Rat der
Europäischen Union

Brüssel, den 18. Oktober 2023
(OR. en)

14372/23

JAI 1332	**COPEN 363**
COSI 179	**FREMP 292**
ENFOPOL 431	**JAIEX 66**
ENFOCUSTOM 110	**CFSP/PESC 1410**
IXIM 194	**COPS 489**
CT 155	**HYBRID 73**
CRIMORG 137	**DISINFO 85**
FRONT 327	**TELECOM 306**
ASIM 92	**DIGIT 223**
VISA 208	**COMPET 1008**
CYBER 247	**RECH 456**
DATAPROTECT 278	**CULT 122**
CATS 58	**COTER 185**
DROIPEN 151	**CORDROGUE 94**

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	18. Oktober 2023
Empfänger:	Frau Thérèse BLANCHET, Generalsekretärin des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2023) 665 final
Betr.:	MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT Sechster Fortschrittsbericht über die Umsetzung der EU-Strategie für eine Sicherheitsunion

Die Delegationen erhalten in der Anlage das Dokument COM(2023) 665 final.

Anl.: COM(2023) 665 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 18.10.2023
COM(2023) 665 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

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

I. Einleitung

Vor drei Jahren hat die Kommission die Strategie für eine Sicherheitsunion für den Zeitraum 2020 bis 2025[1] angenommen, in der die wichtigsten Prioritäten der Union für den Bereich Sicherheit festgelegt sind. Seitdem wurden im Hinblick auf alle vier Pfeiler der Strategie erhebliche Fortschritte erzielt, indem in allen Bereichen – vom Schutz kritischer Einrichtungen bis hin zur Stärkung der Cyberresilienz – wegweisende Rechtsvorschriften erlassen wurden. Allerdings entwickelt sich die Bedrohungslage in Europa und seiner Nachbarschaft inzwischen weiter. Die Terroranschläge in einer unserer Schulen in Frankreich und auf den Straßen Brüssels in den letzten Tagen führen uns eindringlich vor Augen, wie dringend es ist, unsere Sicherheitsarchitektur weiter anzupassen und zu stärken. Die Gefahr durch Cyberangriffe steigt weiter und wird unter anderem dadurch verschärft, dass in den gegenwärtigen Konflikten böswillige Akteure Partei ergreifen. Hybride Bedrohungen, darunter auch Desinformation, nehmen weiterhin zu. Europol hat festgestellt, dass durch den russischen Angriffskrieg gegen die Ukraine eine erhebliche Zunahme der Cyberangriffe auf Ziele in der EU ausgelöst wurde und von prorussischen Hackergruppen groß angelegte, politisch motivierte Angriffe koordiniert werden.[2] Dies wurde deutlich, als Internetzugänge blockiert und wesentliche Dienstleistungen, wie beispielsweise die Stromversorgung, unterbrochen wurden.[3]

Mit der Strategie für eine Sicherheitsunion soll die EU in die Lage versetzt werden, der sich wandelnden Bedrohungslage besser standzuhalten. Die Ereignisse, mit denen die Union aufgrund der durch die Pandemie und den Krieg ausgelösten Krisen konfrontiert wurde, lassen die Bedeutung des mit der Strategie verfolgten Ansatzes deutlich zutage treten, und zwar mit Entschlossenheit die verschiedenen Elemente des EU-Sicherheitsökosystems zusammenzuführen und – auch bei der Bekämpfung von organisierter Kriminalität, Terrorismus und Radikalisierung – nicht länger zwischen Cybersicherheit und physischer Sicherheit zu unterscheiden.

Die Union muss jedoch wachsam sein und kontinuierlich prüfen, welche weiteren Anstrengungen unternommen werden müssen, um die Bürgerinnen und Bürger zu schützen. In der Strategie sind vorrangige Bereiche festgelegt, in denen die Union einen Mehrwert erbringen kann, indem sie die Mitgliedstaaten bei der Verbesserung der Sicherheit für alle Menschen in Europa unterstützt. Seit der Annahme der Strategie wurden alle darin festgelegten Maßnahmen in Angriff genommen und neue Maßnahmen aufgenommen, um den aktuellen Sicherheitsproblemen zu begegnen.

Insgesamt legte die Kommission im Rahmen der Strategie für eine Sicherheitsunion 36 Gesetzgebungsinitiativen vor. Die interinstitutionellen Verhandlungen über mehr als die Hälfte dieser Vorschläge sind bereits abgeschlossen, und es wurden solide neue Rechtsvorschriften verabschiedet (vgl. die Tabelle im Anhang). Über mehrere wichtige Initiativen, die von der Kommission vorgeschlagen wurden, verhandeln das Europäische Parlament und der Rat jedoch gegenwärtig noch. Da die laufende Wahlperiode mit der

---

1 COM(2020) 605 final.

2 Distributed-Denial-of-Service-Angriffe (DDoS-Angriffe): vgl. Europol, Cyber-attacks: the apex of crime-as-a-service, Europol Spotlight Report Series, Amt für Veröffentlichungen der Europäischen Union, Luxemburg, 13. September 2023.

3 Im Zuge des Konflikts in der Ukraine wird häufig Wiper-Schadsoftware eingesetzt, um Daten und Systeme zu zerstören; so wurde beispielsweise der Internetzugang von Tausenden Kunden in der EU blockiert, und ein großes deutsches Energieunternehmen verlor den Zugriff auf die Fernsteuerung von mehr als 5 800 Windrädern. Europäisches Parlament, The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict, September 2023, PE 702.594.

Europawahl im Juni 2024 endet, muss nun zügig gehandelt werden, um diese anhängigen Dossiers abzuschließen, damit die Sicherheitsunion den Bürgerinnen und Bürgern uneingeschränkt zugutekommt. Daher liegt der Schwerpunkt dieses sechsten Fortschrittsberichts über die Strategie für eine Sicherheitsunion auf der Darstellung der maßgeblichen Dossiers mit und ohne Gesetzgebungscharakter, die von der Kommission angenommen wurden und für deren Abschluss und wirksame Umsetzung mehr Anstrengungen unternommen werden müssen.

Was die EU-Vorschriften betrifft, über die bereits eine Einigung erzielt wurde, so werden deren Vorteile nur dann spürbar, wenn sie in die Praxis umgesetzt werden. Der Schwerpunkt muss auf ihrer ordnungsgemäßen und vollständigen Umsetzung, Durchführung und Anwendung durch die Mitgliedstaaten liegen. Im Jahr 2023 sorgte die Kommission weiterhin für die Umsetzung der EU-Strategie für eine Sicherheitsunion, indem sie ihre institutionellen Befugnisse nutzte, um Vertragsverletzungsverfahren einzuleiten, wenn Mitgliedstaaten EU-Rechtsvorschriften nicht oder nicht ordnungsgemäß umgesetzt hatten.

In diesem Bericht wird auch zusammenfassend dargestellt, in welchen Bereichen die Mitgliedstaaten und/oder Agenturen der EU tätig werden müssen. Die Agenturen der EU spielen eine entscheidende Rolle, wenn es darum geht, die Durchführung der Initiativen im Rahmen der Sicherheitsunion zu unterstützen, und ihre Zuständigkeiten wurden in den letzten Jahren erweitert. In diesem Bericht werden einige der wichtigsten neuen Aufgaben dargelegt, die den Agenturen übertragen wurden, damit sie die Mitgliedstaaten bei der Durchführung wichtiger Initiativen im Rahmen der Sicherheitsunion besser unterstützen können.

Darüber hinaus wurde angesichts der geopolitischen Lage die Bedeutung der äußeren Sicherheit für die innere Sicherheit der Union deutlich. Ein stärkerer Rahmen für die innere Sicherheit der EU ist untrennbar mit einer Vertiefung der Partnerschaften und der Zusammenarbeit mit Drittländern verbunden. Die EU muss auch weiterhin aktiv ausloten, wie ihr weltweites Engagement zur Gewährleistung der Sicherheit ihrer Bürgerinnen und Bürger beitragen kann.

II. Ein zukunftsfähiges Sicherheitsumfeld

Cybersicherheit und Resilienz kritischer Infrastrukturen

Im Rahmen der Sicherheitsunion setzt sich die Union dafür ein, dass alle europäischen Bürgerinnen und Bürger sowie alle europäischen Unternehmen sowohl online als auch offline gut geschützt sind und zugleich die Schaffung eines offenen, sicheren und stabilen Cyberraums vorangetrieben wird. Die zunehmende Tragweite, Häufigkeit und Wirkung von Cybersicherheitsvorfällen stellt eine erhebliche Bedrohung für den störungsfreien Betrieb von Netz- und Informationssystemen und den Binnenmarkt dar. Durch den russischen Angriffskrieg gegen die Ukraine wurde diese Bedrohung weiter verstärkt, während zahlreiche staatsnahe, kriminelle Hacktivisten zur Verschärfung der derzeitigen geopolitischen Spannungen beitragen. Die Sabotage der Nord-Stream-Pipelines im letzten Herbst hat gezeigt, wie sehr wichtige Sektoren, wie beispielsweise Energie, digitale Infrastruktur, Verkehr und Weltraum, auf resiliente kritische Infrastrukturen angewiesen sind. Angesichts des jüngsten Vorfalls, bei dem in der Ostsee eine Gasleitung und ein Datenkabel zwischen Estland und Finnland beschädigt wurden, wurde deutlich, dass in diesen Situationen eine hohe Abwehrbereitschaft erforderlich ist. Obwohl die Ursache des Schadens noch nicht geklärt ist und die Ermittlungen noch laufen, gibt der Informationsaustausch, der auf unterschiedlichen Ebenen zwischen den Mitgliedstaaten und der Kommission stattfand, Anlass zur Hoffnung. Die Störungen hatten

weder auf europäischer noch auf lokaler Ebene unmittelbare Auswirkungen auf die Internetanbindung oder die Sicherheit der Gasversorgung. Dies ist ein Hinweis darauf, dass in den letzten Monaten Fortschritte erzielt und die Anstrengungen zur Verbesserung der Abwehrbereitschaft verstärkt wurden.

Ein klarer und solider Rechtsrahmen ist daher für die Sicherstellung des Schutzes und der Resilienz dieser kritischen Infrastrukturen unverzichtbar. In diesem Zusammenhang wurde mit der zeitgleichen Annahme der überarbeiteten Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (im Folgenden „NIS-2-Richtlinie“)[4] und der Richtlinie über die Resilienz kritischer Einrichtungen (im Folgenden „CER-Richtlinie“)[5], die beide am 16. Januar 2023 in Kraft traten, ein entscheidender Durchbruch erzielt. Nun sind die Mitgliedstaaten dringend gehalten, diese grundlegenden Rechtsvorschriften zügig und vollständig bis spätestens zum 17. Oktober 2024 umzusetzen, um einen soliden Unionsrahmen für den Schutz kritischer Infrastrukturen der Union vor physischen Bedrohungen und Cyberbedrohungen zu schaffen.

Im Juli 2023 legte die Kommission in einer delegierten Verordnung der Kommission wesentliche Dienste in den elf unter die CER-Richtlinie fallenden Sektoren fest.[6] Im nächsten Schritt müssen die Mitgliedstaaten Risikobewertungen zu diesen Diensten vornehmen. Im Anschluss an die Empfehlung des Rates[7] vom 8. Dezember 2022 wurden – beginnend mit dem Energiesektor – die Arbeiten an den Stresstests für kritische Infrastrukturen verstärkt; darüber hinaus wurden die Bemühungen um die Vertiefung der Zusammenarbeit mit der NATO und wichtigen Partnerländern intensiviert. Im Ergebnis legte die EU-NATO-Taskforce zur Resilienz kritischer Infrastruktur im Juni 2023 einen Bericht vor, in dem die gegenwärtigen Sicherheitsprobleme im Zusammenhang mit kritischen Infrastrukturen in vier Schlüsselsektoren (Energie, Verkehr, digitale Infrastruktur und Weltraum) dargestellt und Empfehlungen zur Stärkung der Resilienz ausgesprochen werden. Die Empfehlungen, die unter anderem eine Verstärkung der Koordinierung, des Informationsaustauschs und der Übungen zum Gegenstand haben, werden von den Bediensteten der EU und der NATO im Rahmen des strukturierten Dialogs über Resilienz umgesetzt.

