Rat der
Europäischen Union

Brüssel, den 14. Dezember 2020
(OR. en)

14019/20

JAI 1110	**DROIPEN 124**
COSI 250	**COPEN 384**
ENFOPOL 348	**FREMP 146**
ENFOCUSTOM 142	**JAIEX 119**
IXIM 138	**CFSP/PESC 1121**
CT 118	**COPS 478**
CRIMORG 119	**HYBRID 46**
FRONT 345	**DISINFO 47**
ASIM 95	**TELECOM 264**
VISA 139	**DIGIT 151**
CYBER 278	**COMPET 633**
DATAPROTECT 151	**RECH 522**
CATS 104	

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	10. Dezember 2020
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2020) 797 final
Betr.:	MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT Erster Fortschrittsbericht zur EU-Strategie für die Sicherheitsunion

Die Delegationen erhalten in der Anlage das Dokument COM(2020) 797 final.

Anl.: COM(2020) 797 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 9.12.2020
COM(2020) 797 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

Erster Fortschrittsbericht zur EU-Strategie für die Sicherheitsunion

I EINLEITUNG

Das Thema Sicherheit spielt für die Bürgerinnen und Bürger eine zentrale Rolle. Die jüngsten auf europäischem Boden begangenen Terroranschläge haben zusätzlich verdeutlicht, dass auf EU-Ebene Handlungsbedarf besteht. Am 24. Juli 2020 nahm die Kommission die **EU-Strategie für die Sicherheitsunion für den Zeitraum 2020 bis 2025**[1] an, die gezielte Maßnahmen in Schwerpunktbereichen vorsieht, in denen die EU einen Mehrwert gegenüber einzelstaatlichen Anstrengungen erbringen kann. Die Strategie baut auf den Fortschritten auf, die im Rahmen der Europäischen Sicherheitsagenda für den Zeitraum 2015 bis 2020[2] erzielt wurden, und setzt neue Schwerpunkte, durch die sichergestellt werden soll, dass die Sicherheitspolitik der EU der sich wandelnden Bedrohungslage Rechnung trägt, dass langfristige, nachhaltige Widerstandsfähigkeit aufgebaut wird, dass die Organe und Einrichtungen der EU, die Regierungen, der Privatsektor und Einzelpersonen in einen gesamtgesellschaftlichen Sicherheitsansatz eingebunden werden und dass die vielen verschiedenen Politikbereiche mit direkten Auswirkungen auf die Sicherheit zusammengebracht werden. Im Mittelpunkt steht dabei die uneingeschränkte Achtung der Grundrechte, da die Sicherheit der Union nur gewährleistet werden kann, wenn sich die Bürgerinnen und Bürger darauf verlassen können, dass ihre Grundrechte in vollem Umfang gewahrt bleiben.

Die Bedrohung durch transnationale Terrornetzwerke ruft uns eindringlich in Erinnerung, dass ein koordiniertes Vorgehen der EU unerlässlich ist, um die Europäerinnen und Europäer wirksam zu schützen und unsere gemeinsamen Werte und unsere europäische Lebensweise zu wahren. Sie ist ein Beispiel dafür, wie immer komplexere grenz- und sektorübergreifende Sicherheitsbedrohungen entstanden sind, die eine engere Zusammenarbeit im Sicherheitsbereich auf allen Ebenen wichtiger denn je machen. Dies gilt für die organisierte Kriminalität oder den Drogenhandel, aber auch für die digitale Welt, in der Cyberangriffe und Cyberkriminalität weiter zunehmen. All diese Herausforderungen machen nicht an unseren Grenzen halt und sind Ausdruck eines engen Zusammenhangs zwischen der inneren und der äußeren Sicherheit. Die COVID-19-Krise hat auch die europäische Sicherheit stärker ins Blickfeld gerückt und die Widerstandsfähigkeit der kritischen Infrastrukturen, der Krisenvorsorge, der strategischen Wertschöpfungsketten und der Krisenmanagementsysteme Europas sowie die Widerstandsfähigkeit unserer Gesellschaften gegenüber Manipulationsversuchen und gezielter Desinformation auf den Prüfstand gestellt.

Die Strategie für die Sicherheitsunion besteht aus vier strategischen Prioritäten für Maßnahmen auf EU-Ebene: ein zukunftsfähiges Sicherheitsumfeld, die Bewältigung sich wandelnder Bedrohungen, der Schutz der Europäerinnen und Europäer vor Terrorismus und organisierter Kriminalität und eine starke europäische Sicherheitsgemeinschaft. Im Mittelpunkt der Strategie steht die Umsetzung, die auch zentrales Thema dieses Berichts ist: eine Umsetzung, die die uneingeschränkte Mitwirkung der nationalen Behörden erfordert, die bei der Aufrechterhaltung der Sicherheit in der EU an vorderster Front stehen. Dieser Bericht ist der erste im Rahmen der Strategie vorgelegte Umsetzungsbericht, mit dem die Kommission der von ihr eingegangenen Verpflichtung nachkommt, regelmäßig über die Fortschritte Bericht zu erstatten[3]. Er deckt den Zeitraum

---

1 COM(2020) 605.
2 COM(2016) 230.
3 Während der Anhörung von Vizepräsident Schinas vor dem Europäischen Parlament am 3.10.2019.

seit dem 31. Oktober 2019 ab, als der letzte Fortschrittsbericht zur Sicherheitsunion im Rahmen des vorherigen Mandats der Kommission veröffentlicht wurde[4].

II EIN ZUKUNFTSFÄHIGES SICHERHEITSUMFELD

1. *Schutz und Widerstandsfähigkeit kritischer Infrastruktur*

Die Bürgerinnen und Bürger sind in ihrem Alltag auf physische und digitale Infrastrukturen angewiesen, die von einer zunehmenden Vernetzung und Interdependenz geprägt sind. Diese Infrastrukturen sind für das Funktionieren der Wirtschaft und der Gesellschaft von entscheidender Bedeutung. Ohne zuverlässige Energieversorgung, planbaren Verkehr, umfassende Gesundheitssysteme oder ein digital gestütztes Finanznetz wäre unsere derzeitige Lebensweise nicht möglich. Die COVID-19-Pandemie hat noch eindringlicher gezeigt, wie wichtig es ist, die **Widerstandsfähigkeit kritischer Sektoren und Akteure zu gewährleisten**. Die EU hat anerkannt, dass der Schutz kritischer Infrastrukturen vor Bedrohungen, seien es natürliche oder von Menschen verursachte Katastrophen oder Terroranschläge, im Interesse aller ist. Die aktuelle Bedrohungslage für kritische Infrastrukturen ist breit gefächert. Hierzu zählen: Terrorismus, hybride Aktionen, Cyberangriffe, durch Insider verursachte Vorfälle; Bedrohungen im Zusammenhang mit neuen und aufkommenden Technologien (wie Drohnen, 5G, künstliche Intelligenz); Herausforderungen im Zusammenhang mit dem Klimawandel; Unterbrechung der Lieferketten; und Einmischung in Wahlen. Unsere derzeitigen Vorschriften müssen modernisiert und erweitert werden[5]. Ihr Schwerpunkt muss sich vom Schutz hin zur Widerstandsfähigkeit verlagern, indem die sektorale Abdeckung kohärenter und einheitlicher gestaltet wird und kritische Unternehmen, die wesentliche Dienstleistungen erbringen, in den Vordergrund rücken.

Dies wird das Ziel der künftigen Vorschläge zur Förderung der Widerstandsfähigkeit **physischer und digitaler Infrastrukturen** sein. Allgemein geht es darum, die Vorsorge auf nationaler und EU-Ebene durch den Aufbau robuster Fähigkeiten zur Verhütung, Erkennung, Abwehr und Abschwächung von Bedrohungen zu verbessern und im Krisenfall handlungsfähig zu sein. Durch die bestehenden Rechtsvorschriften ist es bereits gelungen, das Risikomanagement in kritischen Sektoren zu stärken und zu verbessern; hier muss noch nachgelegt werden. Ein zentrales Ziel der überarbeiteten Richtlinie zum Schutz kritischer Infrastrukturen wird darin bestehen, ein hohes gemeinsames Maß an Widerstandsfähigkeit in einer ausreichenden Zahl von Schlüsselsektoren zu fördern. Ebenso wird die Aktualisierung der Richtlinie über Netz- und Informationssysteme (NIS) auf mehr Kohärenz bei der Ermittlung der Betreiber wesentlicher Dienste durch die Mitgliedstaaten abzielen[6]. Generell sind die Fähigkeiten der Mitgliedstaaten im Bereich der Cybersicherheit trotz erheblicher Fortschritte immer noch unterschiedlich ausgeprägt, weshalb durch die Überarbeitung eine Stärkung der Cybersicherheit allgemein angestrebt

---

4 COM(2019) 552.

5 Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern (ABl. L 345 vom 23.12.2008, S. 75). und Richtlinie (EU) 2016/1148 des europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

6 COM(2019) 546. Die Kommission hat außerdem eine öffentliche Konsultation (7. Juli bis 2. Oktober 2020) und Länderbesuche in allen Mitgliedstaaten durchgeführt, um durch Treffen mit Betreibern und nationalen Behörden die Konformität bei der Umsetzung der Richtlinie zu überprüfen.

wird[7]. Daraus werden umfassendere und kohärentere Ansätze für die Widerstandsfähigkeit der physischen und digitalen Infrastruktur hervorgehen.

Während die Arbeiten an diesem kohärenteren Rahmen voranschreiten, setzen ergänzende **sektorspezifische Initiativen** gezielt an spezifischen Schwachstellen an. Die besonderen Herausforderungen, die das Thema der Cybersicherheit für den Energiesektor darstellt, werden nun auf der Grundlage der Empfehlung der Kommission aus dem Jahr 2019 angegangen[8], wobei die Merkmale des Sektors wie die Echtzeitanforderungen, das Risiko von Kaskadeneffekten und die Kombination von herkömmlichen und neuen Technologien berücksichtigt werden. Derzeit wird an einem speziellen Netzkodex zur Cybersicherheit für grenzüberschreitende Stromflüsse sowie zum Schutz der Widerstandsfähigkeit und Cybersicherheit kritischer Energieinfrastrukturen gearbeitet. Das Thematische Netz für den Schutz kritischer Energieinfrastrukturen (Thematic Network on Critical Energy Infrastructure Protection) wurde ebenfalls neu aufgelegt und mit neuen Schwerpunkten und Zielen versehen und hielt sein erstes Treffen im Juni 2020 mit mehr als 100 Online-Teilnehmern ab. Dieses Netz bietet eine Plattform zur Förderung der grenzüberschreitenden Zusammenarbeit zwischen den Betreibern kritischer Energieinfrastrukturen und den Eigentümern im Energiesektor.

Um eine gemeinsame Grundlage für die Zusammenarbeit der Mitgliedstaaten bei der **Risikovorsorge im Elektrizitätssektor** zu schaffen, hat das Europäische Netz der Fernleitungsnetzbetreiber im September 2020 das wichtigste regionale Szenario für Stromversorgungskrisen gemäß der Verordnung über die Risikovorsorge vorgelegt[9]. Dieses Szenario umfasst (Cyber-)Angriffe sowie Pandemien und extreme Wetterereignisse. Die Mitgliedstaaten werden nationale Krisenszenarien und Risikovorsorgepläne ausarbeiten, um Stromversorgungskrisen vorzubeugen und einzudämmen (erste Entwürfe sollen im April 2021 vorgelegt werden). Als Beitrag zu diesem Prozess wurde im Juni 2020 ein Katalog bewährter Verfahren herausgegeben[10], der auf der engmaschigen Überwachung der Auswirkungen von COVID-19 auf den Energiesektor durch die Koordinierungsgruppen „Strom“, „Erdgas“ und „Öl“ sowie die Gruppe der europäischen Aufsichtsbehörden für nukleare Sicherheit (ENSREG) und die EU-Gruppe der für Offshore-Erdöl- und Erdgasaktivitäten zuständigen Behörden (EUOAG) basiert.

Die zunehmende und komplexe Abhängigkeit von digitalen Prozessen bei der Erbringung von Finanzdienstleistungen erfordert auch eine Verbesserung der Cybersicherheit im **Finanzsektor**. Die Sicherheit der IKT-Systeme ist zwar anerkannter Bestandteil des Risikomanagements von Finanzunternehmen, doch hat sich dies in der EU-Regulierungslandschaft für Finanzdienstleistungen noch nicht in vollem Umfang niedergeschlagen. Am 24. September 2020 hat die Kommission ihr Digitales Finanzpaket samt einer digitalen Finanzstrategie angenommen[11], mit dem klar formulierten Ziel, die mit dem digitalen Wandel einhergehenden Herausforderungen anzugehen sowie die Widerstandsfähigkeit, den Datenschutz und eine angemessene Aufsicht zu fördern. Dazu gehört auch ein Legislativvorschlag zur Betriebsstabilität digitaler Systeme[12], der

---

7 COM(2019) 546.
8 C(2019) 2400.
9 ABl. L 158 vom 14.6.2019, S. 1.
10 Energieversorgungssicherheit: good practices to address pandemic risks [Energieversorgungssicherheit: Bewährte Verfahren zur Bekämpfung von Pandemie-Risiken) (SWD(2020) 104].
11 https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en.
12 COM(2020) 595.

sicherstellen soll, dass Sicherheitsvorkehrungen zur Eindämmung von Cyberangriffen und anderer Risiken getroffen werden[13]. Diese Initiative trägt zu einem starken und dynamischen digitalen Finanzsektor in Europa bei und verbessert damit die Fähigkeit Europas, seine strategische Autonomie im Finanzdienstleistungssektor und weitergehend auch seine Fähigkeit zur Regulierung und Beaufsichtigung des Finanzsystems zu stärken, und damit die Stabilität des europäischen Finanzsystems zu schützen.

In Notsituationen großen Ausmaßes erfordert die hohe wechselseitige Abhängigkeit zwischen Sektoren und Ländern ein koordiniertes Vorgehen, um in Zukunft eine rasche und wirksame Reaktion sowie eine bessere Prävention und Vorsorge in ähnlichen Situationen zu gewährleisten. Bei der Überarbeitung des Beschlusses über das Katastrophenschutzverfahren der Union[14] hat die Kommission vorgeschlagen, **Ziele für Katastrophenresilienz** und eine **Resilienzplanung** auszuarbeiten[15] und dabei den Schwerpunkt verstärkt auf den Aufbau längerfristiger sektorübergreifender Widerstandsfähigkeit gegenüber grenzüberschreitenden Katastrophen zu setzen. Mit dem vorgeschlagenen neuen Ansatz für den Aufbau von Widerstandsfähigkeit werden die nationalen Maßnahmen im Bereich des Katastrophenrisikomanagements ergänzt. Auf der Grundlage des Kommissionsvorschlags vom 2. Juni 2020[16] hat der Rat am 26. November eine Einigung über ein Verhandlungsmandat zur Stärkung der Katastrophenprävention, -vorsorge und -reaktion erzielt.

Die COVID-19-Pandemie hat gezeigt, welche Auswirkungen Gesundheitskrisen auf die Sicherheit in der EU und weltweit haben können, und verdeutlicht, dass die Bereitschafts- und Reaktionsplanung für Epidemien und andere schwerwiegende grenzüberschreitende Gesundheitsbedrohungen intensiviert werden muss. Im Paket der Kommission vom 11. November 2020 zum Thema „**Schaffung einer europäischen Gesundheitsunion**: Die Resilienz der EU stärken“ werden die nächsten Schritte zur Bewältigung grenzübergreifender Gesundheitsbedrohungen dargelegt. Das Paket, mit dem ein verstärkter Rahmen für die grenzüberschreitende Zusammenarbeit bei allen Gesundheitsbedrohungen geschaffen würde, enthält drei Legislativvorschläge zur: Verbesserung der Rechtsvorschriften zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren sowie Stärkung des Europäischen Zentrums für die Prävention und die Kontrolle von Krankheiten (ECDC) und der Europäischen Arzneimittel-Agentur (EMA). Zusammen werden diese Vorschläge einen soliden und kosteneffizienten Rahmen herbeiführen, der die EU und ihre Mitgliedstaaten beim Umgang mit künftigen Gesundheitskrisen auf eine sicherere Grundlage stellt.

Ein wesentliches Element zum Schutz wichtiger digitaler Vermögenswerte der EU und der Mitgliedstaaten besteht darin, für kritische Infrastrukturen einen Kanal für **sichere Kommunikation** bereitzustellen. Unterstützt wird dies durch die Entwicklung einer Netzinfrastruktur für eine sichere und widerstandsfähige staatliche Satellitenkommunikation als Bestandteil des EU-Weltraumprogramms.

---

[13] Der Vorschlag bietet eine kohärente Ausgangsbasis für die Anforderungen an das IKT-Risikomanagement, die Meldung von IKT-Vorfällen an die Finanzaufsichtsbehörden, digitale Tests und den Austausch von Informationen. Darüber hinaus sieht der Vorschlag vor, dass kritische IKT-Drittanbieter einem Aufsichtsrahmen auf europäischer Ebene unterstellt werden.

[14] Beschluss Nr. 1313/2013/EU vom 17. Dezember 2013 über ein Katastrophenschutzverfahren der Union.

[15] COM(2020) 220.

[16] Vorschlag zur Änderung des Beschlusses Nr. 1313/2013/EU über ein Katastrophenschutzverfahren der Union – Mandat für Verhandlungen mit dem Europäischen Parlament.

2. ***Cybersicherheit***

Die Vorteile des digitalen Wandels sind ebenso eindeutig wie die Tatsache, dass ein solcher Wandel zwangsläufig mit einer Zunahme potenzieller Schwachstellen einhergeht[17]. Kritische Infrastrukturen sind häufig das Ziel von Cyberangriffen, die zunehmend komplexer werden[18]. **Cybersicherheit** sollte daher nicht nur ein Anliegen der politischen Entscheidungsträger sein, sondern auch im Bewusstsein all jener verankert werden, die online arbeiten oder kommunizieren.

Um das Vertrauen in digitale Produkte, Verfahren und Dienste und deren Sicherheit zu stärken, wurde mit dem Rechtsakt zur Cybersicherheit vom Juni 2019 ein **EU-Rahmen für die Cybersicherheitszertifizierung** geschaffen. Die Kommission hat die EU-Agentur für Cybersicherheit (ENISA) aufgefordert, zwei Systeme für die Cybersicherheitszertifizierung zu erstellen, deren Ausarbeitung mittlerweile bereits weit fortgeschritten ist. An dieser Arbeit sind auch nationale Behörden für die Cybersicherheitszertifizierung, die Industrie, Verbraucher, Akkreditierungs-, Normungs- und Zertifizierungsstellen sowie der Europäische Datenschutzausschuss beteiligt.

Eines dieser Systeme ist ein System für **Cloud-Dienste**, das einen sicheren und vertrauenswürdigen Markt in diesem Bereich fördern soll, ein zentrales Element der im Februar 2020 angenommenen **europäischen Datenstrategie**[19]. Dadurch würde sektorübergreifend eine gemeinsame Sicherheitsbasis für Cloud-Dienste geschaffen, die auf dem größten gemeinsamen Nenner der bestehenden (europäischer und internationaler) Normen, Systeme und Verfahren aufbaut und ein wesentliches Element des freien Datenflusses in der EU bilden wird[20]. Außerdem wird das System die Einführung von

---

17 ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected (Bedrohungslandschaft 2020: Cyberangriffe werden immer komplexer, gezielter, stärker verbreitet und weniger entdeckt).

18 Seit Ausbruch der Pandemie haben die EU-Agenturen und die Mitgliedstaaten einen erheblichen Anstieg der Cyberangriffe, auch auf den Gesundheitssektor, registriert.

19 COM(2020) 66.

20 Verordnung (EU) 2018/1807.

Cloud-Technologien fördern, indem es den Cloud-Nutzern, insbesondere kleinen und mittleren Unternehmen und der öffentlichen Verwaltung, nachvollziehbare Garantien hinsichtlich des Sicherheitsniveaus bietet.

Wie in der Strategie für die Sicherheitsunion betont wird, könnten die Folgen von systemischen und umfangreichen Störungen vor dem Hintergrund des derzeitigen Aufbaus der 5G-Infrastruktur in der EU und der möglichen Abhängigkeit vieler wesentlicher Dienste von 5G-Netzen besonders gravierend ausfallen. Aus dieser Erkenntnis resultierten gemeinsame Bemühungen der Mitgliedstaaten, angemessene Sicherheitsmaßnahmen zu entwickeln und einzuführen. Entsprechend der Empfehlung der Kommission vom März 2019 zur **Cybersicherheit der 5G-Netze**[21] führten die Mitgliedstaaten nationale Risikobewertungen durch, die in einen EU-weit koordinierten Risikobewertungsbericht[22] mündeten, in dem die mit 5G-Netzen verbundenen Sicherheitsherausforderungen ermittelt wurden. Auf dieser Grundlage veröffentlichte die NIS-Kooperationsgruppe[23] am 29. Januar 2020 das **EU-Instrumentarium der Risikominderungsmaßnahmen**[24], in dem die erforderlichen strategischen und technischen Maßnahmen dargelegt werden. Das Instrumentarium umfasst Maßnahmen zur Verschärfung der Sicherheitsanforderungen für Mobilfunknetzbetreiber, zur Gewährleistung der Anbietervielfalt für einzelne Mobilfunknetzbetreiber, zur Bewertung des Risikoprofils der Anbieter und zur Anwendung von Beschränkungen für Anbieter, die als mit einem hohen Risiko behaftet gelten. Die Kommission wird die Umsetzung des Instrumentariums unterstützen und dabei in vollem Umfang die ihr zur Verfügung stehenden Kompetenzen und Mittel[25] nutzen, darunter Telekommunikations- und Cybersicherheitsvorschriften, die Koordinierung im Bereich der Normung sowie der EU-weiten Zertifizierung und den EU-Rahmen für die Überprüfung ausländischer Direktinvestitionen[26].

Die NIS-Kooperationsgruppe veröffentlichte im Juli 2020 einen Fortschrittsbericht über die Umsetzung der Maßnahmen des Instrumentariums[27]. Darin wurde festgestellt, dass eine große Mehrheit der Mitgliedstaaten die im Instrumentarium empfohlenen Maßnahmen bereits übernommen hat oder derzeit umsetzt. Zu den Maßnahmen, deren Umsetzung weniger weit fortgeschritten war, gehörten die Verringerung des Risikos der Abhängigkeit von Lieferanten, die mit einem hohen Risiko behaftet sind, und die Entwicklung von herstellerneutralen Strategien sowohl auf Unternehmensebene als auch auf nationaler Ebene.

In den letzten Monaten reagierten die EU-Einrichtungen und die Mitgliedstaaten auf das im Zuge der **COVID-19-Krise** erhöhte Cybersicherheitsrisiko, indem sie den Informationsaustausch intensivierten und die Vorsorge für potenzielle Cyberkrisen

---

21 COM(2019) 2335.

22 Bericht zur EU-weit koordinierte Risikobewertung der Cybersicherheit in 5G-Netzen.

23 Die NIS-Kooperationsgruppe wurde eingerichtet, um die strategische Zusammenarbeit und den Informationsaustausch zwischen den EU-Mitgliedstaaten im Bereich der Cybersicherheit zu gewährleisten.

