätigkeiten zu verstärken und auszubauen, sodass es nun kremlfreundliche Desinformation in Internet, Rundfunk und sozialen Medien in 19 Sprachen – von Englisch bis hin zu Serbisch und Arabisch – überwacht und analysiert. Aufgrund der verbesserten Überwachungskapazität hat sich die Zahl der aufgedeckten Desinformationsaktivitäten mehr als verdoppelt, wobei im Jahr 2019 bislang etwa 2000 Fälle von Desinformation ermittelt wurden, gegenüber 765 im Vorjahreszeitraum. Die East StratCom Task Force spielte eine entscheidende Rolle bei der Überwachung und Aufdeckung kremlfreundlicher Desinformation, die auf die Europawahl 2019 abzielte. Ergänzend zu den Forschungsarbeiten wurde eine Sensibilisierungskampagne organisiert, um auf die versuchte Einflussnahme auf Wahlprozesse in aller Welt aufmerksam zu machen. Im Rahmen dieser in enger Zusammenarbeit mit dem Europäischen Parlament und der Kommission durchgeführten Kampagne, an der sich über 300 Journalisten beteiligten, wurden mehr als 20 Medieninterviews geführt.

Des Weiteren hat die Kommission Maßnahmen ergriffen, um **die Verbreitung von Desinformation und Mythen über die Organe und die Politik der EU einzudämmen**. So wurde ein Netz von Kommunikationsexperten eingerichtet, das über ein Online-Portal interaktives Informationsmaterial zur EU-Politik, zum Problem der Desinformation und zu deren Auswirkungen auf die Gesellschaft bereitstellt. Zudem hat die Kommission in Zusammenarbeit mit dem Europäischen Parlament und dem Europäischen Auswärtigen Dienst in den sozialen Medien eine Reihe von Kampagnen zur Bekämpfung von Desinformation³⁹ ins Leben gerufen.

V. UMSETZUNG WEITERER VORRANGIGER DOSSIERS IM SICHERHEITSBEREICH

1. Umsetzung legislativer Maßnahmen im Rahmen der Sicherheitsunion

Die im Rahmen der Sicherheitsunion vereinbarten Maßnahmen können ihre positive Wirkung auf die Sicherheit nur dann voll entfalten, wenn alle Mitgliedstaaten für ihre zügige und vollständige Umsetzung Sorge tragen. Zu diesem Zweck unterstützt die Kommission die Mitgliedstaaten aktiv bei der Umsetzung der EU-Rechtsvorschriften, unter anderem durch die Bereitstellung von Finanzmitteln und die Erleichterung des Austauschs bewährter Verfahren. Die Kommission macht in vollem Umfang von den ihr durch die Verträge verliehenen

³⁸ www.euvsdisinfo.eu

³⁹ https://europa.eu/euprotects/content/homepage_de

Befugnissen zur Durchsetzung des EU-Rechts Gebrauch und leitet gegebenenfalls Vertragsverletzungsverfahren ein.

Die Frist für die Umsetzung der **EU-Richtlinie über Fluggastdatensätze**⁴⁰ endete am 25. Mai 2018. Bislang haben 25 Mitgliedstaaten die vollständige Umsetzung mitgeteilt;⁴¹ damit wurden seit Juli 2018, als die Kommission gegen 14 Mitgliedstaaten Vertragsverletzungsverfahren einleitete, erhebliche Fortschritte erzielt.⁴² Zwei Mitgliedstaaten haben ungeachtet der laufenden Vertragsverletzungsverfahren, die am 19. Juli 2018 eingeleitet wurden, die vollständige Umsetzung noch nicht mitgeteilt.⁴³ 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**⁴⁴ endete am 8. September 2018. Bislang haben 22 Mitgliedstaaten die vollständige Umsetzung mitgeteilt; damit wurden seit November 2018, als die Kommission gegen 16 Mitgliedstaaten Vertragsverletzungsverfahren einleitete, erhebliche Fortschritte erzielt.⁴⁵ Drei Mitgliedstaaten haben ungeachtet der laufenden Vertragsverletzungsverfahren die vollständige Umsetzung noch nicht mitgeteilt.⁴⁶ Am 25. Juli 2019 übermittelte die Kommission zwei Mitgliedstaaten mit Gründen versehene Stellungnahmen, weil sie die vollständige Umsetzung der Richtlinie nicht mitgeteilt hatten.⁴⁷ Daraufhin kündigten beide Mitgliedstaaten an, die diesbezügliche gesetzgeberische Arbeit vor Ablauf dieses Jahres abzuschließen.