Zugleich nahm die Kommission am 6. September 2023 einen Vorschlag[8] für eine Empfehlung des Rates für einen Konzeptentwurf zur Koordinierung der Reaktion – auf EU-Ebene – auf Störungen kritischer Infrastrukturen von erheblicher grenzüberschreitender Bedeutung an. Am 4. Oktober 2023 wurde eine Übung in Form einer szenariobasierten Diskussion über den Konzeptentwurf organisiert, um zu prüfen, wie dieser in der Praxis angewandt würde, und Informationen für die laufenden Verhandlungen über den Vorschlag im Rat zusammenzutragen.

Auf Aufforderung des Rates[9] führen die Kommission, der Hohe Vertreter und die NIS-Kooperationsgruppe Risikobewertungen durch und erstellen Risikoszenarien aus der Perspektive der Cybersicherheit. Der Schwerpunkt dieser Arbeit liegt auf den Sektoren Telekommunikation und Elektrizität. Durch die Einbeziehung aller einschlägigen zivilen und

---

4 Richtlinie (EU) 2022/2555 vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und Richtlinie (EU) 2018/1972 (NIS-2-Richtlinie).

5 Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates.

6 C(2023) 4878.

7 Empfehlung des Rates vom 8. Dezember 2022 für eine unionsweite koordinierte Vorgehensweise zur Stärkung der Resilienz kritischer Infrastruktur.

8 COM(2023) 526 final.

9 Schlussfolgerungen des Rates vom 23. Mai 2022 zur Entwicklung der Cyberabwehr der Europäischen Union und Aufruf von Nevers vom 9. März 2022 zur Stärkung der Cybersicherheitskapazitäten der EU.

militärischen Agenturen und Netzwerke wird erstmals eine umfassende und ganzheitliche unionsweite Bewertung vorgenommen. Diese wird die koordinierten Risikobewertungen kritischer Lieferketten gemäß der NIS-2-Richtlinie sowie die Risikobewertungen und Stresstests für kritische Infrastrukturen in den Sektoren Energie, digitale Infrastruktur, Kommunikation, Verkehr und Weltraum ergänzen. Im Sinne der Koordinierung und Kohärenz sollten diese Tätigkeiten aufeinander aufbauen, um die Einführung eines standardisierten Ansatzes zu erleichtern, und als Richtschnur für die Entwicklung künftiger Übungen dienen. Der Erfolg dieser Tätigkeiten wird nun von der aktiven Mitwirkung der Mitgliedstaaten abhängen.

Das Funktionieren der Volkswirtschaften und Gesellschaften ist in steigendem Maße von weltraumgestützten Diensten und Daten abhängig; dies gilt insbesondere in den Bereichen Sicherheit und Verteidigung. Der Weltraum ist ein zunehmend umkämpfter strategischer Bereich, und seine Bedeutung für die Sicherheit ist insbesondere infolge der russischen Invasion in die Ukraine gestiegen. Die Weltraumstrategie der Europäischen Union für Sicherheit und Verteidigung wurde im März 2023 angenommen und hat die Stärkung der strategischen Stellung und Autonomie der Union im Weltraum zum Ziel. Als eine wichtige Maßnahme im Rahmen dieser Strategie wird die Kommission im Jahr 2024 ein EU-Weltraumgesetz vorschlagen, in dem die Sicherheit, Nachhaltigkeit und Resilienz/Sicherheitsaspekte von Weltraumtätigkeiten in der EU geregelt werden.

Was die externe Dimension betrifft, so bildet eine sichere Infrastruktur die Grundlage für die Resilienz der Weltwirtschaft und der globalen Lieferketten;[10] aus diesem Grund hat die Global-Gateway-Strategie der EU eine starke Sicherheitsdimension. Angesichts der Verbindungen zwischen den Infrastrukturen der EU und ihrer Partnerländer ist eine weitere internationale Zusammenarbeit von maßgeblicher Bedeutung für die Stärkung der globalen Cyberresilienz und die Förderung eines freien, offenen, sicheren und geschützten Cyberraums.

Cyberresilienzgesetz

Für die Cybersicherheit in Europa ist es von zentraler Bedeutung, dass sich die Verbraucherinnen und Verbraucher sowie die Unternehmen auf sichere digitale Produkte verlassen können. Um diesem Erfordernis Rechnung zu tragen, nahm die Kommission am 15. September 2022 einen Vorschlag für ein Cyberresilienzgesetz[11] an. Mit dieser Rechtsvorschrift würden verbindliche horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen eingeführt, die diese während eines Zeitraums von fünf Jahren bzw. während der gesamten Produktlebensdauer, je nachdem, welcher Zeitraum kürzer ist, genügen müssten. Zudem würden die Bedingungen für die Konzeption und Entwicklung sicherer Produkte mit digitalen Elementen festgelegt, wobei sichergestellt würde, dass Hardware- und Softwareprodukte mit möglichst wenigen Schwachstellen in Verkehr gebracht werden. Diese Rechtsvorschrift wäre mit Blick auf die Anhebung der europäischen Cybersicherheitsstandards in allen Bereichen ein zentraler Meilenstein und dürfte international Maßstäbe setzen; dies würde der Cybersicherheitsbranche der Union auf den globalen Märkten einen klaren Vorteil verschaffen. Das Europäische Parlament und der Rat haben im Juli 2023 ihre jeweiligen Standpunkte festgelegt, und die Verhandlungen sollten zügig vorangebracht werden.

Die Cybersicherheitszertifizierung ist ebenfalls von maßgeblicher Bedeutung für die Stärkung des Vertrauens in IKT-Produkte und -Dienstleistungen; sie ermöglicht es Verbrauchern, Unternehmen und Behörden, fundierte Entscheidungen zu treffen, bei denen ein angemessenes Cybersicherheitsniveau gewährleistet ist. Die Arbeit an der Cybersicherheitszertifizierung

[10] JOIN(2021) 30 final.
[11] COM(2022) 454 final.

schreitet voran, und das auf gemeinsamen Kriterien beruhende System der EU für die Cybersicherheitszertifizierung wird gegenwärtig im Ausschussverfahren bewertet. Das mögliche EU-System für die Cybersicherheitszertifizierung für Cloud-Dienste (EU Cloud Security Certification Scheme, EUCS) wird gegenwärtig von der Agentur der Europäischen Union für Cybersicherheit (ENISA) vorbereitet und in der Europäischen Gruppe für die Cybersicherheitszertifizierung erörtert. Im Rahmen der intensiven Zusammenarbeit mit Sachverständigen aus unterschiedlichen Sektoren sowie mit Verbrauchern und Anbietern sollte ein tragfähiges rechtliches und technisches Konzept entstehen, mit dem die erforderlichen Sicherheitsgarantien gemäß dem Unionsrecht sowie den internationalen und WTO-Verpflichtungen bereitgestellt werden. Darüber hinaus bereitet die ENISA das mögliche System EU5G und die EUid-Brieftasche (European Digital Identity Wallet, EUIDW) vor. Gemeinsame Anstrengungen aller Mitgliedstaaten sind von entscheidender Bedeutung, um die Sicherheit von IKT-Produkten, -Systemen und -Prozessen insgesamt zu verbessern.

Verordnungen über die Informationssicherheit und Cybersicherheit in den Organen, Einrichtungen und sonstigen Stellen der EU

Die im März 2022 zeitgleich vorgeschlagenen Verordnungen zur Regelung der Cybersicherheit und der Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der Union sind in unterschiedlichem Tempo vorangekommen. Im vergangenen Juni wurde eine politische Einigung über die Verordnung über die Cybersicherheit erzielt, mit der eine Stärkung des Cybersicherheitsstands aller Organe, Einrichtungen und sonstigen Stellen der EU ermöglicht wird und die zeigt, dass die EU der raschen Umsetzung dieses Vorschlags große Bedeutung beimisst. Vor diesem Hintergrund ist es besonders bedenklich, dass im Hinblick auf den zeitgleich vorgelegten Vorschlag für eine Verordnung über die Informationssicherheit, die für die Vollendung eines soliden Rechtsrahmens für die Organe, Einrichtungen und sonstigen Stellen der EU unverzichtbar ist, unerwartet langsam Fortschritte erzielt werden. Die beiden vorgeschlagenen Verordnungen sollten vor den Wahlen zum Europäischen Parlament angenommen werden, um der europäischen Verwaltung im gegenwärtigen geopolitischen Kontext Glaubwürdigkeit zu verleihen und ihre Resilienz zu stärken. Durch die Festlegung einer Reihe von Mindestvorschriften und -standards für die Informationssicherheit in allen Organen, Einrichtungen und sonstigen Stellen der EU würde für alle Beteiligten Gewissheit geschaffen und ein kohärenter Schutz vor den sich wandelnden Bedrohungen sowohl für ihre nicht als Verschlusssache eingestuften als auch für ihre als EU-Verschlusssachen eingestuften Informationen gewährleistet. In ihrer Gesamtheit böten diese neuen Vorschriften eine belastbare Grundlage für den sicheren Informationsaustausch zwischen den Organen, Einrichtungen und sonstigen Stellen der EU sowie zwischen ihnen und den Mitgliedstaaten mit standardisierten Verfahren und Maßnahmen für den Schutz des Informationsflusses. Somit würde mit ihnen den wiederholten Aufforderungen des Rates entsprochen, die Resilienz der Organe, Einrichtungen und sonstigen Stellen der EU zu stärken und den Entscheidungsprozess der Union vor böswilliger Einflussnahme zu schützen.

Cybersolidaritätsgesetz

Aufbauend auf dem starken strategischen, politischen und rechtlichen Rahmen, der bereits geschaffen wurde, würden die Erkennung von Cyberbedrohungen, die Resilienz und die Abwehrbereitschaft auf allen Ebenen des Cybersicherheitsökosystems der Union durch den am 18. April 2023 von der Kommission angenommenen Vorschlag für ein

Cybersolidaritätsgesetz[12] weiter verbessert. Diese Ziele würden im Wesentlichen durch drei Maßnahmen umgesetzt:

(1) Aufbau eines ***europäischen Cyberschutzschildes***, um gemeinsame Fähigkeiten zur Erkennung und Lageerfassung aufzubauen und zu verbessern. Dieser Schutzschild würde aus nationalen Sicherheitseinsatzzentren („nationalen SOCs“) und grenzübergreifenden Sicherheitseinsatzzentren („grenzgreifenden SOCs“) bestehen.
(2) Schaffung eines ***Cybernotfallmechanismus*** zur Unterstützung der Mitgliedstaaten bei der Vorsorge für, Bewältigung von und sofortigen Wiederherstellung nach schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes. Die Unterstützung bei der Bewältigung von Vorfällen würde unter anderem aus der EU-Cybersicherheitsreserve geleistet, die auch den Organen, Einrichtungen und sonstigen Stellen der Union sowie – wenn die Assoziierungsabkommen über ihre Teilnahme am Programm Digitales Europa dies vorsehen – mit dem Programm Digitales Europa assoziierten Drittländern zur Verfügung gestellt würde.
(3) Einrichtung eines ***europäischen Überprüfungsmechanismus für Cybersicherheitsvorfälle*** zur Überprüfung und Bewertung von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes. Der Bericht über die Überprüfung von Sicherheitsvorfällen würde von der ENISA koordiniert und erstellt.

Die Beratungen im Rat und im Europäischen Parlament wurden aufgenommen. Durch einen Abschluss der Verhandlungen vor dem Ende der laufenden Wahlperiode des Europäischen Parlaments würden die Bemühungen um den Schutz der Bürgerinnen und Bürger sowie der Unternehmen in der Union deutlich an Fahrt gewinnen.