24 https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

25 COM(2020) 50.

26 Verordnung (EU) 2019/452. Darin wird ausdrücklich auch auf „kritische Infrastrukturen“ (sowie „kritische Technologien“) im weiteren Sinne als „Faktoren, die von den Mitgliedstaaten oder der Kommission bei der Bewertung der potenziellen Auswirkungen einer Investition berücksichtigt werden können“ Bezug genommen.

27 Bericht über die Fortschritte der Mitgliedstaaten bei der Umsetzung des EU-Instrumentariums für 5G-Cybersicherheit.

ausbauten. Die Zusammenarbeit auf EU-Ebene wurde in wichtigen Foren (NIS-Kooperationsgruppe und Computer-Notfallteams (CSIRTs)-Netz) sowie durch neue Formen der Koordinierung und Instrumente des Informationsaustauschs[28] vertieft. Im September 2020 fand eine zweite Planübung statt, die Blueprint Operational Level Exercise (Blue OLEx)[29], bei der auch das „Cyber Crisis Liaison Organisation Network" (CyCLONe) der Mitgliedstaaten ins Leben gerufen wurde, das den Plan für schnelle Notfallmaßnahmen bei umfangreichen, grenzüberschreitenden Cybervorfällen oder -krisen[30] weiter umsetzen soll.

Im globalen Cyberspace gehen Cyberangriffe und -bedrohungen häufig von außerhalb der EU aus. Um diesen Herausforderungen wirksam zu begegnen, arbeiten die EU und die Mitgliedstaaten gemeinsam daran, die internationale Sicherheit und Stabilität im Cyberraum voranzubringen, verantwortungsvolles staatliches Handeln zu fördern, die globale Widerstandsfähigkeit zu erhöhen und das Bewusstsein für Cyberbedrohungen und böswillige Cyberaktivitäten zu schärfen, auch bei internationalen Partnern[31]. Am 30. April 2020 veröffentlichte der Hohe Vertreter im Namen der EU eine Erklärung, in der er böswillige Handlungen im Cyberraum verurteilte und seine Solidarität mit den Opfern zum Ausdruck brachte[32].

Am 30. Juli 2020 beschloss der Rat **erstmals Cybersanktionen der EU** gegen sechs natürliche Personen und drei Organisationen, die für Cyberangriffe verantwortlich oder daran beteiligt waren. Dazu zählen der versuchte Cyberangriff auf die Organisation für das Verbot chemischer Waffen (OVCW) und die in der Öffentlichkeit unter den Namen „WannaCry", „NotPetya" und „Operation Cloud Hopper" bekannt gewordenen Angriffe. Am 22. Oktober 2020 verhängte der Rat Sanktionen gegen zwei weitere natürliche Personen und eine Organisation, die für den Cyberangriff auf den Deutschen Bundestag verantwortlich oder daran beteiligt waren. Diesen Beschlüsse waren mehrfache Warnungen der EU und Mitgliedstaaten vorausgegangen, dass man böswillige Cyberaktivitäten verhindern, davon abschrecken und auf sie reagieren müsse, unter anderem durch gezielte

---

28 Die Organe und Einrichtungen der EU kamen in einer COVID-19-Taskforce zusammen und riefen eine Reihe wöchentlicher Berichte mit dem Titel „Sectorial Situational Awareness and Analysis" (sektorspezifische Lagebeurteilung und -analyse) ins Leben. Die ENISA und Europol starteten Kampagnen über Möglichkeiten zur Aufrechterhaltung der Cybersicherheit während der COVID-19-Pandemie. Das CERT-EU gab Leitlinien für die Einrichtung sicherer VPNs heraus. Im Sommer 2019 richtete die Kooperationsgruppe einen neuen Arbeitsbereich zur Cybersicherheit im Gesundheitswesen ein, und die Kommission und die ENISA riefen das EU Health Information Sharing and Analysis Centre (Europäisches Zentrum für Informationsaustausch und Analysen im Gesundheitswesen) ins Leben.

29 https://www.enisa.europa.eu/news/enisa-news/blue-olex-2020-the-european-union-member-states-launch-the-cyber-crisis-liaison-organisation-network-cyclone.

30 C(2017) 6100.

31 Die EU fördert den strategischen Rahmen für Konfliktverhütung, Stabilität und Zusammenarbeit im Cyberraum, unter anderem durch ihre Teilnahme an den Beratungen der Vereinten Nationen über Cyberfragen. Zwei wichtige Prozesse sind die offene Arbeitsgruppe zu Entwicklungen auf dem Gebiet der Information und Telekommunikation im Kontext der internationalen Sicherheit und die Gruppe von Regierungssachverständigen (GGE) zur Förderung eines verantwortungsvollen staatlichen Handelns im Cyberraum. Zu den behandelten Themen gehören die Wirkung des Völkerrechts, die Umsetzung vereinbarter unverbindlicher, freiwilliger Normen für verantwortungsvolles staatliches Handeln und vertrauensbildende Maßnahmen sowie die Weiterentwicklung der Umsetzung durch gezielten Kapazitätsaufbau.

32 https://www.consilium.europa.eu/de/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/#

Nutzung der in der „Cyber Diplomacy Toolbox“ des Rates aus dem Jahr 2017[33] vorgesehenen Cybersanktionen.

Die Verhandlungen zwischen den gesetzgebenden Organen über neue Ausfuhrvorschriften, die den Verkauf von Technologien für digitale Überwachung an Regimes einschränken, welche sich an der Unterdrückung von Menschenrechten beteiligen[34], sind ebenfalls vorangekommen. Diese Vorschriften werden nach ihrer Annahme zu einem verantwortungsvolleren, stärker wettbewerbsorientierten und transparenteren Handel mit Gütern mit doppeltem Verwendungszweck führen[35]. Die vorgeschlagenen Änderungen, die aufgrund technologischer Entwicklungen und zunehmender Sicherheitsrisiken erforderlich wurden, umfassen neue Kriterien für die Erteilung oder Ablehnung von Ausfuhrlizenzen für bestimmte Güter.

3. Schutz des öffentlichen Raums

Wie in der EU-Agenda zur Terrorismusbekämpfung anerkannt wurde[36], ist der Schutz des öffentlichen Raums durch Stärkung der Widerstandsfähigkeit gegenüber Sicherheitsbedrohungen nach wie vor ein wesentlicher Bestandteil der Bemühungen um eine wirksame und echte Sicherheitsunion. Bei der Ausarbeitung von Leitlinien und der Bereitstellung praktischer Unterstützung und finanzieller Mittel[37] arbeitet die Kommission – im Einklang mit dem **Aktionsplan von 2017 für einen besseren Schutz des öffentlichen Raums**[38] und der Sammlung bewährter Verfahren zum Schutz des öffentlichen Raums aus dem Jahr 2019[39] – mit einem breiten Spektrum öffentlicher und privater Interessenträger zusammen. Wie aus der EU-Agenda zur Terrorismusbekämpfung hervorgeht, wird die Kommission ihre Unterstützung für lokale und regionale Gebietskörperschaften verstärken, die eine zentrale Rolle beim Schutz des öffentlichen Raums und bei der Verhütung von Radikalisierung spielen. Dies beinhaltet auch die Ausarbeitung eines EU-Protokolls über urbane Sicherheit und Resilienz für Städte, in dem Grundprinzipien und Ziele für die lokalen Gebietskörperschaften in diesen Gebieten festgelegt werden.

---

[33] Beschluss (GASP) 2020/1127 des Rates vom 30. Juli 2020 zur Änderung des Beschlusses (GASP) 2019/797 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen (ABl. L 246 vom 30.7.2020, S. 12), Beschluss (GASP) 2020/1537 des Rates vom 22. Oktober 2020 zur Änderung des Beschlusses (GASP) 2019/797 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen (ABl. L 351I vom 22.10.2020, S. 5) und Beschluss (GASP) 2020/651 des Rates vom 14. Mai 2020 zur Änderung des Beschlusses (GASP) 2019/797 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen (ABl. L 153 vom 15.5.2020, S. 4) als Teil des Dokuments 9916/17.

[34] COM(2016) 616. Der Vorschlag der Kommission zielt auf eine Änderung und Neufassung der Verordnung Nr. 428/2009 des Rates über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung und der Durchfuhr von Gütern mit doppeltem Verwendungszweck ab.

[35] Dabei handelt es sich um eine äußerst große Gruppe von Gütern, Materialien, Software und Technologien, die sowohl für zivile als auch für militärische Zwecke verwendet werden können.

[36] COM(2020) 795.

[37] Die ISF-Schutzaufforderung aus dem Jahr 2019 umfasst das „Secu4All“-Projekt, das einen umfassenden Schulungszyklus vorsieht, der lokale Gebietskörperschaften in die Lage versetzen soll, den Bürgerinnen und Bürgern ein sicheres urbanes Umfeld zu bieten. Weiterer Bestandteil ist „DroneWISE“ zur Stärkung der Fähigkeit der Ersthelfer, feindselige unbemannte Luftfahrzeuge abzuwehren. Im Jahr 2020 wird eine neue Aufforderung in Höhe von 12 Mio. EUR zum Schutz des öffentlichen Raums erfolgen.

[38] COM(2017) 612.

[39] SWD(2019) 140.

Da sich Terroranschläge zunehmend gegen **Gotteshäuser** richten, wird ein besonderer Schwerpunkt auf die Zusammenarbeit zwischen staatlichen Stellen und religiösen Führern und Gemeinschaften gelegt. Ziel ist, das Sicherheitsbewusstsein zu verbessern und zur Umsetzung bewährter Verfahren und Schulungen in Gotteshäusern beizutragen. Schon mit einfachen Maßnahmen kann man vermeiden, dass Menschen sterben. So wurde im Oktober 2019 eine Synagoge in Halle Ziel eines Terroranschlags. Dank einer verstärkten Tür, eines Panikknopfs und Sicherheitskameras konnten jedoch zahlreiche Leben gerettet werden.

Um die Sicherheit im öffentlichen Raum, insbesondere in Gotteshäusern, weiter zu verbessern, hat die Kommission 20 Mio. EUR für Projekte, die von Interessenträgern geleitet werden, bereitgestellt.

Darüber hinaus arbeitet die Kommission an einer Reaktion auf **neu auftretende Risiken für den öffentlichen Raum**, darunter **unbemannte Luftfahrzeugsysteme** (UAS). Drohnen bieten zwar erhebliche wirtschaftliche und beschäftigungspolitische Chancen, stellen aber auch ein beträchtliches Risiko für den öffentlichen Raum, kritische Infrastrukturen und andere sensible Standorte wie Haftanstalten dar. Gemindert wird dieses Risiko durch die jüngsten EU-Vorschriften[40] in diesem Bereich, und zwar durch die Verbesserung der Sicherheit von Drohneneinsätzen. Ab Januar 2021 müssen sich Drohnenbetreiber auch bei den nationalen Behörden registrieren lassen. Zur Gewährleistung eines sichereren Drohnenbetriebs könnte diese Regelung durch einen **Rechtsrahmen für U-Space**[41], Europas unbemanntes Flugverkehrsmanagementsystem, ergänzt werden. Zusammen genommen werden diese Maßnahmen den Flugbetrieb von Drohnen in Gebieten mit Zugangsbeschränkung durch Einzelpersonen erschweren und außerdem die Identifizierung und strafrechtliche Verfolgung von Straftätern erleichtern.

Darüber hinaus unterstützt die Kommission Strafverfolgungsbehörden, Betreiber kritischer Infrastrukturen, Organisatoren von Massenveranstaltungen und andere Interessenträger bei der Bekämpfung des Einsatzes nicht kooperativer Drohnen, beispielsweise durch Zusammenarbeit mit der Agentur der Europäischen Union für Flugsicherheit EASA bei der Entwicklung **bewährter Verfahren**, die die **Akteure am Flughafen** bei der Reaktion auf Vorfälle mit unbefugten Drohnen **unterstützen**, durch die Förderung einheitlicherer **Testverfahren für Gegenmaßnahmen** und die Entwicklung eines Praxishandbuchs für Interessenträger mit Schwerpunkt auf dem urbanen Umfeld.

An einem **digitalen Herbstseminar der EU zum Schutz des öffentlichen Raums**, das im Oktober 2020 von der Gemeinsamen Forschungsstelle der Kommission veranstaltet wurde, nahmen mehr als 200 Stadtplaner sowie öffentliche und private Betreiber öffentlicher Räume teil. In den Sitzungen wurde eine breite Palette von Themen behandelt, wie etwa der Schutz vor Explosionen und Amokfahrten, die Eindämmung der Bedrohungen durch feindliche Drohnen im urbanen Umfeld und der Einsatz von Überwachungs- und Detektionstechnologien.

Die Kommission hat zudem ihre aktive Unterstützung der im Januar 2019 im Rahmen der EU-Städteagenda ins Leben gerufenen **Partnerschaft für die Sicherheit im öffentlichen**

---

[40] 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, S. 45).

[41] Die Kommission kann zu diesem Zweck eine Durchführungsverordnung vorlegen, deren Annahme nach einem Prüfverfahren unter Beteiligung des Flugsicherheitsausschusses erfolgen würde.

Raum fortgeführt, die ihren neuen Aktionsplan[42] veröffentlicht hat, mit dem die urbane Sicherheit auf verschiedenen Verwaltungsebenen angegangen werden soll. Zu den Maßnahmen gehören die Schaffung eines Rahmens für ein Selbstbewertungsinstrument, Empfehlungen für Politikgestaltung, mehrstufige Verwaltungsführung und Finanzierung, Innovation durch intelligente Lösungen und Technologien, darunter auch das Konzept der eingebauten Sicherheit („security by design"), der Prävention und sozialen Inklusion. Die Partnerschaft wird nun in die Umsetzungsphase eintreten.

Unterstützung für die Verbesserung der Sicherheit im öffentlichen Raum auf lokaler Ebene wurde auch über die 4. Ausschreibungsrunde der Initiative „Urban Innovative Actions" bereitgestellt. Drei Städte wurden ausgewählt und erproben nun mit Mitteln aus dem Europäischen Fonds für regionale Entwicklung neue Lösungen im Bereich der urbanen Sicherheit (Piräus in Griechenland, Tampere in Finnland und Turin in Italien).

Im Bereich der Reaktionsfähigkeit hat die Kommission auch einen europäischen Rahmen entwickelt, der die Vorsorge und Reaktion bei Vorfällen mit einer Vielzahl von Verbrennungsopfern verbessern soll und dabei auf die Nutzung der gesamten europäischen Behandlungskapazitäten durch eine EU-weite Zusammenarbeit setzt. Zur Versorgung einer großen Anzahl von Patienten mit schweren Verbrennungen kann das Katastrophenschutzverfahren der Union genutzt werden, das Zugang zu Brandbetten in spezialisierten Behandlungszentren, Experten für die Bewertung von Verbrennungen und Kapazitäten für den Abtransport der Verletzten bietet.

III BEWÄLTIGUNG SICH WANDELNDER BEDROHUNGEN

1. Cyberkriminalität

Straftäter machen sich häufig Lücken in der Cybersicherheit zunutze. Während der COVID-19-Krise wurde dies deutlicher denn je. So war eine Zunahme der „klassischen" Cyberkriminalität unter Einsatz von Schadsoftware und Ransomware (d. h. zum Diebstahl von personenbezogenen Daten und Zahlungsdaten oder zur Erpressung von Opfern)

[42] Der Aktionsplan wurde angenommen und ist auf Futurium abrufbar: https://ec.europa.eu/futurium/en/security-public-spaces/security-public-spaces-partnership-final-action-plan-0.

ebenso zu beobachten wie eine rasante Verbreitung neuer Websites, die Nutzer zur Installation von Schadsoftware verleiten. Es kam zu Cyberangriffen auf die Gesundheits- und Forschungsinfrastruktur, durch die IKT-Systeme blockiert wurden, die nur gegen Zahlung von „Lösegeld“ oder im Austausch für Informationen über die Impfstoffentwicklung entriegelt werden konnten[43]. Auch in Bezug auf den sexuellen Missbrauch von Kindern und Material über einen solchen Missbrauch war ein erheblicher Anstieg zu beobachten[44].

Eine wirksame Reaktion auf Cyberkriminalität erfordert einen soliden Rahmen für strafrechtliche Ermittlungen und Strafverfolgungsmaßnahmen, und ein wichtiger erster Schritt ist in diesem Zusammenhang die vollständige Umsetzung und Anwendung der Richtlinie über **Angriffe auf Informationssysteme**[45]. Nach der Einleitung von Vertragsverletzungsverfahren im Jahr 2019 überwacht die Kommission die Maßnahmen Bulgariens, Italiens, Portugals und Sloweniens. Auch bei der Anwendung der **Richtlinie zur Bekämpfung des sexuellen Missbrauchs von Kindern**[46] aus dem Jahr 2011 sind Fortschritte vonnöten. Zu den Bereichen, in denen weiterhin Handlungsbedarf besteht, gehören Prävention, materielles Strafrecht sowie Hilfs-, Unterstützungs- und Schutzmaßnahmen für Opfer im Kindesalter. Seit 2018 hat die Kommission Vertragsverletzungsverfahren gegen 25 Mitgliedstaaten eingeleitet[47].

Am 24. Juli 2020 nahm die Kommission eine **EU-Strategie für eine wirksamere Bekämpfung des sexuellen Missbrauchs von Kindern**[48] an, die ein effektives Vorgehen der EU in diesem Bereich ermöglichen soll. Eine besondere Herausforderung hat sich auch dadurch ergeben, dass bestimmte Online-Kommunikationsdienste wie Webmail- oder Nachrichtenübermittlungsdienste ab dem 21. Dezember 2020 in den Anwendungsbereich der e-Datenschutzrichtlinie fallen und von den überarbeiteten Definitionen des europäischen Kodex für die elektronische Kommunikation erfasst werden. Infolgedessen besteht eindeutig die Gefahr, dass Anbieter solcher Dienste, die gegenwärtig auf freiwilliger Basis wichtige Tätigkeiten zur Aufdeckung, Bekämpfung und Meldung von sexuellem Missbrauch von Kindern im Internet vornehmen, diese in Zukunft einstellen müssen. Die Kommission hat daher einen Vorschlag für eine **Verordnung**[49] vorgelegt, durch die - bis eine langfristige rechtliche Lösung gefunden ist - sichergestellt werden soll, dass diese auf freiwilliger Basis erfolgenden Tätigkeiten unter bestimmten Bedingungen fortgesetzt werden können. Die Kommission arbeitet derzeit an einem Vorschlag für eine solche Lösung, der 2021 angenommen werden soll.

Im Rahmen des Projekts ECHO („European network of Cybersecurity centres and competence Hub for innovation and Operations“) wurde eine **COVID-19-Allianz für Cyberabwehr** („COVID-19 Cyber Defence Alliance“) ins Leben gerufen, um innovative Konzepte zur Bekämpfung von Straftaten im Zusammenhang mit COVID-19 zu

---

43 Internet Organised Crime Threat Assessment (Bedrohungslage im Bereich der organisierten Kriminalität im Internet, IOCTA) 2020, Oktober 2020.

44 Report on Exploiting isolation (Bericht über die Ausnutzung der Isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic (Täter und Opfer von sexuellem Missbrauch von Kindern im Internet während der COVID-19-Pandemie), Europol, 19.6.2020.

45 Richtlinie 2013/40/EU.

46 Richtlinie 2011/93/EU.

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

48 COM(2020) 607.

49 COM(2020) 568.

entwickeln. Im April 2020 wurde eine spezielle EIC-COVID-Plattform[50] eingerichtet, um die Zivilgesellschaft, Innovatoren, Partner und Investoren in ganz Europa zu vernetzen und so die Entwicklung innovativer Lösungen zu ermöglichen.

Zur Gewährleistung einer wirksameren Verfolgung von Straftaten und angesichts der Bedeutung elektronischer Informationen und Beweismittel in strafrechtlichen Ermittlungen sollten die Strafverfolgungs- und Justizbehörden im Rahmen ihrer strafrechtlichen Ermittlungen rasch Zugang zu diesen Informationen und Beweismitteln erhalten. Dies wurde in der Gemeinsamen Erklärung der Innenministerinnen und Innenminister der EU vom 13. November 2020 anerkannt[51]. Europol, Eurojust und das Europäische Justizielle Netz haben am 1. Dezember 2020 ihren zweiten „SIRIUS EU Digital Evidence Situation Report" veröffentlicht. In dem Bericht wird auf die zunehmende Bedeutung elektronischer Beweismittel für strafrechtliche Ermittlungen hingewiesen[52]. Zu den Vorschlägen der Kommission über den **grenzüberschreitenden Zugang zu elektronischen Beweismitteln**[53] vom April 2018 hat das Europäische Parlament noch nicht Stellung genommen, weshalb die gesetzgebenden Organe noch keine Verhandlungen aufgenommen haben. Verzögerungen bei der Annahme dieser Vorschläge behindern die Arbeit der Strafverfolgungs- und Justizbehörden und erschweren die laufenden Bemühungen, durch internationale Verhandlungen kompatible Regeln für den grenzüberschreitenden Zugang zu elektronischen Beweismitteln zu schaffen[54].

Auf internationaler Ebene nimmt die Kommission im Namen der EU an den laufenden Verhandlungen über das Zweite Zusatzprotokoll zum **Budapester Übereinkommen** des Europarats **über Computerkriminalität** teil. Dieses Protokoll würde den zuständigen Strafverfolgungsbehörden verbesserte und weitreichende Instrumente für die grenzüberschreitende Zusammenarbeit bei der Untersuchung und Verfolgung von Cyberstraftaten und anderen schweren Formen der Kriminalität, einschließlich der direkten Zusammenarbeit mit Diensteanbietern, an die Hand geben. Da die meisten dieser verbesserten, verstärkten Formen der Zusammenarbeit den Austausch personenbezogener Daten beinhalten werden, ist es unerlässlich, dass das künftige Protokoll angemessene Datenschutzgarantien vorsieht, und zwar nicht nur unter dem Gesichtspunkt der Grundrechte, sondern auch, um Rechtssicherheit, gegenseitiges Vertrauen und die

---

[50] Die Kommission hat gemeinsam mit dem Europäischen Innovationsrat und den Mitgliedstaaten einen europaweiten EUvsVirus-Hackathon + Matchathon ausgerichtet https://covid-eic.easme-web.eu/.

[51] Gemeinsame Erklärung der Innenministerinnen und Innenminister der EU zu den jüngsten Terroranschlägen in Europa, 13. November 2020, 12634/20.