Die Frist für die Umsetzung der **Richtlinie über die Kontrolle des Erwerbs und des Besitzes von Waffen**⁴⁸ endete am 14. September 2018. Bislang haben 13 Mitgliedstaaten die vollständige Umsetzung mitgeteilt. Ungeachtet der laufenden Vertragsverletzungsverfahren, die am 22. November 2018 eingeleitet wurden, haben 15 Mitgliedstaaten die vollständige Umsetzung noch nicht mitgeteilt.⁴⁹ Am 25. Juli 2019 übermittelte die Kommission 20 Mitgliedstaaten mit Gründen versehene Stellungnahmen, weil sie die vollständige Umsetzung der Richtlinie nicht mitgeteilt hatten. Daraufhin teilten fünf Mitgliedstaaten die

⁴⁰ Richtlinie (EU) 2016/681 vom 27. April 2016. Dänemark beteiligte sich nicht an der Annahme dieser Richtlinie und ist weder durch sie gebunden noch zu ihrer Anwendung verpflichtet.

⁴¹ Die Angaben zur Mitteilung der vollständigen Umsetzung beruhen auf den Erklärungen der Mitgliedstaaten und berühren nicht die Prüfung der Umsetzung durch die Kommissionsdienststellen (Stand: 17. Oktober 2019).

⁴² Siehe die Mitteilung „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Sechzehnter Fortschrittsbericht“ (COM(2018) 690 final vom 10.10.2018).

⁴³ Slowenien hat eine teilweise Umsetzung mitgeteilt. Spanien hat noch nicht mitgeteilt, dass es die Richtlinie umgesetzt hat (Stand: 17. Oktober 2019).

⁴⁴ Richtlinie (EU) 2017/541 vom 15. März 2017. Im Vereinigten Königreich sowie in Irland und Dänemark ist diese Richtlinie nicht anwendbar.

⁴⁵ Siehe die Mitteilung „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Siebzehnter Fortschrittsbericht“ (COM(2018) 845 final vom 11.12.2018).

⁴⁶ Griechenland und Luxemburg haben keine nationalen Umsetzungsmaßnahmen mitgeteilt. Polen hat nationale Maßnahmen mitgeteilt, die einer teilweisen Umsetzung entsprechen (Stand: 17. Oktober 2019).

⁴⁷ Griechenland und Luxemburg.

⁴⁸ Richtlinie (EU) 2017/853 vom 17. Oktober 2019.

⁴⁹ Belgien, Tschechien, Estland, Polen, Schweden, die Slowakei und das Vereinigte Königreich haben für einen Teil der neuen Vorschriften Umsetzungsmaßnahmen mitgeteilt. Zypern, Deutschland, Griechenland, Spanien, Luxemburg, Ungarn, Rumänien und Slowenien haben keinerlei Umsetzungsmaßnahmen mitgeteilt (Stand: 17. Oktober 2019).

vollständige Umsetzung der Richtlinie mit.⁵⁰

Die Frist für die Umsetzung der **Richtlinie zum Datenschutz bei der Strafverfolgung**⁵¹ endete am 6. Mai 2018. Bislang haben 25 Mitgliedstaaten die vollständige Umsetzung mitgeteilt; damit wurden seit Juli 2018, als die Kommission Vertragsverletzungsverfahren gegen 19 Mitgliedstaaten einleitete, erhebliche Fortschritte erzielt.⁵² Drei Mitgliedstaaten haben ungeachtet der laufenden Vertragsverletzungsverfahren die vollständige Umsetzung noch nicht mitgeteilt.⁵³ Am 25. Juli 2019 beschloss die Kommission, beim Gerichtshof der Europäischen Union gegen zwei Mitgliedstaaten⁵⁴ Klage wegen Nichtumsetzung der Richtlinie zu erheben, und richtete an einen Mitgliedstaat⁵⁵ ein Aufforderungsschreiben wegen unvollständiger Umsetzung der Richtlinie.⁵⁶