Akademie für Cybersicherheitskompetenzen

Angesichts der zunehmenden Cyberbedrohungen braucht die EU dringend Fachkräfte mit den Kompetenzen und Fähigkeiten, die nötig sind, um Cyberangriffe zu verhindern und zu entdecken, davon abzuschrecken und die EU dagegen zu verteidigen. Der Bedarf an Arbeitskräften im Cybersicherheitsbereich wird gegenwärtig auf 883 000 Fachkräfte geschätzt, wobei sich die Zahl der unbesetzten Stellen im Jahr 2022 auf 260 000 bis 500 000 belief. Alle gesellschaftlichen Gruppen sollten darin bestärkt werden, diese Lücke zu schließen, allerdings machten im Jahr 2022 Frauen nur 20 % der Absolventinnen und Absolventen im Cybersicherheitsbereich und 19 % der Fachkräfte für Informations- und Kommunikationstechnologien aus. Im Rahmen des Europäischen Jahres der Kompetenzen 2023 brachte die Kommission am 18. April 2023[13] eine Initiative zur Einrichtung einer Akademie für Cybersicherheitskompetenzen auf den Weg, um die Fachkräftelücke im Cybersicherheitsbereich zu schließen; diese Initiative wurde von den Mitgliedstaaten begrüßt.[14] Mit der Akademie für Cybersicherheitskompetenzen würden die laufenden einschlägigen Initiativen zusammengeführt und besser koordiniert. Die Kommission fordert die Mitgliedstaaten, die regionalen und kommunalen Behörden sowie die europäischen öffentlichen Einrichtungen auf, gezielte Strategien oder Initiativen auf den Weg zu bringen oder Cybersicherheitskompetenzen in die einschlägigen, weiter gefassten Strategien oder Initiativen (z. B. in den Bereichen Cybersicherheit, digitale Kompetenzen oder Beschäftigung) einzubeziehen. Auch die Einbindung privater Interessenträger wird von entscheidender

[12] COM(2023) 209 final.
[13] COM(2023) 207 final.
[14] Schlussfolgerungen des Rates vom 22. Mai 2023 zur EU-Cyberabwehrpolitik.

Bedeutung sein, um die Lücke bei Cybersicherheitskompetenzen zu schließen und dem damit verbundenen Arbeitskräftemangel in Europa entgegenzuwirken.

Drohnen

Eine weitere Bedrohung für den öffentlichen Raum und kritische Infrastrukturen geht zunehmend vom böswilligen Einsatz von Drohnen aus. Die Zahl der Vorfälle mit Drohnen ist sowohl innerhalb als auch außerhalb der Union gestiegen, und Lösungen zur Drohnenabwehr stellen für die Strafverfolgungsbehörden und andere öffentliche Stellen in der Union sowie für private Betreiber kritischer Infrastrukturen ein Schlüsselinstrument dar. Zugleich wird durch den rechtmäßigen Einsatz von Drohnen ein erheblicher Beitrag zum grünen und zum digitalen Wandel geleistet.[15] Wie in ihrer im November 2022 angenommenen Drohnenstrategie 2.0 angekündigt, nimmt die Kommission heute eine Mitteilung über die Abwehr potenzieller Bedrohungen, die von Drohnen ausgehen, an; begleitend werden zwei Handbücher mit praktischen Leitlinien zu den wichtigsten technischen Aspekten bereitgestellt.[16] Mit dieser Initiative soll ein umfassender und harmonisierter politischer Rahmen geschaffen, ein gemeinsames Verständnis der geltenden Vorschriften zur Bekämpfung möglicher Bedrohungen durch Drohnen aufgebaut und dafür gesorgt werden, dass gegebenenfalls Anpassungen an die rasche technologische Entwicklung vorgenommen werden. Die Mitgliedstaaten und die einschlägigen privaten Betreiber sind gehalten, eng mit der Kommission zusammenzuarbeiten, um die vollständige Umsetzung dieser Initiative sicherzustellen.

Maritime Sicherheit und Luftsicherheit

Illegale Handlungen – wie Seeräuberei, bewaffnete Raubüberfälle auf See, die Schleusung von Migranten und Menschenhandel, der Handel mit Waffen und Betäubungsmitteln sowie Terrorismus – stellen nach wie vor eine Gefahr für die maritime Sicherheit dar und werden durch sich wandelnde Bedrohungen, darunter hybride Angriffe und Cyberangriffe, weiter verschärft. Am 10. März 2023 nahmen die Kommission und der Hohe Vertreter eine Gemeinsame Mitteilung über die Aktualisierung der EU-Strategie für maritime Sicherheit an[17], die nun im Einklang mit dem aktualisierten Aktionsplan umgesetzt werden sollte.

Im Bereich der Luftsicherheit nahm die Kommission am 2. Februar 2023 eine Arbeitsunterlage der Kommissionsdienststellen mit dem Titel „Working towards an enhanced and more resilient aviation security policy“[18] (Gestaltung einer besseren und resilienteren Luftsicherheitspolitik) an; darin wird ein ehrgeiziges Programm vorgelegt, das darauf abzielt, 1) die Regelungsstruktur für die Luftsicherheit zu modernisieren, 2) die Entwicklung und Umsetzung innovativerer Lösungen zu fördern und 3) die Grundstandards für die Luftsicherheit zu aktualisieren, damit die Flughäfen in der Union uneingeschränkt neue Spitzentechnologien nutzen können, um gegen die vorrangigen Bedrohungen vorzugehen. Innerhalb von zwei Jahren müssen 14 Leitinitiativen umgesetzt werden.

Die Kommission fordert das Europäische Parlament und den Rat auf, die Verhandlungen über die folgenden Dossiers zügig und in jedem Falle vor dem Ende der laufenden Wahlperiode des Europäischen Parlaments abzuschließen:

- Vorschlag für ein Cyberresilienzgesetz,
- Vorschlag für ein Cybersolidaritätsgesetz,

[15] COM(2022) 652 final.
[16] COM(2023) 659 final.
[17] JOIN(2023) 8 final.
[18] SWD(2023) 37 final.

- Vorschlag für eine Verordnung über die Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der EU.

Die Kommission fordert die Mitgliedstaaten auf,

- die Umsetzung der Richtlinie über die Resilienz kritischer Einrichtungen sowie die Stresstests für kritische Infrastrukturen im Energiesektor vorrangig voranzutreiben,
- die Empfehlung des Rates für einen Konzeptentwurf zur Koordinierung der Reaktion – auf Unionsebene – auf Störungen kritischer Infrastrukturen von erheblicher grenzüberschreitender Bedeutung anzunehmen,
- die NIS-2-Richtlinie vollständig und zügig umzusetzen, um die Cybersicherheit wesentlicher und wichtiger Einrichtungen deutlich zu verbessern,
- sich aktiv an der Durchführung von Risikobewertungen in Bezug auf die Cybersicherheit und an der Erstellung von Risikoszenarien für kritische Infrastrukturen und Lieferketten zu beteiligen,
- Folgemaßnahmen zur Akademie für Cybersicherheitskompetenzen zu ergreifen und dabei auf europäischer Ebene umfassend mitzuwirken, gezielte nationale Strategien oder Initiativen zu Cybersicherheitskompetenzen auf den Weg zu bringen und wichtige Interessenträger, einschließlich regionaler und kommunaler Behörden, einzubeziehen,
- mit den einschlägigen privaten Betreibern und der Kommission zusammenzuarbeiten, um die Durchführung aller in der Mitteilung über die Abwehr potenzieller Bedrohungen, die von Drohnen ausgehen, aufgeführten Maßnahmen sicherzustellen,
- den Aktionsplan für die EU-Strategie für maritime Sicherheit umzusetzen und regelmäßig über die Erfolge Bericht zu erstatten,
- die 14 festgelegten Leitinitiativen zur Verbesserung der Luftsicherheit umzusetzen.

III. Umgang mit sich wandelnden Bedrohungen

Angesichts der neuen geopolitischen Spannungen ist sehr deutlich geworden, dass die Herausforderungen für die Sicherheit der EU nicht nur größer, sondern auch unbeständiger und durch den hybriden Charakter vieler Bedrohungen weiter verschärft werden. Im Zusammenhang mit der Sicherheit muss auch auf gesellschaftliche und technologische Veränderungen reagiert werden. Im Zuge der COVID-19-Pandemie haben sich mehr Möglichkeiten für Cyberkriminelle ergeben, wobei insbesondere die Bedrohung durch Darstellungen sexuellen Kindesmissbrauchs im Internet zugenommen hat. Kriminelle und böswillige Akteure sind stets bereit, sich technologische Entwicklungen zunutze zu machen. Angesichts dieser oftmals komplexen und mehrdimensionalen Bedrohungen muss die EU entschlossen und konsequent handeln.

Verordnung über die Bekämpfung des sexuellen Kindesmissbrauchs im Internet

Im Rahmen der von Europol vorgenommenen Bewertung der Bedrohungslage im Bereich der organisierten Kriminalität im Internet wurde festgestellt, dass im Jahr 2022 sowohl Häufigkeit als auch Schwere der sexuellen Ausbeutung und des sexuellen Missbrauchs von Kindern weiter zugenommen haben, wobei sich die Täter nach wie vor technische Möglichkeiten zunutze

machen, um ihre Taten und Identitäten zu verschleiern.[19] Das gegenwärtige System, das auf der freiwilligen Aufdeckung und Meldung durch die Unternehmen basiert, hat sich als unzureichend für den Schutz von Kindern erwiesen. Im Rahmen einer Übergangsverordnung haben Unternehmen die Möglichkeit einer freiwilligen Aufdeckung und Meldung, sofern diese nach der Datenschutz-Grundverordnung (DSGVO) rechtmäßig ist. Diese Übergangsverordnung läuft im August 2024 aus. Im Mai 2022 legte die Kommission einen Vorschlag für eine Verordnung[20] vor, um der missbräuchlichen Nutzung von Online-Diensten zum Zwecke des sexuellen Missbrauchs von Kindern entgegenzuwirken. In dem vorgeschlagenen Rahmen wird ein besonderer Schwerpunkt auf die Prävention gelegt. Die Unternehmen wären verpflichtet, das Risiko der Nutzung ihrer Systeme zum Zwecke des sexuellen Missbrauchs von Kindern zu bewerten und Präventivmaßnahmen zu ergreifen. Als letztes Mittel und ausschließlich im Falle eines erheblichen Risikos könnten nationale Gerichte oder unabhängige Verwaltungsbehörden gezielte Aufdeckungsanordnungen gegen Diensteanbieter erlassen. Ein neues, unabhängiges EU-Zentrum würde den Diensteanbietern ihre Bemühungen erleichtern, indem es als Wissenszentrum dient, zuverlässige Informationen über identifiziertes Material bereitstellt, Meldungen der Anbieter über sexuellen Kindesmissbrauch im Internet entgegennimmt, diese Meldungen analysiert, um fehlerhafte Meldungen zu ermitteln, und die Opfer unterstützt. Es ist von entscheidender Bedeutung, dass die neuen Vorschriften schnellstmöglich verabschiedet und umgesetzt werden, um Kinder vor weiterem Missbrauch zu schützen, zu verhindern, dass Material erneut im Internet erscheint, und die Straftäter vor Gericht zu bringen. Der Rat und das Parlament führen gegenwärtig Verhandlungen über das Dossier und beabsichtigen, vor dem Ende der Wahlperiode des Parlaments eine Einigung zu erzielen.

Richtlinie zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt

Cybergewalt hat sich zu einer neuen Form der Gewalt gegen Frauen und der häuslichen Gewalt entwickelt, die sich über das Internet und IT-Tools über die einzelnen Mitgliedstaaten hinaus ausbreitet. Im März 2022 legte die Kommission einen Vorschlag für eine Richtlinie zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt vor, der auch spezifische Vorschriften über Cybergewalt und Maßnahmen zur Schließung der Lücken in den Bereichen Schutz, Zugang zur Justiz und Prävention beinhaltet. Durch die frühzeitige Annahme und Umsetzung dieser Richtlinie würden den Mitgliedstaaten zusätzliche Instrumente zur Bekämpfung dieser Form der Kriminalität an die Hand gegeben. Die gesetzgebenden Organe haben im Juli 2023 interinstitutionelle Verhandlungen aufgenommen und beabsichtigen, diese vor dem Ende der laufenden Wahlperiode des Europäischen Parlaments abzuschließen.

