Rat der
Europäischen Union

Brüssel, den 16. Dezember 2022
(OR. en)

16124/22

JAI 1695	**DROIPEN 165**
COSI 328	**COPEN 450**
ENFOPOL 648	**FREMP 275**
ENFOCUSTOM 179	**JAIEX 106**
IXIM 298	**CFSP/PESC 1733**
CT 227	**COPS 616**
CRIMORG 184	**HYBRID 120**
FRONT 464	**DISINFO 112**
ASIM 108	**TELECOM 528**
VISA 203	**DIGIT 248**
CYBER 409	**COMPET 1045**
DATAPROTECT 369	**RECH 665**
CATS 74	**CULT 133**

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	13. Dezember 2022
Empfänger:	Frau Thérèse BLANCHET, Generalsekretärin des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2022) 745 final
Betr.:	MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT Fünfter Fortschrittsbericht über die Umsetzung der EU-Strategie für eine Sicherheitsunion

Die Delegationen erhalten in der Anlage das Dokument COM(2022) 745 final.

Anl.: COM(2022) 745 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 13.12.2022
COM(2022) 745 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

Fünfter Fortschrittsbericht über die Umsetzung der EU-Strategie für eine Sicherheitsunion

1. EINLEITUNG

Im Juli 2020 hat die Kommission eine umfassende EU-Strategie für eine Sicherheitsunion[1] angenommen. Seitdem hat sich die Bedrohungslage jedoch in erheblicher Weise verändert. Während der COVID-19-Krise sind, insbesondere durch die Verlagerung zahlreicher Aktivitäten ins Internet, einige Schwachstellen verstärkt zu Tage getreten. Cyberangriffe haben in ihrem Umfang zugenommen und treten nunmehr auch in neuer Form auf.[2] Die Auswirkungen des russischen Angriffskriegs gegen die Ukraine machen sich auch im Bereich der inneren Sicherheit der EU bemerkbar. So haben die Gefahr des Menschenhandels, die Bedrohung durch chemische und nukleare Zwischenfälle und der illegale Handel mit Feuerwaffen zugenommen. Der Angriffskrieg hat auch der Manipulation von Informationen und der Einmischung durch ausländische Akteure Vorschub geleistet. Die jüngste Sabotage der Nord-Stream-Pipelines hat gezeigt, wie sehr wichtige Sektoren wie Energie, digitale Infrastruktur, Verkehr und Raumfahrt auf resiliente kritische Infrastrukturen angewiesen sind. Wieder einmal wurde deutlich, dass sowohl die physische als auch die digitale Sicherheit eng miteinander verflochten sind und gemeinsam geschützt werden müssen.

In diesem Fortschrittsbericht über die Strategie für eine Sicherheitsunion soll ein Halbzeitüberblick über die Umsetzung der Strategie gegeben und herausgestellt werden, was bislang erreicht wurde bzw. was vor Ablauf der laufenden Mandatsperiode der Kommission noch getan werden muss. Seit Juli 2020 hat die EU wichtige Schritte unternommen, um die Maßnahmen in den vier Schlüsselbereichen der Strategie[3] abzuschließen. In diesem Bericht wird festgestellt, dass die überwältigende Mehrheit der in der Strategie vorgesehenen Maßnahmen in Angriff genommen wurde.[4] Damit die Strategie für eine Sicherheitsunion ihre volle Wirkung für die Bürgerinnen und Bürger entfalten kann, bleibt allerdings noch einiges zu tun. So müssen insbesondere die ausstehenden Legislativvorschläge durch das Europäische Parlament und den Rat angenommen sowie die vereinbarten Rechtsvorschriften durch die Mitgliedstaaten umgesetzt werden. Die Ziele der Sicherheitsunion lassen sich zudem durch ein enges Zusammenspiel mit den einschlägigen EU-Initiativen in Bereichen wie Energieversorgungssicherheit, Europäische Gesundheitsunion und Aktionsplan für Demokratie in Europa erreichen. Die Kommission hat in diesem Zusammenhang auch drei Vorschläge vorgelegt, die zusammen mit diesem Bericht angenommen wurden: Sie betreffen den illegalen Handel mit Kulturgütern, wesentliche Informationen durch vorab übermittelte Fluggastdaten[5] und die Bekämpfung des Menschenhandels[6].

---

1 COM(2020) 605 final.

2 ENISA-Bericht zur Bedrohungslage 2022.

3 1) ein zukunftsfähiges Sicherheitsumfeld, 2) die Bewältigung sich wandelnder Bedrohungen, 3) der Schutz der Europäer vor Terrorismus und organisiertem Verbrechen und 4) eine starke europäische Sicherheitsgemeinschaft.

4 Die Tabelle im Anhang gibt einen Überblick über die legislativen und nichtlegislativen Maßnahmen seit Veröffentlichung der EU-Strategie für eine Sicherheitsunion.

5 EU-Aktionsplan zur Bekämpfung des illegalen Handels mit Kulturgütern (COM(2022) 800 final) und zwei Vorschläge zur Überarbeitung der Richtlinie über vorab übermittelte Fluggastdaten (COM(2022) 729 final und 731 final).

6 Der Vorschlag für eine überarbeitete Richtlinie zur Verhütung und Bekämpfung des Menschenhandels (COM(2022) 732 final) und der vierte Fortschrittsbericht über Maßnahmen gegen den Menschenhandel sollen am 19. Dezember 2022 angenommen werden.

2. SCHUTZ DER PHYSISCHEN UND DER DIGITALEN INFRASTRUKTUR VOR PHYSISCHEN ANGRIFFEN, CYBERANGRIFFEN UND HYBRIDEN ANGRIFFEN

Schutz der kritischen Infrastruktur in der EU vor physischen und digitalen Angriffen

Bereits vor den jüngsten Angriffen auf kritische Infrastrukturen hat die EU ihre Resilienz durch zwei miteinander verknüpfte Initiativen gestärkt: die überarbeitete Richtlinie[7] über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union **(Sicherheit der Netzinfrastruktur – „NIS-2-Richtlinie")**[8] und eine neue Richtlinie über die Resilienz kritischer Einrichtungen (**Resilience of Critical Entities – „CER-Richtlinie"**)[9]. In diesem Rahmen geht es um aktuelle und künftige Online- und Offline-Risiken, von Cyberangriffen bis hin zu Naturkatastrophen. Die Richtlinien, auf die sich die beiden gesetzgebenden Organe verständigt haben, werden in den kommenden Wochen in Kraft treten. Mit der **NIS-2-Richtlinie** werden die Maßnahmen für mittlere und große Einrichtungen in einer Reihe von Schlüsselsektoren verbessert.[10] Außerdem werden die Sicherheitsanforderungen gestärkt, unter anderem in Bezug auf die Reaktion auf Sicherheitsvorfälle und das Krisenmanagement, die Sicherheit der Lieferkette, die Behandlung und Offenlegung von Schwachstellen, Cybersicherheitstests und eine wirksame Verschlüsselung. Zudem zielt die Richtlinie darauf ab, die Meldepflicht bei Sicherheitsvorfällen zu straffen, strengere Aufsichtsmaßnahmen einzuführen und die Sanktionsregelungen in den Mitgliedstaaten zu harmonisieren.[11] Bei der **CER-Richtlinie** geht es um die physische Resilienz kritischer Einrichtungen gegenüber von Menschen und durch Naturkatastrophen verursachten Gefahren. Die Richtlinie deckt elf Sektoren ab und ist ein wichtiger Schritt, um kritische Einrichtungen, die wesentliche Dienste erbringen, besser in die Lage zu versetzen, Sicherheitsvorfälle zu verhindern, sich davor zu schützen, darauf zu reagieren, sie abzuwehren, die Folgen eines solchen Vorfalls zu begrenzen, aufzufangen, zu bewältigen und die Wiederherstellung zu gewährleisten.

Im Rahmen des Pakets zur Digitalisierung des **Finanzsektors** wurde zudem der Rechtsakt über die digitale Betriebsstabilität (DORA)[12] verabschiedet. Nach seiner Umsetzung wird DORA die digitale Betriebsstabilität von Unternehmen des Finanzsektors in der EU stärken, indem bestehende Vorschriften gestrafft und auf den neuesten Stand gebracht und bei Defiziten neue Anforderungen eingeführt werden.

Um den Schutz **kritischer Infrastrukturen vor groß angelegten Cyberangriffen weiter zu verbessern,** entwickeln die Kommission, der Hohe Vertreter und die NIS-Kooperationsgruppe[13] **Risikoszenarien** insbesondere für die Cybersicherheit in den Bereichen Energie, Telekommunikation, Verkehr und Weltraum. Ferner wird an Maßnahmen zur Verbesserung des kollektiven Schutzniveaus und der Cyberresilienz von

---

7 Vorschlag zur Überarbeitung der Richtlinie (EU) 2016/1148.

8 COM(2020) 823 final.

9 COM(2020) 829 final.

10 Die folgenden Bereiche sind Gegenstand der NIS-2- und der CER-Richtlinie: Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, digitale Infrastruktur, Gesundheit, Trinkwasser, Abwasser, öffentliche Verwaltung, Weltraum sowie Lebensmittelproduktion, -verarbeitung und -vertrieb.

11 Derzeit laufen Gespräche zwischen nationalen Sachverständigen der NIS-Kooperationsgruppe zur Unterstützung der Mitgliedstaaten bei der Umsetzung und Durchführung der NIS-2-Richtlinie.

12 COM(2020) 595 final. Politische Einigung im Mai 2022 erzielt.

13 Die Gruppe besteht aus Vertretern der Mitgliedstaaten, der Kommission und der Agentur der Europäischen Union für Cybersicherheit (ENISA). Sie unterstützt und erleichtert die strategische Zusammenarbeit der Mitgliedstaaten im Bereich der Sicherheit von Netz- und Informationssystemen.

Weltraumsystemen und -diensten gearbeitet.[14] Darüber hinaus werden gezielte Risikobewertungen in Bezug auf die Cybersicherheit der Kommunikationsinfrastrukturen und -netze in der EU (einschließlich Festnetz- und Mobilnetzinfrastruktur, Satelliten, Unterseekabel und Internet-Routing) durchgeführt.[15] Zur Verbesserung der Katastrophenprävention, -vorsorge und -bewältigung hat die Kommission außerdem eine Initiative zur Entwicklung von Szenarien für **Naturkatastrophen im Zusammenhang mit Sicherheitsbedrohungen** wie Cyberangriffen oder terroristischen Angriffen ins Leben gerufen.

Die Sabotage der Nord-Stream-Gas-Pipelines und andere jüngste Vorfälle haben die Bedrohung für **kritische Infrastrukturen in der EU** und die Dringlichkeit von Maßnahmen deutlich gemacht. Mit dem Rahmen der CER-Richtlinie und der NIS-2-Richtlinie sollen deshalb die Maßnahmen zur Stärkung der Resilienz kritischer Infrastrukturen und zur Verbesserung der Vorsorge und Reaktion in Schlüsselsektoren beschleunigt werden. Dies wird in einer **Empfehlung des Rates**[16] zusammengefasst, die es ermöglichen wird, die wirksame Umsetzung der Richtlinien zu beschleunigen. Sie bietet ein gemeinsames Konzept für die Durchführung von **Stresstests** bei Einrichtungen, die kritische Infrastrukturen betreiben, beginnend mit dem Energiesektor und aufbauend auf vereinbarten gemeinsamen Grundsätzen. Die Arbeiten an den Stresstests werden unverzüglich beginnen, damit sie vor Ende 2023 abgeschlossen werden können. Im April 2023 sollen die Fortschritte bewertet werden. Ein Konzeptentwurf, den die Kommission auf der Grundlage der unterstützenden Beiträge der einschlägigen Agenturen der Union in Zusammenarbeit mit dem Rat erstellt, soll zur Gewährleistung einer koordinierten EU-Reaktion auf erhebliche Störungen kritischer Infrastruktur beitragen.

Im **Energiesektor** arbeitet die Kommission an einem Netzkodex für Aspekte der Cybersicherheit bei grenzüberschreitenden Stromflüssen[17] (einschließlich Vorschriften für Risikobewertungen, gemeinsame Mindestanforderungen, Planung, Überwachung, Berichterstattung und Krisenmanagement), der vollständig mit dem NIS-2-Rahmen in Einklang stehen wird. Im Rahmen einer gesonderten Maßnahme als Reaktion auf den russischen Angriffskrieg gegen die Ukraine erfolgte im März 2022 als Ergänzung zu den Risikominderungsmaßnahmen, insbesondere im Bereich der Cybersicherheit, eine Synchronisierung des ukrainischen und des moldauischen Stromnetzes mit dem kontinentaleuropäischen Netz.

Im **Verkehrssektor** arbeitet die Kommission mit den Mitgliedstaaten, der Agentur der Europäischen Union für Flugsicherheit (EASA) und dem Zentrum der Europäischen Union für Informationsgewinnung und Lageerfassung (EU INTCEN) zusammen und bewertet regelmäßig das Ausmaß der von Konfliktgebieten ausgehenden Bedrohungen und Risiken für die Zivilluftfahrt der EU. Das EU-Warnsystem für Konfliktzonen gilt auf internationaler

---

14 Schlussfolgerungen des Rates zur Entwicklung der Cyberabwehr der Europäischen Union vom 23. Mai 2022.

15 Im Einklang mit dem Aufruf von Nevers zur Stärkung der Cybersicherheitskapazitäten der EU, auf den sich der Rat der für Telekommunikation zuständigen Ministerinnen und Minister auf seiner informellen Tagung am 9. März 2022 geeinigt hat.