Die Kommission prüft gegenwärtig die Umsetzung der **4. Geldwäscherichtlinie**⁵⁷ sowie die Anwendung der Vorschriften durch die Mitgliedstaaten. Die Mitgliedstaaten mussten diese Richtlinie bis zum 26. Juni 2018 in nationales Recht umsetzen. Die Kommission setzt die Vertragsverletzungsverfahren gegen 21 Mitgliedstaaten fort, da sie der Auffassung ist, dass aus den von den Mitgliedstaaten vorgelegten Mitteilungen keine vollständige Umsetzung dieser Richtlinie hervorgeht.⁵⁸

Die Kommission hat die Konformität der Umsetzung der **Richtlinien zur Cyberkriminalität** geprüft. Im Juli und Oktober 2019 leitete sie Vertragsverletzungsverfahren gegen 23 Mitgliedstaaten⁵⁹ ein, da nach ihrer Auffassung die **Richtlinie zur Bekämpfung des sexuellen Missbrauchs von Kindern**⁶⁰ durch die von diesen Mitgliedstaaten mitgeteilten nationalen Umsetzungsvorschriften nicht korrekt umgesetzt wurde. Des Weiteren leitete die Kommission im Juli und Oktober 2019 Vertragsverletzungsverfahren gegen vier Mitgliedstaaten⁶¹ ein, da nach ihrer Auffassung die **Richtlinie über Angriffe auf Informationssysteme**⁶² durch die von diesen Mitgliedstaaten mitgeteilten nationalen Umsetzungsvorschriften nicht korrekt umgesetzt wurde.

⁵⁰ Finnland, Irland, Litauen, die Niederlande und Portugal (Stand: 17. Oktober 2019).

⁵¹ Richtlinie (EU) 2016/680 vom 27. April 2016.

⁵² Siehe die Mitteilung „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Sechszehnter Fortschrittsbericht“ (COM(2018) 690 final vom 10.10.2018).

⁵³ Slowenien hat eine teilweise Umsetzung mitgeteilt. Spanien hat noch nicht mitgeteilt, dass es die Richtlinie umgesetzt hat. Deutschland hat zwar die vollständige Umsetzung mitgeteilt, die Kommission sieht diese Umsetzung jedoch nicht als vollständig an (Stand: 17. Oktober 2019).

⁵⁴ Griechenland und Spanien.

⁵⁵ Deutschland.

⁵⁶ Griechenland hat die vollständige Umsetzung mitgeteilt, die derzeit von der Kommission geprüft wird.

⁵⁷ Richtlinie (EU) 2015/849 vom 20.5.2015.

⁵⁸ Belgien, Bulgarien, Tschechien, Dänemark, Deutschland, Estland, Irland, Frankreich, Italien, Zypern, Lettland, Litauen, die Niederlande, Österreich, Polen, Rumänien, die Slowakei, Finnland, Schweden und das Vereinigte Königreich (Stand: 17. Oktober 2019). Sieben im Zusammenhang mit der Richtlinie eingeleitete Vertragsverletzungsverfahren wurden bereits eingestellt.

⁵⁹ Belgien, Bulgarien, Tschechien, Deutschland, Estland, Griechenland, Spanien, Frankreich, Kroatien, Italien, Lettland, Litauen, Luxemburg, Ungarn, Malta, Österreich, Polen, Portugal, Rumänien, Slowenien, die Slowakei, Finnland und Schweden.

⁶⁰ Richtlinie 2011/93/EU vom 13. Dezember 2011.

⁶¹ Bulgarien, Italien, Portugal und Slowenien.

⁶² Richtlinie 2013/40/EU vom 12. August 2013.

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;⁶³
- die **Richtlinie zur Terrorismusbekämpfung**: 2 Mitgliedstaaten müssen noch die Umsetzung in nationales Recht mitteilen, und 1 Mitgliedstaat muss die Mitteilung der Umsetzung vervollständigen;⁶⁴
- die **Richtlinie über die Kontrolle des Erwerbs und des Besitzes von Waffen**: 8 Mitgliedstaaten müssen noch die Umsetzung in nationales Recht mitteilen, und 7 Mitgliedstaaten müssen die Mitteilung der Umsetzung vervollständigen;⁶⁵
- die **Richtlinie zum Datenschutz bei der Strafverfolgung**: 1 Mitgliedstaat muss noch die Umsetzung in nationales Recht mitteilen, und 2 Mitgliedstaaten müssen die Mitteilung der Umsetzung vervollständigen;⁶⁶
- die **4. Geldwäscherichtlinie**: 21 Mitgliedstaaten müssen noch die Mitteilung der Umsetzung vervollständigen;⁶⁷
- die **Richtlinie zur Bekämpfung des sexuellen Missbrauchs von Kindern**: Gegen 23 Mitgliedstaaten⁶⁸ wurden Vertragsverletzungsverfahren wegen mangelhafter Umsetzung eingeleitet;
- die **Richtlinie über Angriffe auf Informationssysteme**: Gegen 4 Mitgliedstaaten⁶⁹ wurden Vertragsverletzungsverfahren wegen mangelhafter Umsetzung eingeleitet.