5G-Cybersicherheit

Die Sicherheit der 5G-Netze hat für die Kommission hohe Priorität und ist ein wesentlicher Bestandteil ihrer Strategie für eine Sicherheitsunion. 5G-Netze sind eine zentrale Infrastruktur und bilden die Grundlage für ein breites Spektrum von Diensten, die für das Funktionieren des Binnenmarkts und für unverzichtbare gesellschaftliche und wirtschaftliche Funktionen von entscheidender Bedeutung sind. Am 15. Juni 2023 legten die in der NIS-Kooperationsgruppe vertretenen Behörden der EU-Mitgliedstaaten einen mit Unterstützung der Kommission und der ENISA erstellten zweiten Fortschrittsbericht über die Umsetzung des EU-Instrumentariums für die 5G-Cybersicherheit vor. Aus diesem Bericht geht hervor, dass 24 Mitgliedstaaten Rechtsvorschriften erlassen haben oder gegenwärtig erarbeiten, mit denen den nationalen Behörden die Befugnis übertragen wird, Anbieter zu bewerten und Beschränkungen zu

[19] Europol (2023), Internet Organised Crime Threat Assessment (IOCTA) 2023.
[20] COM(2022) 209 final.

verhängen, und in zehn Mitgliedstaaten Beschränkungen angewandt werden. Jedoch sind weitere Maßnahmen erforderlich, um in der Union insgesamt Schwachstellen zu vermeiden, die möglicherweise schwerwiegende nachteilige Auswirkungen auf die Sicherheit der einzelnen Nutzer und Unternehmen sowie der kritischen Infrastruktur der Union hätten. Alle Mitgliedstaaten müssen das Instrumentarium unverzüglich umsetzen. Am selben Tag nahm die Kommission eine Mitteilung über die Umsetzung des Instrumentariums durch die Mitgliedstaaten sowie die Anwendung des Instrumentariums auf die interne Kommunikation der Kommission und die Finanzierungstätigkeiten der Union an. Damit unterstrich die Kommission ihre tiefe Besorgnis über die Risiken, die von den Mobilfunk-Netzausrüstungsanbietern Huawei und ZTE für die Sicherheit der EU ausgehen. In diesem Zusammenhang ergreift die Kommission Maßnahmen, um zu vermeiden, dass ihre interne Kommunikation über Mobilfunknetze geleitet wird, die Ausrüstungen von Huawei und ZTE nutzen. Es werden keine neuen Netzanbindungsdienste beschafft, die auf Ausrüstung dieser Anbieter angewiesen sind, und die Kommission wird mit den Mitgliedstaaten und Telekommunikationsbetreibern zusammenarbeiten, um sicherzustellen, dass diese Anbieter schrittweise von den bestehenden Netzanbindungsdiensten der Kommissionsstandorte ausgeschlossen werden. Des Weiteren prüft die Kommission, wie diese Entscheidung unter uneingeschränkter Einhaltung des Unionsrechts in den einschlägigen Finanzierungsprogrammen und -instrumenten der Union Berücksichtigung finden kann.

Zugang zu Daten für eine wirksame Strafverfolgung

Im heutigen digitalen Zeitalter hat fast jede Straftat eine digitale Komponente. Technologien und Tools – einschließlich jener, die erforderlich sind, um für die Bürgerinnen und Bürger Cybersicherheit, Datenschutz und Privatsphäre zu gewährleisten – werden auch zu kriminellen Zwecken eingesetzt. Dadurch wird es in der EU immer schwerer, eine wirksame Strafverfolgung aufrechtzuerhalten, um die öffentliche Sicherheit zu schützen und Straftaten zu verhindern, aufzudecken, zu untersuchen und strafrechtlich zu verfolgen; obwohl auf Unions- und nationaler Ebene erhebliche Anstrengungen unternommen wurden, sei es durch Rechtsvorschriften oder durch Kapazitätsaufbau und Innovationsinitiativen, bestehen nach wie vor rechtliche und technische Probleme. Die Kommission hat unter Einbeziehung des Ratsvorsitzes eine hochrangige Gruppe für den Zugang zu Daten für eine wirksame Strafverfolgung eingerichtet, um eine Plattform für die Zusammenarbeit eines breiten Spektrums von Interessenträgern und Sachverständigen bei der Auslotung der Probleme zu schaffen, mit denen sich die Strafverfolgungsbehörden konfrontiert sehen (z. B. Verschlüsselung, Vorratsspeicherung von Daten, 5G und Normung). Die Kommission erwartet, dass die hochrangige Gruppe bis Juni 2024 ausgewogene, tragfähige und umsetzbare Empfehlungen formuliert, die der Komplexität dieser Probleme Rechnung tragen und in denen auch die Dimensionen der Cybersicherheit und des Datenschutzes Berücksichtigung finden. Die Mitgliedstaaten und die teilnehmenden Sachverständigen sind daher gehalten, sich aktiv in diesen Prozess einzubringen und wirksame, rechtmäßige und allgemein akzeptierte Lösungen zu erarbeiten.

Hybride Bedrohungen

In einem geopolitischen Umfeld, in dem hybride Bedrohungen immer komplexer und ausgefeilter werden, wurden mit dem Strategischen Kompass der EU für Sicherheit und Verteidigung[21] (im Folgenden „Strategischer Kompass“) eine gemeinsame Bewertung der Bedrohungen und Herausforderungen, mit denen die Union konfrontiert ist, und ein strategischer Aktionsplan vorgelegt. Durch die Zunahme der böswilligen Cyberaktivitäten von

[21] Ratsdokument 7371/22.

Staaten und nichtstaatlichen Akteuren, die unter anderem im Zusammenhang mit dem Krieg gegen die Ukraine zu beobachten ist, wurde noch deutlicher, dass der Cyberraum Gegenstand der Außen- und Sicherheitspolitik sein muss. Die von böswilligen Aktivitäten und Desinformation ausgehenden Risiken erfordern besondere Wachsamkeit, wenn Wahlen bevorstehen – dies gilt auch für die Europawahl im Jahr 2024.

Angesichts des hohen Risikos von Spillover-Effekten hat die EU ihre Maßnahmen für den Aufbau von Cyberkapazitäten und die Förderung von Partnerschaften mit Drittländern fortgesetzt, unter anderem im Rahmen gezielter Cyberdialoge, um ihre Abwehrbereitschaft insgesamt aktiv zu stärken. Wie im 7. Fortschrittsbericht über hybride Bedrohungen vom 14. September 2023[22] ausgeführt, wurde eine Reihe von Instrumenten entwickelt, überarbeitet und gestärkt, um die Fähigkeit der Union, wirksam gegen hybride Bedrohungen vorzugehen, zu verbessern. Dazu zählen unter anderem:

- das Instrumentarium zur Abwehr hybrider Bedrohungen in der EU, mit dem ein Rahmen für eine koordinierte und fundierte Reaktion auf hybride Bedrohungen und Kampagnen sichergestellt werden soll,
- die laufenden Arbeiten an der Einrichtung von EU-Teams für die rasche Reaktion auf hybride Bedrohungen, die für Mitgliedstaaten und Partnerländer sowie bei Missionen und Operationen im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) kurzfristig maßgeschneiderte Unterstützung leisten sollen,
- das überarbeitete Protokoll der EU für das operative Vorgehen bei der Abwehr hybrider Bedrohungen (im Folgenden „EU Playbook“)[23], in dem die Verfahren und Strukturen der Union für den Umgang mit hybriden Bedrohungen und Kampagnen festgelegt sind,
- die überarbeiteten Leitlinien zur Umsetzung des Rahmens für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten[24] („Instrumentarium für die Cyberdiplomatie“), der die Entwicklung dauerhafter, maßgeschneiderter, kohärenter und koordinierter Strategien gegen Akteure ermöglicht, von denen eine anhaltende Cyberbedrohung ausgeht,
- das Instrumentarium gegen Manipulation von Informationen und Einmischung aus dem Ausland zur Stärkung der vorhandenen Instrumente, die der Union zur Verfügung stehen, um Manipulation von Informationen und Einmischung aus dem Ausland zu verhindern, für Abschreckung zu sorgen und darauf zu reagieren,
- die EU-Cyberabwehrpolitik[25], die darauf abzielt, die Cyberabwehrfähigkeiten der EU zu fördern, die Lageerfassung zu verbessern und das gesamte Spektrum der verfügbaren Abwehroptionen zu koordinieren, um die Abwehrbereitschaft zu stärken, auf Cyberangriffe zu reagieren und Solidarität sowie gegenseitigen Beistand sicherzustellen.

Die Mitgliedstaaten werden daher aufgefordert, ihre Zusammenarbeit in diesem Bereich fortzusetzen und zu verbessern, indem sie – unter anderem durch regelmäßige Übungen – für die wirksame Umsetzung der oben genannten Instrumentarien sorgen und eine Einigung über das Konzept der Teams für die rasche Reaktion auf hybride Bedrohungen erzielen, in dessen Rahmen Leitlinien für die weiteren Schritte bei der Einrichtung der Teams bereitgestellt werden.

[22] SWD(2023) 315 final.
[23] SWD(2023) 116 final.
[24] 10289/23 vom 8. Juni 2023.
[25] JOIN(2022) 49 final.

KI im Bereich der Strafverfolgung

Künstliche Intelligenz (KI) ist im Alltag rasch zur Normalität geworden. Die Auswirkungen des Einsatzes von KI in den Bereichen Cyberkriminalität und Cybersicherheit sind noch nicht vollständig bekannt, es ist jedoch offensichtlich, dass er neue Herausforderungen mit sich bringen wird. Der Einsatz von KI in einer sicheren und kontrollierten Form kann von Vorteil sein – in den Händen böswilliger Akteure kann er jedoch gefährlich sein, wenn er beispielsweise der Verschleierung der Identitäten der Täter im Zusammenhang mit Terrorismus oder dem sexuellen Missbrauch von Kindern dient. Daher ist es von entscheidender Bedeutung, dass die Behörden mit den Entwicklungen Schritt halten, um Missbrauch vorzubeugen und auf den missbräuchlichen Einsatz von KI zu reagieren.[26] Die Verhandlungen über das vorgeschlagene Gesetz über künstliche Intelligenz zielen darauf ab, diese Themen anzugehen, und befinden sich in einer entscheidenden Phase, in der die gesetzgebenden Organe technische und politische Fragen erörtern, deren Beantwortung für den Umgang mit dieser Technologie in den nächsten Jahren von maßgeblicher Bedeutung ist. Es müssen – auch für den Bereich der Strafverfolgung – insbesondere im Hinblick auf Hochrisiko-Anwendungen ausgewogene Lösungen gefunden werden.

Die Kommission fordert das Europäische Parlament und den Rat auf, die interinstitutionellen Verhandlungen über die folgenden anhängigen Dossiers zügig und in jedem Falle vor dem Ende der laufenden Wahlperiode des Europäischen Parlaments abzuschließen:

- Vorschlag für eine Verordnung über die Bekämpfung des sexuellen Kindesmissbrauchs im Internet,
- Vorschlag für eine Richtlinie zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt,
- Vorschlag für eine Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz).

Die Kommission fordert die Mitgliedstaaten auf,

- die vollständige Umsetzung des EU-Instrumentariums für 5G-Cybersicherheit unverzüglich abzuschließen,
- die Arbeit der hochrangigen Gruppe für den Zugang zu Daten für eine wirksame Strafverfolgung zu unterstützen, sodass klare, tragfähige und umsetzbare Empfehlungen für einen ausgewogenen Umgang mit gegenwärtigen und zu erwartenden Herausforderungen formuliert werden,
- in Zusammenarbeit mit dem Hohen Vertreter Schritte zu unternehmen, um – unter anderem durch regelmäßige Übungen und unter Berücksichtigung der globalen Entwicklungen – die wirksame Umsetzung des Instrumentariums zur Abwehr hybrider Bedrohungen in der EU, des überarbeiteten Instrumentariums für die Cyberdiplomatie („Instrumentarium für die Cyberdiplomatie“) und des Instrumentariums gegen Manipulation von Informationen und Einmischung aus dem Ausland sicherzustellen,
- eine Einigung über das Konzept der Teams für die rasche Reaktion auf hybride Bedrohungen zu erzielen.