16 Auf den Kommissionsvorschlag COM(2022) 551 final folgte die Annahme einer Empfehlung des Rates am 8. Dezember 2022.

17 Anforderung im Rahmen der Elektrizitätsverordnung (EU) 2019/943.

Ebene als bewährtes Verfahren.[18] Zu den Maßnahmen gehören die Wiederaufnahme der Arbeiten an der Risikobewertung im Luftfrachtverkehr, eine erste Bewertung der Gefahren für Fahrgastschiffe auf EU-Ebene und eine umfassende Ermittlung der Sicherheitsrisiken im Flugverkehr zur Aktualisierung der Bewertung der Bedrohungen für die Zivilluftfahrt.

Auch die **kritische maritime Infrastruktur** wird aufmerksam beobachtet.[19] Derzeit wird ein gemeinsamer Informationsraum für den maritimen Bereich entwickelt, der bis Ende 2023 voll funktionsfähig sein soll. Er wird den Meeresüberwachungsbehörden als Plattform für den freiwilligen Austausch echtzeitnaher Informationen zur Verfügung stehen. Auch das Forum für Europäische Küstenwachfunktionen hat seine Fähigkeit zur Abwehr von Cyberangriffen gestärkt.

Zudem zielen mehrere Forschungsprojekte im Rahmen von **Horizont Europa** zielen darauf ab, unsere digitale Infrastruktur sicherer zu machen und Kapazitäten zur Verhinderung und Eindämmung von Cyberangriffen aufzubauen.[20]

Verbesserung der Cybersicherheit in der EU

Am 16. Dezember 2020 haben die Kommission und der Hohe Vertreter eine neue **Cybersicherheitsstrategie der EU für die digitale Dekade**[21] vorgestellt, mit der die kollektive Resilienz Europas gegenüber Cyberbedrohungen gestärkt und zuverlässige und vertrauenswürdige Dienste und digitale Instrumente für die Bürger und Unternehmen sichergestellt werden sollen. Die Strategie wurde fast vollständig umgesetzt.

Die NIS-2-Richtlinie sieht die Einrichtung des **Europäischen Netzwerks der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe)**[22] zur Unterstützung des koordinierten Managements von Cybersicherheitsvorfällen und Krisen großen Ausmaßes auf operativer Ebene vor. So wird ein regelmäßiger Austausch relevanter Informationen zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU gewährleistet. Die Kommission arbeitet derzeit an der Errichtung eines **Cybersicherheits- und Analysezentrums**, um ihre internen Kapazitäten auszubauen. Sie arbeitet unter anderem im Rahmen der Folgemaßnahmen zu ihrer Empfehlung zur **Gemeinsamen Cyber-Einheit**[23] mit den Mitgliedstaaten zusammen, um eine koordinierte Reaktion der EU auf große Cybervorfälle zu gewährleisten. Die Kommission und der Hohe

---

18 Internationale Zivilluftfahrt-Organisation (Dok. Nr. 10084 *Risk Assessment Manual for Civil aircraft Operations Over or Near Conflict Zones* 2018).

19 Unter anderem durch die Umsetzung von SSZ-Projekten im Bereich der Fähigkeiten und Projekten im Rahmen von Horizont 2020.

20 EU-CIP (*European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection*) und ATLANTIS (*Atlantic Testing Platform for Maritime Robotics: New Frontiers for Inspection and Maintenance of Offshore Energy Infrastructures*).

21 JOIN(2020) 18 final.

22 EU-CyCLONe setzt sich zusammen aus Vertretern der Cyber-Krisenmanagementbehörden der Mitgliedstaaten sowie der Kommission in Fällen, in denen potenzielle oder laufende große Cybersicherheitsvorfälle erhebliche Auswirkungen auf die in der Richtlinie vorgesehenen Dienste und Tätigkeiten haben oder voraussichtlich haben werden.

23 C(2021) 4520 final.

Vertreter beteiligten sich auch aktiv an den 2022 in Zusammenarbeit mit den Mitgliedstaaten organisierten Cyberübungen[24].

Netze und Computersysteme müssen ständig überwacht und analysiert werden, damit Eindringlinge und Anomalien in Echtzeit erkannt werden können. Die Kommission hat vorgeschlagen, ein Netz von **Sicherheitseinsatzzentren** (SOCs) in der gesamten EU aufzubauen, die Kommunikationsnetze überwachen und verdächtige Ereignisse aufdecken. Durch den Ausbau bestehender SOCs, die Einrichtung neuer Zentren und die Verknüpfung von SOCs in mehreren Mitgliedstaaten werden die kollektiven Erkennungsfähigkeiten gestärkt. Sie könnten sich auch auf die moderne künstliche Intelligenz (KI) und Datenanalyse stützen, um zivile Kommunikationsnetze zu schützen und die Erkennung von Cyberangriffen zu beschleunigen.[25]

Um die Abwehrbereitschaft und Reaktionsfähigkeit bei größeren Cybervorfällen zu verbessern, hat die Kommission außerdem ein kurzfristiges Programm zur Unterstützung der Mitgliedstaaten aufgelegt (und zu diesem Zweck der ENISA zusätzliche Mittel zur Verfügung gestellt), einschließlich Penetrationstests kritischer Einrichtungen zur Ermittlung von Schwachstellen. Dabei kann die ENISA den Mitgliedstaaten mit Unterstützung vertrauenswürdiger privater Anbieter von Cybersicherheitsdiensten bei der unverzüglichen Reaktion auf schwerwiegende Sicherheitsvorfälle, die kritische Einrichtungen betreffen, helfen. Der nächste Schritt wird darin bestehen, sicherzustellen, dass die Mitgliedstaaten diese Möglichkeiten in vollem Umfang nutzen.

Sowohl Hardware- als auch Softwareprodukte sind zunehmend Gegenstand von **Cyberangriffen**. Zahl und Komplexität von Cyberangriffen nehmen zu, wobei in erster Linie Schwachstellen in der Software ausgenutzt werden. Zwei Drittel aller im Rahmen der NIS-Richtlinie gemeldeten Vorfälle sind auf die Ausnutzung von Softwareschwachstellen zurückzuführen. Auch die Auswirkungen auf Bürger, Infrastruktur oder Unternehmen nehmen zu.[26] Zwei Drittel aller im Rahmen der NIS-Richtlinie gemeldeten Vorfälle sind auf die Ausnutzung von Softwareschwachstellen zurückzuführen. Im September 2022 legte die Kommission einen Vorschlag für ein **Cyberresilienzgesetz**[27] vor, um Schwachstellen bei Produkten mit digitalen Elementen zu verringern und sicherzustellen, dass rasch Patches und Abhilfemaßnahmen zur Verfügung gestellt werden. Es wird vorgeschlagen, dass Produkte mit digitalen Elementen (Hardware und Software) nur dann in Verkehr gebracht werden, wenn sie spezifische grundlegende Cybersicherheitsanforderungen[28] erfüllen. Hersteller und Entwickler werden verpflichtet, die Cybersicherheit ihrer Produkte für einen Zeitraum von fünf Jahren zu

---

24 Beispielsweise das von Litauen und der ENISA organisierte Blueprint Operational Level Exercise (Blue OLEx) und die vom französischen Ratsvorsitz organisierte Cyberübung EU CyCLES (Cyber Crisis Linking Exercise on Solidarity).

25 Eine erste Phase wurde mit der Aufforderung zur Einreichung von Vorschlägen für den „Kapazitätsaufbau in Sicherheitseinsatzzentren“ und einem Aufruf zur Interessenbekundung betreffend die „Teilnahme an einer gemeinsamen Beschaffung von Instrumenten und Infrastrukturen“ eingeleitet, und zwar mit dem Europäischen Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (ECCC), mit einer EU-Mittelausstattung in Höhe von 110 Millionen Euro aus dem DIGITAL-Programm, veröffentlicht im November 2022.

26 ENISA-Bericht zur Bedrohungslage 2022.

27 COM(2022) 454 final.

28 In der Zwischenzeit hat die Kommission im Oktober 2021 eine delegierte Verordnung im Rahmen der Funkanlagenrichtlinie angenommen, die die Hersteller von Mobilgeräten verpflichtet, ihre Cybersicherheit, den Schutz der Privatsphäre und den Schutz vor Betrug zu verbessern.

gewährleisten und gegenüber den Verbrauchern in Bezug auf die Cybersicherheit transparent zu sein. Dies wird einen wesentlichen Beitrag zur Sicherheit der Lieferkette leisten.[29]

Die **Zertifizierung** spielt eine entscheidende Rolle bei der Stärkung des Vertrauens und der Sicherheit wichtiger Produkte und Dienstleistungen für die digitale Welt. Mit dem Rechtsakt zur Cybersicherheit[30] wird ein europäischer Zertifizierungsrahmen für die Cybersicherheit geschaffen, auf dessen Grundlage die Kommission die ENISA auffordern kann, Zertifizierungssysteme zu entwickeln. Ein auf gemeinsamen Kriterien beruhendes europäisches System für die Cybersicherheitszertifizierung wurde entwickelt, und Systeme für Cloud-Dienste und 5G-Sicherheit sind in Vorbereitung.

Die Kommission arbeitet weiterhin mit den Mitgliedstaaten zusammen, um die Sicherheit und Resilienz der **5G-Netze** sicherzustellen und die Umsetzung des 5G-Instrumentariums der EU auf nationaler und europäischer Ebene zu überwachen. Zwar hat die überwiegende Mehrheit der Mitgliedstaaten die Sicherheitsanforderungen für 5G-Netze bereits verschärft oder ist dabei, sie zu verschärfen, doch ist es nun dringend erforderlich, dass alle Mitgliedstaaten die Maßnahmen des Instrumentariums vollends umsetzen[31] und insbesondere Beschränkungen für Hochrisikoanbieter erlassen, da Verzögerungen die Anfälligkeit der Netze in der Union erhöhen können. Außerdem müssen die Mitgliedstaaten dringend auch den physischen und nichtphysischen Schutz kritischer und sensibler Teile von 5G-Netzen ausbauen, auch durch strenge Zugangskontrollen.

Um die EU und die Mitgliedstaaten dabei zu unterstützen, in der Industriepolitik im Bereich der Cybersicherheit einen proaktiven strategischen Ansatz zu verfolgen, wird das **Europäische Kompetenzzentrum für Cybersicherheitsforschung** (ECCC) mit den nationalen Koordinierungszentren zusammenarbeiten, um Innovationen im Bereich der Cybersicherheit zu fördern und die Kapazitäten der Cybersicherheitstechnologiegemeinschaft zu stärken.[32]

Im September 2022 hat die ENISA offiziell einen **Europäischen Kompetenzrahmen für Cybersicherheit** ins Leben gerufen, in dem die wichtigsten Berufsprofile in diesem Bereich ermittelt und eine gemeinsame europäische Grundlage für die Erleichterung der Anerkennung von Kompetenzen und die Entwicklung von Schulungen im Bereich der Cybersicherheit geschaffen werden. Dieser Rahmen bildet einen Baustein der im Arbeitsprogramm der Kommission 2023 vorgeschlagenen **Akademie für Cybersicherheitskompetenzen**, die einen umfassenden Ansatz zur Deckung des wachsenden Bedarfs an Cybersicherheitsfachkräften in Europa bieten wird.

Die von den **Organen, Einrichtungen und sonstigen Stellen der EU (EU-OESS)** bearbeiteten Verschlusssachen und nicht als Verschlusssache eingestuften vertraulichen Informationen müssen wirksam vor Cyberangriffen geschützt werden. Im März 2022 schlug

---

29 Im Einklang mit den Schlussfolgerungen des Rates zur Sicherheit der IKT-Lieferkette vom 17. Oktober 2022.

30 Verordnung (EU) 2019/881 zur Einführung eines EU-weiten Rahmens für die Cybersicherheitszertifizierung von IKT-Produkten, -Dienstleistungen und -Prozessen.

31 Die Mitgliedstaaten haben mit Unterstützung der Kommission und der ENISA Anfang des Jahres einen Bericht über die Cybersicherheit offener Funkzugangsnetze veröffentlicht, die, wenn sie ausgereifter sind, eine alternative Möglichkeit für die Einführung des Funkzugangs von 5G-Netzen auf der Grundlage offener Schnittstellen bieten werden.

32 Der Verwaltungsrat des ECCC hat seine Arbeit aufgenommen und am 20. Oktober 2022 seine vierte Sitzung abgehalten.

die Kommission eine Verordnung für ein hohes gemeinsames Cybersicherheitsniveau in diesen Institutionen vor[33], bei der die der NIS-2-Richtlinie zugrunde liegenden Grundsätze auf das institutionelle Umfeld der EU angewandt werden. Der Vorschlag umfasst einen neuen interinstitutionellen Cybersicherheitsbeirat und ein gestärktes Cybersicherheitszentrum (CERT-EU)[34], um einen angemessenen Informationsaustausch und eine angemessene Zusammenarbeit mit den Behörden der Mitgliedstaaten zu gewährleisten, beispielsweise durch das Netzwerk der Computer-Notfallteams (CSIRTs-Netzwerk). Parallel dazu hat die Kommission einen Vorschlag für eine Verordnung über die Informationssicherheit in den EU-OESS[35] angenommen, um die Resilienz gegenüber Cyberbedrohungen und hybriden Bedrohungen durch die Schaffung gemeinsamer hoher Standards für die Informationssicherheit für alle Organe, Einrichtungen und sonstigen Stellen der Union zu stärken. Der Rat muss seine Arbeiten an diesem Vorschlag nun beschleunigen, da die Mitgliedstaaten die Kommission mehrfach aufgefordert haben, Maßnahmen auszuarbeiten, wie die Entscheidungsprozesse der EU besser vor böswilligen Aktivitäten aller Art geschützt werden können. Das CERT-EU und die ENISA haben zudem eine neue Art von Cyberübung entwickelt und erprobt, die entsprechend der Empfehlung des Europäischen Rechnungshofs auf die EU-Agenturen zugeschnitten ist.