2. Abwehrbereitschaft und Schutz

Die Stärkung der Widerstandsfähigkeit gegen Sicherheitsbedrohungen ist ein wesentlicher Bestandteil der Bemühungen um eine wirksame und echte Sicherheitsunion. Die Kommission unterstützt die Mitgliedstaaten und die lokalen Behörden bei der Verbesserung des Schutzes des öffentlichen Raums im Rahmen der Umsetzung des im Oktober 2017 verabschiedeten Aktionsplans und der *Partnership for Security in Public Spaces* [Partnerschaft für die Sicherheit im öffentlichen Raum], die im Januar 2019 im Zuge der Durchführung der EU-Städteagenda geschlossen wurde. Die betreffenden Städte haben sich an die Kommission

⁶³ Slowenien hat eine teilweise Umsetzung mitgeteilt. Spanien hat noch nicht mitgeteilt, dass es die Richtlinie umgesetzt hat (Stand: 17. Oktober 2019).

⁶⁴ Griechenland und Luxemburg haben noch nicht mitgeteilt, dass sie die Richtlinie umgesetzt haben. Polen hat eine teilweise Umsetzung mitgeteilt (Stand: 17. Oktober 2019).

⁶⁵ Belgien, Tschechien, Estland, Polen, Schweden, die Slowakei und das Vereinigte Königreich haben für einen Teil der neuen Vorschriften Umsetzungsmaßnahmen mitgeteilt. Zypern, Deutschland, Griechenland, Spanien, Luxemburg, Ungarn, Rumänien und Slowenien haben keinerlei Umsetzungsmaßnahmen mitgeteilt (Stand: 17. Oktober 2019).

⁶⁶ Slowenien hat eine teilweise Umsetzung mitgeteilt. Spanien hat noch nicht mitgeteilt, dass es die Richtlinie umgesetzt hat. Deutschland hat zwar die vollständige Umsetzung mitgeteilt, die Kommission sieht diese Umsetzung jedoch nicht als vollständig an (Stand: 17. Oktober 2019).

⁶⁷ Belgien, Bulgarien, Tschechien, Dänemark, Deutschland, Estland, Irland, Frankreich, Italien, Zypern, Lettland, Litauen, Ungarn, die Niederlande, Österreich, Polen, Rumänien, die Slowakei, Finnland, Schweden und das Vereinigte Königreich (Stand: 17. Oktober 2019).

⁶⁸ Belgien, Bulgarien, Tschechien, Deutschland, Estland, Griechenland, Spanien, Frankreich, Kroatien, Italien, Lettland, Litauen, Luxemburg, Ungarn, Malta, Österreich, Polen, Portugal, Rumänien, Slowenien, die Slowakei, Finnland und Schweden.

⁶⁹ Bulgarien, Italien, Portugal und Slowenien.

gewandt und um Unterstützung bei der Bewältigung der Probleme ersucht, mit denen sie im Zusammenhang mit dem Schutz des öffentlichen Raums konfrontiert waren.