[26] Vgl. beispielsweise den am 17. April 2023 veröffentlichten Bericht von Europol mit dem Titel „ChatGPT – the impact of Large Language Models on Law Enforcement“.

IV. Schutz der Europäerinnen und Europäer vor Terrorismus und organisierter Kriminalität

Das Risiko, dass durch globale oder lokale Ereignisse neue terroristische Aktivitäten ausgelöst werden, ist allgegenwärtig. Zugleich zählen die organisierte Kriminalität und der Drogenhandel zu den schwerwiegendsten Bedrohungen für die Sicherheit der EU. Um die gemeinsamen Anstrengungen der Union zur Bekämpfung dieser Bedrohungen zu verstärken, wird die gemeinsame Arbeit an der Umsetzung der EU-Strategie zur Bekämpfung der organisierten Kriminalität[27], der Strategie der EU zur Bekämpfung des Menschenhandels[28], der EU-Agenda zur Drogenbekämpfung und des Drogenaktionsplans[29] sowie der EU-Agenda für Terrorismusbekämpfung[30] vorangetrieben. Um jedoch auf die besorgniserregende Verschlechterung der Lage im Bereich der organisierten Kriminalität und des Drogenhandels zu reagieren, müssen die Mitgliedstaaten und die EU ihre Anstrengungen intensivieren, um das gemeinsame Vorgehen gegen kriminelle Netze zu verstärken und die Opfer von Straftaten besser zu schützen; daher wurde zeitgleich mit diesem Bericht ein EU-Fahrplan zur Bekämpfung des Drogenhandels und der organisierten Kriminalität[31] veröffentlicht.

Im Bereich der Terrorismusbekämpfung verstärkt die EU auch ihr Instrumentarium für die Außenpolitik[32], indem sie hochrangige Dialoge zur Terrorismusbekämpfung führt, das Netzwerk der zu den EU-Delegationen entsandten Experten für Terrorismusbekämpfung/Sicherheit umfassend nutzt und – unter anderem im Rahmen des Ko-Vorsitzes des Globalen Forums „Terrorismusbekämpfung“ (Global Counter-Terrorism Forum, GCTF) – an multilateralen Foren teilnimmt.

Drogenhandel

Wenn im Juli 2024 das neue Mandat der Europäischen Beobachtungsstelle für Drogen und Drogensucht in Kraft tritt, wird die EU besser gerüstet sein, um gegen ein komplexes Sicherheits- und Gesundheitsproblem vorzugehen, von dem Millionen von Menschen in der EU und weltweit betroffen sind. Des Weiteren überarbeitet[33] die Kommission gegenwärtig die Verordnungen über Drogenausgangsstoffe[34], um die größten Herausforderungen, die im Zuge der 2020 vorgenommenen Evaluierung[35] ermittelt wurden, zu bewältigen; in der genannten Evaluierung wurde darauf hingewiesen, dass die durch Designer-Ausgangsstoffe aufgeworfenen Probleme in Angriff genommen werden müssen[36], um das Angebot illegaler Drogen einzudämmen.

---

27 COM(2021) 170 final.
28 COM(2021) 171 final.
29 COM(2020) 606 final.
30 COM(2020) 795 final.
31 COM(2023) 641 final.
32 Wie im Strategischen Kompass und in den im Juni 2022 angenommenen Schlussfolgerungen des Rates zur Bewältigung der externen Dimension einer sich stetig wandelnden terroristischen und gewaltextremistischen Bedrohungslage gefordert.
33 Drogenausgangsstoffe – Überarbeitung der EU-Vorschriften (europa.eu).
34 Verordnung (EG) Nr. 273/2004 betreffend Drogenausgangsstoffe und Verordnung (EG) Nr. 111/2005 des Rates zur Festlegung von Vorschriften für die Überwachung des Handels mit Drogenausgangsstoffen zwischen der Union und Drittländern.
35 COM(2020) 768 final.
36 Maßnahme 23 des Drogenaktionsplans, COM(2020) 606 final.

Angesichts der beispiellosen Zunahme des Angebots illegaler Drogen in Europa muss jedoch die Bekämpfung des Drogenhandels in Zusammenarbeit mit internationalen Partnern intensiviert werden. Die Mitgliedstaaten und die EU müssen weitere Maßnahmen ergreifen, um kriminelle Netze zu zerschlagen und die Opfer von Straftaten besser zu schützen. Die Kommission legt heute einen EU-Fahrplan zur Bekämpfung des Drogenhandels und der organisierten Kriminalität vor. Darin werden 17 Maßnahmen in vier Schwerpunktbereichen festgelegt: Stärkung der Resilienz von Logistik-Drehkreuzen durch eine Europäische Hafenallianz, Zerschlagung krimineller Netze, Verstärkung der Präventionsmaßnahmen und Intensivierung der Zusammenarbeit mit internationalen Partnern. Diese Maßnahmen müssen in den Jahren 2024 und 2025 umgesetzt werden.

Feuerwaffen

Der unerlaubte Handel mit Feuerwaffen leistet der organisierten Kriminalität in der EU und ihren Nachbarländern Vorschub. In der EU befinden sich schätzungsweise 35 Millionen illegale Feuerwaffen in der Hand von Zivilpersonen, und im Schengener Informationssystem sind etwa 630 000 Feuerwaffen erfasst, die als gestohlen oder verloren gemeldet wurden. Durch das Aufkommen von Expresspaketdiensten und die Entwicklung neuer Technologien, wie beispielsweise des 3D-Drucks, entstehen für den unerlaubten Handel mit Feuerwaffen neue Möglichkeiten, Kontrollen zu umgehen. Der russische Angriffskrieg gegen die Ukraine hatte ebenfalls eine Zunahme der Gefahr einer Verbreitung von Feuerwaffen zur Folge. Im Oktober 2022 nahm die Kommission einen Vorschlag zur Aktualisierung der geltenden Rechtsvorschriften über die Einfuhr, Ausfuhr und Durchfuhr ziviler Feuerwaffen an, um die in den geltenden Vorschriften bestehenden Schlupflöcher zu schließen, aufgrund deren mehr Feuerwaffen in die EU geschmuggelt und umgelenkt werden können.[37] Mittelfristig werden diese neuen Vorschriften dazu beitragen, dass die Gefahr einer Umgehung von Embargos bei der Ausfuhr von Feuerwaffen für den zivilen Gebrauch sinkt und verstärkt Kontrollen bei der Einfuhr dieser Feuerwaffen aus Drittländern vorgenommen werden. Beide gesetzgebenden Organe müssen noch ihre Standpunkte zu diesem Dossier festlegen, um vor dem Ende der laufenden Wahlperiode des Parlaments eine Einigung über dieses Dossier zu erzielen.

Menschenhandel

Menschenhandel ist eine besonders schwere Form der organisierten Kriminalität und ein schwerwiegender Verstoß gegen die Grundrechte. Innerhalb der EU handelt es sich bei Opfern des Menschenhandels in erster Linie um Opfer des Menschenhandels zum Zwecke der sexuellen Ausbeutung und der Ausbeutung der Arbeitskraft, aber auch um Opfer des Menschenhandels zum Zwecke der Zwangsbettelei, der Zwangskriminalität und anderer Formen der Ausbeutung. Im Dezember 2022 legte die Kommission einen Vorschlag zur Änderung der Richtlinie zur Bekämpfung des Menschenhandels[38] vor, um die Defizite im geltenden Rechtsrahmen mit aktualisierten Vorschriften zu beheben. Nach ihrer Annahme wäre die überarbeitete Richtlinie auch auf Zwangsheirat und illegale Adoption anwendbar und enthielte eine ausdrückliche Bezugnahme auf die Online-Dimension des Menschenhandels. Des Weiteren wäre darin eine verpflichtende Sanktionsregelung für die Täter und eine Formalisierung der Einrichtung nationaler Verweismechanismen vorgesehen; diese Formalisierung zielt darauf ab, die frühzeitige Erkennung der Opfer und ihre grenzüberschreitende Verweisung an Unterstützungs- und Betreuungsdienste zu verbessern. Die wissentliche Inanspruchnahme der von Opfern des Menschenhandels erbrachten Dienste würde zu einer Straftat, und die jährliche Erhebung von Daten über den Menschenhandel, die

[37] COM(2022) 480 final.
[38] COM(2022) 732 final.

von Eurostat zu veröffentlichen wären, würde verpflichtend vorgeschrieben. Der Rat legte seine allgemeine Ausrichtung im Juni 2023 fest, während die Festlegung des Standpunkts des Europäischen Parlaments noch aussteht. Es wird ein rasches Handeln erforderlich sein, um vor dem Ende der laufenden Wahlperiode des Parlaments eine Einigung zu erzielen.

Umweltkriminalität

Umweltkriminalität stellt mittlerweile eine globale Bedrohung dar und nimmt Schätzungen zufolge jährlich um 5 % bis 7 % zu. Für die organisierte Kriminalität ist sie sehr attraktiv, da dabei erhebliche Gewinne erzielt werden können, sich aus den Unterschieden zwischen den Rechtsvorschriften der einzelnen Mitgliedstaaten Schlupflöcher ergeben und nur ein geringes Risiko besteht, dass die Straftaten aufgedeckt werden. Nach Angaben von Europol gibt es Hinweise darauf, dass die Erträge aus diesen Aktivitäten für die Terrorismusfinanzierung verwendet werden. Im Dezember 2021 nahm die Kommission einen Vorschlag zur Ersetzung der Richtlinie über den strafrechtlichen Schutz der Umwelt aus dem Jahr 2008 an. Der Schwerpunkt dieses Vorschlags liegt auf der Präzisierung und Aktualisierung der Definitionen der Kategorien von Umweltkriminalität und der Festlegung wirksamer, abschreckender und verhältnismäßiger Sanktionsarten und Strafmaße für natürliche und juristische Personen. Zu den neuen Straftatbeständen zählen Straftaten im Zusammenhang mit Entwaldung, Verstößen gegen das EU-Chemikalienrecht, der illegalen Entnahme von Oberflächen- oder Grundwasser und dem illegalen Recycling von Schiffen. Der Vorschlag zielt darauf ab, die Strafverfolgungskette deutlich zu stärken und die grenzüberschreitende Zusammenarbeit zwischen den Behörden der Mitgliedstaaten und den Agenturen und Einrichtungen der EU zu fördern. Das Europäische Parlament und der Rat haben ihre jeweiligen Standpunkte zu dem Vorschlag festgelegt und führen gegenwärtig Verhandlungen, die sie bis Ende des Jahres abgeschlossen haben sollten. Es muss ein überarbeiteter Aktionsplan[39] zur Bekämpfung des illegalen Artenhandels umgesetzt werden, um die Prävention und Durchsetzung weiter zu verbessern.

Abschöpfung und Einziehung von Vermögenswerten

Es ist von entscheidender Bedeutung, Straftätern ihre Erträge aus illegalen Geschäften zu entziehen, um die organisierte Kriminalität zu unterbinden. Aus diesem Grund schlug die Kommission nicht nur vor, den Strafverfolgungsbehörden einen EU-weiten Zugang zu Bankkontoinformationen zu ermöglichen[40] (über diesen Vorschlag wurde im Juni 2023 eine politische Einigung erzielt), sondern legte im Mai 2022 auch einen Vorschlag für die Abschöpfung und Einziehung von Vermögenswerten[41] vor, um die Möglichkeiten zum Aufspüren sowie zur Ermittlung, Sicherstellung, Einziehung und Verwaltung von Vermögenswerten zu verbessern. Die wichtigsten Bestimmungen des Vorschlags betreffen die Anforderungen in Bezug auf Finanzermittlungen, zusätzliche Befugnisse und Instrumente der Vermögensabschöpfungsstellen sowie wirksamere Sicherstellungs- und Einziehungsmaßnahmen für ein breiteres Spektrum von Straftaten. Einer der Straftatbestände, auf die diese Maßnahmen anwendbar würden, wäre der Verstoß gegen restriktive Maßnahmen der Union. Im Dezember 2022 nahm die Kommission einen gesonderten Vorschlag zur Angleichung der strafrechtlichen Definitionen und Sanktionen für Verstöße gegen restriktive Maßnahmen der Union an. Die wirksame Umsetzung und Durchsetzung restriktiver Maßnahmen der Union hat für die Kommission nach wie vor oberste Priorität und wird durch die Arbeit der Taskforce „Freeze and Seize“ unterstützt, die von der Kommission als Reaktion

[39] COM(2022) 581 final.
[40] COM(2021) 429 final.
[41] COM(2022) 245 final.

auf den russischen Angriffskrieg gegen die Ukraine eingesetzt wurde. Das Europäische Parlament und der Rat haben ihre Standpunkte zu beiden Vorschlägen angenommen und beabsichtigen, bis Jahresende eine Einigung zu erzielen.