[52] Dem Bericht zufolge ist das Volumen der grenzüberschreitenden Anfragen von EU-Behörden bei Anbietern von Online-Diensten im Jahr 2019 erheblich gestiegen, wobei die überwiegende Mehrheit dieser Anfragen von Deutschland (37,7 % der Anfragen), Frankreich (17,9 %) und dem Vereinigten Königreich (16,4 %) gestellt wurde. Die Anträge auf Zugang zu elektronischen Daten haben sich in Polen verdoppelt und in Finnland fast verdreifacht. Darüber hinaus stiegen die Anträge auf Offenlegung in Notfallsituationen innerhalb eines Jahres um fast die Hälfte.

[53] COM(2018) 226 und COM (2018) 225.

[54] So verabschiedete die VN-Generalversammlung am 27. Dezember 2019 die Resolution 74/247 „Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien zu kriminellen Zwecken", mit der ein offener zwischenstaatlicher Ad-hoc-Sachverständigenausschuss eingesetzt wurde, der ein umfassendes internationales Übereinkommen über Cyberkriminalität ausarbeiten soll. Die EU steht der Schaffung eines neuen internationalen Rechtsinstruments zur Cyberkriminalität ablehnend gegenüber, da das Übereinkommen von Budapest über Computerkriminalität bereits einen umfassenden multilateralen Rechtsrahmen bietet. Im Juli 2020 einigten sich die VN-Mitgliedstaaten auf eine Verschiebung der ersten Maßnahmen: Die EU leistete einen Beitrag zu diesem Prozess auf der Grundlage eines Gemeinsamen Standpunkts (Dok. 7677/2/20).

Wirksamkeit der operativen Zusammenarbeit im Bereich der Strafverfolgung zu gewährleisten.

Diese Verhandlungen sollen 2021 abgeschlossen werden. Parallel dazu verhandelt die Kommission entsprechend dem vom Rat (Justiz und Inneres) im vergangenen Jahr erteilten Mandat über ein **Abkommen zwischen der EU und den USA über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln**. Dieses Abkommen würde die vorgeschlagenen internen EU-Vorschriften für die direkte grenzüberschreitende Zusammenarbeit mit Diensteanbietern ergänzen, indem Rechtskollisionen beseitigt und gemeinsame Regeln und Garantien festgelegt werden. Am 25. September 2019 wurden förmliche Verhandlungen aufgenommen, und es fanden bereits mehrere Verhandlungsrunden statt. Das Ergebnis der Verhandlungen hängt jedoch weitgehend davon ab, dass bei den internen Vorschriften für elektronische Beweismittel Fortschritte erzielt werden.

Das Thema der **Speicherung und Nutzung von Daten für Strafverfolgungszwecke** wurde von der Kommission im Anschluss an das im Jahr 2016 ergangene Urteil in der Rechtssache Tele2/Watson[55] durch Expertenkonsultationen mit einschlägigen Diensteanbietern, Polizei- und Justizbehörden, der Zivilgesellschaft, Datenschutzbehörden, Hochschulen und EU-Agenturen weiterverfolgt. In die Überlegungen flossen auch eine Studie über die Datenspeicherungspraktiken der Anbieter elektronischer Kommunikationsdienste und die Bedürfnisse und Praktiken der Strafverfolgungsbehörden beim Zugang zu Daten, die Ermittlung relevanter technologischer Herausforderungen und ein Überblick über die nationalen Rechtsrahmen ein.[56] Diese Arbeit hat verdeutlicht, dass die Strafverfolgungsbehörden Zugang zu Daten haben müssen, um ihre Aufgaben wirksamer wahrnehmen zu können.

Am 6. Oktober 2020 erließ der Gerichtshof Urteile[57] zu den nationalen Rechtsvorschriften Belgiens, Frankreichs und des Vereinigten Königreichs über die Speicherung, die Übermittlung und den Zugang zu Nichtinhaltsdaten zum Zwecke der Strafverfolgung und der nationalen Sicherheit. Die Kommission wird die verfügbaren Optionen prüfen, um sicherzustellen, dass Terroristen und andere Straftäter identifiziert und verfolgt werden können, wobei sie das EU-Recht in der Auslegung des Gerichtshofs beachten und auch andere beim Gerichtshof zu diesem Thema anhängige Rechtssachen berücksichtigen wird.

Ein weiteres wichtiges Element bei der Bekämpfung der Cyberkriminalität waren die Arbeiten mit dem Ziel, die Verfügbarkeit und Richtigkeit von Registrierungsdaten für Internet-Domänennamen („**WHOIS-Informationen**“) im Einklang mit den Bemühungen der Zentralstelle für die Vergabe von Internet-Namen und -Adressen (ICANN) zu gewährleisten. Im Rahmen der diesbezüglichen Beratungen soll erreicht werden, dass berechtigte Zugangsinteressenten, darunter Strafverfolgungsbehörden und Cybersicherheitsdienstleister, einen effizienten Zugang zu allgemeinen Top-Level-Domain-Registrierungsdaten erhalten, wobei die geltenden Datenschutzvorschriften uneingeschränkt zu beachten sind. Die endgültigen Empfehlungen für eine neue WHOIS-Strategie wurden am 10. August 2020 veröffentlicht. Sobald ihre Überprüfung abgeschlossen ist, wird der ICANN-Vorstand einen Beschluss fassen. Die Kommission

---

[55] Urteil in den verbundenen Rechtssachen C-203/15 und C-698/15, Tele2 Sverige AB und Watson u. a., 21. Dezember 2016.

[56] https://data.europa.eu/doi10.2837/26288

[57] Urteile in der Rechtssache C-623/17, Privacy International, und in den verbundenen Rechtssachen C-511/18, La Quadrature du Net u. a., C-512/18, French Data Network u. a., und C-520/18, Ordre des barreaux francophones et germanophone u. a.

wird die in dieser Überprüfung enthaltenen Schlussfolgerungen daraufhin prüfen, inwieweit sie den Aspekten des Datenschutzes und des öffentlichen Interesses an der Gewährung eines effektiven Zugangs für Strafverfolgungsbehörden und Cybersicherheitsdienstleister ausreichend Rechnung tragen.

2. Moderne Strafverfolgung

Mit den technologischen Entwicklungen, die derzeit nahezu alle gesellschaftlichen Bereiche, einschließlich der Sicherheit, von Grund auf verändern, müssen auch Strafverfolgung und Justiz Schritt halten. Um die Sicherheit in dieser Phase des Umbruchs zu verbessern, ist es unerlässlich, künstliche Intelligenz, Big Data und Hochleistungsrechnen in die Sicherheitspolitik einzubeziehen, ohne den wirksamen Schutz der Grundrechte zu schwächen.

Die Kommission befasst sich mit einer Reihe wichtiger Arbeitsbereiche[58]. Am 25. November 2020 schlug die Kommission[59] das Daten-Governance-Gesetz vor, einen Rahmen für die vereinfachte gemeinsame Nutzung und Weiterverwendung personenbezogener und nicht personenbezogener Daten zu Innovations- und Entwicklungszwecken. Dieses Gesetz sieht virtuelle oder physische sektorspezifische Datenräume für die Industrie und öffentliche Stellen vor. Nationale Strafverfolgungsbehörden sollen für ihre eigenen Innovationszwecke Zugriff auf Daten erhalten, die in anderen Datenräumen untergebracht sind. Gleichzeitig wäre der Zugriff auf Daten, die sich im Besitz der nationalen Strafverfolgungs- und Sicherheitsbehörden befinden, nur zulässig, wenn dies nach EU-Recht oder nationalem Recht zulässig ist. Auch nationale Strafverfolgungsbehörden könnten darauf zugreifen, sofern einzelne betroffene Personen ihre Daten freiwillig für das Gemeinwohl und ausschließlich zum Zweck der wissenschaftlichen Forschung zur Verfügung stellen.

Nach der Veröffentlichung des Weißbuchs zur Künstlichen Intelligenz (KI) wurde nun mit den Vorbereitungsarbeiten für eine neue **KI-Initiative** begonnen[60]. In dem Weißbuch werden zwar die Chancen anerkannt, die die KI-Technologien für die Sicherheit und das Wohlergehen der Bürger und der Gesellschaft insgesamt bedeuten, jedoch auch verschiedene Risiken aufgezeigt – wie Cyberbedrohungen, Gefährdungen der persönlichen Sicherheit oder der Verlust der Konnektivität. In der öffentlichen Konsultation äußerten die Teilnehmer Bedenken insbesondere dahingehend, dass der Einsatz der KI zu einer Verletzung der Grundrechte führen könne und das Risiko diskriminierender Ergebnisse berge[61]. In ihrer Mitteilung über die Schaffung von Vertrauen in eine auf den Menschen ausgerichtete KI[62] wies die Kommission eindringlich auf die Notwendigkeit hin, die Widerstandsfähigkeit der KI-Systeme sowohl gegenüber offenen Angriffen als auch gegenüber subtileren Versuche der Manipulation zu verbessern und Maßnahmen zu ergreifen, um dieses Risiko zu mindern.

Verschlüsselung spielt eine zentrale Rolle bei der Gewährleistung einer starken Cybersicherheit und des wirksamen Schutzes der Grundrechte, etwa des Rechts auf Privatsphäre, einschließlich der Vertraulichkeit der Kommunikation, und des Schutzes personenbezogener Daten sowie bei der Sicherung des Vertrauens in Dienste und

---

58 Einschließlich der Datenstrategie der EU (siehe oben).
59 COM(2020) 767.
60 COM(2020) 65.
61 90 % bzw. 87 % der Befragten halten diese Bedenken für wichtig oder sehr wichtig.
62 COM(2019) 168.

Produkte, die auf Verschlüsselungstechnologien, beispielsweise Lösungen für digitale Identitäten, beruhen. Gleichzeitig kann sie auch eingesetzt werden, um Straftaten vor der Strafverfolgung und Justiz zu verschleiern, was deren Untersuchung, Aufdeckung und Verfolgung erschwert. Die Mitgliedstaaten im Rat haben Lösungen gefordert, die den Strafverfolgungs- und Justizbehörden die Möglichkeit geben, unter uneingeschränkter Achtung der Privatsphäre, des Datenschutzes und der Garantien für ein faires Verfahren auf elektronische Beweismittel zuzugreifen[63]. Die Kommission wird mit den Mitgliedstaaten zusammenarbeiten, um rechtliche, operative und technische Lösungen für den rechtmäßigen Zugang zu elektronischen Informationen in verschlüsselten Umgebungen zu ermitteln, die gleichzeitig die Sicherheit der Kommunikation gewährleisten.

Zu den praktischen Maßnahmen, die in diesem Zusammenhang ergriffen wurden, zählt eine **Entschlüsselungsplattform** bei Europol, die den Strafverfolgungsbehörden dabei helfen soll, rechtmäßigen Zugriff auf verschlüsselte Informationen zu erhalten, die sich auf Geräten befinden, welche im Rahmen strafrechtlicher Ermittlungen beschlagnahmt wurden[64]. Die Europäische Gruppe für Schulung und Ausbildung in Bezug auf Cyberkriminalität hat Pilot-Schulungsmodule entwickelt, die in die Arbeit der Agentur für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (CEPOL) einfließen werden. Außerdem wurde ein Netz von Verschlüsselungsexperten der Mitgliedstaaten eingerichtet, um bewährte Verfahren und Fachwissen auszutauschen und die Entwicklung eines Instrumentariums technischer und praktischer Instrumente zu unterstützen.

Das **System für den digitalen Austausch elektronischer Beweismittel (eEDES)** wird ein Instrument für einen sicheren, raschen und effizienten grenzüberschreitenden Austausch von Europäischen Ermittlungsanordnungen, Rechtshilfeersuchen und Beweismitteln in digitaler Form bieten. Es sollte schrittweise erweitert und auf andere Instrumente der justiziellen Zusammenarbeit in Strafsachen ausgeweitet werden, und sein künftiger Anwendungsbereich wird in einem Legislativvorschlag zur Digitalisierung der Verfahren der justiziellen Zusammenarbeit festgelegt werden, der für 2021 geplant ist[65].

3. Bekämpfung illegaler Online-Inhalte

Radikalisierung, die zu gewalttätigem Extremismus und Terrorismus führt, ist ein vielschichtiges und grenzüberschreitendes Phänomen, das sich das rasche Wachstum des Internets zunutze machen konnte. Das Internet wird nach wie vor verwendet, um anfällige Personen zu radikalisieren und anzuwerben. Im Juli entfernte die bei Europol angesiedelte Meldestelle für Internetinhalte 2 000 Links zu terroristischen Inhalten – darunter Handbücher und Anleitungen zur Durchführung von Angriffen. Die Beweise für die Rolle des Internets bei der Radikalisierung der an den Anschlägen in Frankreich und in Österreich beteiligten Personen und der Zurschaustellung ihrer Straftaten verdeutlichen weiter, dass ein klarer Rechtsrahmen erforderlich ist, um die Verbreitung terroristischer Online-Inhalte bei gleichzeitiger Wahrung wirksamer Garantien zum Schutz der Grundrechte zu verhindern. Die Verhandlungen zwischen dem Europäischen Parlament und dem Rat über die vorgeschlagene **Verordnung zur Verhinderung der Verbreitung**

---

63 ST 13084 2020 – Entschließung des Rates zur Verschlüsselung – Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung.

64 Dieses mit 6 Mio. EUR ausgestattete Projekt wird auch von der Gemeinsamen Forschungsstelle der Kommission unterstützt.

65 Mitteilung über die Digitalisierung der Justiz in der EU, COM(2020) 710, 2. Dezember 2020.

terroristischer Online-Inhalte[66] wurden in den letzten Wochen intensiviert. Der Abschluss dieser Verhandlungen in Verbindung mit der Einführung insbesondere des neuen und wirksamen operativen Instruments der Entfernungsanordnung zur grenzüberschreitenden Beseitigung terroristischer Inhalte innerhalb einer Stunde nach Erhalt einer solchen Anordnung ist für die Bekämpfung terroristischer Inhalte, darunter der Inhalte, die zur Radikalisierung beitragen, von entscheidender Bedeutung.

In der Zwischenzeit fungiert das **EU-Internetforum** weiterhin als Katalysator für Maßnahmen und stellt eine wichtige Plattform dar, die die Mitgliedstaaten und die Industrie zusammenbringt, um die Verbreitung terroristischer Online-Inhalte zu verhindern und radikalisierenden Botschaften entgegenzuwirken. Das Forum arbeitet an der Entwicklung einer Referenzliste der in den Mitgliedstaaten verbotenen Symbole und Gruppen, die als Grundlage für die Regelungen zur Moderation von Inhalten auf der Plattform dienen könnten.

Das EU-Internetforum hat seinen Wirkungsbereich auf den **sexuellen Missbrauch von Kindern im Internet** ausgeweitet. Das Forum wird einen gemeinsamen Raum für den Austausch bewährter Verfahren und die Ermittlung von Hindernissen bieten, mit denen private und öffentliche Akteure konfrontiert sind, und damit einen Beitrag zur Verbesserung des gegenseitigen Verständnisses und zur gemeinsamen Ausarbeitung von Lösungen leisten. Außerdem ermöglicht es eine politische Koordinierung auf höchster Ebene, um die Effizienz und Wirksamkeit der Maßnahmen zu maximieren. Im Rahmen des EU-Internetforums wurde ein Prozess eingerichtet, der technische Experten aus Wissenschaft, Industrie, Behörden und Organisationen der Zivilgesellschaft umfasst und mögliche technische Lösungen zur Aufdeckung und Meldung von sexuellem Missbrauch von Kindern in der End-zu-End-verschlüsselten elektronischen Kommunikation erfassen und vorläufig bewerten soll. Solche technischen Lösungen sollten nicht zu einer Schwächung der Verschlüsselung führen. Dieser Ansatz ergänzt die anderen oben beschriebenen Online- und Offline-Elemente der Bekämpfung des sexuellen Missbrauchs von Kindern.

Darüber hinaus hat die Kommission weiterhin das Fachwissen und die Erfahrungen der EU im Rahmen des unabhängigen beratenden Ausschusses des neu eingerichteten **Globalen Internetforums zur Bekämpfung des Terrorismus** sowie in der Arbeitsgruppe Krisenreaktion, die sie gemeinsam mit Microsoft leitet, weitergegeben. Zusammen mit Europol unterstützte die Kommission die Mitgliedstaaten weiterhin bei der Umsetzung des **EU-Krisenprotokolls**. Die EU-Meldestelle für Internetinhalte veranstaltete am 23. November 2020 eine zweite Planübung, um Leitlinien zur Verbesserung der operativen Reaktionen und der Echtzeitkoordinierung zwischen den Mitgliedstaaten und Anbietern von Online-Diensten auszuarbeiten.

Im Juni 2020 veröffentlichte die Kommission die Ergebnisse der jüngsten Überwachung der Umsetzung des **Verhaltenskodex für die Bekämpfung illegaler Hassreden im Internet**[67]. Daraus ging hervor, dass IT-Unternehmen 90 % der gemeldeten Inhalte innerhalb von 24 Stunden prüfen und 71 % der als illegale Hassreden eingestuften Inhalte entfernen. Allerdings wurden auch Defizite bei der Transparenz und den Rückmeldungen an die Nutzer festgestellt. Die Umsetzung des Verhaltenskodex in den letzten vier Jahren floss auch in die Überlegungen darüber ein, wie der künftige Vorschlag für ein Gesetz über

---

66 COM(2018) 640.

67 https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en.

digitale Dienste zur Eindämmung illegaler Online-Inhalte beitragen könnte, ohne die Meinungsfreiheit zu beeinträchtigen. In ihrer Rede zur Lage der Union 2020 kündigte Präsidentin von der Leyen ferner an, dass die Kommission bis Ende 2021 vorschlagen werde, die Liste der EU-Straftatbestände gemäß Artikel 83 Absatz 1 AEUV auf Hassverbrechen und Hassreden auszuweiten[68].

4. ***Hybride Bedrohungen***

Angesichts der veränderlichen Natur hybrider Bedrohungen setzte der Rat im Juli 2019 die **horizontale Arbeitsgruppe zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen** ein. Ihr Hauptziel ist die Unterstützung der strategischen und horizontalen Koordinierung zwischen den Mitgliedstaaten im Bereich der Resilienz von Staat und Gesellschaft, die Verbesserung der strategischen Kommunikation und die Bekämpfung von Desinformation. Die bisherigen Arbeiten umfassen unter anderem Folgemaßnahmen zu den Untersuchungen über hybride Risiken[69] sowie eine Betrachtung speziell zu hybriden Bedrohungen und Desinformation in den Partnerländern der Europäischen Nachbarschaftspolitik. Die Tätigkeiten der horizontalen Arbeitsgruppe wurden in einem Jahresbericht vorgestellt, der am 14. September 2020 angenommen wurde.

Im Dezember 2019 nahm der Rat „ Schlussfolgerungen über zusätzliche Anstrengungen zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen“[70] an, in denen ein umfassendes Konzept für die Sicherheit und die Abwehr hybrider Bedrohungen gefordert wird, das in allen einschlägigen Politikbereichen strategischer, koordinierter und kohärenter wirkt. Im Juli 2020 wurden zwei wichtige Folgemaßnahmen durchgeführt. Zunächst erstellten die Kommissionsdienststellen und der EAD eine **Bestandsaufnahme der Maßnahmen und Dokumente im Zusammenhang mit der Reaktion der EU auf hybride Bedrohungen**[71]. Die Bestandsaufnahme enthält ein Gesamtinventar der Maßnahmen zur Bekämpfung von hybriden Bedrohungen auf EU-Ebene und entsprechende Strategiepapiere. Es dient als Ausgangspunkt für die Einrichtung einer zugangsbeschränkten Online-Plattform als zentrale Anlaufstelle für alle mit hybriden Bedrohungen zusammenhängenden Maßnahmen, politischen und legislativen Dokumente sowie einschlägigen Studien. Zweitens befasste sich der jüngste **Jahresbericht über die Abwehr hybrider Bedrohungen**[72] mit der Umsetzung in den Bereichen Lageerfassung, Aufbau von Resilienz, Vorsorge und Krisenreaktion sowie der internationalen Zusammenarbeit, insbesondere der Zusammenarbeit zwischen der EU und der NATO bei der Abwehr hybrider Bedrohungen. In dem Bericht wurden zwar einige Fortschritte bei der Koordinierung auf EU-Ebene festgestellt, jedoch sind angesichts des beispiellosen Ausmaßes und der Vielfalt hybrider Bedrohungen sind derzeit weitere Schritte auf EU-

---

68 Nähere Ausführungen hierzu auch in der Strategie zur Gleichstellung von LGBTIQ für den Zeitraum 2020 bis 2025 (COM(2020) 698).

69 Maßnahme 1 des Gemeinsamen Rahmens für die Abwehr hybrider Bedrohungen von 2016, siehe JOIN/2016/018.

70 Schlussfolgerungen des Rates der EU - Dok. 14972/19.

71 SWD(2020) 152: Joint Staff Working Document, Mapping of the measures related to enhancing resilience and countering hybrid threats (Gemeinsame Arbeitsunterlage, Bestandsaufnahme der Maßnahmen zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen).

72 SWD(2020) 153: Joint Staff working document, 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 Gemeinsame Arbeitsunterlage, 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).

Ebene erforderlich, um die externe und die interne Dimension nahtlos zu integrieren und die Bemühungen der Mitgliedstaaten zur Abwehr hybrider Bedrohungen und zur Stärkung ihrer Resilienz zu unterstützen.

Parallel dazu wird an der Umsetzung der in der neuen Sicherheitsstrategie dargelegten Maßnahmen gearbeitet, bei denen es darum geht, Erwägungen zu hybriden Bedrohungen durchgängig in der Politikgestaltung zu berücksichtigen, eine zugangsbeschränkte Online-Plattform zu entwickeln, sektorspezifische Referenzwerte für die Widerstandsfähigkeit der EU festzulegen und den Informationsfluss zu der weiteren Verbesserung der Lageerfassung zu straffen[73]. Grundlage hierfür ist die Arbeit der **EU-Analyseeinheit für hybride Bedrohungen** (HFC), die innerhalb des EU-Zentrums für Informationsgewinnung und -analyse (EU INTCEN) eingerichtet wurde und nach wie vor die wichtigste EU-Anlaufstelle für hybride Bedrohungsanalysen ist. Sie hat bereits mehr als 180 schriftliche Berichte über hybride Bedrohungen und Cyberbedrohungen erstellt. Eines der HFC-Projekte ist die **Analyse von Trends bei hybriden Bedrohungen**[74], die Daten zu folgenden Themen liefert: wiederkehrende Analyse der hybriden Tätigkeiten neuer Akteure, Gegen Mitgliedstaaten, Institutionen, Partner und Interessen der EU gerichtete Aktivitäten der Auslandsaufklärung; staatliche und nichtstaatliche Akteure, die die COVID-19-Pandemie unter Einsatz hybrider Mittel ausnutzen.