Wichtige konkrete Beispiele

Europäischer Monat der Cybersicherheit mit Workshops, Kampagnen in den sozialen Medien und Vorträgen. 2014 startete die Initiative mit 184 Aktivitäten, im Oktober 2022 zählte sie bereits 500. Die Maßnahmen tragen dazu bei, die Online-Reaktion der Nutzer im Falle einer Cybersicherheitsbedrohung zu verbessern (wie von 73 % der im Jahr 2021 befragten Mitgliedstaaten angegeben).

Cybersecurity Higher Education Database (CyberHEAD): Mit rund 70 000 Abfragen pro Jahr ist CyberHEAD seit zwei Jahren die meistbesuchte Website der ENISA. Sie ermöglicht es jungen Menschen, sachkundig aus der Vielfalt der Möglichkeiten auszuwählen, die die Hochschulbildung im Bereich der Cybersicherheit bietet, und sie hilft Hochschulen, ausgezeichnete Studierende anzuziehen, die etwas für die Cybersicherheit in Europa tun wollen.

Abwehr hybrider Bedrohungen, Bekämpfung ausländischer Einflussnahme und Verbesserung der Cyberabwehr der EU

Der **Strategische Kompass der EU** für Sicherheit und Verteidigung enthält einen ehrgeizigen Aktionsplan zur Stärkung der Handlungsfähigkeit und der Resilienz der EU sowie zur Optimierung ihrer Investition in die Verteidigungsfähigkeiten.

Die Abwehr **hybrider Bedrohungen** fällt zwar in erster Linie in die Zuständigkeit der Mitgliedstaaten, doch ergänzt die EU die nationalen Maßnahmen durch Unterstützung der Koordinierung, Verbesserung der Lageeinschätzung, Förderung der Zusammenarbeit mit gleichgesinnten Ländern und internationalen Organisationen und Bereitstellung gemeinsamer Reaktionsoptionen. In den letzten zehn Jahren wurden mehr als 200 Maßnahmen zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen auf EU-Ebene ergriffen. Die EU-Analyseeinheit für hybride Bedrohungen des INTCEN trägt zur Entscheidungsfindung in

[33] COM(2022) 122 final.

[34] Das CERT-EU hat auch erheblich in die weitere Verbesserung seiner bestehenden Dienste für die EU-OESS sowie in neue Dienste investiert, um Cyberangriffe besser zu verhindern, aufzudecken und darauf zu reagieren.

[35] COM(2022) 119 final.

der EU bei und ist die zentrale Stelle für die umfassende Lageerfassung und strategische Vorausschau, die Zusammenstellung von Informationen aus allen Quellen und die Durchführung nachrichtendienstlicher Bewertungen zu hybriden Bedrohungen. Die Arbeiten zur Schaffung der im Strategischen Kompass angekündigten EU-Teams für die rasche Reaktion auf hybride Bedrohungen haben begonnen. Diese Teams sollen die Mitgliedstaaten sowie die Missionen und Operationen im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik ebenso wies Partnerländer bei der Abwehr hybrider Bedrohungen unterstützen, indem sie kurzfristig auf einschlägiges Fachwissen auf nationaler und EU-Ebene, erforderlichenfalls auch auf militärisches Fachwissen, zurückgreifen. Ein hybrides Instrumentarium der EU ist in Ausarbeitung und wird einen Rahmen für eine koordinierte Reaktion auf hybride Kampagnen bieten, die sich gegen die EU und die Mitgliedstaaten richten. In diesem Instrumentarium werden die äußere und innere Dimension in einen nahtlosen Ablauf integriert und nationale und EU-weite Erwägungen zusammengeführt. Erhebliche Fortschritte wurden auch bei der Stärkung der Resilienz und der Abwehr hybrider Bedrohungen durch die Ermittlung bestehender sektorspezifischer Referenzwerte für die Resilienz[36] erzielt. Die Kommission hat zudem die analytische Forschung zum Aufbau der Resilienz gegenüber hybriden Bedrohungen fortgesetzt[37] und die durchgängige Einbeziehung hybrider Erwägungen in die Politikgestaltung abgeschlossen.

Die COVID-19-Pandemie und der Krieg Russlands gegen die Ukraine haben gezeigt, wie sich die Manipulation des Informationsumfelds auf die EU und ihre Partner auf der ganzen Welt auswirken kann. Die **Informationsmanipulation und Einflussnahme aus dem Ausland,** die das Vertrauen in die EU und in die regelbasierte internationale Ordnung schwächen soll, ist auch ein zunehmend wichtiger Bestandteil hybrider Angriffe. Aufbauend auf dem Aktionsplan für Demokratie in Europa hat die Kommission eine Reihe konkreter Maßnahmen und Strukturen eingeführt, darunter den überarbeiteten Verhaltenskodex für den Bereich der Desinformation, das Gesetz über digitale Dienste und den Vorschlag zur Transparenz politischer Werbung (derzeit Gegenstand von Verhandlungen zwischen den Organen), um gegen die Manipulation von Informationen und die Desinformation vorzugehen. Ziel sind neue Verpflichtungen für die Plattformen und zum ersten Mal auch ein rechtsverbindlicher Aufsichtsrahmen. Darüber hinaus arbeitet der EAD, wie im Strategischen Kompass angekündigt, in enger Zusammenarbeit mit der Kommission und den Mitgliedstaaten an der Weiterentwicklung des **EU-Instrumentariums gegen Manipulation von Informationen und Einmischung aus dem Ausland** (FIMI-Instrumentarium), um eine koordinierte Reaktion auf manipulatives Verhalten ausländischer Akteure zu ermöglichen.[38] Der EAD hat ferner die Zusammenarbeit mit internationalen Partnern wie dem Schnellreaktionsmechanismus der G7 und der NATO weiter verstärkt.

Die Kommission verurteilt jegliche Einmischung aus dem Ausland im Hoheitsgebiet der EU-Mitgliedstaaten und ist besorgt über Berichte über chinesische Polizeidienststellen in der EU, die, sollten die Berichte zutreffen, völlig inakzeptabel wären. Obwohl es Sache der

---

36 SWD(2022) 21 final.

37 *Hybrid threats: a comprehensive resilience ecosystem*, JRC130097.

38 Die Arbeiten an den Aufgaben des Strategischen Kompasses zum Aufbau eines Raums für FIMI-Daten und zur Ausstattung der Missionen und Operationen der GSVP mit Fähigkeiten und Ressourcen zur Anwendung der einschlägigen Instrumente dieses Instrumentariums sind im Gange. Der EAD liefert den EU-Mitgliedstaaten über das Schnellwarnsystem der EU weiterhin Informationen im Rahmen der quelloffenen Lageerfassung, sensibilisiert die Öffentlichkeit insbesondere über die Kampagne EUvsDisinfo und hat auch seine Zusammenarbeit mit Interessenträgern wie der NATO und dem Schnellreaktionsmechanismus der G7 weiter verstärkt.

Behörden der Mitgliedstaaten ist, diesen Vorwürfen nachzugehen, ist die Kommission bereit, den Austausch zwischen den Mitgliedstaaten mit Unterstützung von Europol zu erleichtern. Die Kommission hat dieses Thema auf der Tagung des Rates (Justiz und Inneres) im Dezember 2022 zur Sprache gebracht.

Im November 2022 legten die Kommission und der Hohe Vertreter eine neue EU-Strategie für die **Cyberabwehr** vor[39], in der mit Blick auf einen besseren Schutz vor Cyberangriffen Mittel und Wege zur Verbesserung der Zusammenarbeit und der Investitionen in die Cyberabwehr dargelegt werden. Ziel ist es, die Interessen der EU im Cyberraum durch eine verstärkte Zusammenarbeit zwischen den EU-Akteuren im Bereich der Cyberabwehr zu verteidigen und Mechanismen zur Mobilisierung von Kapazitäten auf EU-Ebene, auch im Rahmen von GSVP-Missionen und -Operationen, zu entwickeln. Dadurch sollen die Entwicklung des gesamten Spektrums an Fähigkeiten im Bereich der Cyberabwehr gefördert und die Zusammenarbeit zwischen den militärischen und zivilen Cyber-Gemeinschaften der EU gestärkt werden, indem die Lageerfassung, die Krisenkoordinierung und entsprechende Schulungsmaßnahmen, auch mit dem Privatsektor, verbessert werden. Die Strategie wird auch dazu beitragen, durch die Entwicklung eines strategischen Fahrplans für kritische Cybersicherheits- und Cyberabwehrtechnologien strategische Abhängigkeiten bei kritischen Cybertechnologien zu verringern und die technologische und industrielle Basis der europäischen Verteidigung zu stärken.

Im Strategischen Kompass wird der **Weltraum** als fünfter operativer Bereich genannt, der (neben dem Land, der Hohen See, dem Luftraum und dem Cyberraum) zunehmend umkämpft ist, und die Kommission und der Hohe Vertreter werden darin aufgefordert, die erste Weltraumstrategie für Sicherheit und Verteidigung auszuarbeiten. Im Rahmen der Strategie werden Maßnahmen zur Verbesserung des kollektiven Schutzniveaus und der Resilienz von Weltraumsystemen und -diensten sowie zur Abwehr und zur Reaktion auf Bedrohungen sensibler Weltraumsysteme und -dienste in der EU, einschließlich Cyber-Bedrohungen, vorgeschlagen.

3. BEKÄMPFUNG VON TERRORISMUS UND RADIKALISIERUNG

Fast alle in der EU-Sicherheitsstrategie erwähnten Schlüsselinitiativen zur Unterstützung der Mitgliedstaaten bei der Bekämpfung von Terrorismus und Radikalisierung sind angenommen worden. Ein besonderer Aspekt dabei ist der Schutz vor Gefahren im Internet. Der nächste Schritt besteht nun darin sicherzustellen, dass diese Initiativen ihre volle Wirkung entfalten.

Terrorismusbekämpfung

Seit der Annahme der **EU-Agenda für Terrorismusbekämpfung**[40] im Dezember 2020 ist die EU besser in der Lage, terroristische Bedrohungen zu antizipieren, zu verhindern, sich davor zu schützen und darauf zu reagieren. Auch Initiativen für bestimmte Regionen tragen dazu bei, auf die sich verändernde Bedrohungslage zu reagieren. Angesichts der Entwicklungen in Afghanistan hat der EU-Koordinator für die Terrorismusbekämpfung in Abstimmung mit der Kommission, dem Hohen Vertreter, dem Ratsvorsitz und den einschlägigen EU-Agenturen einen **Aktionsplan zur Terrorismusbekämpfung für**

39 JOIN(2022) 49 final.
40 COM(2020) 795 final.

Afghanistan[41] ausgearbeitet, der von den Mitgliedstaaten im Oktober 2021 gebilligt wurde. Ein konkretes positives Ergebnis ist ein freiwilliges Verfahren für verstärkte Sicherheitskontrollen von aus Afghanistan einreisenden Personen.

Von besonderer Bedeutung sind Maßnahmen gegen die Bedrohung durch **aus Syrien und Irak zurückkehrende ausländische terroristische Kämpfer**. Zwar liegt die Hauptverantwortung in diesem Bereich bei den Mitgliedstaaten, doch hilft ihnen die Zusammenarbeit auf EU-Ebene bei der Bewältigung gemeinsamer Herausforderungen wie der Verfolgung von Personen, die terroristische Straftaten begangen haben, der Prävention der unentdeckten Einreise in den Schengen-Raum sowie der Wiedereingliederung und Rehabilitation zurückgekehrter ausländischer terroristischer Kämpfer. Die Kommission arbeitet weiterhin eng mit den Mitgliedstaaten und wichtigen Partnerländern zusammen, um sicherzustellen, dass Beweismittel aus Kampfgebieten in den EU-Datenbanken und Informationssystemen gespeichert werden. Im Einvernehmen mit den Mitgliedstaaten prüft der EU-Koordinator für die Terrorismusbekämpfung in enger Zusammenarbeit mit dem Hohen Vertreter und der Kommission neue Wege zur Verbesserung der Lebensbedingungen in Gefängnissen und Lagern im Nordosten Syriens als Mittel zur Bekämpfung der Radikalisierung.

Die EU-Rechtsvorschriften zur Terrorismusbekämpfung sind aktualisiert worden. Die 2017 angenommene **Richtlinie zur Terrorismusbekämpfung** wird nun von allen Mitgliedstaaten umgesetzt[42], so dass u. a. Ausbildung und Reisen für terroristische Zwecke sowie Terrorismusfinanzierung als Straftat eingestuft werden. In einer Reihe von Mitgliedstaaten besteht allerdings noch Handlungsbedarf in Bezug auf die mangelhafte Umsetzung der Richtlinie.