Paket zur Bekämpfung der Geldwäsche

In der EU findet Geldwäsche im Zusammenhang mit praktisch allen kriminellen Aktivitäten statt, bei denen Erträge aus Straftaten generiert werden,[42] und ist somit ein wichtiger Hebel für die Bekämpfung der Kriminalität. Im Juli 2021 legte die Kommission ambitionierte Vorschläge für die Verstärkung der Maßnahmen der EU zur Verhinderung von Geldwäsche und Terrorismusfinanzierung vor;[43] sie bilden ein Paket aus vier Legislativvorschlägen für die wirksamere Verhinderung und Aufdeckung der Versuche von Straftätern, das Finanzsystem für Zwecke der Geldwäsche oder Terrorismusfinanzierung zu nutzen. Eine der vier Initiativen des Pakets hat die Sicherstellung der Rückverfolgbarkeit von Kryptowertetransfers zum Gegenstand und wurde im Mai 2023 von den gesetzgebenden Organen angenommen.[44] Die neue Verordnung gilt ab dem 30. Dezember 2024; ab diesem Zeitpunkt müssen alle Anbieter von Krypto-Dienstleistungen bei Kryptowertetransfers Angaben zum Originator und zum Begünstigten einholen und aufbewahren. Die übrigen drei Vorschläge zielen darauf ab, i) eine neue Behörde zur Bekämpfung der Geldwäsche und der Terrorismusfinanzierung einzurichten, die eine gleichbleibend hochwertige Aufsicht im gesamten Binnenmarkt, einschließlich der risikoreichsten grenzüberschreitend tätigen Unternehmen, sicherstellen und die Arbeit der zentralen Meldestellen unterstützen und koordinieren soll, ii) harmonisierte Regeln für den Privatsektor festzulegen und unter anderem in Bezug auf hohe Barzahlungen für Dienstleistungen und Güter eine EU-weite Obergrenze von 10 000 EUR einzuführen und iii) die Befugnisse der zuständigen Behörden und die Instrumente für ihre Zusammenarbeit zu stärken. Es ist davon auszugehen, dass mit diesem Paket die Fähigkeit der EU, Geldwäsche zu bekämpfen und die Bürgerinnen und Bürger der EU vor Terrorismus und organisierter Kriminalität zu schützen, erheblich verbessert wird. Die gesetzgebenden Organe führen gegenwärtig Verhandlungen über die drei anhängigen Vorschläge, um vor dem Ende der laufenden Wahlperiode des Parlaments eine Einigung über dieses Dossier zu erzielen.

Die Kommission fordert das Europäische Parlament und den Rat auf, die interinstitutionellen Verhandlungen über die folgenden anhängigen Dossiers zügig und in jedem Falle vor dem Ende der laufenden Wahlperiode des Europäischen Parlaments abzuschließen:

- Vorschlag für eine Richtlinie über die Abschöpfung und Einziehung von Vermögenswerten,
- Vorschlag für eine Richtlinie zur Angleichung der strafrechtlichen Definitionen und Sanktionen für Verstöße gegen restriktive Maßnahmen der Union,
- Vorschlag für eine Richtlinie zur Bekämpfung des Menschenhandels,
- Vorschlag für eine Richtlinie zur Verbesserung des strafrechtlichen Schutzes der Umwelt,
- Vorschlag für ein Paket zur Bekämpfung der Geldwäsche,

[42] Europol, Enterprising criminals – Europe's fight against the global networks of financial and economic crime, 2020.

[43] COM(2021) 420 final.

[44] Verordnung (EU) 2023/1113 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über die Übermittlung von Angaben bei Geldtransfers und Transfers bestimmter Kryptowerte und zur Änderung der Richtlinie (EU) 2015/849.

- Vorschlag zur Aktualisierung der geltenden Rechtsvorschriften über die Einfuhr, Ausfuhr und Durchfuhr ziviler Feuerwaffen.

Die Kommission fordert die Mitgliedstaaten sowie die Agenturen und Einrichtungen der EU auf,

- gemeinsam auf die Umsetzung der 17 Maßnahmen des EU-Fahrplans zur Bekämpfung des Drogenhandels und der organisierten Kriminalität in den Jahren 2023 und 2024 hinzuwirken.

V. Eine starke europäische Sicherheitsgemeinschaft

Seit einigen Jahren haben die Sicherheitsbedrohungen zunehmend grenzüberschreitenden Charakter, sodass auf allen Ebenen weitere Synergien und eine engere Zusammenarbeit erforderlich sind. Seit der Annahme der Strategie für eine Sicherheitsunion wurden wichtige Initiativen in die Wege geleitet, um die grenzüberschreitende Zusammenarbeit zu intensivieren, die verfügbaren Instrumente und Verfahren sowohl an den Außengrenzen als auch innerhalb des Schengen-Raums zu straffen und zu modernisieren und den Informationsaustausch zwischen Strafverfolgungs- und Justizbehörden mit Blick auf eine wirksamere Bekämpfung der organisierten Kriminalität zu verbessern. Vor diesem Hintergrund ist die wirksame Umsetzung des Interoperabilitätsrahmens für den Datenaustausch von maßgeblicher Bedeutung, um für eine erhöhte Sicherheit zu sorgen, eine wirksame europäische Reaktion auf grenzüberschreitende Bedrohungen zu ermöglichen und zugleich die Freizügigkeit innerhalb der Union zu gewährleisten.

Verbesserung des Informationsaustauschs im Schengen-Raum: vorab übermittelte Fluggastdaten, Fluggastdatensätze und Prüm II

Durch die beiden Vorschläge zu vorab übermittelten Fluggastdaten (Advance Passenger Information – API), die von der Kommission im Dezember 2022[45] angenommen wurden, würde die innere Sicherheit der Union verbessert, indem den Strafverfolgungsbehörden der Mitgliedstaaten zusätzliche Instrumente zur Bekämpfung von schwerer Kriminalität und Terrorismus an die Hand gegeben würden. Insbesondere würden vorab übermittelte Fluggastdaten zu EU-Flügen, die zusammen mit den Fluggastdatensätzen (Passenger Name Records – PNR) der Flugreisenden verwendet würden, die Strafverfolgungsbehörden der Mitgliedstaaten in die Lage versetzen, die Wirksamkeit ihrer Ermittlungen durch gezieltere Maßnahmen erheblich zu steigern. Es ist wichtig, dass die vorgeschlagenen Vorschriften so bald wie möglich angenommen werden: Dies käme nicht nur der Bekämpfung von organisierter Kriminalität und Terrorismus zugute, sondern trüge auch dazu bei, dass im Falle einer vorübergehenden Wiedereinführung von Kontrollen an den Binnengrenzen deutlich weniger systematische Kontrollen aller Reisenden vorgenommen werden müssten, wodurch Flugreisen und die Freizügigkeit erleichtert würden. Am 6. September 2023 empfahl die Europäische Kommission dem Rat, eine Ermächtigung zur Aufnahme von Verhandlungen über Abkommen mit der Schweiz sowie mit Island und Norwegen über die Übermittlung von Fluggastdatensätzen zu erteilen. Der Erlass der drei empfohlenen Beschlüsse trüge zu einer kohärenten und wirksamen externen PNR-Politik der EU bei.

[45] COM(2022) 729, COM(2022) 73.

Der Datenaustausch über das Prümer System wird von den Polizeibehörden im Rahmen der Bekämpfung von organisierter Kriminalität, Drogen, Terrorismus, sexueller Ausbeutung und Menschenhandel tagtäglich genutzt. Mit dem Vorschlag für eine Verordnung über den automatisierten Datenaustausch für die polizeiliche Zusammenarbeit („Prüm II“)[46] wird der bestehende Prüm-Rahmen überarbeitet, um Informationslücken zu schließen und die Verhütung, Aufdeckung und Untersuchung von Straftaten in der EU zu verbessern. Die überarbeiteten Vorschriften über den automatisierten Datenaustausch für die polizeiliche Zusammenarbeit stellen eine Ergänzung zu den in dieser Wahlperiode vorgelegten Vorschlägen sowie zu der bereits angenommenen Empfehlung des Rates zur operativen Zusammenarbeit im Bereich der Strafverfolgung und der Richtlinie über den Informationsaustausch zwischen den Strafverfolgungsbehörden dar. Durch die zügige Annahme und Umsetzung dieser zusammenhängenden Rechtsakte würde der Datenaustausch zwischen den Strafverfolgungsbehörden verbessert, erleichtert und beschleunigt und die Identifizierung von Straftätern vereinfacht.

Vollständig interoperables Grenzmanagementsystem für einen sicheren, starken, digitalen und geeinten Schengen-Raum

Für das reibungslose Funktionieren des Schengen-Raums ohne Binnengrenzen bedarf es des gegenseitigen Vertrauens der Mitgliedstaaten. Dieses wiederum setzt wirksame Kontrollen voraus, sei es an den Außengrenzen der Union oder als alternative Maßnahmen im Hoheitsgebiet der Mitgliedstaaten. Im Vorschlag der Kommission für die Änderung des Schengener Grenzkodexes[47] wird dargelegt, wie die Mitgliedstaaten vermehrt auf Kontrollen an den Binnengrenzen verzichten und stattdessen auf alternative Maßnahmen zurückgreifen können, die ein hohes Maß an Sicherheit gewährleisten können. Es ist wichtig, dass die Änderung des Schengener Grenzkodexes angenommen und vollständig umgesetzt wird, um im Schengen-Raum für ein hohes und angemessenes Maß an Sicherheit zu sorgen. Zudem wird die neue Architektur der Informationssysteme der EU so weiterentwickelt, dass sie besser zur Unterstützung der nationalen Behörden bei der Gewährleistung der Sicherheit und des Grenzmanagements geeignet ist. Diese Architektur umfasst das Schengener Informationssystem, das Europäische Reiseinformations- und -genehmigungssystem, das Einreise-/Ausreisesystem, das aktualisierte Visa-Informationssystem und den Interoperabilitätsrahmen, über den die Systeme vollkommen sicher verknüpft werden. Nach ihrer Fertigstellung würden den nationalen Behörden über diese neue Architektur umfassendere und zuverlässigere Sicherheitsinformationen zur Verfügung gestellt. Alle Komponenten des Interoperabilitätsrahmens sind von wesentlicher Bedeutung, sodass eine Verzögerung bei einem Aspekt oder in einem einzelnen Mitgliedstaat insgesamt eine verzögerte Einführung zur Folge hat. Verzögerungen bei der technischen Entwicklung des Einreise-/Ausreisesystems sollten auf ein Minimum reduziert werden, damit das System schnellstmöglich in Betrieb genommen werden kann und alle Schlüsselelemente des Interoperabilitätsrahmens eingerichtet werden können.

Mit der vorgeschlagenen Screening-Verordnung[48] würde die Sicherheit im Schengen-Raum erhöht, indem einheitliche Vorschriften für die Identifizierung von Drittstaatsangehörigen eingeführt würden, die die Einreisevoraussetzungen gemäß dem Schengener Grenzkodex nicht erfüllen, und die betreffenden Personen an den Außengrenzen Gesundheits- und Sicherheitskontrollen unterzogen würden. Das vorgeschlagene Eurodac-System könnte für die

[46] COM(2021) 784 final.
[47] COM(2021) 891 final.
[48] COM(2020) 612 final.

Erreichung dieser Ziele hilfreich sein, weil darin ein Hinweis eingegeben werden kann, wenn es nach dem Screening den Anschein hat, dass eine Person eine Gefahr für die innere Sicherheit darstellen könnte. Dadurch würde wiederum die Durchführung der vorgeschlagenen Verordnung über Asyl- und Migrationsmanagement erleichtert. Die Kommission fordert die gesetzgebenden Organe auf, die Verhandlungen über diese Dossiers zügig und vor dem Ende der laufenden Legislaturperiode abzuschließen.