Die **Zusammenarbeit zwischen der EU und der NATO** (entsprechend dem umfassenden Rahmen, der durch die Gemeinsamen Erklärungen von Warschau und Brüssel von 2016 und 2018 vorgegeben wurde) erfuhr eine weitere Vertiefung, wie dies im fünften Fortschrittsbericht vom Juni 2020 hervorgehoben wurde, und zwar durch Interaktion der jeweiligen Mitarbeiter und konkrete Ergebnisse in den Bereichen hybride Bedrohungen, Cyberabwehr und Kapazitätsaufbau[75]. Um dem Risiko einer Fragmentierung und Doppelung von Strategien, Instrumenten und Maßnahmen entgegenzuwirken, ist es äußerst wichtig, eine einheitliche, sektorübergreifende Methodik für die Referenzwerte für die Resilienz gegenüber hybriden Bedrohungen zu entwickeln. Auch das Europäische Kompetenzzentrum für die Abwehr hybrider Bedrohungen in Helsinki war an dieser Zusammenarbeit beteiligt. Während der COVID-19-Krise wurde die Zusammenarbeit mit der NATO verstärkt, unter anderem hinsichtlich der pandemiebedingten Desinformation und der Bekämpfung feindseliger Informationsaktivitäten.

Im Allgemeinen hat die COVID-19-Pandemie die sich rasch entwickelnden Risiken der **Desinformation** und die reale Gefährdung für das Leben der Menschen verdeutlicht[76] Am 10. Juni 2020 nahmen die Kommission und der Hohe Vertreter eine **gemeinsame Mitteilung zur Bekämpfung von Desinformation im Zusammenhang mit COVID-19**[77]

---

[73] So schlug die Gemeinsame Forschungsstelle am 26. November 2020 einen neuen Rahmen zur Sensibilisierung für Bedrohungen vor: https://ec.europa.eu/jrc/en/news/jrc-framework-against-hybrid-threats

[74] Die Analyse von Trends bei hybriden Bedrohungen („Hybrid Trends Analysis“) ist ein Instrument, das zusätzlich zu den nationalen Systemen eingesetzt werden soll, um das Ausmaß und die Intensität hybrider Bedrohungen in den Bereichen Politik/Diplomatie, Militär, Wirtschaft, Information, Aufklärung, Cybersicherheit, Soziales, Energie und Infrastruktur zu überwachen.

[75] Die Zusammenarbeit zwischen den Bediensteten im Bereich Cybersicherheit und -abwehr wurde durch die Arbeit an kohärenten Konzepten und Doktrinen, Übungen, Informationsaustausch und gegenseitige Unterrichtungen weiter intensiviert.

[76] Solche realen Folgen waren beispielsweise die Inbrandsetzung von Telekommunikationsinfrastruktur und irreführende Gesundheitsinformationen mit unmittelbaren Auswirkungen.

[77] Gemeinsame Mitteilung JOIN (2020) 8, Bekämpfung von Desinformation im Zusammenhang mit COVID-19 – Fakten statt Fiktion.

an, in der auf die spezifischen Risiken der Desinformation im Umfeld von COVID-19 hingewiesen wird und die Maßnahmen benannt werden, die in diesem Zusammenhang ergriffen werden sollten. Hierzu zählten Maßnahmen großer Online-Plattformen zur Entwicklung von Strategien für den Umgang mit der Bedrohung, eine intensivere Überwachung der Maßnahmen der Plattformen sowie eine gezielte Zusammenarbeit im Rahmen des vom EAD verwalteten Frühwarnsystems. Die Pandemie hat zu vermehrten Anstrengungen bei der Bekämpfung von Desinformation und einer stärkeren Sensibilisierung der Öffentlichkeit geführt. Im ersten Halbjahr 2020 wurden 1963 Fälle von kremlfreundlicher Desinformation neu in die öffentliche Desinformationsdatenbank von **EUvsDisinfo** aufgenommen, von denen fast ein Drittel mit der COVID-19-Infodemie zusammenhing. Von Mitte März bis Ende April 2020 verzeichnete die Website täglich mehr als 10 000 Aufrufe, und die Gesamtzahl der Besucher nahm im Vergleich zum Vorjahreszeitraum um 400 % zu. Die Reaktion der EU umfasste gezielte Kommunikationskampagnen[78] und die Bereitstellung von Sachinformationen über die Pandemie.

Die dabei gewonnenen Erkenntnisse flossen in die Ausarbeitung des am 2. Dezember 2020 angenommenen **Aktionsplans für Demokratie in Europa**[79] ein. Dieser Plan enthält die wichtigsten Maßnahmen zur Stärkung der Widerstandsfähigkeit des demokratischen Gefüges der EU: Förderung freier und fairer Wahlen, Bewältigung der Belastungen, denen freie und unabhängige Medien ausgesetzt sind, und Bekämpfung von Desinformation. Dieser letzte Aspekt wird auf dem Aktionsplan gegen Desinformation von 2018[80] aufbauen, der die Grundlage für verstärkte EU-Maßnahmen zur Bekämpfung von Desinformation und für die Einbeziehung wichtiger Akteure der Zivilgesellschaft und der Privatwirtschaft bildet. Außerdem wird darin bereits auf den nächsten Schritt im Zusammenhang mit dem **Verhaltenskodex für den Bereich der Desinformation** verwiesen, der auf die im September 2020 vorgenommene Bewertung der Wirksamkeit des Kodex folgen soll[81]. Der Kodex ist ein wichtiger und notwendiger Schritt auf dem Weg zur Schaffung eines transparenteren und verantwortungsvolleren Ökosystems der Online-Plattformen; einheitlichere Definitionen, eine kohärentere Umsetzung und mehr Maßnahmen für spezifische Bereiche wie Mikrotargeting würden seine Wirksamkeit jedoch erhöhen. Ein weiteres wichtiges Instrument, das der EU nun zur Verfügung steht, ist die **Europäische Beobachtungsstelle für digitale Medien**, die im Juni 2020 ihre Arbeit aufgenommen hat. Sie bringt wichtige Akteure zusammen, die sich mit dem Thema der Desinformation befassen, etwa Faktenprüfer und Wissenschaftler.

IV SCHUTZ DER EUROPÄERINNEN UND EUROPÄER VOR TERRORISMUS UND ORGANISIERTER KRIMINALITÄT

1. *Terrorismus und Radikalisierung*

Die jüngsten Anschläge haben erneut deutlich gemacht, dass die terroristische Bedrohung in der EU nach wie vor hoch ist. Kurz nach der Ermordung eines Lehrers in Conflans-

[78] So wurde die Kampagne „Think before you share“ (Erst denken, dann teilen) ins Leben gerufen, die Beratung in der Frage bietet, wie die Verbreitung von Desinformation bei jungen Zielgruppen und Multiplikatoren in den Ländern der Östlichen Partnerschaft der EU begrenzt werden kann, und auf den Plattformen der sozialen Medien mehr als 500 000 Mal aufgerufen wurde.

[79] COM(2020) 790.

[80] Gemeinsame Mitteilung JOIN(2018) 36, Aktionsplan gegen Desinformation.

[81] SWD(2020) 180.

Sainte-Honorine am 16. Oktober 2020 wurden am 29. Oktober in der Basilika Notre-Dame in Nizza drei Menschen getötet. Am 2. November kamen bei einem Terroranschlag in Wien vier Menschen ums Leben, und 23 weitere wurden verletzt. Am 13. November verabschiedete der Rat eine Gemeinsame Erklärung der Innenministerinnen und Innenminister der EU zu den jüngsten Terroranschlägen in Frankreich und Österreich.[82] Zu diesen jüngsten dschihadistischen Anschlägen kommt die zunehmende Bedrohung, die von gewaltbereiten Rechtsextremisten und anderen Formen des Terrorismus ausgeht.

Um die Mitgliedstaaten weiter bei der Bekämpfung von Terrorismus und Radikalisierung zu unterstützen, verabschiedet die Kommission heute eine **EU-Agenda zur Terrorismusbekämpfung**[83]. Diese Agenda baut auf den vorhandenen Maßnahmen und Instrumenten auf und wird die Rahmenbedingungen der Union für weitere Fortschritte mit Blick auf die Vorwegnahme von Bedrohungen und Gefahren, die Prävention von Radikalisierung und gewaltbereitem Extremismus, den Schutz von Menschen und Infrastrukturen – unter anderem durch den Schutz der Außengrenzen – und wirksame Folgemaßnahmen nach Anschlägen verbessern. Darüber hinaus wird in der Agenda die künftige Vorgehensweise für die Verbesserung der Zusammenarbeit der Strafverfolgungs- und Justizbehörden sowie für den Einsatz von Technologien und den Austausch relevanter Informationen in der Union unter anderem mit Blick auf das mit der Durchführung der Kontrollen an den Außengrenzen betraute Personal aufgezeigt. Die Durchführung und Durchsetzung der Rechtsvorschriften ist auch weiterhin von zentraler Bedeutung.

Prävention ist ein unverzichtbarer Bestandteil der Terrorismusbekämpfung. Die Anstrengungen der EU im Bereich der **Radikalisierungsprävention** bauen auf den umfassenden Erfahrungen auf, die bislang im Rahmen der Unterstützung der vor Ort tätigen Fachkräfte und der politischen Entscheidungsträger gewonnen wurden. Am 24. November verabschiedete die Kommission einen neuen **Aktionsplan für Integration und Inklusion**[84]. Für die Bekämpfung der Radikalisierung ist es von entscheidender Bedeutung, die Bemühungen um eine Annäherung der Gemeinschaften zu verstärken. Eine stärker von Zusammenhalt und Inklusion geprägte Gesellschaft kann dazu beitragen, die Ausbreitung extremistischer Ideologien zu verhindern, die zu Terrorismus und gewaltbereitem Extremismus führen können. Zur Unterstützung des **Aufklärungsnetzwerks gegen Radikalisierung** wurde unter anderem im Januar 2020 ein weiterer Vertrag über 30 Mio. EUR mit einer Laufzeit von vier Jahren geschlossen, der Hilfe für Fachkräfte vor Ort sowie zusätzliche Unterstützung für politische Entscheidungsträger und Wissenschaftler vorsieht. Diese und weitere Instrumente, etwa das **EU-Internetforum**, werden die Kommission befähigen, die vorrangigen Maßnahmen in Angriff zu nehmen, die in den strategischen Orientierungen für ein koordiniertes EU-Konzept für die Radikalisierungsprävention („Strategic Orientations on a coordinated EU approach to the prevention of radicalisation“) für 2021 aufgeführt sind. Hinzu kommen die in der EU-Agenda zur Terrorismusbekämpfung vorgesehenen Maßnahmen zur Bekämpfung extremistischer Ideologien im Internet, zur Intensivierung der Maßnahmen in Haftanstalten und der Rehabilitations- und Wiedereingliederungsmaßnahmen, unter anderem für ausländische terroristische Kämpfer, sowie zur Verstärkung der Unterstützung für lokale Akteure und Verbesserung der Widerstandsfähigkeit der Gemeinschaften.

---

[82] Gemeinsame Erklärung der Innenministerinnen und Innenminister der EU zu den jüngsten Terroranschlägen in Europa, 13. November 2020, 12634/20.

[83] COM(2020) 795.

[84] COM(2020) 758.

Die **Richtlinie zur Terrorismusbekämpfung**[85] vom März 2017 stellt das wichtigste strafrechtliche Instrument der Terrorismusbekämpfung auf EU-Ebene dar. Sie legt die Mindeststandards für die Definition von terroristischen Straftaten und Straftaten mit terroristischem Hintergrund sowie für Sanktionen fest und gewährt gleichzeitig den Opfern des Terrorismus Schutz, Hilfe und Unterstützung. Am 30. September 2020 nahm die Kommission einen Bericht[86] an, in dem die Maßnahmen bewertet wurden, welche die Mitgliedstaaten ergriffen haben, um der Richtlinie nachzukommen. Darin gelangt die Kommission zu dem Schluss, dass durch die Umsetzung der Richtlinie in innerstaatliches Recht das strafrechtliche Vorgehen der Mitgliedstaaten gegen Terrorismus sowie die Rechte der Opfer des Terrorismus erheblich gestärkt wurden, jedoch nach wie vor Defizite zu verzeichnen sind. So haben nicht alle Mitgliedstaaten in ihrem innerstaatlichen Recht alle in der Richtlinie aufgeführten Straftaten als terroristische Straftaten eingestuft; zudem wurden nicht in allen Mitgliedstaaten Reisen für terroristische Zwecke und Terrorismusfinanzierung unter Strafe gestellt, und die Bestimmungen über die Unterstützung der Opfer wurden nicht vollständig umgesetzt. Im weiteren Verlauf des Jahres 2021 wird die Kommission einen Bericht über die Bewertung der Richtlinie vorlegen.

Die EU unterstützt die Mitgliedstaaten weiterhin dabei, Terroristen die Mittel für Anschläge zu entziehen und die geltenden Vorschriften umzusetzen. Die Verordnung über die Vermarktung und Verwendung von **Ausgangsstoffen für Explosivstoffe**[87], die im Juni 2019 angenommen wurde, gilt ab dem 1. Februar 2021. Um die nationalen Behörden und den Privatsektor bei der Umsetzung der Verordnung zu unterstützen, veröffentlichte die Kommission im Juni 2020 eine Reihe von Leitlinien[88]. Darüber hinaus legte die Kommission im Juni 2020 ein Programm[89] zur Erfassung der Leistungen, Ergebnisse und Auswirkungen der Verordnung auf.

Im November 2019 forderte die Kommission die Mitgliedstaaten auf, die Umsetzung des im Jahr 2017 vorgelegten Aktionsplans für eine gesteigerte Abwehrbereitschaft gegen **chemische, biologische, radiologische und nukleare** Risiken (**CBRN**-Risiken) [90] zu bewerten. Insgesamt wurde festgestellt, dass die meisten Maßnahmen umgesetzt worden waren. Anfang 2020 erstellte die Kommission in Zusammenarbeit mit nationalen Sachverständigen eine Liste hochgefährlicher, problematischer Chemikalien. Dies bildete die Grundlage für eine Zusammenarbeit mit den Geräteherstellern mit dem Ziel, die Detektionskapazitäten zu steigern. Vor Kurzem leitete die Kommission eine Studie über die Durchführbarkeit der Beschränkung des Zugangs zu einigen dieser Chemikalien in die Wege. Zudem laufen die Arbeiten im Rahmen des Katastrophenschutzverfahrens der Union weiter, und mit den Mitgliedstaaten werden Gespräche über zusätzliche CBRN-Reaktionskapazitäten für die Bereiche Dekontaminierung, Detektion, Überwachung und Monitoring sowie den Aufbau von Lagerbeständen geführt.

---

85 Richtlinie (EU) 2017/541.
86 COM(2020) 619.
87 Verordnung (EU) 2019/1148.
88 Bekanntmachung der Kommission – Leitlinien für die Durchführung der Verordnung (EU) 2019/1148 über die Vermarktung und Verwendung von Ausgangsstoffen für Explosivstoffe (ABl. C 210 vom 24.6.2020, S. 1).
89 SWD(2020) 114 final.
90 COM(2017) 610 final.

Am 12. Oktober 2020 beschloss der Rat, die Sanktionsregelungen gegen die Verbreitung und den Einsatz chemischer Waffen um ein Jahr zu verlängern,[91] sodass die EU die Möglichkeit hat, restriktive Maßnahmen gegen an der Entwicklung und am Einsatz chemischer Waffen beteiligte Personen und Organisationen zu verhängen. Am 14. Oktober 2020 verhängte der Rat restriktive Maßnahmen gegen sechs Personen und eine Organisation, die in den Mordversuch an Alexej Nawalny verwickelt waren, der am 20. August 2020 in Russland mit einem toxischen Nervenkampfstoff der Nowitschok-Gruppe vergiftet worden war.[92]

Finanzinformationen sind ebenfalls von maßgeblicher Bedeutung für die Identifizierung terroristischer Netze, da Terroristen auf Finanzmittel angewiesen sind, um ihre Ausgaben für Reisen, Ausbildung und Ausrüstung zu decken, und die **Bekämpfung der Terrorismusfinanzierung** für Ermittlungen in Terrorismusfällen unverzichtbar ist. Zu den zentralen Anliegen zählen die Ausschöpfung des gesamten Potenzials der vorhandenen Instrumente und nachrichtendienstlichen Informationen, die ordnungsgemäße Umsetzung der international vereinbarten Standards und die Bewältigung der sich verändernden Herausforderungen, die von neuen Technologien und Plattformen der sozialen Medien ausgehen[93] (siehe unten).

Das **Verkehrsnetz** war und ist weiterhin Zielscheibe des Terrorismus. Zu den Maßnahmen der EU in dieser Hinsicht gehört ein risikobasiertes Bewertungskonzept zum Schutz des Luftfahrtsektors.[94] Konfliktgebiete stellen eine ernsthafte Bedrohung für die Zivilluftfahrt dar, und der Austausch von Informationen und der Ergebnisse von Risikobewertungen trägt maßgeblich zur Risikominderung bei.[95] Das auf **Risikobewertungen** basierende Warnsystem der EU für Konfliktgebiete ist als vorbildliches Verfahren anerkannt, und internationale Standards für den Informationsaustausch wurden in EU-Rechtsvorschriften aufgenommen.[96] Auf der Grundlage der im Bereich der Zivilluftfahrt gewonnenen Erfahrungen hat die Kommission das auf Risikobewertungen basierende Konzept auf andere Verkehrsträger ausgeweitet. Die Umsetzung des von der EU beschlossenen **Aktionsplans zur Verbesserung der Sicherheit im Schienenverkehr**[97] kommt gut voran, wobei die Sachkompetenz der EU-Plattform für die Sicherheit im Schienenpersonenverkehr, einer von der Kommission speziell eingerichteten Expertengruppe, von großem Nutzen ist. Im Bereich des Seeverkehrs ist das auf

---

[91] Beschluss (GASP) 2020/1466 des Rates vom 12. Oktober 2020 zur Änderung des Beschlusses (GASP) 2018/1544 über restriktive Maßnahmen gegen die Verbreitung und den Einsatz chemischer Waffen (ABl. L 335 vom 13.10.2020, S. 16).

[92] Beschluss (GASP) 2020/1482 des Rates vom 14. Oktober 2020 zur Änderung des Beschlusses (GASP) 2018/1544 über restriktive Maßnahmen gegen die Verbreitung und den Einsatz chemischer Waffen (ABl. L 341 vom 15.10.2020, S. 9) und Durchführungsverordnung (EU) 2020/1480 des Rates vom 14. Oktober 2020 zur Durchführung der Verordnung (EU) 2018/1542 über restriktive Maßnahmen gegen die Verbreitung und den Einsatz chemischer Waffen (ABl. L 341 vom 15.10.2020, S. 1).

[93] Entsprechend den Ausführungen der EU vom November 2019 bei der von Australien ausgerichteten Ministerkonferenz zur Bekämpfung der Terrorismusfinanzierung mit dem Titel *No Money For Terror* (Kein Geld für den Terror).

[94] Die im Rahmen des integrierten Verfahrens für die Bewertung der Sicherheitsrisiken im EU-Flugverkehr gewonnenen Erkenntnisse fließen in die Entscheidungsfindung im Zusammenhang mit der Luftfrachtsicherheit, den Luftsicherheitsstandards und den von Konfliktgebieten ausgehenden Risiken für die Zivilluftfahrt ein.

[95] Der tragische Absturz von Flug 752 der Ukraine International Airlines am 8. Januar 2020 machte erneut deutlich, wie wichtig der Austausch von Informationen und den Ergebnissen von Risikobewertungen für die Sicherheit der Zivilluftfahrt ist.

[96] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R1583

[97] COM(2018) 470 final.

Risikobewertungen basierende Konzept gut bekannt und wird weithin angewendet, und die Kommission arbeitet mit den Mitgliedstaaten und Interessengruppen zusammen, um die Sicherheit der Passagiere zu stärken. Dies ist Bestandteil der **EU-Strategie für maritime Sicherheit** und des dazugehörigen **Aktionsplans**, die 2018 überarbeitet wurden und auch eine Sicherheits- und Verteidigungsdimension beinhalten. Darauf wird im jüngsten Durchführungsbericht eingegangen, der am 23. Oktober 2020 angenommen und veröffentlicht wurde.[98]

Europol unterstützt die Mitgliedstaaten bei Ermittlungen im Zusammenhang mit Terrorismus über das **Europäische Zentrum zur Terrorismusbekämpfung (ECTC)**. Die Zahl der Anträge der Mitgliedstaaten auf operative Unterstützung nahm weiter zu, und mittlerweile ist das ECTC an nahezu allen wichtigen Ermittlungen in Terrorismusfällen beteiligt. Im Jahr 2019 unterstützte Europol insgesamt 632 verschiedene Operationen im Bereich der Terrorismusbekämpfung. Die Ermittler in den Mitgliedstaaten wissen diese Tätigkeit zunehmend zu schätzen, sodass ihr Zufriedenheitswert zwischen 2018 und 2019 von 8/10 auf 9,1/10 stieg. Das ECTC koordinierte im Jahr 2019 insgesamt 18 Aktionstage.[99]

Zudem unterstützte **Eurojust** in den Jahren 2019 und 2020 insgesamt 116 Ermittlungen in Terrorismusfällen. Gegenwärtig wird ein Gesetzgebungsvorschlag für den digitalen Informationsaustausch über grenzüberschreitende Fälle von Terrorismus erarbeitet, um das 2019 eingerichtete justizielle Terrorismusregister[100] weiterzuentwickeln und die Arbeit im Zusammenhang mit rechts- und linksextremistischen Gruppierungen auszuweiten.

Am 30. Juli 2020 hat Rat die EU-Liste der Personen, Vereinigungen und Körperschaften, die restriktiven Maßnahmen zur Bekämpfung des Terrorismus unterliegen, letztmals aktualisiert. In der aktuellen Liste sind 14 Personen und 21 Körperschaften aufgeführt. Ebenfalls am 30. Juli 2020 verhängte der Rat im Rahmen der Sanktionsregelung gegen ISIL/Da'esh und Al-Qaida restriktive Maßnahmen gegen eine Person. Gegenwärtig werden im Rahmen dieser Regelung, die am 19. Oktober 2020 um ein Jahr verlängert wurde, fünf Personen eigenständig in der Liste geführt.[101]

---

98 Report by Commission services, the European External Action Service and the European Defence Agency on the implementation of the revised EU Maritime Security Strategy Action Plan (Bericht der Kommissionsdienststellen, des Europäischen Auswärtigen Dienstes und der Europäischen Verteidigungsagentur über die Durchführung des überarbeiteten Aktionsplans für die EU-Strategie für maritime Sicherheit), SWD(2020) 252.

99 2019 Consolidated annual activity report (Konsolidierter jährlicher Tätigkeitsbericht 2019), Europol, 9. Juni 2020.

100 Das justizielle Terrorismusregister wird von Eurojust rund um die Uhr verwaltet und bietet den nationalen Behörden proaktive Unterstützung. Diese zentral gesammelten Informationen werden die Staatsanwälte dabei unterstützen, ihre Verfahren aktiver zu koordinieren und Personen oder Netzwerke zu identifizieren, gegen die in Fällen mit potenziell grenzübergreifender Dimension ermittelt wird.