Von maßgeblicher Bedeutung für die Terrorismusbekämpfung ist es, **Terroristen die Mittel zu entziehen, mit denen sie Anschläge begehen**. Fast alle Mitgliedstaaten haben inzwischen die überarbeiteten Rechtsvorschriften über Feuerwaffen[43] in ihr nationales Recht übernommen. Im Februar 2021 traten neue Rechtsvorschriften in Kraft, mit denen der Zugang zu Ausgangsstoffen für Explosivstoffe, die Terroristen zur Herstellung von Bomben verwenden können, eingeschränkt wurde. Aufbauend auf dem Ansatz zur Regelung des Zugangs zu Ausgangsstoffen für Explosivstoffe prüft die Kommission, wie der Zugang zu bestimmten gefährlichen Chemikalien, die zur Durchführung von Anschlägen verwendet werden könnten, beschränkt werden könnte.

Der **öffentliche Raum** stand wiederholt im Fokus von Terroranschlägen. Die Kommission hat ein Handbuch über die Gestaltung des öffentlichen Raums zur Erhöhung der Sicherheit herausgegeben.[44] Es beruht auf detaillierten technischen Leitlinien[45], Instrumenten für die Beurteilung von Schwachstellen öffentlicher Räume[46] und die umfassende Unterstützung der wichtigsten Interessenträger[47] sowie einer Empfehlung zu freiwilligen

41 Afghanistan: Aktionsplan zur Terrorismusbekämpfung, 29. September 2021.
42 COM(2021) 701 final. Die Mitgliedstaaten waren verpflichtet, die Richtlinie bis zum 8. September 2018 in nationales Recht umzusetzen.
43 COM(2015) 750 final.
44 SWD(2022) 398 final.
45 Guideline – Building Perimeter Protection, EUR 30346 EN.
46 http://counterterrorism.jrc.ec.europa.eu.
47 Siehe insbesondere: EU Digital Autumn School, JRC127168, und Terrorism and Extremism Database – User Guide, JRC130461.

Leistungsanforderungen für im öffentlichen Raum (außerhalb der Luftfahrt) genutzte Röntgengeräte[48]. Darüber hinaus wurden im Jahr 2022 aus dem Fonds für die innere Sicherheit 14,5 Millionen Euro für Projekte zum besseren Schutz des öffentlichen Raums, einschließlich Kultstätten, bereitgestellt. **Drohnen** sind ein hochinnovatives Instrument, das für rechtmäßige, aber auch böswillige Zwecke eingesetzt werden kann, darunter für Angriffe auf den öffentlichen Raum, Einzelpersonen und kritische Infrastrukturen. Im November 2022 hat die Kommission die **Drohnenstrategie 2.0**[49] angenommen, der 2023 ein detaillierteres EU-Konzept zur Bekämpfung des böswilligen Einsatzes von Drohnen folgen soll.

Bekämpfung von Radikalisierung, die zu gewaltbereitem Extremismus und Terrorismus im Online- und Offline-Bereich führt

Die Vorbeugung und Bekämpfung von **Radikalisierung** ist für eine wirksame Politik zur Terrorismusbekämpfung von entscheidender Bedeutung. Die Kommission unterstützt die Mitgliedstaaten mit dem Aufklärungsnetzwerk gegen Radikalisierung, das 6000 Experten umfasst, die im Bereich der Prävention tätig sind. Unterstützung erhalten die Mitgliedstaaten insbesondere bei der Bekämpfung gewaltorientierter extremistischer Ideologien und zur Radikalisierung führender Polarisierung, Online-Radikalisierung und Missbrauch neuer Technologien sowie beim Umgang mit und der Vorbereitung der Wiedereingliederung von aus der Haft entlassenen Straftätern. Verbindungen zwischen gewaltbereiten extremistischen Gruppen und Ideologien und Ausdrucksformen von Hetze sind Gegenstand des EU-Verhaltenskodex zur Bekämpfung illegaler Hassrede im Internet[50].

Die EU ergreift zudem Maßnahmen gegen ausländische Einflussnahme und gegen die finanzielle Unterstützung radikaler/extremistischer Ansichten in den Mitgliedstaaten. Die Kommission bleibt ihrerseits wachsam, um zu verhindern, dass mit EU-Mitteln Projekte unterstützt werden, die mit den europäischen Werten unvereinbar sind oder unrechtmäßige Zwecke verfolgen. In diesem Zusammenhang werden die von der Kommission verwalteten Projekte seit Ende 2021 unmittelbar nach der Unterzeichnung der Finanzhilfevereinbarung auf der eigens dafür vorgesehenen Plattform „Funding & tender opportunities“ veröffentlicht. Es ist von entscheidender Bedeutung, dass die Mitgliedstaaten diese Plattform nutzen, um die Begünstigten zu überprüfen und der Kommission alle ihnen vorliegenden zusätzlichen Informationen zur Verfügung zu stellen. In diesem Zusammenhang sieht die von der Kommission vorgeschlagene Überarbeitung der Haushaltsordnung vor, eine Verurteilung wegen „Aufstachelung zum Hass“ als Grund für den Ausschluss von der Finanzierung durch die EU aufzunehmen. Die Kommission fordert das Europäische Parlament und den Rat auf, diese Frage im endgültigen Text wirksam anzugehen. Darüber hinaus führt die Kommission interne Sensibilisierungsmaßnahmen durch und entwickelt interne Arbeitsmethoden, um eine strengere Kontrolle bei der Projektauswahl sicherzustellen.

Ein weiterer Schwerpunkt ist die Prävention von Radikalisierung im Internet. Im Juni 2022 ist die **Verordnung zur Bekämpfung der Verbreitung terroristischer Online-Inhalte**[51] in

---

48 In diesem Rechtsakt wird den Mitgliedstaaten empfohlen, bei der Vergabe öffentlicher Aufträge für Röntgengeräte, die zur Erkennung von Sicherheitsbedrohungen im öffentlichen Raum verwendet werden, die EU-Leistungsanforderungen zu berücksichtigen (C(2022) 4179).

49 COM(2022) 652 final.

50 https://ec.europa.eu/commission/presscorner/detail/de/IP_16_1937.

51 Verordnung (EU) 2021/784 des Europäischen Parlaments und des Rates vom 29. April 2021 zur Bekämpfung der Verbreitung terroristischer Online-Inhalte, ABl. L 172 vom 17.5.2021, S. 79.

Kraft getreten. Seitdem können die zuständigen nationalen Behörden verlangen, dass terroristische Inhalte innerhalb einer Stunde nach Erhalt der Entfernungsanordnung entfernt werden. Anbieter von Online-Diensten, die terroristischen Inhalten ausgesetzt sind, müssen spezifische Maßnahmen ergreifen, um ihre Plattformen vor Missbrauch zu schützen. Dies ergänzt die Arbeit des **EU-Internetforums**, das von der Kommission ins Leben gerufen wurde, um Mitgliedstaaten, Internetunternehmen und die Zivilgesellschaft zusammenzubringen und die Verbreitung gewaltorientierter extremistischer und terroristischer Online-Inhalte zu verhindern. Das EU-Internetforum unterstützt Technologieunternehmen und Anbieter von Internetinfrastruktur seit kurzem bei ihren Bemühungen um die Moderation von Inhalten, unter anderem durch ein Verzeichnis der von Terroristen betriebenen Websites und ein jährlich aktualisiertes Informationspaket über gewaltbereite rechtsextreme Gruppen, Symbole und Manifeste[52]. Seit 2019 befasst sich dieses Forum auch mit der Verhinderung des sexuellen Missbrauchs von Kindern im Internet.

Wichtige konkrete Beispiele

Zusammenarbeit mit Eurojust führt zur Verurteilung eines ausländischen Terrorismuskämpfers: 2021 wurde der Hauptverdächtige einer Anti-Terror-Ermittlung wegen der Beteiligung an einer terroristischen Organisation zu einer Freiheitsstrafe von vier Jahren verurteilt, nachdem die italienischen Behörden mittels des Justiziellen Terrorismusregisters Verbindungen zwischen einem verdächtigen ausländischen Kämpfer und anderen Fällen von Terrorismus aufdecken konnten. Dank der von Eurojust koordinierten Zusammenarbeit nationaler Behörden konnten europäische Ermittlungsanordnungen vollstreckt und Rechtshilfeersuchen in Strafverfahren ausgetauscht werden.

Von Europol koordiniertes Vorgehen gegen Anleitungen zum Bau von Bomben im Internet: Im Rahmen einer Reihe regelmäßiger gemeinsamer Initiativen wurden an einem von Europol koordinierten Aktionstag im Februar 2022, an dem acht Mitgliedstaaten und das Vereinigte Königreich teilnahmen, Hunderte von Online-Inhalten aufgespürt, darunter Anleitungen, wie Bomben aus Ausgangsstoffen hergestellt und bei Terroranschlägen eingesetzt werden können. Die Informationen wurden an die Anbieter der Online-Dienste weitergeleitet.

[52] Zu erwähnen sind in diesem Zusammenhang außerdem die Aktualisierung des EU-Krisenprotokolls, Handbücher mit Leitlinien zur böswilligen Verwendung grenzwertiger Inhalte und Videospiele, die zu Radikalisierung führen, sowie eine Studie über die Auswirkungen algorithmischer Verstärkung in Bezug auf den Weg der Nutzer zu Radikalisierung.

4. BEKÄMPFUNG DER ORGANISIERTEN KRIMINALITÄT

Die Zusammenarbeit zwischen Straftätern im Umfeld der organisierten Kriminalität in Europa befindet sich in einem ständigen Wandel. Kriminelle Netze sind an einer Vielzahl krimineller Handlungen beteiligt, etwa im Zusammenhang mit Drogenhandel, organisierter Eigentumskriminalität, Betrug, Schleuserkriminalität und Menschenhandel.[53] Cyberkriminalität und geschlechtsspezifische Cybergewalt haben durch die stärkere Nutzung des Internets und von Online-Diensten weiter zugenommen. Die vermehrte Nutzung verschlüsselter Kommunikationskanäle gewährleistet zwar den Schutz der Privatsphäre und der Grundrechte, bringt aber für die Strafverfolgung zusätzliche Herausforderungen mit sich.[54] Außerdem haben sich durch die Verwerfungen aufgrund des russischen Angriffskriegs gegen die Ukraine neue Möglichkeiten für kriminelle Vereinigungen ergeben, die diese rasch zu nutzen wussten.

Im April 2021 nahm die Kommission die **EU-Strategie zur Bekämpfung der organisierten Kriminalität 2021-2025**[55] an. Darin hebt sie hervor, dass es von entscheidender Bedeutung ist, die Strukturen der organisierten Kriminalität zu zerschlagen und dabei die Gruppen, die ein größeres Risiko für die Sicherheit Europas darstellen, sowie die Personen in den höheren Rängen der kriminellen Organisationen ins Visier zu nehmen. Die Umsetzung der Strategie kommt gut voran, wobei mehrere Leitaktionen bereits angenommen oder durchgeführt wurden. Zudem unterstützt die Kommission die Mitgliedstaaten bei der Bekämpfung der kriminellen Bedrohungen für die EU auch finanziell.[56]

Cyberkriminalität

Die beschleunigte Digitalisierung während der COVID-19-Pandemie hat zu vermehrten Cyberbedrohungen etwa durch Ransomware[57] geführt. **Ransomware** birgt erhebliche Cybersicherheitsrisiken für kritische Infrastrukturen und die öffentliche Sicherheit. Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3) von Europol hat zusammen mit der Gemeinsamen Taskforce gegen die Cyberkriminalität (J-CAT) vor Kurzem das „International Ransomware Response Model“ entwickelt, um eine umfassende Strafverfolgung zu gewährleisten. Die EU nahm 2022 am Gipfeltreffen der Initiative zur Bekämpfung von Ransomware zur Stärkung der internationalen Zusammenarbeit im Bereich Ransomware teil. 36 Länder sowie die EU haben vereinbart, die Arbeit an der Internationalen Taskforce für die Bekämpfung von Ransomware voranzubringen, um die Stärkung der Resilienz und die Verhinderung und Bekämpfung von Störungen zu koordinieren sowie illegale Finanzierungstätigkeiten zu unterbinden.[58] Die Kommission und Europol haben gemeinsam eine Entschlüsselungsplattform[59] eingerichtet, mit der der Zeitaufwand für den

---

53 Europol: EU-Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität, 2021 – *A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime*, Amt für Veröffentlichungen der Europäischen Union, Luxemburg.

54 Bewertung der Bedrohungslage im Bereich der organisierten Kriminalität im Internet (IOCTA), 2021.

55 COM(2021) 170 final.

56 Im Juli 2022 stellte die Kommission über den Fonds für die innere Sicherheit (ISF) 15,7 Millionen Euro für die Mitgliedstaaten bereit, um langfristige Projekte und Aktivitäten im Rahmen der Europäischen multidisziplinären Plattform gegenkriminelle Bedrohungen (EMPACT) zu unterstützen. Ziel ist es, die vom Rat für 2022-2025 angenommenen zehn EU-Prioritäten im Bereich der Bekämpfung der organisierten Kriminalität umzusetzen.

57 Bewertung der Bedrohungslage im Bereich der organisierten Kriminalität im Internet (IOCTA).

58 *International Counter Ransomware Initiative 2022*, Washington DC, 1. November 2022.

59 Die Europol-Entschlüsselungsplattform befindet sich am Sitz der Gemeinsamen Forschungsstelle Ispra.

forensischen Zugang zu digitalen Beweismitteln verkürzt und ein Beitrag zur Bekämpfung verschlüsselter krimineller Kommunikationsnetze geleistet wird. Dies trägt in hohem Maße zur Bekämpfung der organisierten Kriminalität bei.