Korruptionsbekämpfung

Korruption schadet den Demokratien, der Wirtschaft und der Sicherheit in der Union, da sie der organisierten Kriminalität und feindlicher ausländischer Einflussnahme Vorschub leistet. Die erfolgreiche Verhütung und Bekämpfung von Korruption ist daher sowohl für den Schutz der Werte der EU und der Wirksamkeit der EU-Politik als auch für die Aufrechterhaltung der Rechtsstaatlichkeit und des Vertrauens in die Regierenden und die öffentlichen Institutionen äußerst wichtig. Wie von Präsidentin von der Leyen in ihrer Rede zur Lage der Union 2022 angekündigt, nahm die Kommission am 3. Mai 2023 ein Paket von Maßnahmen zur Korruptionsbekämpfung[49] an. Der Vorschlag der Kommission für eine Richtlinie zur Bekämpfung der Korruption beinhaltet strengere Vorschriften über die strafrechtliche Ahndung von Korruptionsdelikten und die EU-weite Angleichung der Strafen. Des Weiteren sind darin wirksame Ermittlungen und Strafverfolgungsmaßnahmen vorgesehen, und es liegt ein deutlicher Schwerpunkt auf der Prävention und der Schaffung einer Kultur der Integrität, in der Korruption nicht toleriert wird. Im Europäischen Parlament und im Rat wurden die Beratungen über diesen Vorschlag aufgenommen. Darüber hinaus werden die Mitgliedstaaten ersucht, die in dem am 5. Juli 2023 angenommenen Bericht über die Rechtsstaatlichkeit 2023 ausgesprochenen Empfehlungen zum Pfeiler Korruptionsbekämpfung umzusetzen. In einem Vorschlag des Hohen Vertreters, der von der Kommission unterstützt wird, wird zudem die Schaffung einer speziellen Sanktionsregelung im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik (GASP) angeregt, um weltweit gegen schwere Korruptionshandlungen vorzugehen.

Stärkung der Rechte von Opfern

Am 12. Juli 2023 schlug die Kommission Änderungen an der Opferschutzrichtlinie vor, um den Zugang von Opfern zu Informationen, Unterstützung und Schutz zu verbessern und ihnen die Teilnahme an Strafverfahren sowie den Zugang zu Entschädigung zu erleichtern. Eines der übergeordneten Ziele der Überarbeitung besteht darin, einen Beitrag zu einem hohen Maß an Sicherheit zu leisten, indem ein sichereres Umfeld geschaffen wird, in dem die Opfer Straftaten anzeigen können, und ihnen die Angst vor Repressalien genommen wird.

Die Kommission fordert das Europäische Parlament und den Rat auf, die interinstitutionellen Verhandlungen über die folgenden anhängigen Dossiers zügig und in jedem Falle vor dem Ende der laufenden Wahlperiode des Europäischen Parlaments abzuschließen:

- Vorschlag für eine Prüm-II-Verordnung,
- Vorschläge zu vorab übermittelten Fluggastdaten,
- Vorschläge zur Korruptionsbekämpfung und insbesondere zur Schaffung einer speziellen Sanktionsregelung im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik (GASP),
- Vorschlag für eine Änderung des Schengener Grenzkodexes,
- Vorschlag für eine Opferschutzrichtlinie,

[49] COM(2023) 234 final.

- Vorschlag zum Screening.

Die Kommission fordert die Mitgliedstaaten auf,

- schnellstmöglich für die Inbetriebnahme des Einreise-/Ausreisesystems zu sorgen, um die Einrichtung der Architektur der EU für den Informationsaustausch abzuschließen.

VI. Umsetzung

Die Gewährleistung der Sicherheit Europas als Ganzes ist eine gemeinsame Verantwortung, wobei jeder Akteur seinen Beitrag leisten muss – von der Kommission und den gesetzgebenden Organen, die neue, strikte, umfassende und praktische Vorschriften erlassen, über die Mitgliedstaaten, die diese Vorschriften zügig umsetzen, durchführen und anwenden, bis hin zu der Vielzahl von Behörden, Organisationen und Interessenträgern, die vor Ort die operative Arbeit leisten. Den in den Bereichen Justiz, Inneres und Cybersicherheit tätigen Agenturen der EU kommt ebenfalls eine zentrale Bedeutung zu, die durch die jüngsten Erweiterungen ihrer Zuständigkeiten weiter gewachsen ist.

Verbesserte Überprüfung der Begünstigten von EU-Mitteln

Bei der Ausführung des EU-Haushalts muss die Kommission sicherstellen, dass die Begünstigten von EU-Mitteln die Werte der EU achten. Es gibt bereits belastbare Mechanismen und Kontrollsysteme für die Bestimmung der möglichen Begünstigten von EU-Mitteln, und auch die laufenden Verhandlungen über eine Neufassung der Haushaltsordnung zielen darauf ab, der Kommission wirksamere rechtliche Mittel an die Hand zu geben, damit sie gegebenenfalls tätig werden kann. Darüber hinaus arbeitet die Kommission gegenwärtig an der weiteren Verbesserung der Überprüfung der derzeitigen und künftigen Begünstigten von EU-Mitteln, indem sie strengere Leitlinien für die Verpflichtungen im Hinblick auf die Achtung der Werte der EU und die Folgen von Verstößen gegen diese Werte festlegt. Dadurch wird bezüglich der Verantwortlichkeiten sowohl der Begünstigten als auch der für die Durchführung der Kontrollen auf EU-Ebene zuständigen Akteure Klarheit geschaffen; dies kann als Vorbild für das Vorgehen auf nationaler Ebene dienen. Bei Verstößen gegen die Finanzierungsbedingungen wird die Kommission die Zusammenarbeit mit den Begünstigten des betreffenden Projekts unverzüglich einstellen und die Mittel gegebenenfalls wieder einziehen. Es ist wichtig, dass die Mitgliedstaaten die Kommission proaktiv unterrichten, wenn ihnen mögliche Risiken im Zusammenhang mit Organisationen zur Kenntnis gelangen, die EU-Mittel beantragen.

Vertragsverletzungsverfahren

Im Bereich der Sicherheit hat die Kommission zahlreiche Vertragsverletzungsverfahren durchgeführt. Beispielsweise wurde im Jahr 2023 eine ganze Reihe von Vertragsverletzungsverfahren wegen der Nichteinhaltung von Verpflichtungen gemäß der 2021 angenommenen Verordnung zur Bekämpfung der Verbreitung terroristischer Online-Inhalte[50] eingeleitet (16 Mitgliedstaaten); darüber hinaus richtete die Kommission im Laufe der Jahre 2022 und 2023 an 20 Mitgliedstaaten ergänzende Aufforderungsschreiben wegen der nicht ordnungsgemäßen Umsetzung der Richtlinie zur Bekämpfung des sexuellen Missbrauchs von

[50] Verordnung (EU) 2021/784 zur Bekämpfung der Verbreitung terroristischer Online-Inhalte.

Kindern aus dem Jahr 2011[51]. Eine erhebliche Zahl anhängiger Vertragsverletzungsverfahren betrifft Fälle, in denen die nationalen Rechtsvorschriften nicht mit der Richtlinie zur Terrorismusbekämpfung[52] aus dem Jahr 2017 in Einklang stehen oder die Vorschriften zur Erleichterung der Nutzung von Finanz- und sonstigen Informationen für die Verhütung, Aufdeckung, Untersuchung oder Verfolgung bestimmter Straftaten[53] nicht umgesetzt wurden. Weitere Vertragsverletzungsverfahren sind anhängig im Zusammenhang mit den Rechtsvorschriften über Feuerwaffen, den Vorschriften über in Drogen verwendete psychoaktive Substanzen, der Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln, der Bekämpfung von Geldwäsche, dem Austausch von Strafregisterinformationen zwischen den EU-Mitgliedstaaten und der Opferschutzrichtlinie. Für die Mitgliedstaaten, die vereinbarte Initiativen und Maßnahmen durchführen, wurde (technische und finanzielle) Unterstützung bereitgestellt, und die Kommission steht mit Blick auf eine bestmögliche Durchführung weiterhin für eine Zusammenarbeit mit den Mitgliedstaaten zur Verfügung.

Überwachung durch Schengen-Evaluierungen und das neue Governance-System

Der Schengen-Evaluierungs- und Überwachungsmechanismus hat weiterhin zur wirksamen Anwendung der Schengen-Vorschriften beigetragen, die auf die Erhöhung der Sicherheit im Raum ohne Kontrollen an den Binnengrenzen abzielen. Im Jahr 2023 wurden erste Evaluierungen im Rahmen des verbesserten Schengen-Evaluierungs- und Überwachungsmechanismus durchgeführt, bei denen strategische Schwachstellen mit grenzüberschreitenden Auswirkungen auf die Sicherheit und Gefahrenabwehr in der EU zeitnah ermittelt und behoben werden konnten. Darüber hinaus leitete die Kommission im Jahr 2023 eine thematische Schengen-Evaluierung zur Beurteilung der Vorgehensweisen der Mitgliedstaaten in die Wege, die bei der Bekämpfung des Drogenschmuggels in die EU und insbesondere des Drogenhandels im großen Stil ähnlichen Herausforderungen gegenüberstehen. Mit diesen Evaluierungen wurde eine stärkere und umfassendere Ausrichtung auf die Schengen-Sicherheitsaspekte eingeführt. Auf der Grundlage der Ergebnisse der regelmäßigen, thematischen und unangekündigten Evaluierungen legte der Rat im Juni 2023 die Prioritäten des Schengen-Zyklus für den Zeitraum 2023–2024 fest. In diesem Zusammenhang wurden Schwerpunktbereiche bestimmt, in denen zusätzliche Impulse erforderlich sind, um den Schengen-Raum sicherer und stärker zu machen. Die wirksame und zügige Umsetzung dieser Prioritäten und die verstärkte strategische Koordinierung im Schengen-Rat werden zur Folge haben, dass massiver gegen die organisierte Kriminalität vorgegangen und die grenzüberschreitende operative Zusammenarbeit intensiviert wird.

Aufgaben der Agenturen und Einrichtungen der EU

Partnerschaftliche Zusammenarbeit ist für die Durchführung der Initiativen im Rahmen der Sicherheitsunion unverzichtbar, da konkrete Ergebnisse nur durch die Arbeit unterschiedlicher nationaler und europäischer Behörden und Einrichtungen erzielt werden können. Beispielsweise ermöglicht EMPACT (die Europäische multidisziplinäre Plattform gegen kriminelle Bedrohungen) eine strukturierte, multidisziplinäre Zusammenarbeit der

[51] Richtlinie 2011/93/EU zur Bekämpfung des sexuellen Missbrauchs von Kindern.

[52] Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates.

[53] Richtlinie (EU) 2019/1153 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Festlegung von Vorschriften zur Erleichterung der Nutzung von Finanz- und sonstigen Informationen für die Verhütung, Aufdeckung, Untersuchung oder Verfolgung bestimmter Straftaten und zur Aufhebung des Beschlusses 2000/642/JI des Rates.