101 Beschluss (GASP) 2020/1132 des Rates vom 30. Juli 2020 zur Aktualisierung der Liste der Personen, Vereinigungen und Körperschaften, auf die die Artikel 2, 3 und 4 des Gemeinsamen Standpunkts 2001/931/GASP über die Anwendung besonderer Maßnahmen zur Bekämpfung des Terrorismus Anwendung finden, und zur Aufhebung des Beschlusses (GASP) 2020/20 (ABl. L 247 vom 31.7.2020, S. 18), Beschluss (GASP) 2020/1126 des Rates vom 30. Juli 2020 zur Änderung des Beschlusses (GASP) 2016/1693 betreffend restriktive Maßnahmen gegen ISIL (Da'esh) und Al-Qaida und mit ihnen verbündete Personen, Gruppen, Unternehmen und Einrichtungen (ABl. L 246 vom 30.7.2020, S. 10) und Beschluss (GASP) 2020/1516 des Rates vom 19. Oktober 2020 zur Änderung des Beschlusses (GASP) 2016/1693 betreffend restriktive Maßnahmen gegen ISIL (Da'esh) und Al-Qaida und mit ihnen verbündete Personen, Gruppen, Unternehmen und Einrichtungen (ABl. L 348 vom 20.10.2020, S. 15).

Ein wichtiges Element der Strategie zur Terrorismusbekämpfung betrifft die von den derzeit in Syrien und im Irak aufhältigen **ausländischen terroristischen Kämpfern** ausgehende Bedrohung. Unbeschadet der primären Zuständigkeit der Mitgliedstaaten für diese Fragen trägt die Unterstützung und Zusammenarbeit auf EU-Ebene dazu bei, dass sie gemeinsame Herausforderungen bewältigen können: Verfolgung von Personen, die terroristische Straftaten begangen haben, Prävention der unentdeckten Einreise in den Schengen-Raum sowie Wiedereingliederung und Rehabilitation zurückgekehrter ausländischer terroristischer Kämpfer. Beispielsweise arbeitet die Kommission eng mit den Mitgliedstaaten und wichtigen Partnerländern zusammen, um sicherzustellen, dass Beweismittel aus Kampfgebieten ausgetauscht und wirksam dafür eingesetzt werden, diese Personen zu identifizieren, an den Grenzen auszumachen und strafrechtlich zu verfolgen. Das von Eurojust im Jahr 2020 veröffentlichte Memorandum über Beweismittel aus Kampfgebieten[102] macht deutlich, dass es zwar in vielfacher Hinsicht schwierig ist, derartige Daten zu beschaffen und sicherzustellen, dass sie die Kriterien für zulässige Beweismittel erfüllen, diese Daten jedoch dazu beitragen können, Terrorverdächtige vor Gericht zu stellen.

Darüber hinaus fördert die Kommission einen Dialog mit Mitgliedstaaten und humanitären Akteuren, um einen umfassenden und faktengestützten Überblick über die Situation in den Lagern im Nordosten Syriens zu gewinnen, in denen Familienangehörige europäischer ausländischer terroristischer Kämpfer untergebracht sind. Ein besonderer Schwerpunkt liegt dabei auf der Situation der Kinder in den syrischen Lagern. Zudem unterstützt die Kommission die Mitgliedstaaten beim Erfahrungsaustausch über nationale Maßnahmen und Mechanismen zur besseren Steuerung der **Rehabilitation und Wiedereingliederung** von zurückkehrenden ausländischen terroristischen Kämpfern und von Kindern. Das Aufklärungsnetzwerk gegen Radikalisierung führt auch Studienbesuche durch und bietet eine maßgeschneiderte Beratung hinsichtlich eines besseren Umgangs mit verurteilten Rückkehrern, insbesondere nach der Entlassung aus Haftanstalten, sowie hinsichtlich der Rolle von Familien und lokalen Gemeinschaften bei der Wiedereingliederung.

Partnerschaften und Zusammenarbeit mit Drittländern und Partnern in der Nachbarschaft der EU bei der Terrorismusbekämpfung sind ebenfalls von grundlegender Bedeutung für die Verbesserung der Sicherheit innerhalb der EU und die bessere Verknüpfung der internen und der externen Dimension der EU-Sicherheitspolitik. Der Rat hat dazu aufgerufen, das auswärtige Engagement der EU im Bereich der Terrorismusbekämpfung weiter zu verstärken,[103] wobei ein besonderer Schwerpunkt auf dem Westbalkan, Nordafrika, dem Nahen und Mittleren Osten, der Sahelzone, dem Horn von Afrika und Asien liegen sollte. Im Rahmen der diesbezüglichen Maßnahmen kommen alle Instrumente des auswärtigen Handelns zum Einsatz, darunter die hochrangigen Dialoge über Terrorismusbekämpfung und das Netzwerk der 17 zu den EU-Delegationen entsandten **Experten für Terrorismusbekämpfung/Sicherheit**[104], das weiterhin Unterstützung leistete, um die Zusammenarbeit und den Ausbau der Kapazitäten zu

[102] https://www.eurojust.europa.eu/eurojust-memorandum-battlefield-evidence-0

[103] Schlussfolgerungen des Rates zum auswärtigen Handeln der EU zur Prävention und Bekämpfung von Terrorismus und Gewaltextremismus vom 16. Juni 2020 (8868/20).

[104] Äthiopien (Verbindungsbeamte bei der Afrikanischen Union), Algerien, Bosnien und Herzegowina (regionale Experten für den Westbalkan), Indonesien (regionale Experten für Südostasien und Verbindungsbeamte beim ASEAN-Regionalforum (ARF)), Irak, Jordanien, Kenia (regionale Experten für das Horn von Afrika), Kirgisistan (regionale Experten für Zentralasien), Libanon, Libyen, Marokko, Nigeria, Pakistan, Saudi-Arabien, Tschad (regionale Experten für den Sahel), Tunesien und Türkei.

fördern. Gegenwärtig wird über die Möglichkeit nachgedacht, dieses Netzwerk zu verstärken und auszuweiten.

Der Gemeinsame Aktionsplan zur Terrorismusbekämpfung für den **westlichen Balkan** und die entsprechenden bilateralen Vereinbarungen, die 2019 mit den einzelnen Partnern geschlossen wurden[105], ermöglichen es, den Schwerpunkt auf eine Region zu legen, die für die gemeinsamen Sicherheitsziele und den Schutz der Menschen in der EU von maßgeblicher Bedeutung ist. Beim Ministerforum EU-Westbalkan für Justiz und Inneres vom 22. Oktober 2020 bekräftigten die EU und die Westbalkan-Partner ihre Entschlossenheit, die Ziele des Gemeinsamen Aktionsplans auch nach 2020 weiterzuverfolgen.[106] Die Zusammenarbeit mit dem Westbalkan umfasst auch die Steuerung der Rückkehr ausländischer terroristischer Kämpfer und ihrer Familienangehörigen und die stärkere Einbindung in Maßnahmen zur Eindämmung der Radikalisierung. Zudem setzt die EU ihre regelmäßige Zusammenarbeit mit dem **Nahen und Mittleren Osten sowie mit Nordafrika und Zentralasien**[107] im Bereich der Terrorismusbekämpfung fort. Im Mittelpunkt der Zusammenarbeit mit **Zentralasien** stand die Eindämmung chemischer, biologischer, radiologischer und nuklearer Bedrohungen. Der Gemischte Kooperationsausschuss **EU/Golf-Kooperationsrat** trat am 25. Juni 2020 zusammen und erörterte Themen wie die Bekämpfung der Radikalisierung und das Vorgehen gegen Terrorismusfinanzierung und Geldwäsche sowie Cybersicherheit und die Zusammenarbeit mit Europol. Ende 2019 führte die EU gemeinsam mit der NATO erstmals ein Audit zu chemischen, biologischen, radiologischen und nuklearen Bedrohungen in einem der Golfstaaten durch. Insgesamt standen Ende 2019 etwa 465 Mio. EUR für laufende Projekte zur Terrorismusbekämpfung und zur Prävention von gewaltbereitem Extremismus außerhalb der EU bereit; dies entspricht einer Steigerung um 15 % gegenüber dem Vorjahr.

Des Weiteren vertiefte die EU weiter ihre Zusammenarbeit mit den **Vereinten Nationen** im Bereich der Terrorismusbekämpfung[108], insbesondere mit dem Büro der Vereinten Nationen für Terrorismusbekämpfung und dem Exekutivdirektorium des Ausschusses zur Bekämpfung des Terrorismus, unter anderem über jährliche hochrangige Dialoge und zuletzt im Sommer 2020 durch aktive Teilnahme an der virtuellen Woche der Vereinten Nationen gegen Terrorismus. Darüber hinaus verfolgte die Kommission aufmerksam die Beratungen über die Neufassung der Definition terroristischer Straftaten im Übereinkommen des **Europarats** zur Verhütung des Terrorismus und regte eine enge Angleichung an die im EU-Recht verankerten Definitionen an. Die enge Zusammenarbeit zwischen der **NATO** und der EU bei der Terrorismusbekämpfung und im Bereich chemischer, biologischer, radiologischer und nuklearer Stoffe wurde fortgeführt, wobei Informationen über den Ausbau der Kapazitäten ausgetauscht wurden, um

---

[105] Albanien, Bosnien und Herzegowina, das Kosovo*, Montenegro, Nordmazedonien und Serbien.

[106] Gemeinsame Presseerklärung https://www.consilium.europa.eu/de/press/press-releases/2020/10/23/joint-press-statement-eu-western-balkans-ministerial-forum-on-justice-and-home-affairs/pdf.

[107] Die Maßnahmen zur Terrorismusbekämpfung werden beispielsweise in der neuen EU-Strategie für Zentralasien hervorgehoben.

*Diese Bezeichnung berührt nicht die Standpunkte zum Status und steht im Einklang mit der Resolution 1244/1999 des VN-Sicherheitsrates und dem Gutachten des Internationalen Gerichtshofs zur Unabhängigkeitserklärung des Kosovos.

[108] Im Jahr 2019 wurde eine Rahmenvereinbarung über die Zusammenarbeit zwischen der EU und den Vereinten Nationen im Bereich der Terrorismusbekämpfung unterzeichnet: https://eeas.europa.eu/sites/eeas/files/2019042019_un-eu_framework_on_counter-terrorism.pdf.

Überschneidungen zu vermeiden und die Komplementarität der Maßnahmen sicherzustellen.

2. Bekämpfung der organisierten Kriminalität

Die organisierte Kriminalität ist auf dem Vormarsch, operiert zunehmend grenzüberschreitend und verlagert sich ins Internet.

Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität (SOCTA) (Europol, 2017)

Die Maßnahmen der Kommission betrafen unter anderem die Bekämpfung von Drogen, illegalen Feuerwaffen, Finanzkriminalität, der illegalen Einfuhr von Kulturgütern, des Menschenhandels und der Umweltkriminalität sowie die Unterstützung der Strafverfolgungs- und Justizbehörden der Mitgliedstaaten und der Partner in der Nachbarschaft. Von maßgeblicher Bedeutung war darüber hinaus die Zusammenarbeit mit Drittländern, insbesondere in der Nachbarschaft, etwa dem westlichen Balkan, sowie mit internationalen Organisationen, darunter mit dem Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung (UNODC)[109].[110]

Im Jahr 2019 erhielt und bearbeitete das bei **Europol** angesiedelte Europäische Zentrum für schwere und organisierte Kriminalität annähernd 55 000 operative Beiträge und damit 12 % mehr als im Vorjahr. Was die Zahl der Operationen betrifft, so unterstützte das Zentrum die Länder in 726 Fällen.[111] Von entscheidender Bedeutung ist weiter, dass der Rechtsrahmen der EU zur Bekämpfung der organisierten Kriminalität[112], mit dem die Angleichung der Rechtsvorschriften der Mitgliedstaaten über Straftatbestände im Zusammenhang mit der Beteiligung an einer kriminellen Vereinigung angestrebt wird und die Sanktionen für diese Straftaten festgelegt werden, in allen Mitgliedstaaten vollständig umgesetzt wird. Die Kommission hat eine Studie in die Wege geleitet, um die Optionen für eine Verbesserung dieses Rechtsrahmens auszuloten. Weitere Maßnahmen zur Intensivierung der Bekämpfung der organisierten Kriminalität in der EU werden in der EU-Agenda zur Bekämpfung der organisierten Kriminalität zusammengestellt, die im ersten Quartal 2021 angenommen werden soll.

---

[109] Am 8. Dezember 2020 fand ein hochrangiger Dialog zwischen der EU und dem UNODC statt.

[110] Ende 2019 standen etwa 830 Mio. EUR für laufende Aktionen gegen die organisierte Kriminalität außerhalb der Union bereit.

[111] 2019 Consolidated Annual Activity Report (Konsolidierter jährlicher Tätigkeitsbericht 2019), Europol, 9. Juni 2020.

[112] Rahmenbeschluss 2008/841/JI des Rates vom 24. Oktober 2008 zur Bekämpfung der organisierten Kriminalität (ABl. L 300 vom 11.11.2008, S. 42).

Die Sicherstellung und Einziehung von Erträgen aus Straftaten zählt zu den wirksamsten Mitteln der Bekämpfung der organisierten Kriminalität. Das neue **Europäische Zentrum für Finanz- und Wirtschaftskriminalität** (EFECC), das im Juni 2020 bei Europol eingerichtet wurde, wird die operative Unterstützung der Mitgliedstaaten und der EU-Einrichtungen im Bereich der Finanz- und Wirtschaftskriminalität verbessern und die systematische Durchführung von Finanzermittlungen erleichtern. Um die Bemühungen der EU um eine wirksamere Ermittlung, Sicherstellung und Einziehung von durch Straftaten erlangtem Vermögen zu unterstützen, verabschiedete der Rat im Juni 2020 Schlussfolgerungen zur Verbesserung der Finanzermittlungen zur Bekämpfung der schweren und organisierten Kriminalität.[113] Im Jahr 2021 wird die Kommission die Rechtsvorschriften über die Sicherstellung und Einziehung von Erträgen aus Straftaten[114] und die Vermögensabschöpfungsstellen[115] überprüfen.

Bei der Bekämpfung der organisierten Kriminalität müssen Garantien gelten, um sicherzustellen, dass die Strafverfolgungsbehörden innerhalb bestimmter Grenzen wirksam arbeiten können, wie sie beispielsweise für den Schutz personenbezogener Daten erforderlich sind. Die Richtlinie zum Datenschutz bei der Strafverfolgung von 2016[116], die den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Zusammenhang mit Straftaten zum Gegenstand hat, schützt das Grundrecht auf Datenschutz in allen Fällen, in denen Strafverfolgungsbehörden personenbezogene Daten zum Zweck der Strafverfolgung verarbeiten. Sie stellt sicher, dass die personenbezogenen Daten von Opfern, Zeugen und Tatverdächtigen ordnungsgemäß geschützt werden, und erleichtert die grenzüberschreitende Zusammenarbeit bei der Bekämpfung von Kriminalität und Terrorismus. Die Frist für die Umsetzung der Richtlinie zum Datenschutz bei der Strafverfolgung endete am 6. Mai 2018. Die meisten Mitgliedstaaten haben bereits Rechtsvorschriften zur Umsetzung der Richtlinie verabschiedet. Jedoch sind derzeit noch einige Vertragsverletzungsverfahren anhängig.[117] Die Kommission prüft gegenwärtig die Konformität der nationalen Umsetzungsvorschriften mit der Richtlinie.

Bekämpfung illegaler Drogen

Im Juli 2020 nahm die Kommission eine neue **EU-Agenda zur Drogenbekämpfung und einen entsprechenden Aktionsplan für den Zeitraum 2021-2025**[118] an, die an die aktuelle EU-Drogenstrategie und den dazugehörigen Aktionsplan[119] anschließen. Darin werden der politische Rahmen und die vorrangigen Maßnahmen für die nächsten fünf Jahre festgelegt. Im Mittelpunkt der Agenda stehen die folgenden Maßnahmen: 1) verbesserte Sicherheitsmaßnahmen gegen den illegalen Drogenhandel, von den

---

[113] Schlussfolgerungen des Rates 8927/20.

[114] Richtlinie 2014/42/EU.

[115] Beschluss 2007/845/JI des Rates.

[116] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 119).

[117] Ungeachtet der Vertragsverletzungsverfahren haben drei Mitgliedstaaten (Deutschland, Slowenien, Spanien) die vollständige Umsetzung noch nicht mitgeteilt. Die Kommission erhob beim Gerichtshof gegen einen Mitgliedstaat Klage wegen Nichtumsetzung der Richtlinie und richtete im Mai 2020 an die beiden anderen Mitgliedstaaten weitere mit Gründen versehene Stellungnahmen wegen unvollständiger Umsetzung der Richtlinie.

[118] COM(2020) 606.

[119] Die EU-Drogenstrategie (2013–2020) und der Drogenaktionsplan der EU 2017–2020.

organisierten kriminellen Gruppen über das Außengrenzenmanagement bis hin zur illegalen Herstellung und zum illegalen Vertrieb; 2) erhöhte Prävention, einschließlich der Sensibilisierung für die schädlichen Auswirkungen von Drogen und insbesondere für den Zusammenhang zwischen Drogenkonsum, Gewalt und anderen Formen der Kriminalität; 3) Reduzierung drogenbedingter Schäden durch Zugang zu Behandlung, Minderung der Gesundheitsrisiken und -schäden und einen ausgewogenen Ansatz für das Problem des Drogenkonsums in Haftanstalten. Am 30. November 2020 nahm die Kommission zudem einen Bericht über die Evaluierung der EU-Verordnungen über Drogenausgangsstoffe an, in dem sie zu dem Schluss gelangt, dass weitere Maßnahmen erforderlich seien, um zu verhindern, dass kriminelle Vereinigungen in der EU Zugang zu den Stoffen haben, die sie für die Herstellung illegaler synthetischer Drogen benötigen.[120]

Darüber hinaus hat die EU konkrete Projekte finanziert, mit denen die Bekämpfung illegaler Drogen verbessert werden soll, beispielsweise das Drogenforum der Zivilgesellschaft. In dem am 22. September 2020 veröffentlichten Europäischen Drogenbericht 2020 der Europäischen Beobachtungsstelle für Drogen und Drogensucht[121] werden die jüngsten Entwicklungen im Bereich des Drogenkonsums und der Drogenmärkte in der EU, der Türkei und Norwegen aufgezeigt. Dem Bericht zufolge ist in der EU eine steigende Verfügbarkeit von Kokain zu beobachten, wobei die Sicherstellungen ein Rekordhoch von 181 Tonnen erreicht haben, während sich die Sicherstellungen von Heroin mit 9,7 Tonnen nahezu verdoppelt haben; zugleich wurde eine hohe Verfügbarkeit von Drogen mit hohem Reinheitsgrad festgestellt. Des Weiteren werden in dem Bericht das Aufkommen neuartiger synthetischer Opioide, bestimmte gesundheitliche Belange und die durch die COVID-19-Pandemie hervorgerufenen Probleme beleuchtet.

Die Drogenbekämpfung wird auf unterschiedlichen Ebenen weitergeführt. Das **Legislativpaket zu neuen psychoaktiven Substanzen** (NPS) wurde im Herbst 2017 verabschiedet[122] und ist seit November 2018 in vollem Umfang anwendbar. Gegen fünf Mitgliedstaaten sind noch immer Vertragsverletzungsverfahren anhängig.[123] Mittlerweile wurde der erste delegierte Rechtsakt zur Aufnahme einer neuen psychoaktiven Substanz (Isotonitazen) in die Definition von Drogen verabschiedet.[124]

---

120 Bericht der Kommission an das Europäische Parlament und den Rat: Evaluierung der EU-Verordnungen über Drogenausgangsstoffe, COM(2020) 768 final vom 30. November 2020.

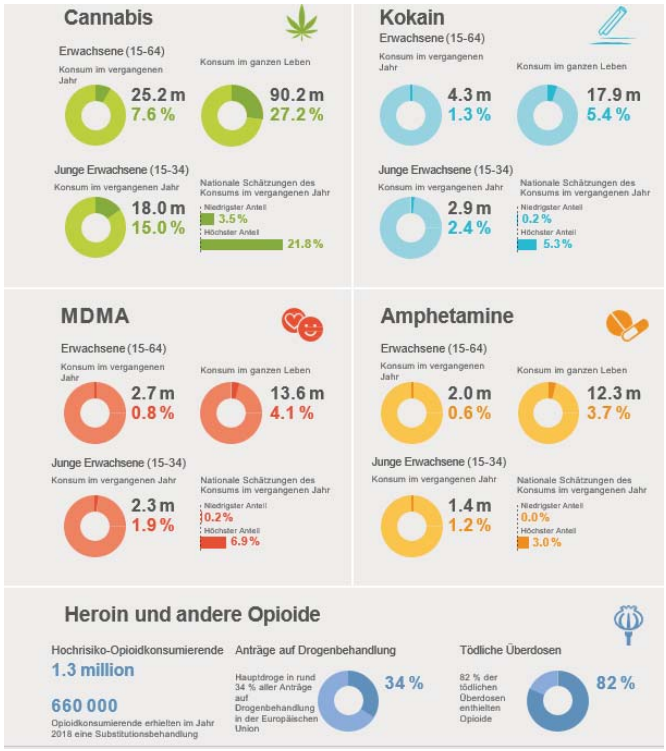
121 European Drug Report 2020: Trends and Developments (Europäischer Drogenbericht 2020: Trends und Entwicklungen), EMCDDA, 22. September 2020.

122 Verordnung (EU) 2017/2101 des Europäischen Parlaments und des Rates vom 15. November 2017 zur Änderung der Verordnung (EG) Nr. 1920/2006 in Bezug auf den Informationsaustausch zu neuen psychoaktiven Substanzen und das Frühwarnsystem und das Risikobewertungsverfahren für neue psychoaktive Substanzen (ABl. L 305 vom 21.11.2017, S. 1) und Richtlinie (EU) 2017/2103 des Europäischen Parlaments und des Rates vom 15. November 2017 zur Änderung des Rahmenbeschlusses 2004/757/JI des Rates zur Aufnahme neuer psychoaktiver Substanzen in die Drogendefinition und zur Aufhebung des Beschlusses 2005/387/JI des Rates (ABl. L 305 vom 21.11.2017, S. 12).

123 Finnland, Irland, Österreich, Portugal und Slowenien.

124 Delegierte Richtlinie (EU) 2020/1687 der Kommission vom 2. September 2020 zur Änderung des Anhangs des Rahmenbeschlusses 2004/757/JI des Rates im Hinblick auf die Aufnahme der neuen psychoaktiven Substanz N, N-Diethyl-2-[[4-(1-methylethoxy)-phenyl]-methyl]-5-nitro-1H-benzimidazol-1-ethanamin (Isotonitazen) in die Definition von Drogen, C/2020/5897 (ABl. L 379 vom 13.11.2020, S. 55).