Die EU hat eine wichtige Rolle bei den erfolgreichen Verhandlungen über das Zweite Zusatzprotokoll zum **Budapester Übereinkommen über Computerkriminalität** vom Mai 2022 gespielt. Darin sind auch dringend benötigte Instrumente für die grenzüberschreitende Zusammenarbeit bei der Ermittlung und Verfolgung von Cyberkriminalität sowie detaillierte Datenschutzbedingungen und -garantien vorgesehen. Das Zweite Zusatzprotokoll sollte rasch von allen Mitgliedstaaten unterzeichnet werden, und das Europäische Parlament ist aufgefordert, seine Zustimmung zu erteilen, um eine baldige Ratifizierung zu ermöglichen. Darüber hinaus verhandelt die Kommission im Namen der EU über ein neues Übereinkommen der Vereinten Nationen über Cyberkriminalität.

Allein im Jahr 2021 wurden weltweit 85 Millionen Bilder und Videos von **sexuellem Missbrauch von Kindern** angezeigt. Eingedenk der hohen Dunkelziffer ist sexueller Missbrauch von Kindern erschreckend weit verbreitet. Weil Kinder mehr Zeit im Internet verbringen, werden sie häufiger Opfer einer gezielten Kontaktaufnahme in Missbrauchsabsicht, sodass es immer mehr selbsterstellte Missbrauchsdarstellungen gibt. Im Einklang mit der im Juli 2020 angenommenen EU-Strategie für eine wirksamere Bekämpfung des sexuellen Missbrauchs von Kindern[60] und der umfassenden EU-Kinderrechtsstrategie vom März 2021[61] hat die Kommission im Mai 2022 einen Vorschlag zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern[62] mit neuen Verpflichtungen für Anbieter von Online-Diensten angenommen. Sollte es nicht gelingen, das erhebliche Risiko durch Prävention zu verringern, können die Diensteanbieter angewiesen werden, Darstellungen von sexuellem Missbrauch von Kindern im Internet aufzuspüren, zu melden, zu entfernen und zu blockieren. In dem Vorschlag ist außerdem die Einrichtung eines speziellen EU-Zentrums vorgesehen, das die Umsetzung erleichtern soll. Die im August 2021 verabschiedeten befristeten Rechtsvorschriften, in denen das Freiwilligkeitsprinzip in Bezug auf die Aufdeckung und Meldung von Darstellungen sexuellen Missbrauchs von Kindern im Internet durch die Anbieter von Online-Diensten beibehalten wurde[63], laufen im Sommer 2024 aus. Das Europäische Parlament und der Rat müssen deshalb rasch zu einer Einigung über die vorgeschlagene Verordnung gelangen. Anfang nächsten Jahres wird ergänzend zu dieser Initiative ein Vorschlag zur Aktualisierung der Richtlinie von 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie[64] vorgelegt.

Cybergewalt gegen Frauen und Mädchen stellt eine neue Dimension **geschlechtsspezifischer Cybergewalt** dar, die im Zunehmen begriffen ist. Im Jahr 2020 hat schätzungsweise die Hälfte der jungen Frauen geschlechtsspezifische Cybergewalt erlebt.[65] In ihrem im März 2022 angenommenen Vorschlag für eine Richtlinie zur Bekämpfung von Gewalt gegen Frauen und

---

60 COM(2020) 607 final.
61 COM(2021) 142 final.
62 COM(2022) 209 final.
63 COM(2020) 568 final.
64 Richtlinie 2011/93/EU vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates, ABl. L 335 vom 17.12.2011.
65 Wissenschaftlicher Dienst des Europäischen Parlaments (EPRS): *Combating gender-based violence: Cyberviolence, European added value assessment*, 2021.

häuslicher Gewalt[66] hat die Kommission gezielte Vorschriften zur Bekämpfung geschlechtsspezifischer Gewalt gegen Frauen im Internet und im realen Leben[67] vorgeschlagen.

Organisierte Kriminalität

Der **Menschenhandel** ist ein Kerngeschäft der organisierten Kriminalität in der EU.[68] Obwohl er bereits in der EU-Strategie für eine Sicherheitsunion als Priorität eingestuft wurde, haben sich während der COVID-19-Pandemie neue Möglichkeiten für Straftäter ergeben, erhebliche Gewinne zu erzielen und ihre kriminellen Aktivitäten auszuweiten. Eine rasche Koordinierung auf EU-Ebene trägt dazu bei, dem infolge des russischen Angriffskriegs gegen die Ukraine gestiegenen Risiko des Menschenhandels vorzubeugen. Der EU-Koordinator für die Bekämpfung des Menschenhandels hat einen **Gemeinsamen Plan zur Bekämpfung des Menschenhandels**[69] ausgearbeitet, um die Arbeit der Kommission mit jener der Mitgliedstaaten, der EU-Agenturen und des Europäischen Auswärtigen Dienstes zu verknüpfen, damit der Gefahr des Menschenhandels begegnet und potenziellen Opfern Unterstützung geboten werden kann. Diese Bemühungen haben dazu beigetragen, dass die Zahl der bestätigten Fälle von Menschenhandel trotz anhaltend großer Bedrohung nach wie vor gering ist.

Im April 2021 wurde mit der EU-Strategie zur Bekämpfung des Menschenhandels 2021-2025[70] ein umfassender interner und externer Handlungsrahmen geschaffen. Daran anknüpfend wird die Kommission einen Vorschlag zur Änderung der **Richtlinie zur Bekämpfung des Menschenhandels**[71] vorlegen, mit dem Lücken im derzeitigen Rechtsrahmen geschlossen und dieser aktualisiert werden soll. Ziel ist es, der Online-Dimension des Menschenhandels Rechnung zu tragen und eine Verringerung der Nachfrage zu erreichen. Im September 2022 veranstaltete EMPACT einen gemeinsamen Aktionstag zu kriminellen Netzen, die Websites und Social-Media-Plattformen nutzen, um Opfer für sexuelle Ausbeutung ausfindig zu machen. In diesem Zusammenhang fand der erste EU-weite Hackathon gegen Menschenhandel statt, der von Europol und Eurojust sowie von Strafverfolgungsbehörden aus 20 Ländern unterstützt wurde. Dabei wurden elf mutmaßliche Menschenhändler und 45 mögliche Opfer ermittelt.[72]

Im Gegensatz zum Menschenhandel werden Schleuser für die irreguläre Einreise in die EU aus freien Stücken in Anspruch genommen und bezahlt. Die Tätigkeit von Schleusern ist jedoch strafbar, gefährdet oftmals Leben und kann zusätzliche Sicherheitsrisiken für die EU nach sich ziehen. Die Verhütung und Bekämpfung der **Schleusung von Migranten** ist ein zentrales Ziel der EU-Strategie für eine Sicherheitsunion, der EU-Strategie zur Bekämpfung

66 COM(2022) 105 final.

67 Laut dem Vorschlag sollen die nicht-einvernehmliche Weitergabe von intimem Material, Cyberstalking, Cybermobbing und die Aufstachelung zu Gewalt oder Hass im Internet auf EU-Ebene als Straftatbestände eingestuft werden. Dies soll durch einen neuen Rahmen für die Zusammenarbeit zwischen Internetplattformen zum besseren Schutz der Sicherheit von Frauen im Internet ergänzt werden.

68 Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität (SOCTA), 2021.

69 *An Anti-Trafficking Plan to protect people fleeing the war in Ukraine* (europa.eu).

70 COM(2021) 171 final.

71 Der vierte Fortschrittsbericht zum Menschenhandel, der zusammen mit diesem Vorschlag angenommen werden soll, enthält detaillierte Informationen über die Umsetzung der EU-Strategie von 2019 bis 2022 sowie wichtige Daten und Statistiken.

72 20 countries spin a web to catch human traffickers during a hackathon | Europol (europa.eu)

der organisierten Kriminalität und des neuen Migrations- und Asylpakets[73]. In diesem Zusammenhang bedarf es einer ständigen internationalen Zusammenarbeit und Koordinierung auf allen Ebenen. Bei der Umsetzung des EU-Aktionsplans gegen die Schleusung von Migranten für den Zeitraum 2021-2025[74] sind Fortschritte zu verzeichnen, wobei mit Marokko, Niger und dem Westbalkan operative Partnerschaften zur Bekämpfung der Schleusung entwickelt werden, die von den Organen, Einrichtungen und sonstigen Stellen der EU sowie mit EU-Mitteln unterstützt werden.

Schätzungen zufolge weist der **illegale Drogenmarkt** einen Einzelhandelswert von 30 Milliarden Euro pro Jahr auf und ist nach wie vor der größte kriminelle Markt und eine wichtige Einnahmequelle für kriminelle Vereinigungen in der EU. Zudem stellt er eine Bedrohung für die soziale Stabilität und die Gesundheit dar. Im Jahr 2021 führten die Maßnahmen und die Zusammenarbeit der EU dazu, dass Drogen im Wert von sieben Milliarden Euro beschlagnahmt wurden.[75] Die **EU-Agenda zur Drogenbekämpfung und der Aktionsplan für den Zeitraum 2021-2025**[76] vom Juli 2020 enthalten konkrete Maßnahmen zur Intensivierung der Maßnahmen auf EU-Ebene, einschließlich der Umwandlung der Europäischen Beobachtungsstelle für Drogen und Drogensucht in die Drogenagentur der Europäischen Union. Durch den Vorschlag vom Januar 2022 für ein überarbeitetes Mandat der Agentur[77] sollen ihre Fähigkeiten zur Überwachung und Bewertung der Bedrohungslage sowie ihre Möglichkeiten, auf neue Herausforderungen zu reagieren, gestärkt werden. Der Rat hat im Juni 2022 eine allgemeine Ausrichtung angenommen, und auch das Europäische Parlament ist mit dieser Thematik befasst. Darüber hinaus hat die Kommission eine Zusammenarbeit im Rahmen des EU-Internetforums zur Bekämpfung des Online-Drogenhandels initiiert und eine spezifische thematische Schengen-Evaluierung des Schmuggels von Kokain in EU-Häfen vorgeschlagen. Die Unterstützung für das Operationszentrum für den Kampf gegen den Drogenhandel im Atlantik wurde aufgestockt. Darüber hinaus setzt die EU ihren politischen Dialog zum Thema Drogen mit Drittländern fort, wobei im Juli 2022 ein zweiter Dialog mit China geführt und im Juni 2022 ein neuer Dialog mit Kolumbien aufgenommen wurde.

Nach Angaben von Europol entgehen fast 99 Prozent der Erträge aus Straftaten der **Einziehung** in der EU und verbleiben in den Händen von Straftätern.[78] Bei der Behandlung der von der Kommission im Juli 2021 vorgelegten Vorschläge zur besseren Bekämpfung von Geldwäsche und Terrorismusfinanzierung in der EU[79] im Rat sind Fortschritte zu verzeichnen. Im Mai 2022 hat die Kommission vorgeschlagen, die EU-Vorschriften über die Abschöpfung und Einziehung von Vermögenswerten zu verschärfen und zu modernisieren.[80]

---

73 COM(2020) 609 final.
74 COM(2021) 591 final.
75 Jahresbericht 2021 von Eurojust.
76 COM(2020) 606 final.
77 COM(2022) 18 final.
78 Europol: *Does crime still pay? Criminal Asset Recovery in the EU – Survey of statistical information 2010-2014, 2016*.
79 COM(2021) 421 final, COM(2021) 420 final, COM(2021) 423 final, COM(2021) 422 final. Im Juni 2022 wurden eine politische Einigung über die Verordnung über Geldtransfers erzielt und eine partielle allgemeine Ausrichtung bezüglich der Verordnung zur Errichtung der Behörde zur Bekämpfung der Geldwäsche und Terrorismusfinanzierung (mit Ausnahme der Bestimmungen über Ressourcen und Sitz) angenommen.
80 COM(2022) 245 final.

Der Vorschlag wird in den Arbeitsgruppen des Rates erörtert, wobei in mehreren Bereichen Fortschritte erzielt wurden.

Die **Europäische Staatsanwaltschaft**, die zum Schutz der finanziellen Interessen der EU errichtet wurde, hat ihre Tätigkeit vor über einem Jahr aufgenommen. Bei ihr gingen 4006 Strafanzeigen ein, die zu 929 Ermittlungen führten, die wiederum Sicherstellungsentscheidungen in Höhe von 259 Millionen Euro zur Folge hatten. In den Ermittlungsverfahren, die in den ersten sieben Monaten ihrer Tätigkeit anhängig waren, ging es um einen geschätzten Gesamtschaden für den Unionshaushalt von 5,4 Milliarden Euro.[81]

Außerdem arbeitet die Kommission, wie im Aktionsplan für geistiges Eigentum[82] angekündigt und in der Strategie zur Prävention und Bekämpfung der organisierten Kriminalität hervorgehoben, an einem EU-Instrumentarium zur Bekämpfung von Nachahmungen.

Korruption untergräbt nicht nur das Vertrauen zwischen dem Staat und seinen Bürgerinnen und Bürgern, sondern stellt auch eine Bedrohung für die Sicherheit dar. Sie ist ein wichtiges Instrument für die organisierte Kriminalität und ermöglicht eine Vielzahl krimineller Aktivitäten. Sie ist ein zentrales Thema des jährlichen Berichts über die Rechtsstaatlichkeit.[83] Obwohl einige EU-Mitgliedstaaten weiterhin zu den Ländern mit den weltweit besten Ergebnissen bei der Korruptionsbekämpfung zählen, bestehen nach wie vor zahlreiche Herausforderungen, insbesondere in Zusammenhang mit strafrechtlichen Ermittlungen, Strafverfolgungsmaßnahmen und der Verhängung von Strafen für Korruption. Viele Mitgliedstaaten haben Maßnahmen zur Stärkung der Korruptionsprävention und der Integritätsrahmen eingeleitet, doch sind die für die Korruptionsbekämpfung bereitgestellten Mittel oft unzureichend. Die Kommission arbeitet derzeit an einem Paket zur Korruptionsbekämpfung für das Jahr 2023, mit dem die Rechtsvorschriften in diesem Bereich aktualisiert und gestrafft werden sollen.