Der Austausch bewährter Verfahren zwischen lokalen Behörden und mit privaten Betreibern ist für die Erhöhung der Sicherheit des öffentlichen Raums von entscheidender Bedeutung. Dieses Thema stand im Mittelpunkt der **European Week of Security** [Europäische Woche der Sicherheit], die vom 14. bis zum 18. Oktober 2019 in Nizza, Frankreich, stattfand und im Rahmen des von der EU finanzierten Projekts „*Protect Allied Cities against Terrorism in Securing Urban Areas*“ [Städtebündnis für den Schutz vor Terrorismus durch die Sicherung des städtischen Raums] organisiert wurde. Bei dieser Veranstaltung, zu der 500 Vertreter von Städten, nationalen Behörden und Forschungseinrichtungen aus ganz Europa zusammenkamen, wurden zum einen die Bedeutung einer engen Zusammenarbeit zwischen allen beteiligten Akteuren sowohl des öffentlichen als auch des privaten Sektors und zum anderen die Relevanz neuer Technologien für einen besseren Schutz der Städte hervorgehoben. Des Weiteren wurde der Schutz des öffentlichen Raums im Rahmen der **Europäischen Woche der Regionen und Städte**, die vom 7. bis zum 10. Oktober 2019 in Brüssel stattfand, bei einem Workshop zur Städteagenda für die EU-Partnerschaft für die Sicherheit im öffentlichen Raum thematisiert. Im Mittelpunkt standen dabei die Rolle der lokalen Behörden in der Sicherheitspolitik, die Vorschriften und Finanzierungsmöglichkeiten der EU für die Bewältigung der wichtigsten Herausforderungen im städtischen öffentlichen Raum sowie zentrale Themen, wie etwa Innovation durch intelligente Lösungen und Technologien, darunter auch das Konzept der eingebauten Sicherheit („security by design“), Prävention und soziale Inklusion. Einen weiteren Beitrag zur Förderung der Innovationskraft der Städte in diesen Bereichen leistete die Kommission mit der jüngsten Ausschreibungsrunde ihrer Initiative *Urban Innovative Actions*, deren Ergebnisse im August 2019 bekanntgegeben wurden. Im Rahmen eines der ausgewählten Projekte werden drei Städte (Piräus in Griechenland, Tampere in Finnland und Turin in Italien) neue Lösungen für Fragen der städtischen Sicherheit testen.⁷⁰

Um einen **besseren Schutz von Gotteshäusern** zu gewährleisten und die Bedürfnisse unterschiedlicher Religionsgemeinschaften zu eruieren, organisierte die Kommission am 7. Oktober 2019 ein Treffen mit Vertretern der jüdischen, muslimischen, christlichen und buddhistischen Gemeinschaften. Das Treffen war Teil der Umsetzung des EU-Aktionsplans für einen besseren Schutz des öffentlichen Raums aus dem Jahr 2017 und machte deutlich, dass hinsichtlich des Sicherheitsbewusstseins und der Abwehrbereitschaft erhebliche Unterschiede zwischen den einzelnen Religionsgemeinschaften bestehen und somit dem weiteren Austausch bewährter Verfahren große Bedeutung zukommt. Darüber hinaus wurde bei dem Treffen klar, dass die Einführung grundlegender Sicherheitsmaßnahmen und ein höheres Sicherheitsbewusstsein der Bewahrung der Offenheit und Zugänglichkeit von Gotteshäusern nicht entgegenstehen. Die Kommission wird auf ihrer elektronischen Expertenplattform bewährte Verfahren und Aufklärungsmaterial zusammenführen und die Sicherheitsbehörden der Mitgliedstaaten im Rahmen des öffentlich-privaten Forums für den Schutz des öffentlichen Raums auf diese Thematik aufmerksam machen.

Ein spezifischer Bereich, der weiterer Aufmerksamkeit bedarf, ist die wachsende Bedrohung der Sicherheit kritischer Infrastrukturen und des öffentlichen Raums durch **Drohnen**.

⁷⁰ Für die *Urban Innovative Actions* wird eine Kofinanzierung aus Mitteln des Europäischen Fonds für regionale Entwicklung gewährt. Weitere Informationen sind verfügbar unter: <https://www.uia-initiative.eu/en/call-proposals/4th-call-proposals>.

Ergänzend zur jüngsten EU-Rechtsvorschrift⁷¹ über den sicheren Betrieb von Drohnen in von bemannten Luftfahrzeugen genutztem Luftraum und ohne die Möglichkeiten einer sinnvollen Nutzung von Drohnen in Frage zu stellen, unterstützt die Kommission die Mitgliedstaaten bei der Beobachtung von Trends bei der böswilligen Nutzung von Drohnen, der Finanzierung einschlägiger Forschungsarbeiten und der Förderung der Erprobung von Abwehrmaßnahmen. Bei der hochrangigen internationalen Konferenz zur Abwehr der von unbemannten Luftfahrzeugsystemen ausgehenden Gefahren, die am 17. Oktober 2019 in Brüssel stattfand, wurde deutlich, dass der Austausch von Erfahrungen und bewährten Verfahren von entscheidender Bedeutung ist. Bei dieser von der Kommission organisierten Veranstaltung kamen 250 Vertreter aus Mitgliedstaaten, internationalen Organisationen, Drittländern, der Industrie, Hochschulen und der Zivilgesellschaft zusammen, um die mit Drohnen verbundenen Sicherheitsprobleme und die Möglichkeiten ihrer Bewältigung zu erörtern. Wie das Treffen zeigte, sind diesbezüglich regelmäßige Sicherheitsbewertungen und eine enge Zusammenarbeit zwischen Luftfahrt- und Strafverfolgungsbehörden bei der Weiterentwicklung der europäischen Rechtsvorschriften über den sicheren Betrieb von Drohnen erforderlich. Darüber hinaus besteht die Notwendigkeit einer weiteren Erprobung von Abwehrmaßnahmen gegen Drohnen im Rahmen eines koordinierten europäischen Ansatzes. Ferner bestand Einigkeit darüber, dass ein enges Zusammenwirken von Behörden und Industrie eine entscheidende Voraussetzung dafür darstellt, dass Drohnen sicher, zuverlässig im Betrieb und nur schwer zu missbräuchlichen Zwecken einsetzbar sind.