Auf **internationaler Ebene** arbeitete die EU aktiv in der Suchtstoffkommission der Vereinten Nationen mit[125], insbesondere um aktuelle Informationen über die Aufnahme neuer psychoaktiver Substanzen[126] und die erneute Aufnahme von Cannabis und Cannabis-verwandten Stoffen[127] vorzulegen. Der Rat billigte die Aufnahme von zwei neuen Dialogen, und zwar mit China und Iran[128], und die Europäische Beobachtungsstelle für Drogen und Drogensucht erzielte Fortschritte bei den Arbeitsvereinbarungen mit Drittstaaten[129].



Bekämpfung der Finanzkriminalität

Es wurden neue Rechtsvorschriften verabschiedet, um die Bekämpfung der Finanzkriminalität und der Geldwäsche zu verbessern. Mit der im Jahr 2019 angenommenen Richtlinie zur Festlegung von Vorschriften zur Erleichterung der Nutzung von Finanz- und sonstigen Informationen für die Verhütung, Aufdeckung, Untersuchung oder Verfolgung bestimmter Straftaten wurde den Strafverfolgungsbehörden sowie den Vermögensabschöpfungsstellen Zugang zu den nationalen zentralen Bankkontenregistern für die Zwecke der Bekämpfung schwerer Straftaten gewährt. Darüber hinaus soll mit der Richtlinie die Zusammenarbeit zwischen den Strafverfolgungsbehörden und den zentralen Meldestellen (FIU) verbessert und der Informationsaustausch zwischen diesen Meldestellen erleichtert werden. Im Juni 2020 veröffentlichte die Kommission einen Bericht mit dem Titel „Abschöpfung und Einziehung von Vermögenswerten: Straftaten dürfen sich nicht auszahlen“[130]. Darin wies sie auf das Potenzial für eine stärkere Harmonisierung der Regelungen für die Vermögensabschöpfung[131] hin, durch die eine Modernisierung der EU-Rechtsvorschriften über die Vermögensabschöpfung und eine

[125] Ein Leitungsgremium des Büros der Vereinten Nationen für Drogen- und Verbrechensbekämpfung (UNODC).
[126] COM(2019) 631.
[127] COM(2019) 624, COM(2020) 659.
[128] Beim Gipfeltreffen EU-China, das am 16./17. Juli 2018 in Peking stattfand, wurde vereinbart, einen jährlichen Dialog EU-China über Drogen aufzunehmen. Die Modalitäten des künftigen Dialogs wurden am 30. Oktober 2019 vom AStV bestätigt. Am 5. März 2020 billigte der Rat die Aufnahme eines neuen Dialogs EU-Iran über Drogen.
[129] Stellungnahmen der Kommission über den Entwurf einer Arbeitsvereinbarung mit dem Kosovo vom 14. April 2020 und über den Entwurf einer Arbeitsvereinbarung mit Serbien vom 16. Dezember 2019.
[130] COM(2020) 217.
[131] Einschließlich einer Bewertung der Richtlinie 2014/42/EU vom 3. April 2014 über die Sicherstellung und Einziehung von Tatwerkzeugen und Erträgen aus Straftaten in der Europäischen Union (ABl. L 127 vom 29.4.2014, S. 39) und des Beschlusses 2007/845/JI des Rates vom 6. Dezember 2007 über die Zusammenarbeit zwischen den Vermögensabschöpfungsstellen der Mitgliedstaaten auf dem Gebiet des Aufspürens und der Ermittlung von Erträgen aus Straftaten oder anderen Vermögensgegenständen im Zusammenhang mit Straftaten (ABl. L 332 vom 18.12.2007, S. 103).

Stärkung der Kapazitäten der nationalen Behörden für die Bekämpfung der organisierten Kriminalität erreicht würden. Zudem wurde eine externe Studie für weitere Analysen zur Vermögensabschöpfung in Auftrag gegeben. Die Verordnung über die gegenseitige Anerkennung von Sicherstellungs- und Einziehungsentscheidungen[132] gilt ab dem 19. Dezember 2020 und wird eine deutliche Verbesserung der Zusammenarbeit zwischen den Mitgliedstaaten ermöglichen.

Im Mai 2020 verabschiedete die Kommission **einen Aktionsplan für eine umfassende Politik der Union zur Verhinderung von Geldwäsche und Terrorismusfinanzierung**[133], um den Rechtsrahmen der EU zu stärken. Am 5. November billigte der Rat Schlussfolgerungen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung[134], in denen er die Kommission insbesondere ersuchte, an der Annahme eines einheitlichen Regelwerks, der Einführung einer unabhängigen Aufsicht und der Koordinierung der zentralen Meldestellen zu arbeiten. Im Einklang mit den Schlussfolgerungen des Rates zur Verbesserung der Finanzermittlungen[135] beurteilt die Kommission gegenwärtig auch die Notwendigkeit einer Vernetzung der zentralen Bankkontenregister, durch die der Zugang der zentralen Meldestellen und der Strafverfolgungsbehörden zu Informationen über Bankkonten erheblich beschleunigt würde. Zugleich werden weiterhin Maßnahmen ergriffen, um sicherzustellen, dass die jüngsten EU-Standards von den Mitgliedstaaten wirksam umgesetzt werden. Die Bestimmungen der fünften Geldwäscherichtlinie zielen darauf ab, eine höhere Transparenz der Eigentümerstrukturen von Unternehmen zu gewährleisten. Die Frist für die Umsetzung der Richtlinie endete am 1. Januar 2020, und die Kommission leitete gegen 16 Mitgliedstaaten Vertragsverletzungsverfahren ein.[136] Eine weitere wichtige Maßnahme ist die neue Verordnung über die Überwachung von Barmitteln[137], die im Oktober 2018 erlassen wurde und ab dem 3. Juni 2021 gilt. Mit dieser Verordnung wird das vorhandene System der Überwachung von Barmitteln, die in die oder aus der EU verbracht werden, verbessert; die einschlägigen Durchführungsbestimmungen werden derzeit erarbeitet.

Was das auswärtige Handeln betrifft, so werden die Bemühungen um die Unterstützung der Partnerländer bei der Bekämpfung von Geldwäsche und Terrorismusfinanzierung fortgesetzt. In diesem Zusammenhang spielen der EAD und die EU-Delegationen eine Schlüsselrolle bei der Förderung und Unterstützung der politischen Zusammenarbeit mit Drittländern und internationalen Organisationen wie der Arbeitsgruppe „Bekämpfung der Geldwäsche und der Terrorismusfinanzierung“ (FATF).

Ergänzend dazu hat die Kommission eine globale Fazilität geschaffen, um die Partnerländer außerhalb der EU bei der Errichtung eines wirksamen Rahmens für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung im Einklang mit den internationalen Standards zu unterstützen. Diese Maßnahme, die mit 20 Mio. EUR

---

[132] Verordnung (EU) 2018/1805 des Europäischen Parlaments und des Rates vom 14. November 2018 über die gegenseitige Anerkennung von Sicherstellungs- und Einziehungsentscheidungen (ABl. L 303 vom 28.11.2018, S. 1).

[133] C(2020) 2800 final.

[134] Schlussfolgerungen des Rates 12608/20.

[135] Schlussfolgerungen des Rates 8927/20.

[136] Belgien, Estland, Griechenland, Irland, Luxemburg, Niederlande, Österreich, Polen, Portugal, Rumänien, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn und Zypern sowie Vereinigtes Königreich.

[137] Verordnung (EU) 2018/1672 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 über die Überwachung von Barmitteln, die in die Union oder aus der Union verbracht werden, und zur Aufhebung der Verordnung (EG) Nr. 1889/2005 (ABl. L 284 vom 12.11.2018, S. 6).

ausgestattet ist, dient auch der Förderung der Zusammenarbeit zwischen Akteuren aus dem Finanzbereich und der Justiz auf nationaler, regionaler und internationaler Ebene.

Bekämpfung der Korruption

Korruption stellt an sich bereits eine Straftat dar und ist darüber hinaus ein entscheidender Faktor für organisierte Kriminalität. Die Verhütung und Bekämpfung von Korruption unterliegt der regelmäßigen Überwachung und Bewertung des Rechtsrahmens der Mitgliedstaaten gemäß dem neuen **Rechtsstaatlichkeitsmechanismus**[138]. Der erste EU-weite Bericht über Rechtsstaatlichkeit wurde am 30. September 2020 angenommen.[139] Er ließ erkennen, dass viele Mitgliedstaaten im Bereich der Rechtsstaatlichkeit über hohe Standards verfügen, jedoch noch erhebliche Herausforderungen zu meistern sind. Der Bericht enthält objektive und sachliche jährliche Bewertungen aller Mitgliedstaaten, deren Ziel es ist, die Kenntnis und das Verständnis neuer Entwicklungen in den einzelnen Mitgliedstaaten zu verbessern, um in der Lage zu sein, Risiken zu ermitteln, mögliche Lösungen zu erarbeiten und frühzeitig gezielte Unterstützung bereitzustellen. Die **Europäische Staatsanwaltschaft** (EUStA) wird in den derzeit 22 teilnehmenden EU-Mitgliedstaaten gegen Straftaten zulasten des EU-Haushalts vorgehen. Sie wird befugt sein, gegen für Straftaten zulasten des EU-Haushalts, etwa Betrug, Korruption und schweren grenzüberschreitenden Mehrwertsteuerbetrug, verantwortliche Personen zu ermitteln, sie strafrechtlich zu verfolgen und Anklage gegen sie zu erheben. Die EUStA wird ihre Tätigkeit voraussichtlich im ersten Quartal 2021 aufnehmen.[140]

Die Kommission prüft derzeit die Umsetzung der Vorschriften in der **Richtlinie über die strafrechtliche Bekämpfung von gegen die finanziellen Interessen der Union gerichtetem Betrug**[141] in nationales Recht und hat Vertragsverletzungsverfahren gegen die Mitgliedstaaten eingeleitet, die die vollständige Umsetzung noch nicht mitgeteilt haben.[142] Im Jahr 2021 wird die Kommission einen Bericht vorlegen, in dem sie bewertet, inwieweit die Mitgliedstaaten die erforderlichen Maßnahmen ergriffen haben, um der Richtlinie nachzukommen.

Bekämpfung des illegalen Handels mit Kulturgütern

Das Hauptziel der im April 2019 erlassenen **Verordnung über das Verbringen und die Einfuhr von Kulturgütern**[143] ist es, die Einfuhr von unzulässig aus ihrem Herkunftsland ausgeführten Kulturgütern in die Union zu unterbinden. Um die ordnungsgemäße Durchführung dieser Verordnung sicherzustellen, bereitet die Kommission gegenwärtig die Verabschiedung von Durchführungsbestimmungen vor, unter anderem für ein zentrales elektronisches System für die Einfuhr von Kulturgütern, das die Speicherung und den

---

138 Der europäische Rechtsstaatlichkeitsmechanismus bietet ein Verfahren für einen Dialog über Rechtsstaatlichkeit zwischen der Kommission, den Mitgliedstaaten, dem Rat, dem Europäischen Parlament, den nationalen Parlamenten, der Zivilgesellschaft und weiteren Interessenträgern. Fundament dieses neuen Verfahrens sind die Berichte über Rechtsstaatlichkeit.

139 COM(2020) 580.

140 Der Durchführungsbeschluss des Rates zur Ernennung der Europäischen Staatsanwälte der Europäischen Staatsanwaltschaft trat am 29. Juli 2020 in Kraft. Das Kollegium Europäischer Staatsanwälte trat am 28. September 2020 erstmals zusammen. Die EUStA wird demnächst Arbeitsvereinbarungen mit Europol, Eurojust und dem OLAF schließen.

141 Richtlinie (EU) 2017/1371 des Europäischen Parlaments und des Rates vom 5. Juli 2017 über die strafrechtliche Bekämpfung von gegen die finanziellen Interessen der Union gerichtetem Betrug (ABl. L 198 vom 28.7.2017, S. 29).

142 Gegenwärtig sind Vertragsverletzungsverfahren gegen Irland, Österreich und Rumänien anhängig.

143 Verordnung (EU) 2019/880.

Austausch von Informationen zwischen den Mitgliedstaaten sowie die Abwicklung der erforderlichen Einfuhrformalitäten ermöglichen wird.[144] Bis Ende 2020 wird ein allgemeines Verbot in Kraft treten, durch das die Zollbehörden der Mitgliedstaaten die rechtlichen Mittel erhalten, um bei Sendungen, die unzulässig aus ihren Herkunftsländern ausgeführte Kulturgüter beinhalten könnten, Kontrollen vorzunehmen und tätig zu werden.

Bekämpfung des illegalen Handels mit Feuerwaffen

Am 24. Juli 2020 veröffentlichte die Kommission **einen neuen EU-Aktionsplan gegen den unerlaubten Handel mit Feuerwaffen (2020-2025)[145]**. Zuvor hatten die Außen- und die Innenminister der EU-Mitgliedstaaten und der westlichen Balkanstaaten auf einer hochrangigen Konferenz am 31. Januar 2020 die Notwendigkeit weiterer Maßnahmen zur Bekämpfung des illegalen Handels mit Schusswaffen betont. Der Aktionsplan umfasst spezifische Maßnahmen zur Verbesserung der rechtlichen Kontrolle von Feuerwaffen, des Wissens über die Bedrohung durch Feuerwaffen, der Zusammenarbeit in der Strafverfolgung und der internationalen Zusammenarbeit mit Schwerpunkt auf Südosteuropa. Die Kommission hat Schritte unternommen, um sicherzustellen, dass die im Mai 2017 angenommene Richtlinie über die Kontrolle des Erwerbs und des Besitzes von Waffen[146] von den Mitgliedstaaten vollständig umgesetzt wird. Jedoch haben zehn Mitgliedstaaten die vollständige Umsetzung der Richtlinie noch nicht mitgeteilt[147]; zudem wurde der anschließend erlassene Durchführungsrechtsakt von der großen Mehrheit der Mitgliedstaaten noch nicht umgesetzt. Infolgedessen hat die Kommission Vertragsverletzungsverfahren eingeleitet.[148] Darüber hinaus bewertet die Kommission derzeit eingehend die mitgeteilten Umsetzungsmaßnahmen und wird im ersten Halbjahr 2021 einen Bericht über die Umsetzung der Richtlinie vorlegen. Des Weiteren hat die Kommission mit der Bewertung der möglichen Modernisierung des Rechtsrahmens für

---

144 Das elektronische System für die Einfuhr von Kulturgütern (EKG) muss spätestens am 28. Juni 2025 eingerichtet sein. Die Kommission hat einen ersten Fortschrittsbericht über die Entwicklung des EKG angenommen (COM(2020) 342 final).

145 COM(2020) 608: Dieser neue Aktionsplan schließt auch die französisch-deutsche Westbalkaninitiative „Fahrplan für eine nachhaltige Lösung für den illegalen Besitz und Missbrauch von Kleinwaffen und leichten Waffen (SALW) und zugehöriger Munition sowie den unerlaubten Handel damit bis 2024“ ein.

146 Richtlinie (EU) 2017/853. Ebenfalls von großer Bedeutung sind zwei Durchführungsrichtlinien vom 16. Januar 2019 zur Festlegung technischer Spezifikationen für die Kennzeichnung von Feuerwaffen sowie für Schreckschuss- und Signalwaffen.

147 Tschechische Republik, Dänemark, Spanien, Zypern, Luxemburg, Ungarn, Polen, Slowenien, Slowakei und Schweden.

148 Bezüglich dieser Richtlinie sind 25 Vertragsverletzungsverfahren anhängig (Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Lettland, Litauen, Luxemburg, Malta, Niederlande, Österreich, Polen, Portugal, Rumänien, Schweden, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn und Zypern sowie Vereinigtes Königreich); bezüglich der Durchführungsrichtlinien sind 34 Vertragsverletzungsverfahren anhängig (Durchführungsrichtlinie (EU) 2019/68 der Kommission vom 16. Januar 2019 zur Festlegung technischer Spezifikationen für die Kennzeichnung von Feuerwaffen und deren wesentlichen Bestandteilen gemäß der Richtlinie 91/477/EWG des Rates über die Kontrolle des Erwerbs und des Besitzes von Waffen (ABl. L 15 vom 17.1.2019, S. 18): Belgien, Bulgarien, Deutschland, Finnland, Griechenland, Irland, Italien, Kroatien, Luxemburg, Österreich, Polen, Rumänien, Schweden, Slowenien, Spanien, Tschechische Republik, Ungarn und Zypern sowie Vereinigtes Königreich; Durchführungsrichtlinie (EU) 2019/69 der Kommission vom 16. Januar 2019 zur Festlegung technischer Spezifikationen für Schreckschuss- und Signalwaffen gemäß der Richtlinie 91/477/EWG des Rates über die Kontrolle des Erwerbs und des Besitzes von Waffen (ABl. L 15 vom 17.1.2019, S. 22): Bulgarien, Finnland, Griechenland, Irland, Italien, Kroatien, Luxemburg, Niederlande, Polen, Rumänien, Schweden, Slowenien, Spanien, Tschechische Republik, Ungarn und Zypern sowie Vereinigtes Königreich).

Maßnahmen im Zusammenhang mit der Einfuhr, Ausfuhr und Durchfuhr von Feuerwaffen begonnen.[149]

Bekämpfung des Menschenhandels

In der EU-Strategie für eine Sicherheitsunion wurde die Notwendigkeit hervorgehoben, im Rahmen der Agenda zur Bekämpfung der organisierten Kriminalität ein neues strategisches Konzept zur Bekämpfung des Menschenhandels zu erarbeiten. Darüber hinaus veröffentlichte die Kommission im Oktober 2020 gemäß Artikel 20 der Richtlinie zur Bekämpfung des Menschenhandels[150] ihren dritten Bericht über die Fortschritte bei der Bekämpfung des Menschenhandels[151].
Diesem Bericht zufolge wurden Fortschritte bei der transnationalen Zusammenarbeit, bei grenzüberschreitenden operativen Strafverfolgungs- und Justizmaßnahmen, bei der Einrichtung nationaler und transnationaler Verweismechanismen für die Opfer sowie bei der Weiterentwicklung der Wissensbasis über den Menschenhandel erzielt. Bei der Bekämpfung des Menschenhandels sowohl innerhalb der EU als auch darüber hinaus greifen die Mitgliedstaaten zunehmend auf EU-Agenturen zurück, um Informationen auszutauschen, gemeinsame Aktionen durchzuführen und gemeinsame Ermittlungsgruppen einzusetzen.[152] Die operative Zusammenarbeit hat greifbare Ergebnisse erbracht,

[149] Geregelt durch die Verordnung (EU) Nr. 258/2012 des Europäischen Parlaments und des Rates vom 14. März 2012 zur Umsetzung des Artikels 10 des Protokolls der Vereinten Nationen gegen die unerlaubte Herstellung von Schusswaffen, dazugehörigen Teilen und Komponenten und Munition und gegen den unerlaubten Handel damit, in Ergänzung des Übereinkommens der Vereinten Nationen gegen die grenzüberschreitende organisierte Kriminalität (VN-Feuerwaffenprotokoll) und zur Einführung von Ausfuhrgenehmigungen für Feuerwaffen, deren Teile, Komponenten und Munition sowie von Maßnahmen betreffend deren Einfuhr und Durchfuhr (ABl. L 94 vom 30.3.2012, S. 1).

[150] Richtlinie 2011/36/EU des Europäischen Parlaments und des Rates vom 5. April 2011 zur Verhütung und Bekämpfung des Menschenhandels und zum Schutz seiner Opfer sowie zur Ersetzung des Rahmenbeschlusses 2002/629/JI des Rates (ABl. L 101 vom 15.4.2011, S. 1).

[151] Bericht der Kommission an das Europäische Parlament und den Rat: Dritter Bericht über die Fortschritte bei der Bekämpfung des Menschenhandels (2020) gemäß Artikel 20 der Richtlinie 2011/36/EU zur Verhütung und Bekämpfung des Menschenhandels und zum Schutz seiner Opfer, COM(2020) 661 final; ergänzend dazu wurde eine Studie über die Erhebung von Daten zum Menschenhandel in der EU für den Zeitraum 2017 bis 2018 vorgelegt.

[152] Beispielsweise arbeitete die Europäische Arbeitsbehörde mit Europol zusammen, um gegen den Menschenhandel in der EU zum Zweck der Ausbeutung in allen Formen, darunter auch der sexuellen Ausbeutung und der Ausbeutung von Arbeitskräften, sowie gegen alle Formen des Kinderhandels

insbesondere im Rahmen der Europäischen multidisziplinären Plattform gegen kriminelle Bedrohungen: Im Jahr 2019 wurden in diesem Zusammenhang 825 Festnahmen vorgenommen sowie 8 824 Verdächtige und 1 307 potenzielle Opfer ermittelt, darunter 69 Minderjährige. Des Weiteren wurden 94 organisierte kriminelle Gruppen ermittelt oder zerschlagen und Vermögenswerte in Höhe von 1,5 Mio. EUR von Bankkonten, Unternehmen und Webdomänen eingefroren. Anlässlich des Europäischen Tags gegen Menschenhandel am 18. Oktober 2020 veröffentlichte die Kommission eine Studie über die Kosten des Menschenhandels und eine weitere über die nationalen und transnationalen Verweismechanismen.[153]

Schleusung von Migranten

Das Europäische Zentrum zur Bekämpfung der Migrantenschleusung berichtete über eine fortgesetzte Zunahme der Aktivitäten im Zusammenhang mit der **Schleusung von Migranten**, insbesondere im Westbalkan und seinen Nachbarländern, sowie der Sekundärbewegungen innerhalb der EU. Im Jahr 2019 trug Europol zur Ermittlung von 14 218 Personen bei, die verdächtigt wurden, an der Schleusung von Migranten beteiligt zu sein.[154] Im Mai 2020 setzte Eurojust die Fokusgruppe der im Bereich der Migrantenschleusung tätigen Staatsanwälte (Focus Group for Prosecutors on Migrant Smuggling) ein, die als bedeutendes Forum für regelmäßige Kontakte zwischen den wichtigsten auf nationaler Ebene handelnden Akteuren der Justiz in den EU-Mitgliedstaaten und zur Unterstützung ihrer gemeinsamen operativen Maßnahmen dient.[155]

Bekämpfung der Umweltkriminalität

Umweltstraftaten sind Handlungen, die gegen Umweltvorschriften verstoßen und erhebliche Schäden oder Risiken für die Umwelt und die menschliche Gesundheit verursachen oder verursachen können.[156] Zu den wichtigsten Formen der **Umweltkriminalität** zählen die rechtswidrige Emission oder Einleitung von Stoffen in die Luft, in Gewässer oder den Boden, der illegale Handel mit wildlebenden Arten, der illegale Handel mit ozonabbauenden Stoffen und die illegale Verbringung oder Ablagerung von Abfällen. Wie die jüngste Evaluierung der Richtlinie über den strafrechtlichen Schutz der Umwelt[157] erkennen ließ, gingen die Fortschritte bei der Entwicklung eines europäischen Rahmens nicht mit einer spürbaren Wirkung vor Ort einher, beispielsweise in Bezug auf eine bessere grenzüberschreitende Zusammenarbeit und gerechtere Rahmenbedingungen für die Ahndung von Verstößen in den Mitgliedstaaten. Insbesondere führten sie nicht zu mehr Verurteilungen oder zur Verhängung abschreckenderer Sanktionen in den Mitgliedstaaten. Daher wurde beschlossen, die Richtlinie bis Ende 2021 zu überprüfen.