Der EU-Aktionsplan gegen den unerlaubten Handel mit **Feuerwaffen** 2020-2025[84] wurde zusammen mit der Strategie für eine Sicherheitsunion im Juli 2020 angenommen. Im Anschluss daran wurde im Oktober 2022 ein Vorschlag zur Überarbeitung der Vorschriften über Einfuhr-, Ausfuhr- und Durchfuhrmaßnahmen für Feuerwaffen[85] mit einem umfassenderen Schwerpunkt auf dem Aspekt der Digitalisierung vorgelegt. Insgesamt dürfte dies die Rückverfolgbarkeit ziviler Feuerwaffen verbessern. Außerdem wird daran gearbeitet, die Ukraine und die Republik Moldau in Bezug auf **Kleinwaffen und leichte Waffen** (SALW) im Zusammenhang mit dem russischen Angriffskrieg gegen die Ukraine besser zu unterstützen.

Der illegale Handel mit Kulturgütern ist für die organisierte Kriminalität und bisweilen auch für Konfliktparteien und Terroristen ein lukratives Geschäft.[86] Er leistet auf diese Weise der organisierten Kriminalität Vorschub und wirkt sich nachteilig auf das kulturelle Erbe aus. Selbst legal erworbene Kulturgüter können von Kriminellen zum Zwecke der Geldwäsche,

---

81 Erster Jahresbericht der Europäischen Staatsanwaltschaft, 2022.

82 COM(2020) 760.

83 Die jüngste Ausgabe des Berichts wurde am 13. Juli 2022 angenommen (COM (2022) 500).

84 COM(2020) 608 final.

85 COM(2022) 480.

86 Siehe u. a. die Resolutionen 2199 (2015), 2253 (2015), 2322 (2016), 2347 (2017), 2462 (2019) und 2617 (2021) des Sicherheitsrates der Vereinten Nationen sowie die Erklärung von Rom der G20-Kulturminister vom 30. Juli 2021.

der Umgehung von Sanktionen, der Steuerhinterziehung oder der Terrorismusfinanzierung missbraucht werden. Um den **illegalen Handel mit Kulturgütern wirksamer zu bekämpfen**, nimmt die Kommission heute einen Aktionsplan an.[87]

Laut Interpol und dem Umweltprogramm der Vereinten Nationen steht die **Umweltkriminalität** nach dem Drogenhandel, dem Menschenhandel und der Fälschung weltweit an vierter Stelle der kriminellen Aktivitäten. Derzeit werden ehrgeizige Vorschläge der Kommission für eine neue Richtlinie über den strafrechtlichen Schutz der Umwelt[88], eine neue Abfallverbringungsverordnung[89] und eine neue Verordnung zur Entwaldung[90] verhandelt. Nach ihrer Annahme wird die Durchsetzungskette gestärkt sowie für höhere Strafen und geeignete Ermittlungsinstrumente gesorgt. Ergänzend dazu ist ein überarbeiteter Aktionsplan zur Bekämpfung des illegalen Artenhandels[91] vorgesehen.

Wichtige konkrete Beispiele

Encrochat: Die Justiz- und Strafverfolgungsbehörden in Belgien, Frankreich und den Niederlanden haben mit Unterstützung von Europol und Eurojust gemeinsame Operationen durchgeführt, um die Nutzung verschlüsselter Kommunikation durch in großem Stil agierende kriminelle Vereinigungen zu verhindern. Der betreffende Dienst hatte zum Zeitpunkt seiner Sperrung 60 000 Abonnenten, davon schätzungsweise 90 % Kriminelle.

Die polizeiliche und justizielle Zusammenarbeit in der EU ermöglichte die Zerschlagung einer großen kriminellen Organisation (Operation „Pollino“): Eine 2016 von Italien, Deutschland und den Niederlanden eingesetzte gemeinsame Ermittlungsgruppe führte einen von Eurojust koordinierten und von Europol unterstützten Aktionstag durch, aufgrund dessen 34 Personen zu einer Freiheitsstrafe von insgesamt mehr als 400 Jahren verurteilt wurden. Später wurden zwölf Personen zu über 173 Jahren Haft verurteilt, wobei die Verfahren in mehreren Mitgliedstaaten noch nicht beendet sind.

4. GEWÄHRLEISTUNG DER SICHERHEIT UNSERER GRENZEN UND UNTERSTÜTZUNG VON STRAFVERFOLGUNG UND JUSTIZIELLER ZUSAMMENARBEIT

Neben den wirtschaftlichen und sozialen Vorteilen ist ein gut funktionierender **Schengen-Raum** von entscheidender Bedeutung für die Sicherheit der EU. Es bedarf deshalb eines wirksamen Managements der EU-Außengrenzen und einer verstärkten Zusammenarbeit bei der Strafverfolgung. Im Juni 2021 nahm die Kommission eine Strategie für einen reibungslos funktionierenden und resilienten Schengen-Raum[92] an, in der dargelegt wird, wie sich die EU auch ohne Kontrollen an den Binnengrenzen durch Maßnahmen in den Bereichen Sicherheit sowie polizeiliche und justizielle Zusammenarbeit wirksam vor Sicherheitsbedrohungen schützen kann. Als Folgemaßnahme zu der Strategie wurde ein jährlicher Schengen-Zyklus (ein neues Governance-Modell für den Schengen-Raum) eingeführt, und im ersten Schengen-Statusbericht[93] vom Mai 2022 wurden die Fortschritte in

87 COM(2022) 800.
88 COM(2021) 851 final.
89 COM(2021) 709 final.
90 COM(2021) 706 final.
91 COM(2022) 581 final.
92 COM(2021) 277 final.
93 COM(2022) 301 final.

diesem Bereich erfasst. Ein zentraler Schritt besteht in der Änderung des Schengener Grenzkodex[94] durch den Vorschlag der Kommission vom Dezember 2021, der neue Bestimmungen zur Unterstützung einer wirksamen Zusammenarbeit im Sicherheitsbereich sowie Maßnahmen für ein effizienteres Management der Außengrenzen in Krisensituationen umfasst. Ausgehend von der allgemeinen Ausrichtung des Rates vom Juni 2022 müssen das Europäische Parlament und der Rat die Verhandlungen nun rasch abschließen. Die Kommission hat des Weiteren die Vorteile hervorgehoben, die sich aus der Einbeziehung Bulgariens, Rumäniens und Kroatiens in alle Aspekte des Schengen-Raums ergeben, wodurch die Sicherheit und das gegenseitige Vertrauen im Schengen-Raum gestärkt würden.[95] Im Dezember 2022 hat der Rat einen Beschluss über die vollständige Anwendung des Schengen-Besitzstands in Kroatien angenommen.[96]

In einem Raum ohne Kontrollen an den Binnengrenzen sollten Polizeibeamte in einem Mitgliedstaat Zugang zu allen Informationen haben, die ihren Kollegen in einem anderen Mitgliedstaat zur Verfügung stehen. Eine umfassende und wirksame Zusammenarbeit muss die Norm sein. Deshalb ist es von entscheidender Bedeutung, die den Strafverfolgungs- und Justizbehörden in der gesamten EU zur Verfügung stehenden Instrumente für den **Informationsaustausch und die grenzüberschreitende Zusammenarbeit** zu stärken. Durch das Paket zur polizeilichen Zusammenarbeit vom Dezember 2021[97] wurden die verfügbaren Instrumente erheblich verbessert. Mit der **Richtlinie über den Informationsaustausch** wurde nun eine politische Einigung zwischen dem Europäischen Parlament und dem Rat erzielt, und im Juni 2022 hat der Rat eine Empfehlung zur Verstärkung der grenzüberschreitenden polizeilichen Zusammenarbeit angenommen. Die Verhandlungen über die Verordnung zur Überarbeitung des Prüm-Rahmens[98] werden fortgesetzt, um einen effizienteren automatisierten Datenaustausch zwischen Strafverfolgungsbehörden in bestimmten Bereichen wie DNA, daktyloskopische Daten und Fahrzeugregisterdaten zu ermöglichen und diesen Austausch auf die Bereiche Polizeiakten und Gesichtsbilder auszuweiten. Durch eine rasche Einigung über die **Prüm-II-Verordnung** stünde den Strafverfolgungsbehörden in den Mitgliedstaaten das gesamte neue Instrumentarium für den Informationsaustausch zur Verfügung.

Um die grenzüberschreitende Kriminalität wirksamer bekämpfen zu können, müssen die Strafverfolgungs- und Justizbehörden der Mitgliedstaaten mit der Unterstützung von EU-Agenturen wie Europol und Eurojust eng zusammenarbeiten. Das im Juni 2022 in Kraft getretene neue Mandat von **Europol** ermöglicht es der Agentur, ihr Fachwissen und ihre operativen Fähigkeiten auszubauen, um die Mitgliedstaaten bei der Bekämpfung von schwerer und organisierter Kriminalität sowie Terrorismus besser zu unterstützen. Das neue Mandat stärkt zudem den Datenschutzrahmen von Europol sowie die Aufsicht des Europäischen Datenschutzbeauftragten. Die Ermittlungsbehörden und Gerichte der einzelnen Mitgliedstaaten müssen bei der Ermittlung und Verfolgung von Straftaten zusammenarbeiten und einander unterstützen sowie Informationen und Beweismittel sicher und rasch

---

94 COM(2021) 891 final.

95 COM(2022) 636 final.

96 Ab dem 1. Januar 2023 werden die Personenkontrollen an den Land- und Seebinnengrenzen zwischen Kroatien und den anderen Ländern des Schengen-Raums aufgehoben. Die Kontrollen an den Luftbinnengrenzen werden ab dem 26. März 2023 aufgehoben.

97 COM(2021) 782 final, COM (2021) 780 final.

98 COM(2021) 784 final.

austauschen. Das im Dezember 2021 angenommene **Paket zur Digitalisierung der Justiz**[99] umfasst praktische Schritte zur Verbesserung des digitalen Informationsaustauschs in Fällen des grenzüberschreitenden Terrorismus, zur Einrichtung einer Plattform für die Zusammenarbeit zur Unterstützung der Arbeit gemeinsamer Ermittlungsgruppen sowie zur Förderung der Digitalisierung der grenzüberschreitenden justiziellen Zusammenarbeit und des Zugangs zur Justiz in Zivil-, Handels- und Strafsachen. Eine rasche Annahme dieses Pakets durch das Europäische Parlament und den Rat würde den Informationsaustausch zwischen den Justizbehörden erheblich erleichtern.

Elektronische Beweismittel sind Teil fast jedes Ermittlungsverfahrens. Die im November 2022 erzielte vorläufige politische Einigung über **elektronische Beweismittel**[100] wird einen sicheren Austausch von Beweismaterial ermöglichen, das für die Justizbehörden in den Mitgliedstaaten von entscheidender Bedeutung für die Bekämpfung von Straftaten ist.

Die **Sicherung der EU-Außengrenzen** ist eine gemeinsame Verantwortung. Die ersten Teams der ständigen Reserve der Europäischen Grenz- und Küstenwache, die aktuell etwa 4800 Frontex- und nationale Beamte umfasst, werden seit Januar 2021 erfolgreich eingesetzt.

Der in diesem Jahr auf den meisten Migrationsrouten verzeichnete Anstieg der irregulären Einreisen hat gezeigt, wie wichtig systematische Identitäts- und Sicherheitskontrollen aller an den Außengrenzen der EU ankommenden Migranten sowie Gesundheitskontrollen auf der Basis gemeinsamer Standards sind. Sicherheit ist ein wichtiger Aspekt des neuen Migrations- und Asylpakets. Dadurch, dass Migranten, wie im **Screening-Vorschlag** vorgesehen, rasch den jeweils geeigneten Verfahren zugeführt werden, wäre gewährleistet, dass alle Grundrechtsverpflichtungen bei den Sicherheitskontrollen uneingeschränkt gewahrt werden. Ein Standpunkt des Europäischen Parlaments zu diesem Vorschlag steht noch aus.

Die **Instrumentalisierung von Migranten** für politische Zwecke durch das belarussische Regime brachte im zweiten Halbjahr 2021 beispiellose rechtliche, praktische und menschliche Herausforderungen mit sich, auch in Bezug auf die Sicherheit. Im Vorschlag zum Schengener Grenzkodex wird auch auf die Instrumentalisierung von Migranten für politische Zwecke durch Drittstaaten eingegangen. Mitgliedstaaten, die sich mit einer solchen Situation konfrontiert sehen, könnten beispielsweise die Zahl der Grenzübergangsstellen beschränken und die Grenzüberwachung intensivieren.