3. *Externe Dimension*

Da die meisten Sicherheitsrisiken, mit denen die Union konfrontiert ist, über ihre Außengrenzen hinausgehen und globale Bedrohungen darstellen, spielt die Zusammenarbeit mit Partnerländern, Organisationen und einschlägigen Interessenträgern für den Aufbau einer wirksamen und echten Sicherheitsunion eine entscheidende Rolle.

Der Austausch von Informationen ist für diese Zusammenarbeit von zentraler Bedeutung. Gemeinsam mit diesem Bericht hat die Kommission eine Empfehlung für einen Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen über ein **Abkommen zwischen der EU und Neuseeland über den Austausch personenbezogener Daten zwischen Europol und den zuständigen neuseeländischen Behörden zur Bekämpfung von schwerer Kriminalität und Terrorismus** angenommen. Durch ein solches Abkommen wird Europol befähigt, bei der Prävention und Bekämpfung der in seinen Zuständigkeitsbereich fallenden Straftaten enger mit den neuseeländischen Behörden zusammenzuarbeiten. Die im April 2019 zwischen Europol und der neuseeländischen Polizei geschlossene Arbeitsvereinbarung bietet einen Rahmen für eine strukturierte Zusammenarbeit auf strategischer Ebene, jedoch keine Rechtsgrundlage für den Austausch personenbezogener Daten. Der Austausch personenbezogener Daten unter uneingeschränkter Achtung des EU-Rechts und der Grundrechte ist für eine wirksame operative polizeiliche Zusammenarbeit unerlässlich. Auf der Grundlage der terroristischen Bedrohung, der migrationsbedingten Herausforderungen und des operativen Bedarfs von Europol hat die Kommission bereits acht vorrangige Länder in der Region Naher Osten/Nordafrika ermittelt, mit denen Verhandlungen

⁷¹ Durchführungsverordnung (EU) 2019/947 der Kommission vom 24. Mai 2019 über die Vorschriften und Verfahren für den Betrieb unbemannter Luftfahrzeuge.

aufgenommen werden sollten.⁷² Angesichts des operativen Bedarfs der Strafverfolgungsbehörden in der EU und der möglichen Vorteile einer engeren Zusammenarbeit in diesem Bereich, wie sie auch im Nachgang des Anschlags von Christchurch vom März 2019 deutlich wurden, hält es die Kommission für erforderlich, auch Neuseeland als vorrangiges Land zu betrachten und in Kürze Verhandlungen aufzunehmen.

Ein weiterer Eckpfeiler der Sicherheitskooperation der Union mit Drittländern ist die Übermittlung von **Fluggastdatensätzen**. Am 27. September 2019 nahm die Kommission eine Empfehlung für einen Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen über ein Abkommen zwischen der **EU und Japan** über die Übermittlung von Fluggastdatensätzen zur Verhütung und Bekämpfung von Terrorismus und anderer grenzübergreifender schwerer Kriminalität unter uneingeschränkter Achtung von Datenschutzgarantien und der Grundrechte an.⁷³ Die Empfehlung wird derzeit im Rat auf Arbeitsgruppenebene geprüft, und die Kommission fordert den Rat auf, ihr zeitnah ein Mandat für Verhandlungen mit Japan zu erteilen. Mit Blick auf die Sicherheit bei den Olympischen Spielen 2020 wäre der rechtzeitige Abschluss einschlägiger Abkommen ein großer Gewinn.