---

vorzugehen. Dies steht auch im Einklang mit dem Protokoll von 2014 zum Übereinkommen (Nr. 29) der Internationalen Arbeitsorganisation über Zwangsarbeit. Bei diesem Protokoll handelt es sich um eine Kernarbeitsnorm, die Zwangsarbeit als Straftat benennt und sich mit der Prävention, dem Opferschutz, der Entschädigung und der internationalen Zusammenarbeit in Bezug auf moderne Formen der Zwangsarbeit, darunter im Zusammenhang mit Menschenhandel, befasst.

153 Studien über die wirtschaftlichen, sozialen und menschlichen Kosten des Menschenhandels in der EU bzw. zur Überprüfung der Funktionsweise der nationalen und transnationalen Verweismechanismen der Mitgliedstaaten, verfügbar unter https://ec.europa.eu/anti-trafficking.

154 Europäisches Zentrum zur Bekämpfung der Migrantenschleusung, 4th annual report, 15. Mai 2020.

155 http://www.eurojust.europa.eu/press/PressReleases/Pages/2020/2020-05-29.aspx

156 Richtlinie 2008/99/EG des Europäischen Parlaments und des Rates vom 19. November 2008 über den strafrechtlichen Schutz der Umwelt (ABl. L 328 vom 6.12.2008, S. 28).

157 SWD(2020) 259 final.

Am 29./30. Oktober 2019 veranstaltete Eurojust gemeinsam mit dem Europäischen Netz der in Umweltsachen tätigen Staatsanwälte (EPNE) eine Konferenz zum Thema Internationale Kooperation und Zusammenarbeit im Kampf gegen Umweltkriminalität, um Staatsanwälte und andere Fachkräfte innerhalb und außerhalb der EU für die Umweltkriminalität zu sensibilisieren und die Zusammenarbeit zwischen ihnen zu fördern.

Der im Jahr 2016 angenommene Aktionsplan der EU zur Bekämpfung des illegalen Artenhandels wird gegenwärtig evaluiert. Bis Januar 2021 läuft ein Projekt zur Bekämpfung des Artenhandels innerhalb der und über die EU unter Nutzung des Internets und von Paketzustelldiensten; Ziel ist die Störung und Zerschlagung der im Bereich des Artenhandels aktiven cyberkriminellen Netze.[158]

V. EINE STARKE EUROPÄISCHE SICHERHEITSGEMEINSCHAFT

Eine echte, effektive Sicherheitsunion muss das gemeinsame Anliegen aller Bereiche unserer Gesellschaft sein. Um Vorsorge und Resilienz auf allen Ebenen zu gewährleisten, vor allem mit Blick auf jene, die besonders gefährdet sind wie Opfer und Zeugen, müssen alle Beteiligten – die Exekutive einschließlich der Strafverfolgung ebenso wie der Privatsektor, das Bildungswesen und die Bürgerinnen und Bürger selbst – eingebunden, entsprechend ausgestattet und gut miteinander vernetzt werden.

1. Zusammenarbeit und Informationsaustausch

Einer der wichtigsten Beiträge, die die EU zum Schutz der Bürgerinnen und Bürger leisten kann, ist es, diejenigen, die für die Sicherheit verantwortlich sind, so zu unterstützen, dass sie gut zusammenarbeiten. Zusammenarbeit und Informationsaustausch sind wirksame Instrumente zur Bekämpfung von Kriminalität und Terrorismus, zur Bewältigung von Bedrohungen, etwa im Bereich der Cybersicherheit, und zur Durchsetzung von Recht und Gesetz. Zur Unterstützung des Informationsaustauschs zwischen den Strafverfolgungs- und Justizbehörden wurde eine Reihe von Instrumenten geschaffen.

Heute verabschiedet die Kommission ein überarbeitetes Mandat für **Europol**[159], das mehrere gezielte Verbesserungen für dessen Tätigkeit herbeiführen soll. Auf diese Weise wird Europol zu einem besseren Umgang mit der veränderlichen Natur der unter Nutzung des Internets begangenen Straftaten und mit Finanzkriminalität befähigt. Zudem wird dadurch die Zusammenarbeit mit dem Privatsektor verstärkt und eine Anpassung der Datenschutzbestimmungen an die geltenden EU-Regeln vorgenommen.

Europol und andere EU-Agenturen wie Frontex, CEPOL und Eurojust haben mit Unterstützung der Kommission die „**Europäische multidisziplinäre Plattform gegen kriminelle Bedrohungen**“ (EMPACT)[160] weiterentwickelt, die sich in den EU-Politikzyklus zur Bekämpfung der schweren und internationalen organisierten Kriminalität einfügt. Die Zusammenarbeit im Rahmen von EMPACT hat sich weiterhin als ein

---

[158] https://wwf.be/fr/wildlife-cybercrime/

[159] COM (2020) 796.

[160] EMPACT ist das EU-Instrument der polizeilichen Zusammenarbeit; Ziel ist es, den wichtigsten Bedrohungen für die Sicherheit der EU zu begegnen, indem die Zusammenarbeit zwischen den zuständigen Dienststellen der Mitgliedstaaten, den EU-Organen und -Einrichtungen sowie Drittländern und Organisationen intensiviert wird. Im Rahmen von EMPACT arbeiten unterschiedliche Interessenträger zusammen (multidisziplinäres Konzept), um die Zusammenarbeit zwischen den Mitgliedstaaten, den Organen und Einrichtungen der EU sowie Drittländern und Organisationen, einschließlich des Privatsektors, zu verbessern und zu intensivieren.

wirksames Instrument zur Bekämpfung der organisierten Kriminalität in ganz Europa erwiesen, beispielsweise im Zuge der „gemeinsamen Aktionstage“ im September, Oktober und November 2020.[161] Dies ist ein eindeutiger Beleg für den Wert der Zusammenarbeit. Ferner wurden auch weniger quantifizierbare Ziele verfolgt: verbessertes Lagebild, Schulungen und Kapazitätsaufbau, Prävention, Zusammenarbeit mit Nicht-EU-Partnern und Bekämpfung der Online-Kriminalität.[162] Die 2020 vorgenommene unabhängige Evaluierung des EU-Politikzyklus 2018–2021/EMPACT[163] ergab, dass sich dieser bei der Bewältigung der akutesten Bedrohungen durch organisierte kriminelle Gruppen als zunehmend relevant und wirksam erwiesen hat. Ein zusätzlicher Nutzen entsteht durch die Bereitstellung einer Kooperationsplattform, dank deren die Mitgliedstaaten bei der Bekämpfung der schweren und organisierten Kriminalität bessere Ergebnisse erzielen können, als es ihnen im Alleingang möglich wäre. Bei der Evaluierung wurden darüber hinaus Chancen für die Weiterentwicklung dieses sehr hilfreichen Instruments im nächsten Zyklus (2022 bis 2025) aufgezeigt und diesbezügliche Empfehlungen ausgesprochen.

Die Kommission wird im Jahr 2021 eine Initiative für **einen EU-Kodex für die polizeiliche Zusammenarbeit** auf den Weg bringen, um eine Straffung, Verbesserung, Weiterentwicklung, Modernisierung und Vereinfachung der Zusammenarbeit der zuständigen nationalen Behörden bei der Strafverfolgung zu erreichen. Dies wird für die Mitgliedstaaten eine große Hilfe bei der Bekämpfung der schweren und organisierten Kriminalität sowie des Terrorismus sein.

Zudem ist eine Zusammenarbeit zwischen der **Polizei und anderen wichtigen Strafverfolgungsbehörden** sowie weiteren staatlichen Stellen wie etwa den Zollbehörden erforderlich. Die **Zollbehörden** der EU spielen eine Schlüsselrolle bei der Gewährleistung der Sicherheit der Außengrenzen und der Lieferketten und tragen damit zur inneren Sicherheit der Europäischen Union bei. Die neuen und sich abzeichnenden Bedrohungen betreffen die wichtigsten Schnittstellen zwischen den Zoll- und Strafverfolgungsbehörden, wobei insbesondere die wichtige Aufgabe der „Aufdeckung und Verhütung“ im Rahmen von Zollkontrollen und die federführende Rolle der Zollbehörden im Güterbereich von Bedeutung sind. Die Kommission unterstützt und fördert die Zusammenarbeit zwischen den Zollbehörden und Europol[164], was unmittelbare Auswirkungen auf Maßnahmen in Bereichen wie Feuerwaffen, Umweltkriminalität, kriminelle Finanzströme und Cyberkriminalität hat. Gegenwärtig sind Zollbehörden an mehreren von Europol geleiteten

---

[161] Gemeinsame Aktionstage im Rahmen von EMPACT: „Operation BOSPHORUS“: Sicherstellung von 1 776 Feuerwaffen (2. bis 11. November); gemeinsame Aktionstage „Mobile 3“: Sicherstellung von mehr als 350 gestohlenen Fahrzeugen und mehr als 1000 gestohlenen Fahrzeugteilen (12./13. Oktober); gemeinsame Aktionstage gegen den Menschenhandel zum Zweck der Arbeitsausbeutung: Beamte ermittelten 715 potenzielle Opfer von Arbeitsausbeutung (14. bis 20. September); gemeinsame Aktionstage gegen die Kriminalität in Südosteuropa: Sicherstellung von 51 Waffen verschiedener Gattungen und 47 Kilogramm unterschiedlicher Drogen (September).

[162] Alle detaillierten Informationsblätter zu den Ergebnissen samt Zahlen, aufgeschlüsselt nach den EMPACT-Prioritäten der EU für die Verbrechensbekämpfung, sind abrufbar unter: https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf, Dok. 7623/20, 5. Mai 2020.

[163] In den Schlussfolgerungen des Rates vom 27. März 2017 zur Fortsetzung des EU-Politikzyklus zur Bekämpfung der organisierten und schweren internationalen Kriminalität im Zeitraum 2018–2021 (7704/17) war eine unabhängige Bewertung vorgesehen.

[164] Siehe beispielsweise den Aktionsplan der Gruppe „Zusammenarbeit im Zollwesen“. Zu den Schwerpunktbereichen für den Zeitraum 2020–2021 zählen unter anderem: höhere Präsenz von Zollbeamten in den Verbindungsbüros bei Europol, direkter Zugang der Zollbehörden zur Netzanwendung für sicheren Datenaustausch (SIENA) von Europol, verstärkte Vertretung der Zollbeamten in den nationalen Europol-Stellen und Teilnahme der Leiter der Polizei- und Zollbehörden am Treffen der europäischen Polizeichefs.

Aktionen gegen die schwere und internationale organisierte Kriminalität[165] beteiligt und nehmen an CEPOL-Schulungen teil. Diese Tätigkeiten tragen zur Förderung und Weiterentwicklung der behördenübergreifenden Zusammenarbeit bei und verbessern das Zusammenwirken der wichtigsten Akteure.

Leistungsfähige und wirksame Informationssysteme sind für die Verbesserung des Informationsaustauschs zwischen den Justiz- und Strafverfolgungsbehörden in der EU unverzichtbar. Das **Schengener Informationssystem (SIS)** wurde durch aktualisierte Bestimmungen verstärkt, die an potenziellen Defiziten ansetzen, und zwar durch die Schaffung zusätzlicher Ausschreibungskategorien, die Erweiterung der Liste der Sachen, für die Ausschreibungen eingegeben werden können, und die Zulassung neuer Datenkategorien für die Eingabe.[166] Die neuen Regelungen traten am 28. Dezember 2018 in Kraft und sollten ab Dezember 2021 uneingeschränkt zur Anwendung kommen.[167]

Ebenso wurde 2019 das **Europäische Strafregisterinformationssystem (ECRIS)** um ein zusätzliches System ergänzt, das einen effizienten Austausch von Strafregisterinformationen über in der EU verurteilte Drittstaatsangehörige ermöglicht (ECRIS-TCN). Die Arbeiten an der technischen Entwicklung und Implementierung dieses zentralisierten Systems laufen derzeit, und seine Inbetriebnahme wird für 2023 erwartet.

Am 24. Juli 2020 nahm die Kommission den Bericht über die Überprüfung der Richtlinie über die Verwendung von Fluggastdatensätzen (PNR)[168] an, der die ersten zwei Jahre der Anwendung der PNR-Richtlinie zum Gegenstand hat[169]. Aus dem Bericht geht hervor, dass die Entwicklung des EU-weiten PNR-Systems gut voranschreitet. Die Nutzung von PNR-Daten ist für die Bekämpfung des Terrorismus sowie der schweren und organisierten Kriminalität unverzichtbar und hat bereits greifbare Ergebnisse erbracht. Nur ein Mitgliedstaat hat der Kommission die vollständige Umsetzung bislang noch nicht mitgeteilt.[170] Am 3. Dezember 2020 übermittelte die Kommission diesem Mitgliedstaat eine mit Gründen versehene Stellungnahme wegen Nichtmitteilung der vollständigen Umsetzung der Richtlinie.

Am 9. September 2020 veröffentlichte die Kommission die Evaluierung der **Richtlinie über vorab übermittelte Fluggastdaten** aus dem Jahr 2004.[171] Darin werden mehrere

---

[165] Verbrauch-/Mehrwertsteuerbetrug, Handel mit Feuerwaffen, Umweltkriminalität, kriminelle Finanzströme, Bekämpfung des sexuellen Missbrauchs von Kindern.

[166] Verordnung (EU) 2018/1860 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Nutzung des Schengener Informationssystems für die Rückkehr illegal aufhältiger Drittstaatsangehöriger (ABl. L 312 vom 7.12.2018, S. 1), Verordnung (EU) 2018/1861 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der Grenzkontrollen, zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen und zur Änderung und Aufhebung der Verordnung (EG) Nr. 1987/2006 (ABl. L 312 vom 7.12.2018, S. 14), Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen, zur Änderung und Aufhebung des Beschlusses 2007/533/JI des Rates und zur Aufhebung der Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates und des Beschlusses 2010/261/EU der Kommission (ABl. L 312 vom 7.12.2018, S. 56).

[167] Eine weitere Aktualisierung des SIS wird entsprechend den vorgeschlagenen Änderungen der Europol-Verordnung (COM(2020) XXX) erfolgen.

[168] COM(2020) 305.

[169] Richtlinie (EU) 2016/681.

[170] Slowenien.

[171] SWD(2020) 174.

Defizite und Unstimmigkeiten hervorgehoben, die bei der anstehenden Überarbeitung des geltenden Rechtsrahmens Berücksichtigung finden werden. Ein anderes zentrales Instrument, das Gegenstand einer weiteren Überprüfung ist, sind die **Prüm-Beschlüsse**[172], die vor dem Hintergrund der operativen, technologischen, forensischen und datenschutzrelevanten Entwicklungen untersucht werden sollen.

Die Zusammenarbeit **bei der Bekämpfung des Terrorismus und der organisierten Kriminalität** muss sich über die EU hinaus auch auf **wichtige Drittländer erstrecken**. Am 13. Mai 2020 billigte der Rat die Aufnahme von Verhandlungen mit Neuseeland über den Austausch personenbezogener Daten zwischen Europol und Neuseeland. Die Verhandlungen mit der Türkei über den Austausch personenbezogener Daten zur Bekämpfung der schweren Kriminalität und des Terrorismus werden fortgeführt, während bei den entsprechenden Verhandlungen mit Ägypten, Algerien, Israel, Jordanien, Libanon, Marokko und Tunesien bislang keine Fortschritte erzielt wurden. Am 19. November 2020 verabschiedete die Kommission eine Empfehlung für einen Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen über Abkommen zwischen der Europäischen Union und zehn Drittländern über die Zusammenarbeit beim Austausch personenbezogener Daten zwischen Eurojust und den zuständigen Behörden dieser Drittländer.[173]

In Bezug die **internationale Zusammenarbeit beim Austausch von PNR-Daten** für die Bekämpfung von Terrorismus und schwerer Kriminalität genehmigte der Rat die Aufnahme von Verhandlungen mit Japan über die Unterzeichnung eines PNR-Abkommens.[174] Mittlerweile *werden* die **gemeinsamen Überprüfungen der bestehenden Abkommen zwischen der EU und den USA bzw. Australien** *abgeschlossen.* Darüber hinaus hat die Kommission ein Verfahren zur Überprüfung ihres derzeitigen Gesamtkonzepts für die Übermittlung von PNR-Daten an Drittländer in die Wege geleitet.[175]

Zudem arbeitet die Kommission gemeinsam mit den Vereinten Nationen am Ausbau der Kapazitäten der Partnerländer für die Prävention, Aufdeckung, Ermittlung und Verfolgung terroristischer Straftaten und anderer schwerer Straftaten durch die Erhebung und Analyse von vorab übermittelten Fluggastdaten (API) und Fluggastdatensätzen (PNR).

Die Kommission beteiligte sich an dem Verfahren zur Vereinfachung der Übermittlung von PNR-Daten gemäß den rechtlichen Anforderungen der EU im Rahmen der neuen PNR-Richtlinien[176], die von der Internationalen Zivilluftfahrt-Organisation (ICAO)

---

[172] Der Prüm-Rahmen ermöglicht den automatisierten Austausch von DNA-Profilen, Fingerabdruckdaten und Kfz-Zulassungsdaten zwischen den Strafverfolgungsbehörden. Eine Folgenabschätzung in der Anfangsphase wurde bereits veröffentlicht.

[173] Die Empfehlung sieht die Aufnahme von Verhandlungen mit den folgenden Drittländern vor: Ägypten, Algerien, Armenien, Bosnien und Herzegowina, Israel, Jordanien, Libanon, Marokko, Tunesien und Türkei, COM(2020) 743 final.

[174] 18. Februar 2020.

[175] Fahrplan für die externe Dimension der PNR-Politik der EU, verfügbar unter: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12531-External-dimension-of-the-EU-policy-on-Passenger-Name-Records-.

[176] Beschluss (EU) 2019/2107 des Rates vom 28. November 2019 über den Standpunkt, der im Namen der Europäischen Union im Rat der Internationalen Zivilluftfahrt-Organisation bezüglich der Überarbeitung des Anhangs 9 („Erleichterungen“) Kapitel 9 des Abkommens über die internationale Zivilluftfahrt im Hinblick auf Richtlinien und Empfehlungen für Fluggastdatensätze zu vertreten ist (ABl. L 318 vom 10.12.2019, S. 117).

angenommen wurden[177]. Am 23. Juni 2020 nahm der ICAO-Rat die neuen Richtlinien und Empfehlungen zu PNR[178] an, und die Mitgliedstaaten der ICAO haben bis zum 30. Januar 2021 die Möglichkeit, die ICAO über etwaige Unterschiede zwischen ihren nationalen Regulierungsverfahren und den neuen Richtlinien und Empfehlungen zu PNR zu unterrichten.

2. Der Beitrag starker Außengrenzen

Ein modernes und effizientes Management der Außengrenzen ist für die Gewährleistung der Sicherheit der Bürgerinnen und Bürger der EU von zentraler Bedeutung. Die Einbindung aller relevanten Akteure im Interesse einer größtmöglichen Sicherheit an den Grenzen und ihre Ausstattung mit angemessenen Instrumenten können die Prävention von grenzüberschreitender Kriminalität und Terrorismus konkret beeinflussen. Auch im neuen Migrations- und Asylpaket[179] wird das Erfordernis eines stabilen und gerechten Außengrenzenmanagements, einschließlich Identitäts-, Gesundheits- und Sicherheitskontrollen, hervorgehoben. Dies ist Teil des umfassenden Konzepts und macht deutlich, wie sehr die Migrations-, Asyl-, Integrations- und Grenzmanagementpolitik auf Fortschritte in allen Bereichen angewiesen ist.

Im neuen Paket wird unterstrichen, dass ein wirksamer Schengen-Raum für die Migrationspolitik unverzichtbar ist und darüber hinaus tief greifende Auswirkungen auf die Sicherheit hat. Diese Frage wurde beim ersten Schengen-Forum erörtert, das am 30. November 2020 stattfand. Die Vertreter der Mitgliedstaaten und des Europäischen Parlaments waren sich einig über die Bedeutung eines wirksamen Schengen-Raums, in dem die Freizügigkeit und Sicherheit der Bürgerinnen und Bürger gewährleistet sind. Dieser Prozess wird in die neue Schengen-Strategie einfließen, die 2021 vorgelegt werden soll. Der Schengener Evaluierungs- und Überwachungsmechanismus ist ein Schlüsselinstrument für die Gewährleistung des gegenseitigen Vertrauens sowie einer besseren und kohärenten Umsetzung des Schengen-Besitzstands, auch mit Blick auf dessen sicherheitsrelevante Auswirkungen. Dies war ein wichtiges Thema des am 25. November angenommenen Berichts[180], in dem der aktuelle Stand der Umsetzung des Schengen-Besitzstands dargelegt und eine Bestandsaufnahme der Funktionsweise des Schengener Evaluierungs- und Überwachungsmechanismus vorgenommen wurde.

Die **Interoperabilitätsverordnungen**[181] haben zum Ziel, die EU-Informationssysteme für die Bereiche Sicherheit, Grenzmanagement und Migrationssteuerung zu verbessern und ihre Zusammenarbeit intelligenter und effizienter zu gestalten. Durch die Interoperabilität

---

177 Resolution 2396 (2017) des Sicherheitsrats der Vereinten Nationen.

178 Bezeichnet als Änderung 28 zu Anhang 9 („Erleichterungen“) des Abkommens über die internationale Zivilluftfahrt (Abkommen von Chicago).

179 COM(2020) 609.

180 SWD(2020) 327 final.

181 Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates, der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates (ABl. L 135 vom 22.5.2019, S. 27) und Verordnung (EU) 2019/818 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration) und zur Änderung der Verordnungen (EU) 2018/1726, (EU) 2018/1862 und (EU) 2019/816 (ABl. L 135 vom 22.5.2019, S. 85).

zwischen den EU-Informationssystemen wird die Wirksamkeit und Effizienz der Kontrollen an den Außengrenzen verbessert, ein Beitrag zur Verhinderung illegaler Einwanderung geleistet und ein hohes Maß an Sicherheit gewährleistet. Zudem stellt sie ein wertvolles zusätzliches Instrument für die Strafverfolgungs- und Grenzbehörden dar.[182] Die EU-Mitgliedstaaten, die assoziierten Schengen-Staaten und die zuständigen Agenturen der Union (eu-LISA, die Europäische Agentur für die Grenz- und Küstenwache und Europol) müssen entsprechend vorbereitet sein, und die Kommission überwacht derzeit die vorbereitenden Arbeiten und die Aufnahme des Betriebs, um sicherzustellen, dass die Implementierung bis Ende 2023 vollständig abgeschlossen ist.