Derzeit werden die **Informationssysteme** der EU neu strukturiert, damit sie die Arbeit der nationalen Behörden zur Gewährleistung der Sicherheit sowie des Grenz- und des Migrationsmanagements besser unterstützen können. Im Mittelpunkt steht dabei das erneuerte Schengener Informationssystem, das seinen Betrieb im März 2023 aufnehmen soll. Weitere wichtige Instrumente sind das Einreise-/Ausreisesystem, das im Mai 2023 seine Arbeit aufnehmen soll, das Europäische Reiseinformations- und -genehmigungssystem (ETIAS), das bis Ende 2023 in Betrieb genommen werden soll, sowie die Aktualisierung des Visa-Informationssystems (VIS). Diese Instrumente werden mehr Kontrollen ermöglichen und Sicherheitslücken durch einen besseren Informationsaustausch zwischen den Mitgliedstaaten schließen. Dabei kommt es entscheidend auf die Interoperabilität der Systeme an: Die Agentur der Europäischen Union für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA) und die Mitgliedstaaten müssen

99 COM (2021) 756 final, COM (2021) 757 final, COM (2021) 759 final.
100 COM(2018) 225 final, COM (2018) 226 final.

unverzüglich die notwendigen Maßnahmen ergreifen, um dieses ehrgeizige Projekt bis Ende 2024 vollständig umzusetzen.

Die **Kontrollen von Wareneinfuhren** müssen wirksam sein, um die Risiken für die EU und ihre Bürgerinnen und Bürger gering zu halten und gleichzeitig die Wettbewerbsfähigkeit rechtmäßig agierender EU-Unternehmen zu gewährleisten. Die Sicherheitskontrollen bei importierten Waren wurden durch ein verbessertes EU-Einfuhrkontrollsystem[101] verstärkt, um wirksame risikobasierte Zollkontrollen und Maßnahmen zum Schutz von Luftfracht vor terroristischen Bedrohungen zu unterstützen. Aus dem Instrument für Zollkontrollausrüstung (CCEI)[102] wird zudem die transparente Beschaffung, Wartung und Modernisierung relevanter, modernster und zuverlässiger Zollkontrollausrüstung finanziert.

Die Vorschriften für die **Vorabübermittlung von Fluggastinformationen** (Advance Passenger Information – API) sind teils veraltet bzw. werden nicht einheitlich angewandt, weshalb dieses Instrument nicht in vollem Maße zur Gewährleistung der Sicherheit beitragen kann. Ziel der neuen Vorschläge der Kommission, durch die die derzeitige API-Richtlinie aufgehoben werden soll, ist es, die Nutzung von vorab übermittelten Fluggastinformationen sowohl für das Grenzmanagement als auch für die Strafverfolgung klarer zu fassen und zu verbessern.[103] Die Vorabübermittlung von Fluggastinformationen soll auf ausgewählte Flüge innerhalb der EU ausgeweitet werden, wodurch das den Strafverfolgungsbehörden der Mitgliedstaaten im Schengen-Raum zur Verfügung stehende Instrumentarium erweitert würde. Angesichts der Tatsache, dass immer mehr Drittländer in der Lage sind, diese Informationen für die Strafverfolgung und die Grenzsicherung zu verarbeiten, steht derzeit die externe Dimension der EU-Politik in Sachen **Fluggastdatensätze** im Fokus der Überlegungen. Darüber hinaus arbeitet die Kommission an einem Legislativvorschlag für einen Rahmen für den gegenseitigen Zugang von Beamten vor Ort zu sicherheitsbezogenen Informationen zwischen der EU und wichtigen Drittländern zur Abwehr gemeinsamer Sicherheitsbedrohungen, mit dem sichergestellt werden soll, dass Straftäter und Terroristen wirksam aufgespürt werden können.

Reisedokumentenbetrug erleichtert Kriminellen und Terroristen das Reisen im Verborgenen und spielt eine Schlüsselrolle sowohl beim Menschen- als auch beim Drogenhandel. Dieses Problem muss angegangen werden, wobei gleichzeitig auch der legale Reiseverkehr erleichtert werden muss. Die Mitgliedstaaten stellen deshalb seit August 2021 Personalausweise mit harmonisierten Sicherheitsstandards aus, einschließlich eines Chips mit biometrischen Identifikatoren, der von allen EU-Grenzbehörden überprüft werden kann.[104] Die Kommission bereitet derzeit eine weitere Initiative zur Digitalisierung von Reisedokumenten und zur Erleichterung von Reisen[105] vor, die die Sicherheit erhöhen und die Reise- und Grenzverfahren durch die papierlose Übermittlung von Reisedaten und

---

101 Das Einfuhrkontrollsystem 2 (ICS2) wird in drei Etappen eingeführt (März 2021, März 2022 und März 2023), die jeweils andere Wirtschaftsbeteiligte und Verkehrsträger betreffen.

102 Verordnung (EU) 2021/1077 vom 24. Juni 2021 zur Schaffung des Instruments für finanzielle Hilfe für Zollkontrollausrüstung im Rahmen des Fonds für integrierte Grenzverwaltung.

103 COM(2022) 729 final und 731 final.

104 Auf der Grundlage der Verordnung (EU) 2019/1157 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern und der Aufenthaltsdokumente, die Unionsbürgern und deren Familienangehörigen ausgestellt werden, die ihr Recht auf Freizügigkeit ausüben (ABl. L 188 vom 12.7.2019, S. 67).

105 EUR-lex 52022PC0658.

personenbezogenen Daten sowie biometrische Kontrollen an den Grenzen beschleunigen wird.

Strafverfolgung und neue Technologien

Technologien wie **künstliche Intelligenz** (KI) oder Verschlüsselung können die Arbeit der Strafverfolgungs- und Justizbehörden erleichtern, aber auch behindern. In ihrer Mitteilung über künstliche Intelligenz und im Gesetz über künstliche Intelligenz[106] betont die Kommission, dass KI erheblich zu den Zielen der Strategie für eine Sicherheitsunion beitragen kann, indem sie aktuellen Bedrohungen entgegenwirkt und künftige Risiken und Chancen antizipiert.[107] Im Rahmen von Horizont Europa, dem Forschungs- und Innovationsprogramm der EU für den Zeitraum 2021-2027, stehen Mittel für **Forschungsmaßnahmen und Innovation im Bereich der zivilen Sicherheit** zur Verfügung, u. a. für die Bereiche KI und Biometrie. Allein für die Jahre 2021 und 2022 sind bereits 413,8 Millionen Euro vorgesehen.[108]

Wichtige konkrete Beispiele

Nutzung des Schengener Informationssystems (SIS): 2021 haben die Mitgliedstaaten knapp sieben Milliarden Abfragen im SIS durchgeführt. Die Behörden der Mitgliedstaaten haben im Durchschnitt pro Tag fast 20 Millionen Abfragen vorgenommen, was im Durchschnitt zu 600 Treffern bei ausländischen Ausschreibungen pro Tag geführt und zur Aufklärung einer entsprechenden Zahl von Fällen beigetragen hat. So wurde etwa nach einem brutalen Doppelmord in Rumänien im Jahr 2021 der Täter nur wenige Tage später in Italien aufgespürt. Dies war auf eine SIS-Ausschreibung zur Festnahme zurückzuführen, die italienische Ermittler auf die richtige Fährte brachte, sodass sie den Mann in Rom verhaften konnten.

5. ZUSAMMENHANG ZWISCHEN INNERER UND ÄUSSERER SICHERHEIT: SICHERHEIT IN DER EU-NACHBARSCHAFT UND IN PARTNERLÄNDERN

Zwischen den Geschehnissen in Drittstaaten und der Sicherheit in der EU besteht ein enger Zusammenhang. Um die innere Sicherheit der EU zu erhöhen, müssen wir unsere Nachbarn und Partner bei der Verbesserung ihrer inneren Sicherheit unterstützen sowie mit unseren Verbündeten und internationalen Organisationen wie der NATO oder den Vereinten Nationen zusammenarbeiten.

Der Europäische Auswärtige Dienst (EAD) und die Kommissionsdienststellen arbeiten im Rahmen regelmäßiger Dialoge über **Terrorismusbekämpfung** eng mit wichtigen Partnerländern und internationalen Organisationen zusammen. Derzeit werden über 30 Dialoge über Terrorismusbekämpfung mit Drittstaaten und internationalen Organisationen

106 COM(2021) 206 final.
107 COM(2021) 205 final.
108 Im Rahmen von Horizont Europa sind zudem erhebliche Investitionen in innovative Technologien vorgesehen, durch die die Strafverfolgungsbehörden im Kampf gegen Radikalisierung unterstützt werden sollen, sowie in Projekte in den Bereichen Aufdeckung des illegalen Handels mit Drogen und Sprengstoffen sowie Kulturgütern, Schleuserkriminalität, Sicherheit des öffentlichen Raums und Identitätsdiebstahl.

geführt.[109] Parallel dazu wurde das Netz von Experten für Terrorismusbekämpfung und Sicherheit in den EU-Delegationen in wichtigen Drittländern gestärkt.

Um den Bedrohungen der inneren Sicherheit im Zusammenhang mit dem russischen Angriffskrieg gegen die Ukraine besser begegnen zu können, haben die Kommissionsdienststellen und der EAD (mit dem EU-Koordinator für die Terrorismusbekämpfung) gemeinsam mit der **Ukraine** vereinbart, eine kontinuierliche strukturierte Sicherheitszusammenarbeit einzurichten. Ziel ist es, die operative Zusammenarbeit, auch mit Europol und Frontex, zu verbessern und den Informationsaustausch über Bedrohungen der inneren Sicherheit zu intensivieren. Nach der Invasion Russlands in die Ukraine haben die EU-Agenturen sofortige Unterstützung bei der Reaktion auf die sich in diesem Zusammenhang ergebenden Herausforderungen geleistet. Derzeit verfügt Frontex über 277 Mitarbeiter in der Region, Europol über 15 und die EU-Asylagentur über 60.

Die Strafverfolgungsbehörden der Mitgliedstaaten und ihre Partner arbeiten im Rahmen der **Europäischen multidisziplinären Plattform gegen kriminelle Bedrohungen (EMPACT)** zusammen und organisieren operative Maßnahmen und gemeinsame Aktionstage gegen neue oder sich wandelnde kriminelle Bedrohungen im Zusammenhang mit der Aggression Russlands gegen die Ukraine.

Der **Dialog über Cybersicherheit** zwischen der EU und der Ukraine wurde mit koordinierter politischer, finanzieller und materieller Unterstützung durch die EU intensiviert, um die Ukraine bei der Stärkung ihrer Cyberabwehrfähigkeit zu unterstützen. Mit Gesamtmitteln in Höhe von 29 Millionen Euro zum Ausbau der Cyberabwehrfähigkeit und der digitalen Resilienz der Ukraine wurden Cybersicherheitsausrüstung, Software und ein widerstandsfähiger digitaler Wandel gefördert.

Aufgrund ihrer geografischen Lage kommt der **Republik Moldau** eine Schlüsselrolle bei der Bewältigung der strafrechtlichen und sicherheitspolitischen Auswirkungen der russischen Invasion der Ukraine zu. Im Juli 2022 hat die Kommission in Zusammenarbeit mit dem EAD die Unterstützungsplattform der EU für innere Sicherheit und Grenzmanagement in der Republik Moldau eingerichtet. Ihre Hauptaufgabe besteht darin, die Zusammenarbeit und die operativen Maßnahmen zur Bewältigung gemeinsamer Sicherheitsbedrohungen in sechs von der EU und der Republik Moldau gemeinsam festgelegten Schwerpunktbereichen zu erleichtern: Schusswaffenhandel, Schleuserkriminalität, Menschenhandel, Verhütung und Bekämpfung von Terrorismus und gewaltbereitem Extremismus, Cyberkriminalität und Drogenhandel. Im März 2022 unterzeichnete die Republik Moldau eine Statusvereinbarung mit Frontex auf der Grundlage deren erweiterten Mandats.

Die Zusammenarbeit bei der Strafverfolgung zwischen der EU und den **Ländern des westlichen Balkans**, die sich auch auf EU-Agenturen stützt, wurde in den letzten drei Jahren weiter intensiviert. Im Einklang mit den Schlussfolgerungen des Rates vom März 2021 wurde die Zusammenarbeit mit Drittländern im Bereich der Strafverfolgung in alle operativen Aktionspläne der Europäischen multidisziplinären Plattform gegen kriminelle Bedrohungen (EMPACT) aufgenommen, was zu einer verstärkten Beteiligung der westlichen Balkanstaaten

[109] 2022 fanden Dialoge über Terrorismusbekämpfung mit den Vereinten Nationen, Israel und Indien statt; Dialoge mit der Türkei, Katar und den Vereinten Arabischen Emiraten stehen in Kürze an. 2023 werden voraussichtlich wichtige Dialoge mit folgenden Ländern aufgenommen: Marokko, Tunesien, Ägypten, Kenia, den USA und dem Königreich Saudi-Arabien sowie möglicherweise auch mit Algerien.

an EMPACT-Aktivitäten geführt hat. Im Rahmen des Heranführungsinstruments werden weiterhin erhebliche Mittel für die Reform und Verbesserung der Strafverfolgung bereitgestellt, wobei die EU-Agenturen auch den Aufbau von Kapazitäten der Sicherheitsakteure unterstützen. Bei der Umsetzung des 2018 unterzeichneten Gemeinsamen Aktionsplans zur Terrorismusbekämpfung für den westlichen Balkan wurden gute Fortschritte erzielt. Im Falle Nordmazedoniens und Albaniens wurde nach dem Abschluss der meisten Maßnahmen im Dezember 2022 eine überarbeitete aktualisierte Fassung der jeweiligen bilateralen Abkommen unterzeichnet, um die Zusammenarbeit im Bereich der Terrorismusbekämpfung sowie der Prävention und Bekämpfung von gewaltbereitem Extremismus mit der EU weiter auszubauen.