Mitgliedstaaten, die von allen Organen, Einrichtungen und Agenturen der EU (wie beispielsweise Europol, Frontex, Eurojust, CEPOL, OLAF und eu-LISA) unterstützt wird. Durch die im Rahmen von EMPACT – unter anderem von speziellen operativen Taskforces – durchgeführten Einsätze werden die Anstrengungen der Mitgliedstaaten und der operativen Partner zur Bekämpfung krimineller Netze und schwerer Kriminalität koordiniert. Alleine im Jahr 2022 wurden im Rahmen von EMPACT insgesamt 9 922 Festnahmen vorgenommen, Vermögenswerte und Bargeld im Wert von mehr als 180 Mio. EUR beschlagnahmt, 9 263 Ermittlungen eingeleitet, 4 019 Opfer identifiziert, mehr als 62 Tonnen Drogen beschlagnahmt, 51 hochrangige Ziele identifiziert und 12 hochrangige Zielpersonen festgenommen; darüber hinaus wurden Operationen im Zusammenhang mit dem Angriffskrieg gegen die Ukraine durchgeführt, die in erster Linie die Bekämpfung des Menschenhandels und die Eindämmung von Bedrohungen im Zusammenhang mit Feuerwaffen zum Gegenstand hatten.[54]

Frontex, die Europäische Agentur für die Sicherheit des Seeverkehrs (EMSA) und die Europäische Fischereiaufsichtsagentur (EFCA) intensivieren ihre Zusammenarbeit im Bereich der Küstenwache weiter, um die nationalen Behörden bei der Verbesserung der Sicherheit und Gefahrenabwehr auf See zu unterstützen. Diese Agenturen werden einen wichtigen Beitrag zur Umsetzung der EU-Strategie für maritime Sicherheit leisten.

Mit mehreren im Rahmen der Sicherheitsunion durchgeführten Initiativen wurden einschlägigen Agenturen neue Zuständigkeiten übertragen, was in einigen Fällen auch Auswirkungen auf die Humanressourcen hatte.

Agentur der Europäischen Union für Cybersicherheit (ENISA)

Im Hinblick auf die Abwehrbereitschaft und die Bewältigung von Vorfällen zur Verbesserung der Cybersicherheit hat die Kommission eine kurzfristige Maßnahme zur Unterstützung der Mitgliedstaaten in die Wege geleitet, in deren Rahmen der **Agentur der Europäischen Union für Cybersicherheit (ENISA)** Mittel aus dem Programm „Digitales Europa“ zugewiesen wurden, um die Abwehrbereitschaft und Reaktionsfähigkeit bei großen Cybersicherheitsvorfällen zu stärken. Mit dem im April 2023 angenommenen Vorschlag für das Cybersolidaritätsgesetz, der auf dieser Maßnahme aufbaut, könnten der ENISA nach seiner Annahme durch die gesetzgebenden Organe zusätzliche Aufgaben übertragen werden, wie beispielsweise der Betrieb und die Verwaltung der künftigen Cybersicherheitsreserve der Union oder die Erstellung von Berichten über die Überprüfung von Cybersicherheitsvorfällen großen Ausmaßes. Mit dem vorgeschlagenen Cyberresilienzgesetz würde der ENISA die Aufgabe übertragen, Meldungen von Herstellern über Schwachstellen in Produkten mit digitalen Elementen sowie über Vorfälle, die sich auf die Sicherheit dieser Produkte auswirken, entgegenzunehmen und an die zuständigen Computer-Notfallteams (Computer Security Incident Response Teams – CSIRTs) oder die zuständigen zentralen Anlaufstellen der Mitgliedstaaten weiterzuleiten. Des Weiteren soll die ENISA alle zwei Jahre einen technischen Bericht über aufkommende Trends im Zusammenhang mit Cybersicherheitsrisiken bei Produkten mit digitalen Elementen erstellen und der NIS-Kooperationsgruppe vorlegen.

Europäisches Kompetenzzentrum für Cybersicherheit

Das **Europäische Kompetenzzentrum für Cybersicherheit** bildet gemeinsam mit dem Netzwerk nationaler Koordinierungszentren das neue System der Union zur Unterstützung von

[54] EMPACT-Informationsblätter mit den Ergebnissen für 2022: https://www.consilium.europa.eu/media/65450/2023_225_empact-factsheets-2022_web-final.pdf.

Innovation und Industriepolitik im Bereich der Cybersicherheit. Durch dieses Ökosystem werden die Kapazitäten der Cybersicherheitstechnologiegemeinschaft gestärkt, die Forschungsexzellenz bewahrt und die Wettbewerbsfähigkeit der Cybersicherheitsbranche der Union verbessert. Das Europäische Kompetenzzentrum für Cybersicherheit und das Netzwerk nationaler Koordinierungszentren werden strategische Investitionsentscheidungen treffen und Ressourcen der Union, der Mitgliedstaaten und mittelbar auch der Industrie bündeln, um die technologischen und industriellen Cybersicherheitskapazitäten zu verbessern und auszubauen. Das Europäische Kompetenzzentrum für Cybersicherheit leistet somit einen entscheidenden Beitrag zur Erreichung der ehrgeizigen Cybersicherheitsziele der Programme „Digitales Europa“ und „Horizont Europa“.

Das Europäische Kompetenzzentrum für Cybersicherheit hat mehr als die Hälfte seines Personals eingestellt und wird in Kürze seinen Exekutivdirektor ernennen. Die bereits laufenden Arbeiten haben die Cybersicherheitskomponente des Programms „Digitales Europa“ und die Umsetzung der neuen strategischen Agenda[55] für die Entwicklung und den Einsatz von Technologien zum Gegenstand, in der die vorrangigen Maßnahmen zur Unterstützung von KMU bei der Entwicklung und Nutzung strategischer Technologien, Dienste und Prozesse im Bereich der Cybersicherheit, zur Unterstützung und Qualifizierung der Fachkräfte sowie zum Ausbau der Fachkenntnisse in den Bereichen Forschung, Entwicklung und Innovation im gesamten europäischen Cybersicherheitsökosystem festgelegt sind.

Europol

Mit seinem neuen Mandat wird **Europol** besser gerüstet sein, um die Mitgliedstaaten bei der Bekämpfung der organisierten Kriminalität zu unterstützen. Die Bekämpfung des Drogenhandels ist von oberster Priorität, da der Drogenhandel zunehmend an Bedeutung gewinnt und die Sicherheit der Bürgerinnen und Bürger der EU immer stärker beeinträchtigt. Nachdem der Rat der Europäischen Union am 15. Mai 2023 die entsprechende Ermächtigung erteilt hatte, wirkte die Kommission aktiv auf den Abschluss internationaler Abkommen mit Bolivien, Brasilien, Ecuador, Mexiko und Peru über den Austausch personenbezogener Daten mit Europol zur Verhütung und Bekämpfung von schwerer Kriminalität und Terrorismus hin.

Eurojust

Seit mehr als 20 Jahren leistet **Eurojust** den nationalen Behörden justizielle Unterstützung bei der Bekämpfung einer Vielzahl schwerer und komplexer grenzüberschreitender Straftaten und hat damit seine Position im Raum der Freiheit, der Sicherheit und des Rechts der EU gefestigt. Um die Zusammenarbeit in allen Bereichen zu intensivieren, handelt die Kommission gegenwärtig internationale Abkommen aus, mit denen die Zusammenarbeit zwischen Eurojust und 13 Drittländern[56] beim Austausch personenbezogener Daten zur Bekämpfung von organisierter Kriminalität und Terrorismus erleichtert werden soll. Die Verhandlungen mit Armenien und Libanon sind bereits abgeschlossen, die Verhandlungen mit Algerien und Kolumbien laufen, und die Verhandlungen mit Bosnien und Herzegowina wurden aufgenommen. Die Kommission fordert das Europäische Parlament und den Rat auf, die Abkommen mit diesen Ländern vor dem Ende der Wahlperiode abzuschließen, um die transnationale justizielle Zusammenarbeit zu intensivieren und die Bekämpfung der grenzüberschreitenden Kriminalität auszuweiten.

EUStA

[55] https://cybersecurity-centre.europa.eu/strategic-agenda_de

[56] Ägypten, Algerien, Argentinien, Armenien, Bosnien und Herzegowina, Brasilien, Israel, Jordanien, Kolumbien, Libanon, Marokko, Tunesien und Türkei.

Seit die **Europäische Staatsanwaltschaft (EUStA)** im Juni 2021 ihre operative Tätigkeit aufgenommen hat, hat sie sich als ein wirksamer Bestandteil des Instrumentariums der Union zur Ermittlung und Strafverfolgung bei Straftaten zum Nachteil des Unionshaushalts erwiesen; dies schließt Straftaten im Zusammenhang mit der Beteiligung an einer kriminellen Vereinigung ein, deren Schwerpunkt auf Straftaten zum Nachteil des Unionshaushalts liegt. Die Kommission ersucht die Mitgliedstaaten, die noch nicht an der Verstärkten Zusammenarbeit in Bezug auf die EUStA teilnehmen, sich so bald wie möglich an der EUStA zu beteiligen, damit diese ihr Potenzial zum Schutz der Steuergelder der EU-Bürgerinnen und -Bürger voll entfalten kann.

EUDA

Mit dem neuen Mandat, das im Juni 2023 von den gesetzgebenden Organen angenommen wurde, wird die Europäische Beobachtungsstelle für Drogen und Drogensucht (EMCDDA) zu einer vollwertigen Agentur – der **Drogenagentur der Europäischen Union (EUDA)** –, der eine größere Bedeutung zukommt. Die Agentur wird in der Lage sein, neuen Gesundheits- und Sicherheitsproblemen, die sich im Zusammenhang mit illegalen Drogen stellen, umfassender zu begegnen und einen wirksameren Beitrag zu der in den Mitgliedstaaten und auf internationaler Ebene geleisteten Arbeit zu erbringen. Die Erhebung, Analyse und Verbreitung von Daten wird weiterhin eine der wichtigsten Aufgaben der Agentur sein; dank ihres erweiterten Mandats wird sie jedoch auch in der Lage sein, generelle Kapazitäten zur Bewertung der Gefahrenlage bezüglich Gesundheit und Sicherheit zu entwickeln, neue Gefahren – auch im Zusammenhang mit dem Mischkonsum – zu erkennen, ihre Zusammenarbeit über die nationalen Kontaktstellen zu intensivieren und ein Netz von Laboren zu schaffen, die der Agentur forensische und toxikologische Informationen zur Verfügung stellen. Dies wird es der Agentur erleichtern, Warnmeldungen auszugeben, wenn besonders gefährliche Stoffe auf dem Markt in Erscheinung treten, und Sensibilisierungsmaßnahmen zu ergreifen.

Die Kommission fordert das Europäische Parlament und den Rat auf, die interinstitutionellen Verhandlungen über die folgenden anhängigen Dossiers zügig und in jedem Falle vor dem Ende der laufenden Wahlperiode des Europäischen Parlaments abzuschließen:

- Vorschlag für eine Neufassung der Haushaltsordnung.

Die Kommission fordert die Mitgliedstaaten auf,

- die Kommission proaktiv zu unterrichten, wenn ihnen mögliche Risiken im Zusammenhang mit Organisationen zur Kenntnis gelangen, die EU-Mittel beantragen,
- die Prioritäten des Schengen-Zyklus 2023–2024 für einen sichereren und stärkeren Schengen-Raum zügig umzusetzen,
- sich mit den gegen sie anhängigen Vertragsverletzungsverfahren zu befassen, um die ordnungsgemäße Umsetzung der betreffenden Rechtsvorschriften zu gewährleisten.

VII. Fazit

Die letzten drei Jahre waren von dem kontinuierlichen und entschlossenen Bemühen geprägt, die Idee der Schaffung einer Sicherheitsunion für die EU in die Praxis umzusetzen. In allen Bereichen der Sicherheitspolitik wurden enorme Fortschritte erzielt. Angesichts der in einem

ständigen Wandel befindlichen Bedrohungen müssen die Anstrengungen nun mit neuem Schwung weitergeführt werden. Die Arbeit am Rechtsrahmen muss rechtzeitig vor dem Ende der Wahlperiode im Frühjahr 2024 abgeschlossen werden. Die Mitgliedstaaten sind fortwährend dafür verantwortlich, neue Rechtsvorschriften umzusetzen, durchzuführen und anzuwenden. Für die Durchführung sind konzertierte Anstrengungen – unter anderem mit Unterstützung der Agenturen der EU – und sehr häufig auch eine noch intensivere Zusammenarbeit mit den internationalen Partnern der EU vonnöten.

Nur wenn alle Beteiligten gemeinsam und entschlossen vorgehen, wird es möglich sein, in der Union das Maß an Sicherheit und Gefahrenabwehr zu erreichen, das die Bürgerinnen und Bürger erwarten – unter den gegebenen Umständen sollten alle Akteure vorrangig darum bemüht sein, ihren Beitrag zur Stärkung der Sicherheit in der EU zu leisten.