Am 8. Dezember 2020 haben die beiden gesetzgebenden Organe eine vorläufige Einigung über den **Vorschlag zur Aktualisierung des Visa-Informationssystems[183]** erzielt.

Einige zentrale Rechtsvorschriften müssen jedoch noch verabschiedet werden. Das Europäische Parlament muss seine Bereitschaft erklären, sich mit dem Rat über die Änderungen[184] am Europäischen Reiseinformations- und Genehmigungssystem (ETIAS)[185] zu einigen.

Die Verknüpfung der für die Analyse der Sicherheitsrisiken relevanten Informationssysteme ist für die Erhöhung unserer Sicherheit von entscheidender Bedeutung. Der Ausbau der **Zusammenarbeit zwischen den Zoll- und Grenzverwaltungsbehörden** und die Verstärkung der Synergien zwischen den jeweiligen **Informationssystemen** im Einklang mit dem einschlägigen System von Kontrolle und Gegenkontrolle, einschließlich des Schutzes personenbezogener Daten und der Rechtsvorschriften über die Privatsphäre, stellen eine Priorität des Aktionsplans für den Ausbau der Zollunion dar, der am 28. September 2020 angenommen wurde.[186] In einer von der Kommission in Zusammenarbeit mit Polizei- und Zollexperten der Mitgliedstaaten vorgenommenen vorläufigen Bewertung wird insbesondere die Vernetzung des Schengener Informationssystems (SIS) und von Europol-Daten mit dem Einfuhrkontrollsystem des Zolls (ICS2)[187] empfohlen; hierzu wird nun eine Machbarkeitsstudie veranlasst.

Mit der **Verordnung über die Europäische Grenz- und Küstenwache**[188], die im Dezember 2019 in Kraft trat, wurde eine grundlegende Überarbeitung der Kapazitäten und Instrumente der EU vorgenommen, um die EU-Außengrenzen zu stärken. Auf diese Weise kann der Schutz der Außengrenzen einen erheblich größeren Beitrag zur Sicherheit der EU

---

[182] Vorhandene Systeme: Schengener Informationssystem (SIS), Visa-Informationssystem (VIS), Eurodac; künftige Systeme: Einreise-/Ausreisesystem (EES), Europäisches Reiseinformations- und Genehmigungssystem (ETIAS) und Europäisches Strafregisterinformationssystem für Drittstaatsangehörige (ECRIS-TCN).

[183] COM(2019)12.

[184] COM(2019) 3 final und COM(2019) 4 final.

[185] Verordnung (EU) 2018/1240 des Europäischen Parlaments und des Rates vom 12. September 2018 über die Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 1077/2011, (EU) Nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 und (EU) 2017/2226 (ABl. L 236 vom 19.9.2018, S. 1) und Verordnung (EU) 2018/1241 des Europäischen Parlaments und des Rates vom 12. September 2018 zur Änderung der Verordnung (EU) 2016/794 für die Zwecke der Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) (ABl. L 236 vom 19.9.2018, S. 72).

[186] COM(2020) 581.

[187] System für Fracht-Vorabinformationen, das für die frühzeitige Bewertung der Sicherheitsrisiken für alle die Außengrenzen überschreitenden Warenbewegungen eingesetzt wird.

[188] Verordnung (EU) 2019/1896.

leisten. Das neue Mandat stärkt die Fähigkeit von Frontex, die Mitgliedstaaten beim Außengrenzen- und Rückkehrmanagement zu unterstützen, und erweitert die Möglichkeiten für die Zusammenarbeit mit Drittländern. Gegenwärtig wird daran gearbeitet, die Bereitschaft der ständigen Reserve der Europäischen Grenz- und Küstenwache für ihre erstmalige Entsendung am 1. Januar 2021 zu sichern.

Im Juni 2019 führte die EU **höhere Sicherheitsstandards für Personalausweise** ein, um die Freizügigkeit ihrer Bürgerinnen und Bürger zu fördern und zugleich den Identitätsbetrug einzudämmen.[189] Die Mitgliedstaaten sind verpflichtet, ab August 2021 Personalausweise und Aufenthaltsdokumente auszustellen, die den neuen Sicherheitsstandards entsprechen. Die meisten Mitgliedstaaten gleichen derzeit die Gestaltung ihrer Dokumente an die Anforderungen der Verordnung an.

3. Intensivierung von Sicherheitsforschung und Innovation

Sicherheitsforschung und Innovationsförderung untermauern eine koordinierte Reaktion der EU auf komplexe Probleme und ermöglichen konkrete Maßnahmen zur Minderung von Risiken. Die Sicherheitsunion ist einer der vier Schwerpunktbereiche des Arbeitsprogramms 2018–2020 für **Horizont 2020**[190], auf das 50 % der gesamten öffentlichen Mittel für die Sicherheitsforschung in der EU entfallen. Bei den 2019 im Rahmen von Horizont 2020 durchgeführten Aufforderungen zur Einreichung von Vorschlägen im Bereich der Sicherheitsforschung wurden 42 Projekte ausgewählt, die EU-Fördermittel in Höhe von insgesamt 253 Mio. EUR erhielten. Gegenstand der Projekte sind unter anderem der Schutz von Infrastrukturen, die Katastrophenresilienz, die Bekämpfung von Kriminalität und Terrorismus, die Sicherung der Außengrenzen sowie die Verbesserung der digitalen Sicherheit. Für 2020 beläuft sich die vorläufige Mittelausstattung für entsprechende Projekte auf 265 Mio. EUR. Davon entfallen 20 Mio. EUR auf eine Aufforderung zur Einreichung von Vorschlägen zur künstlichen Intelligenz, durch die die europäischen Strafverfolgungsbehörden beim Ausbau ihrer KI-Kapazitäten sowie bei der Behebung ihrer diesbezüglichen Defizite und der Intensivierung der Zusammenarbeit unterstützt werden. Die vorbereitenden Arbeiten, die gegenwärtig im Rahmen des neuen Forschungsrahmenprogramms Horizont Europa stattfinden, sind dazu gedacht, die Umsetzung der EU-Strategie für eine Sicherheitsunion, die das Grenzmanagement und die Sicherheit betreffende Dimension des neuen Migrations- und Asylpakets, die Maßnahmen der EU zur Verringerung des Katastrophenrisikos sowie die EU-Strategie für maritime Sicherheit zu unterstützen.[191]

Die von der EU finanzierte Sicherheitsforschung hat sich auch bei der Förderung der Zusammenarbeit und der Unterstützung von Sicherheitsfachkräften während der COVID-19-Pandemie als wirksam erwiesen.[192] In diesem Zusammenhang stehen beispielsweise Instrumente für die gemeinsame Bewertung und Ermittlung epidemiologischer Bedrohungen und krimineller Risiken bereit.

---

[189] Verordnung (EU) 2019/1157.

[190] Die EU hat Mittel in Höhe von etwa 91 Mio. EUR für Projekte zur Verbesserung des Schutzes von Infrastrukturen bereitgestellt, die unter anderem auf die kombinierte Eindämmung von Cyber- und physischen Bedrohungen, eine verbesserte und schnelle Reaktion auf Vorfälle und einen besseren Informationsaustausch abzielen.

[191] Mit Cluster 3 des Rahmenprogramms Horizont Europa werden insbesondere die politischen Prioritäten der Kommission „Förderung unserer europäischen Lebensweise“, „ein europäischer Grüner Deal“ und „ein Europa für das digitale Zeitalter“ unterstützt.

[192] Die im Rahmen von Horizont 2020 ergriffenen Maßnahmen zur Unterstützung der Reaktion auf die Pandemie sind einsehbar unter: https://www.researchgate.net/publication/341287556.

Um die Akzeptanz **innovativer Projekte** zu gewährleisten, müssen die EU-Agenturen in die bestehende Sicherheitsforschungs- und Innovationslandschaft eingebunden werden. Im Nachgang zur Tagung des Rates (Justiz und Inneres) vom Oktober 2019 errichten die EU-Agenturen und die Gemeinsame Forschungsstelle der Kommission gegenwärtig auf der Grundlage ihres jeweiligen rechtlichen Mandats das **EU-Innovationszentrum für innere Sicherheit**, das als Kooperationsnetz ihrer Innovationslabors dienen soll. Das Zentrum wird in Form eines Koordinierungsmechanismus gestaltet, durch den die teilnehmenden Einrichtungen beim Austausch von Informationen und Kenntnissen sowie bei der Planung gemeinsamer Projekte und der Verbreitung von Erkenntnissen und technologischen Lösungen mit Relevanz für die innere Sicherheit unterstützt werden sollen.[193]

Mit dem **Europäischen Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung und dem Netz nationaler Koordinierungszentren** leistet Europa einen Beitrag zur Unterstützung von Innovationen und Industriepolitik im Bereich der Cybersicherheit. Ihr Ziel ist es, die Kapazitäten der EU im Bereich der Cybersicherheit zu stärken, unsere Wirtschaft und Gesellschaft gegen Cyberangriffe abzuschirmen, Exzellenz in der Forschung zu sichern und die Wettbewerbsfähigkeit der EU zu verbessern. Triloge sind im Gange.

4. Sicherheitskompetenzen und Sicherheitsbewusstsein

Für eine krisenfestere Gesellschaft mit besser gerüsteten Unternehmen, Verwaltungen und besser vorbereiteten Bürgern kommt es entscheidend darauf an, dass ein Bewusstsein für Sicherheitsfragen und Kompetenzen im Umgang mit potenziellen Bedrohungen vorhanden sind. Wichtig ist auch der Zugang der Opfer zu ihren Rechten.

Fachkräfte der Strafverfolgungs- und Justizbehörden

Die mit der COVID-19-Pandemie einhergehenden Beschränkungen hatten massive Auswirkungen auf die CEPOL, die gezwungen war, ab März 2020 alle geplanten Präsenzveranstaltungen abzusagen. Diese besonderen Umstände sorgten zudem für eine steigende Nachfrage nach Online-Diensten: In den ersten vier Monaten des Jahres verzeichnete die Agentur einen Anstieg der virtuellen Veranstaltungen um 30 % und einen Zuwachs der Online-Nutzer um 100 %. Zu den Aus- und Fortbildungsprioritäten des Zeitraums 2019–2021[194] zählt unter anderem die Bekämpfung der illegalen Migration, des Terrorismus, des Menschenhandels und der Cyberkriminalität sowie des sexuellen Missbrauchs von Kindern. Die Kommission bereitet gegenwärtig die Evaluierung der CEPOL vor, die bis Juli 2021 abgeschlossen sein soll.

Breite Öffentlichkeit

Am Safer Internet Day 2018 wurde die **Kampagne #SaferInternet4EU** gestartet. Die dabei durchgeführten Aktivitäten erreichten in den beiden letzten Jahren EU-weit 63 Millionen Menschen und beinhalteten unter anderem die Verleihung von Auszeichnungen, die Unterstützung von Lehrkräften und Maßnahmen im Bereich der Cyberhygiene. Das Netz der Safer-Internet-Zentren stellte mehr als 1800 neue Ressourcen

[193] Am 21. Februar 2020 bestätigte der Ständige Ausschuss für die operative Zusammenarbeit im Bereich der inneren Sicherheit den Auftrag, die wichtigsten Merkmale, die Aufgaben und die Verwaltungsstruktur des EU-Innovationszentrums für innere Sicherheit.

[194] European Union Strategic Training Needs Assessment 2018-2021 (Strategische Bewertung des Bedarfs an Aus- und Fortbildungsmaßnahmen in der Europäischen Union 2018–2021), EU-STNA Report, CEPOL.

bereit, die Themen wie Falschinformationen, Cybermobbing, Bedenken hinsichtlich der Privatsphäre, Grooming und Cyberhygiene zum Gegenstand hatten.

Im Oktober 2020 wurde zum achten Mal der europäische **Monat der Cybersicherheit** (European Cyber Security Month) begangen, dessen Ziel die Förderung der Online-Sicherheit in der EU ist. Die diesjährige Kampagne war auf Sicherheitsprobleme im Zusammenhang mit der Digitalisierung des täglichen Lebens ausgerichtet, die durch die COVID-19-Pandemie weiter beschleunigt wurde. Unter dem Motto „Think Before U Click" (Erst denken, dann klicken) wurde im Rahmen der Kampagne auf verschiedene Themen der Cybersicherheit aufmerksam gemacht, um die Nutzer dabei zu unterstützen, Cyberbedrohungen besser zu erkennen und sich darauf einzustellen. Die European Cyber Security Challenge 2021 in Prag wird gegenwärtig vorbereitet.

Ein sehr wichtiges Instrument zur Unterstützung der Opfer von Cyberkriminalität ist „No More Ransom"[195], ein Verzeichnis kostenloser Entschlüsselungstools, die es den Opfern ermöglichen, sich zu wehren, ohne die Hacker bezahlen zu müssen. Die Initiative, die vom Europäischen Zentrum zur Bekämpfung der Cyberkriminalität bei Europol unterstützt wird und im Juli 2020 ihren vierten Jahrestag beging, registrierte seit ihrer Gründung mehr als 4,2 Millionen Besucher aus 188 Ländern und trug dazu bei, dass Kriminellen Lösegeldzahlungen in Höhe von insgesamt 632 Mio. US-Dollar entgingen.

Am 1. Juli 2020 stellte die Europäische Kommission die **Europäische Kompetenzagenda[196]** für nachhaltige Wettbewerbsfähigkeit, soziale Gerechtigkeit und Resilienz vor. Darin werden ehrgeizige quantitative Ziele festgelegt, um die vorhandenen Kompetenzen und die Vermittlung neuer Kompetenzen in den nächsten fünf Jahren zu verbessern. Die Kompetenzagenda umfasst gezielte Maßnahmen zur Erhöhung der Zahl der Hochschulabsolventen in Naturwissenschaften, Technologie, Ingenieurwesen, Kunst und Mathematik, die in Spitzenforschungsgebieten wie der Cybersicherheit benötigt werden. Am 10. November 2020 gab die Kommission im Rahmen der fünften Europäischen Woche der Berufsbildung 2020 den Startschuss für den Kompetenzpakt. Dieser dient der Förderung gemeinsamer Aktionen für eine größtmögliche Wirkung von Investitionen in die Verbesserung vorhandener Kompetenzen und die Vermittlung neuer Kompetenzen. Zeitgleich mit der Vorstellung des Pakts wurden die ersten europäischen Kompetenzpartnerschaften in drei Bereichen angekündigt: Automobilindustrie, Mikroelektronik sowie Luft- und Raumfahrt und Verteidigung.

Am 30. September 2020 verabschiedete die Kommission eine Reihe politischer Strategien, die wichtige Auswirkungen auf die Entwicklung der langfristigen Kapazitäten der EU im Bereich der Sicherheitskompetenzen haben werden. Der **Aktionsplan für digitale Bildung 2021-2027[197]** dient der Förderung der Entwicklung eines leistungsfähigen digitalen Bildungsökosystems und dem Ausbau digitaler Kompetenzen für den digitalen Wandel.[198] Am selben Tag wurde eine Mitteilung über die Vollendung des **europäischen Bildungsraums** bis 2025[199] angenommen, in der Grundfertigkeiten und digitale Kompetenzen einen wichtigen Schwerpunkt darstellen. Darüber hinaus wurden in einer

[195] https://www.nomoreransom.org/

[196] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Europäische Kompetenzagenda für nachhaltige Wettbewerbsfähigkeit, soziale Gerechtigkeit und Resilienz (COM(2020) 274).

[197] COM(2020) 624.

[198] https://ec.europa.eu/education/sites/education/files/document-library-docs/deap-communication-sept2020_en.pdf

[199] COM(2020) 625.

Mitteilung über einen neuen **Europäischen Forschungsraum für Forschung und Innovation**[200] die Maßnahmen zur Verbesserung der europäischen Forschungs- und Innovationslandschaft, zur Beschleunigung der Übernahme der digitalen Führungsrolle durch die EU sowie zur Bekämpfung aller Formen der geschlechtsspezifischen Gewalt in Forschungs- und Innovationsorganisationen vorgestellt.

Die im Rahmen des **Programms Erasmus+** durchgeführten Projekte zur Bekämpfung von Radikalisierung, gewaltbereitem Extremismus, sozialer Ausgrenzung, Fehlinformationen und Falschmeldungen tragen ebenfalls zur Eindämmung der Radikalisierung bei.[201] Ein Beispiel hierfür ist das Projekt „Radicalisation Prevention in Prisons" (Radikalisierungsprävention in Haftanstalten), das darauf abzielt, die Kompetenzen der Mitarbeiter vor Ort zu verbessern, damit sie in der Lage sind, Anzeichen für eine Radikalisierung zu erkennen, zu melden und zu interpretieren und angemessen zu reagieren.[202] Im Rahmen des Projekts „No Hate Bootcamp" lernten junge Arbeitnehmer, in ihren lokalen Gemeinschaften als „Botschafter gegen Hassreden" aufzutreten.

Die Kommission selbst ist bemüht, die Öffentlichkeit in ihre Überlegungen zur Sicherheitspolitik der EU einzubeziehen. Die auf EU-Ebene durchgeführten Aktionen werden über eine neue **Website zur EU-Strategie für eine Sicherheitsunion**[203] für die Bürgerinnen und Bürgern besser sichtbar und zugänglich gemacht. Mehrere **öffentliche Konsultationen** wurden in die Wege geleitet, um den Bürgerinnen und Bürgern Gelegenheit zu geben, unmittelbar Einfluss auf die Politikgestaltung zu nehmen.

Alle Opfer von Straftaten haben das Recht auf Unterstützung und Schutz, wobei jedoch den Opfern der schwersten Straftaten, etwa Terrorismus oder sexuelle Ausbeutung von Kindern, besondere Aufmerksamkeit gewidmet werden muss. Am 24. Juni 2020 nahm die Kommission ihre erste **EU-Strategie für die Rechte von Opfern (2020-2025)**[204] an. Darin geht es um die Opfer aller Straftaten, allerdings mit besonderem Augenmerk auf den am meisten gefährdeten Personengruppen (insbesondere Opfer von Terrorismus, minderjährige Opfer sexueller Ausbeutung und Opfer von Menschenhandel). Am 22. September 2020 organisierte die Kommission eine hochrangige Konferenz über Opferrechte, bei der sie die **Plattform für Opferrechte** einweihte, mit der ein stärker horizontal ausgerichteter Ansatz für Opferrechte gefördert werden soll.[205] Darüber hinaus benannte die Kommission ihren ersten **Koordinator für Opferrechte**, der die Kohärenz und Wirksamkeit der Politik im Bereich der Opferrechte sicherstellen soll.

Für die **Opfer von Terrorismus** wurde im Januar 2020 das EU-Kompetenzzentrum für Terroropfer eingerichtet, um nationalen Behörden und Opferschutzorganisationen mit

---

[200] COM(2020) 628.

[201] Bislang wurden etwa 80 Projekte zu radikalisierungsrelevanten Themen finanziert; mehr als 100 Projekte betrafen die Prävention und Bekämpfung von Cybermobbing, und weitere 100 beinhalteten Schulungen für eine kritische und ethische Nutzung des Internet mit dem Ziel, Desinformation im Internet einzudämmen.

[202] http://www.r2pris.org/

[203] https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union-strategy_de.

[204] COM(2020) 258 final.

[205] Die Plattform wird zum ersten Mal die wichtigsten Akteure auf EU-Ebene zusammenführen, darunter das Europäische Netz für die Rechte der Opfer, das Europäische Netz nationaler Kontaktstellen für Entschädigung, den EU-Koordinator für die Terrorismusbekämpfung, einschlägige Agenturen wie Eurojust, die Agentur für Grundrechte, die Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung und das Europäische Institut für Gleichstellungsfragen sowie die Zivilgesellschaft.

Fachwissen, Beratung und Unterstützung zur Seite zu stehen. Das Kompetenzzentrum fördert den grenzüberschreitenden Austausch von bewährten Verfahren und Fachwissen zwischen Fachkräften und Sachverständigen. Es ist nicht darauf ausgelegt, einzelne Opfer von Terrorismus direkt zu unterstützen, sondern soll den nationalen Einrichtungen dabei helfen, professionelle Hilfe und Unterstützung zu leisten, auch durch Leitlinien, die im Jahr 2020 veröffentlicht werden sollen. Das EU-Zentrum ist ein Pilotprojekt mit einer Laufzeit von zwei Jahren. Der Ratsvorsitz befasst sich derzeit mit der Verstärkung des Kompetenzzentrums durch ein Netzwerk der nationalen Kontaktstellen für die Opfer von Terrorismus.

VI FAZIT

Mit der Strategie für eine Sicherheitsunion sollte ein umfassender und dynamischer Rahmen geschaffen werden. Die jüngsten Terroranschläge haben erneut deutlich gemacht, dass die EU in der Lage sein muss, zu reagieren, indem sie ihre Resilienz und Reaktionsfähigkeit durch die Modernisierung und den wirksamen Einsatz der wichtigsten ihr zur Verfügung stehenden Instrumente stärkt. Durch die Anschläge wurde auch offenkundig, dass alle Akteure vollständig in ein gemeinsames Konzept eingebunden sein müssen, damit die Mitgliedstaaten, die EU-Institutionen, der Privatsektor, NRO und die Bürgerinnen und Bürger selbst zum Aufbau einer Sicherheitsbasis beitragen können, die stark und flexibel genug ist, um zu funktionieren. Dieses kohärente und einheitliche Konzept ist zudem die beste Option, um sicherzustellen, dass unsere Grundrechte im Rahmen der Förderung der europäischen Lebensweise geschützt werden.

Dieser Bericht veranschaulicht die zahlreichen derzeit laufenden Arbeiten und macht deutlich, wie diese Dynamik aufrechterhalten werden muss. Die heute vorgestellte EU-Agenda zur Terrorismusbekämpfung hat das Ziel, den europäischen Rahmen für die Terrorismusbekämpfung zu stärken, indem die nächsten erforderlichen Schritte festgelegt werden: Prognose und Prävention von Terrorismus, Schutz der Bürgerinnen und Bürger sowie der Infrastrukturen, und Reaktionsbereitschaft unter Berücksichtigung des Zusammenhangs zwischen der inneren und der äußeren Sicherheit. Wir verfügen bereits über mehr Zusammenarbeit, mehr Maßnahmen zur Eindämmung der Radikalisierung und mehr Instrumente, um Terroristen die Mittel für Anschläge zu entziehen. Nun müssen wir noch einen Schritt weiter gehen. Vor allem muss sichergestellt werden, dass neue Vorschriften zur Bekämpfung terroristischer Inhalte im Internet erlassen werden, wobei eine diesbezügliche Einigung noch in diesem Jahr von vorrangiger Bedeutung ist. Darüber hinaus fordert die Kommission die Mitgliedstaaten dringend auf, die Umsetzung aller vereinbarten Rechtsvorschriften voranzutreiben. Die Gewährleistung der Sicherheit aller Bürgerinnen und Bürger der EU liegt in unser aller Verantwortung, und ein geschlossenes Vorgehen für mehr Sicherheit in Europa muss unser gemeinsames Interesse sein.