Auf globaler Ebene unterstützt die Kommission die **Internationale Zivilluftfahrt-Organisation** bei der Festlegung einer Norm für die Verarbeitung von Fluggastdatensätzen. Damit kommt sie einer Forderung des Sicherheitsrates der Vereinten Nationen nach, der in seiner Resolution 2396 alle Mitgliedstaaten der Vereinten Nationen aufgefordert hat, Kapazitäten zur Sammlung, Verarbeitung und Analyse von Daten aus Fluggastdatensätzen aufzubauen. Am 13. September 2019 legte die Kommission einen Vorschlag⁷⁴ für einen Beschluss des Rates über den Standpunkt vor, der im Namen der EU bei der Internationalen Zivilluftfahrt-Organisation im Hinblick auf Richtlinien und Empfehlungen für Fluggastdatensätze zu vertreten ist. Der Vorschlag wird gegenwärtig im Rat auf Arbeitsgruppenebene geprüft, und die Kommission fordert den Rat auf, zeitnah einen Beschluss zu fassen. Der Standpunkt der Union und ihrer Mitgliedstaaten wurde zudem in einem Informationspapier über die Normen und Grundsätze für die Sammlung, die Verwendung, die Verarbeitung und den Schutz von Fluggastdatensätzen dargelegt, das auf der 40. Tagung der Versammlung der Internationalen Zivilluftfahrt-Organisation vorgelegt wurde.

Was die Ausarbeitung eines neuen Abkommens über Fluggastdatensätze mit **Kanada** betrifft, so strebt die Kommission eine rasche Einigung an. Mittlerweile begannen in diesem Sommer die gemeinsame Überprüfung und Evaluierung des Abkommens über Fluggastdatensätze mit **Australien** sowie die gemeinsame Evaluierung des Abkommens über Fluggastdatensätze mit den **Vereinigten Staaten** mit Besuchen in Canberra und Washington im August bzw. September 2019. Die Kommission unterrichtete den Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments am 14. Oktober 2019 in einer Sitzung unter Ausschluss der Öffentlichkeit über den Stand der Abkommen mit Japan, Australien und Kanada über Fluggastdatensätze.

⁷² Siehe die Mitteilung „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Elfter Fortschrittsbericht“ (COM(2017) 608 final vom 18.10.2017). Die vorrangigen Länder sind Algerien, Ägypten, Israel, Jordanien, Libanon, Marokko, Tunesien und die Türkei.

⁷³ COM(2019) 420 final vom 27.9.2019.

⁷⁴ COM(2019) 416 final vom 13.9.2019.

Fortschritte gibt es auch bei der sicherheitspolitischen Zusammenarbeit mit den **westlichen Balkanstaaten** im Rahmen der Umsetzung des Gemeinsamen Aktionsplans zur Terrorismusbekämpfung für den westlichen Balkan vom Oktober 2018. Am 9. Oktober unterzeichnete die Kommission mit Albanien und der Republik Nordmazedonien nicht verbindliche bilaterale Vereinbarungen zur Terrorismusbekämpfung.⁷⁵ In diesen Vereinbarungen ist festgelegt, welche gezielten vorrangigen Maßnahmen bezüglich der fünf Zielsetzungen des gemeinsamen Aktionsplans⁷⁶ von den Behörden der einzelnen Partnerländer zu ergreifen sind und welche Unterstützung die Kommission dabei zu leisten beabsichtigt. Mit den übrigen westlichen Balkanstaaten werden voraussichtlich in den nächsten Wochen ähnliche Vereinbarungen unterzeichnet. Darüber hinaus schlossen die Kommission und Montenegro am 7. Oktober 2019 eine Vereinbarung über die Zusammenarbeit zwischen Montenegro und der Europäischen Agentur für die Grenz- und Küstenwache (Frontex) im Bereich des Grenzmanagements. Diese Vereinbarung ermöglicht es der Agentur, Montenegro beim Grenzmanagement zu unterstützen, um die irreguläre Migration und grenzüberschreitende Kriminalität zu bekämpfen und so die Sicherheit an der Außengrenze der EU zu verbessern.