Am 18. November 2022 genehmigte der Rat die Aufnahme von Verhandlungen über **Frontex-Statusvereinbarungen** zwischen der EU und Albanien, Serbien, Montenegro sowie Bosnien und Herzegowina.[110] Diese Abkommen sollen es Frontex ermöglichen, unter der Leitung der zuständigen nationalen Behörden Grenzschutzteams für die Wahrnehmung von Grenzkontrollaufgaben zu entsenden. Dies wäre bei der Bekämpfung der Migrantenschleusung von besonderem Nutzen. Nordmazedonien hat im Oktober 2022 eine Statusvereinbarung mit Frontex auf der Grundlage des erweiterten Mandats unterzeichnet.

Auch die **EU und die USA** eint eine lange Geschichte der Partnerschaft und Zusammenarbeit in Sicherheitsfragen, die auf einen systematischeren und zeitgerechteren Informationsaustausch in Fragen wie Terrorismus, Radikalisierung und organisierte Kriminalität ausgerichtet ist. Beide Seiten halten regelmäßig gemeinsame Treffen zu den Bereichen Justiz und Inneres ab, um die Zusammenarbeit in Fragen von gemeinsamem Interesse zu vertiefen, die globale Sicherheit zu fördern und einander über Fortschritte der Gesetzgebung bei Dossiers aus den vorgenannten Bereichen zu informieren. Die europäischen Justiz- und Strafverfolgungsbehörden arbeiten in operativen und legislativen Fragen eng mit ihren US-amerikanischen Amtskollegen zusammen. Die Strafverfolgungsbehörden der Vereinigten Staaten wiederum beteiligen sich aktiv an mehreren EMPACT-Maßnahmen und -Netzen. Zudem wurde ein Abkommen über die operative Zusammenarbeit zwischen den USA und Europol geschlossen. Ein gutes Beispiel für eine wirksame Zusammenarbeit ist die „Operational Task Force Greenlight/Trojan Shield“, eine der bislang größten und komplexesten Strafverfolgungsmaßnahmen im Kampf gegen verschlüsselte kriminelle Aktivitäten. Das Programm zum Aufspüren der Finanzierung des Terrorismus zwischen der EU und den USA liefert zahlreiche konkrete Anhaltspunkte für Ermittlungen im Bereich der Terrorismusbekämpfung.[111] Die Zusammenarbeit beruht zudem auf einer klaren Überwachung der Garantie- und Kontrollmechanismen.

Regelmäßige Dialoge über die Cybersicherheit zwischen der EU und den USA stärken die Zusammenarbeit und Koordinierung sowohl bei der digitalen Diplomatie als auch bei der Cyberabwehrfähigkeit, einschließlich der Normung im Bereich der Cybersicherheit. Darüber hinaus hat der EU-US-Handels- und Technologierat (TTC) durch seine gemeinsame Erklärung zur Cybersicherheit, zu Schritten für eine mögliche Zusammenarbeit in Forschung und Entwicklung über 5G und 6G hinaus, zu Ausfuhrkontrollen, zur Überprüfung von Investitionen sowie zu Sanktionen gegen Russland und Belarus eine Vertiefung der

[110] Beschluss (EU) 2022/2271 des Rates – Albanien; Beschluss (EU) 2022/2272 des Rates – Bosnien und Herzegowina; Beschluss (EU) 2022/2273 des Rates – Montenegro; Beschluss (EU) 2022/2274 des Rates – Serbien.

[111] Siehe die sechste gemeinsame Überprüfung der Durchführung des TFTP-Abkommens, COM(2022) 585.

Zusammenarbeit ermöglicht. Der TTC wird auch die Zusammenarbeit zwischen der EU und den USA im Bereich der Informationsmanipulation und Einflussnahme aus dem Ausland weiter voranbringen.

Wichtige Herausforderungen für die Sicherheit in Afrika wirken sich nicht nur unmittelbar auf die Bevölkerung des Kontinents selbst aus, sondern auch auf die Sicherheit der EU. Es laufen zahlreiche Projekte, mit denen die Partnerländer beim Aufbau von Kapazitäten zur Bewältigung dieser Herausforderungen unterstützt werden sollen. Beispiele hierfür sind die Finanzierung der Internationalen Akademie für die Terrorismusbekämpfung (Académie internationale de lutte contre le terrorisme – AILCT) in Westafrika sowie die regionale Initiative zur Stärkung der Kapazitäten zur Bekämpfung der Geldwäsche und der Terrorismusfinanzierung in der Region am Horn von Afrika.

Die Länder **Lateinamerikas und der Karibik** sind wichtige Partner für die EU. Im Mai 2022 wurde eine neue regionale Team-Europa-Initiative für Sicherheit und Justiz ins Leben gerufen, die darauf abzielt, eine Partnerschaft zwischen der EU und den Ländern Lateinamerikas und der Karibik zur Stärkung der Rechtsstaatlichkeit und zur Bekämpfung der organisierten Kriminalität aufzubauen.

Mit der im Oktober 2020 in Kraft getretenen EU-Verordnung über die **Überprüfung ausländischer Direktinvestitionen**[112] wurde ein Rahmen für einen besseren Schutz vor ausländischen Direktinvestitionen geschaffen, die in mehr als einem Mitgliedstaat ein Risiko für die Sicherheit oder die öffentliche Ordnung darstellen. Im ersten vollständigen Jahr nach ihrem Inkrafttreten wurden der Kommission mehr als 400 Fälle gemeldet. Mit der im September 2021 angenommenen Verordnung über Güter mit doppeltem Verwendungszweck[113] wurde das EU-**Ausfuhrkontrollsystem für Güter mit doppeltem Verwendungszweck** aktualisiert und gestärkt. Zudem wurden neue Bestimmungen eingeführt, die es der EU in Abstimmung mit den Mitgliedstaaten ermöglichen, autonome Kontrollen der Ausfuhr nicht gelisteter Güter und Technologien einzuführen.

In einer globalisierten Welt, in der schwere Kriminalität und Terrorismus zunehmend länderübergreifend aufgestellt sind, müssen die Strafverfolgungs- und Justizbehörden optimal ausgestattet sein, wenn sie im Interesse der Sicherheit ihrer Bürgerinnen und Bürger mit externen Partnern zusammenarbeiten sollen. Dazu müssen für **Europol und Eurojust** Möglichkeiten der Zusammenarbeit und des Informationsaustauschs zwischen den Justizbehörden von Drittstaaten geschaffen werden. Nach der Unterzeichnung des Abkommens über den Austausch personenbezogener Daten zur Bekämpfung von schwerer Kriminalität und Terrorismus[114] zwischen Europol und Neuseeland im Juni 2022 wurden Verhandlungen mit einer Reihe weiterer Länder aufgenommen, die jedoch in den meisten Fällen bisher nur langsam vorankommen. Was Eurojust betrifft, so sind die Verhandlungen mit Armenien, bei denen eine Einigung über den Text erzielt wurde, weit fortgeschritten, und mit Kolumbien, Algerien und Libanon wurden Verhandlungen aufgenommen.

Im April 2022 haben die **EU und die Vereinten Nationen** im Rahmen des vierten Dialogs der Staats- und Regierungschefs über Terrorismusbekämpfung konkrete Schritte unternommen, um ihre bestehende Partnerschaft zu stärken. Ziel ist es, den nach wie vor

112 EU/2019/452.
113 EU/2021/821 Neufassung.
114 Die Vereinbarung wurde vom Europäischen Datenschutzbeauftragten (EDSB) als Modell für künftige Abkommen über den Austausch personenbezogener Daten zu Strafverfolgungszwecken bezeichnet.

bestehenden und sich verändernden Gefahren für den Weltfrieden und die internationale Sicherheit entgegenzuwirken. Die strategische Partnerschaft wurde durch die Einrichtung der neuen „EU-UN Global Terrorism Threats Facility“ weiter gestärkt. Dabei handelt es sich um eine von der EU finanzierte Initiative zur Unterstützung von Staaten, die mit Terrorismus und gewaltbereitem Extremismus konfrontiert sind, u. a. durch Hilfe, Ausbildung und Mentoring. Weitere Themen von gemeinsamem Interesse sind neu aufkommende Bedrohungen im Zusammenhang mit neuen Technologien. Dabei stellt sich auch die Frage, wie sich diese auf junge Menschen auswirken, die als besondere Zielgruppe für Aufstachelung zu Gewalt und Terrorismus aufgrund von Fremdenfeindlichkeit, Rassismus und anderen Formen der Intoleranz oder im Namen einer Religion oder Weltanschauung in den Fokus genommen werden.

Auch die Zusammenarbeit zwischen der **EU** und der **NATO** wurde ausgeweitet, wobei in allen Kooperationsbereichen greifbare Ergebnisse erzielt wurden.[115] Beide Seiten haben ihre Arbeit und Zusammenarbeit angesichts des russischen Angriffskriegs gegen die Ukraine intensiviert. Sie vertreten eine einheitliche politische Position und stimmen sich ab, um der Ukraine bei der Verteidigung des Landes und dem Schutz ihrer Bevölkerung zu helfen. Die strategische Partnerschaft zwischen der EU und der NATO ist zu diesem für die euro-atlantische Sicherheit entscheidenden Zeitpunkt robuster und relevanter denn je. Zum Thema Resilienz wurde im Januar 2022 ein spezieller strukturierter Dialog eingeleitet, der nun vertieft wird, um den Schutz kritischer Infrastrukturen zu unterstützen. In diesem Zusammenhang wird zudem eine EU-NATO-Taskforce eingesetzt. Im Bereich der militärischen Mobilität wurden weitere Verbesserungen in Bezug auf Transport- und Regulierungsaspekte, einschließlich der Beförderung gefährlicher Güter, vorgenommen. Die Abwehr hybrider Bedrohungen ist nach wie vor ein Schlüsselbereich der Zusammenarbeit mit der NATO. Der Austausch umfasst die Bereiche Terrorismusbekämpfung, strategische Kommunikation, Informationsmanipulation und Einflussnahme aus dem Ausland sowie Cyberfragen. Im November 2022 wurde im Rahmen des Konzepts der parallelen und koordinierten Übung (PACE) unter Beteiligung von NATO-Mitarbeitern die Übung „EU Integrated Resolve“ durchgeführt, um das Zusammenspiel zwischen den jeweiligen Krisenreaktionsmechanismen zu verbessern.

Seit September 2022 führt die EU den Ko-Vorsitz des **Globalen Forums „Terrorismusbekämpfung“**. Zu dessen Prioritäten gehören die Bekämpfung der terroristischen Bedrohung in Afrika sowie die Einbeziehung von Gleichstellungs- und Bildungsfragen in die Strategien zur Terrorismusbekämpfung.

Derzeit laufen Verhandlungen über ein Kooperationsabkommen zwischen der EU und **Interpol**, die im ersten Halbjahr 2023 auf technischer Ebene abgeschlossen werden sollen. Hauptziel ist es, den Informationsaustausch zwischen Interpol und den Agenturen und Einrichtungen der EU weiter zu verstärken, die Mitgliedstaaten besser zu unterstützen und die Sicherheit der Bürgerinnen und Bürger nicht nur in der EU, sondern weltweit zu erhöhen.

115 Siehe den Siebten Fortschrittsbericht über die Umsetzung des vom Rat der EU und vom NATO-Rat am 6. Dezember 2016 und 5. Dezember 2017, 20. Juni 2022 gebilligten gemeinsamen Pakets von Vorschlägen.

Wichtige konkrete Beispiele

Operation „Desert Light“ – Zerschlagung eines europäischen Drogenkartells in sechs Ländern: Im November 2022 fanden in der EU und in den Vereinigten Arabischen Emiraten (VAE) Razzien statt, die auf die Kommando- und Kontrollzentren sowie die logistische Infrastruktur für den illegalen Drogenhandel in Europa abzielten. Hochrangige Zielpersonen hatten ein „Superkartell“ gebildet, das rund ein Drittel des Kokainhandels in Europa kontrollierte. Insgesamt wurden mit Unterstützung von Europol nach Ermittlungen in Spanien, Frankreich, Belgien, den Niederlanden und den VAE 49 Verdächtige festgenommen. Im Zuge der Ermittlungen wurden 30 Tonnen Drogen von den Strafverfolgungsbehörden beschlagnahmt.

6. FAZIT

In den letzten zweieinhalb Jahren hat die Kommission in enger Zusammenarbeit mit dem Europäischen Auswärtigen Dienst fast alle in der Strategie für eine Sicherheitsunion vorgesehenen Maßnahmen erfolgreich vorangebracht. Das breite Spektrum an Vorschlägen muss nun angenommen und vor allem umgesetzt werden. Jetzt kommt es auf die Beschlüsse und Maßnahmen des Europäischen Parlaments, des Rates und der einzelnen Mitgliedstaaten an, die sicherstellen müssen, dass die EU ihren Bürgerinnen und Bürgern ein robustes Sicherheitsökosystem bietet.

Das Sicherheitsumfeld, in dem wir leben, befindet sich jedoch in einem ständigen Wandel. Nach der Annahme der Strategie für eine Sicherheitsunion sind mit der COVID-19-Pandemie und den Folgen der russischen Aggression gegen die Ukraine neue Herausforderungen auf die EU zugekommen. Die Online-Bedrohungen haben exponentiell zugenommen, und es bedarf einer raschen Anpassung und Vorausschau. Die EU muss sich weiterhin dafür rüsten, allen sich laufend verändernden Bedrohungen zu begegnen, die die Sicherheit ihrer Bürgerinnen und Bürger gefährden. Für den gemeinsamen Erfolg der EU wird es künftig entscheidend auf ständige Wachsamkeit, Entschlossenheit zum Handeln und gemeinsame Antworten ankommen.