Um die Zusammenarbeit mit den Partnerländern bei der Bewältigung gemeinsamer Sicherheitsbedrohungen zu verbessern, fordert die Kommission den Rat auf,

- den Beschluss über die Ermächtigung zur Aufnahme von Verhandlungen über ein Abkommen zwischen der EU und **Neuseeland** über den Austausch personenbezogener Daten zur Bekämpfung von schwerer Kriminalität und Terrorismus anzunehmen;
- den Beschluss über die Ermächtigung zur Aufnahme von Verhandlungen über ein Abkommen zwischen der EU und **Japan** über den Austausch personenbezogener Daten anzunehmen;
- den vorgeschlagenen **Beschluss des Rates über den Standpunkt, der im Namen der EU bei der Internationalen Zivilluftfahrt-Organisation** im Hinblick auf Richtlinien und Empfehlungen für Fluggastdatensätze zu vertreten ist, anzunehmen.

VI. FAZIT

In diesem Bericht wird das breite Spektrum der Maßnahmen aufgezeigt, welche die EU ergriffen hat, um in Europa gegen gemeinsame Bedrohungen vorzugehen und die kollektive Sicherheit zu verbessern. Auf der Grundlage der gemeinsamen Überzeugung, dass die gegenwärtigen Herausforderungen im Bereich der Sicherheit am besten durch die Zusammenarbeit zwischen den Mitgliedstaaten und mit Drittländern bewältigt werden können, sind die auf dem Weg zu einer wirksamen und echten Sicherheitsunion erzielten Fortschritte das Ergebnis einer engen Zusammenarbeit zwischen zahlreichen unterschiedlichen Akteuren, die Vertrauen aufbauen, ihre Ressourcen gemeinsam nutzen und Bedrohungen geschlossen entgegnetreten: auf allen Regierungsebenen, von Städten und anderen lokalen Akteuren über Regionen und nationale Behörden bis hin zur EU-Ebene mit dem Europäischen Parlament und dem Rat, unter Einbindung von Behörden, EU-Agenturen,

⁷⁵ https://ec.europa.eu/home-affairs/news/news/20191009_security-union-implementing-counter-terrorism-arrangements-albania-north-macedonia_en

⁷⁶ Der gemeinsame Aktionsplan sieht Maßnahmen für die folgenden fünf Zielsetzungen vor: ein solider Rahmen für die Terrorismusbekämpfung; wirksame Prävention und Bekämpfung von gewaltbereitem Extremismus; effektiver Informationsaustausch und wirksame operative Zusammenarbeit; Aufbau von Kapazitäten zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung; Verbesserung des Schutzes der Bürger und der Infrastruktur.

privaten Akteuren und der Zivilgesellschaft und unter Verwendung von Fachwissen, Instrumenten und Ressourcen in unterschiedlichen Politikbereichen, wie etwa der Verkehrspolitik, dem digitalen Binnenmarkt und der Kohäsionspolitik. Bei allen im Zusammenhang mit der Sicherheitsunion ergriffenen Maßnahmen sind der Schutz der Grundrechte sowie der Schutz und die Förderung unserer Werte von entscheidender Bedeutung.

Die Bemühungen um eine wirksame und echte Sicherheitsunion müssen fortgesetzt werden. Über wichtige anhängige Initiativen muss zeitnah eine Einigung erzielt werden; hierzu zählen insbesondere: 1) der Legislativvorschlag über die Entfernung terroristischer Online-Inhalte, 2) der Legislativvorschlag über die Verbesserung des Zugangs der Strafverfolgungsbehörden zu elektronischen Beweismitteln, 3) der Legislativvorschlag über die Errichtung eines Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung sowie eines Netzes nationaler Koordinierungszentren und 4) die anhängigen Legislativvorschläge über solidere und intelligentere Informationssysteme in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung. Die vereinbarten Maßnahmen und Instrumente müssen vor Ort verwirklicht werden, wobei alle Mitgliedstaaten die EU-Rechtsvorschriften zeitnah und vollständig umsetzen müssen, um deren sicherheitsrelevante Vorteile vollständig auszuschöpfen. Insbesondere ist es von entscheidender Bedeutung, dass alle Mitgliedstaaten die kürzlich verabschiedeten Rechtsvorschriften über die Interoperabilität der EU-Informationssysteme in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung umsetzen, um das ehrgeizige Ziel einer vollständigen Interoperabilität bis 2020 zu erreichen. Schließlich muss Europa wachsam gegenüber aufkommenden und sich ändernden Bedrohungen bleiben und auch weiterhin gemeinsam auf die Erhöhung der Sicherheit aller Bürger hinwirken.