Rat der
Europäischen Union

Brüssel, den 25. Juni 2021
(OR. en)

10212/21

JAI 786	**DROIPEN 115**
COSI 130	**COPEN 295**
ENFOPOL 249	**FREMP 194**
ENFOCUSTOM 101	**JAIEX 82**
IXIM 133	**CFSP/PESC 646**
CT 89	**COPS 251**
CRIMORG 65	**HYBRID 37**
FRONT 264	**DISINFO 18**
ASIM 45	**TELECOM 276**
VISA 146	**DIGIT 77**
CYBER 187	**COMPET 513**
DATAPROTECT 178	**RECH 324**
CATS 43	

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	23. Juni 2021
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2021) 440 final
Betr.:	MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT Zweiter Fortschrittsbericht über die Umsetzung der EU-Strategie für eine Sicherheitsunion

Die Delegationen erhalten in der Anlage das Dokument COM(2021) 440 final.

Anl.: COM(2021) 440 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 23.6.2021
COM(2021) 440 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

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

I. Einleitung

Im Juli letzten Jahres nahm die Kommission die EU-Strategie für eine Sicherheitsunion für den Zeitraum 2020 bis 2025[1] an, die gezielte Maßnahmen in Schwerpunktbereichen vorsieht, in denen die EU einen zusätzlichen Nutzen gegenüber einzelstaatlichen Anstrengungen bewirken kann. Die Strategie baut auf der Europäischen Sicherheitsagenda für den Zeitraum 2015–2020 auf, setzt jedoch einen neuen Schwerpunkt und enthält einen koordinierten Ansatz für die verschiedenen Bereiche der Sicherheitspolitik, damit sichergestellt wird, dass die EU auf die sich rasch verändernde Bedrohungslage reagieren kann. Mit dieser Strategie soll sichergestellt werden, dass die EU ihre Rolle bei der Gewährleistung der Sicherheit der Bürgerinnen und Bürger und ihrer Grundrechte uneingeschränkt wahrnimmt, indem sie die gegenwärtigen Risiken angeht und sich auf neue Herausforderungen einstellt, und dass die Werte, die die europäische Lebensweise bestimmen, verwirklicht werden.

Zu diesem dynamischen Wandel kam die COVID-19-Pandemie hinzu. In diesem Zusammenhang ergaben sich neue Möglichkeiten für Online-Kriminalität, wurde die Cyberkriminalität befördert und wurde einer zunehmenden Fälschung und Verbreitung minderwertiger Waren, organisierter Eigentumskriminalität und verschiedenen Arten von Betrug[2] die Tür geöffnet. Einige dieser Delikte haben die Gesundheitssysteme und die Erbringung von Gesundheitsdienstleistungen unmittelbar untergraben. Einige kriminelle Aktivitäten werden zwar wieder auf den Stand vor der Pandemie zurückgehen, doch andere werden sich durch die Pandemie grundlegend verändern.[3]

In der Strategie sind Maßnahmen festgelegt, die über einen Zeitraum von fünf Jahren zu ergreifen sind. Innerhalb eines Jahres wurden zahlreiche Initiativen auf den Weg gebracht.[4] Die Kommission hat eine EU-Agenda zur Terrorismusbekämpfung und Initiativen zur Bekämpfung der organisierten Kriminalität, des Menschenhandels, des Drogenhandels, des sexuellen Missbrauchs von Kindern und des unerlaubten Handels mit Feuerwaffen sowie eine neue Cybersicherheitsstrategie der EU angenommen. Ferner hat die Kommission wichtige neue Rechtsvorschriften zur Stärkung von Europol, zum Schutz kritischer physischer und digitaler Infrastrukturen und zur Bekämpfung der Verbreitung von Material über den sexuellen Missbrauch von Kindern vorgelegt. Das Europäische Parlament und der Rat haben dieses Programm vorangebracht und Beschlüsse zu wichtigen Dokumenten, insbesondere zu terroristischen Online-Inhalten und zur Bekämpfung des sexuellen Missbrauchs von Kindern im Internet, erlassen. Die Arbeiten an den in der Strategie umrissenen Rechtsvorschriften sollten rasch voranschreiten, bei gleichzeitiger Wahrung der ehrgeizigen Zielsetzungen.

Im Juni nahm die Kommission eine neue „Strategie für einen reibungslos funktionierenden und resilienten Schengen-Raum“[5] an, die wirksame Maßnahmen in den Bereichen Sicherheit sowie polizeiliche und justizielle Zusammenarbeit vorsieht, damit dieser Raum der Freiheit, der Sicherheit und des Rechts funktioniert und die EU auch ohne Kontrollen an den Binnengrenzen weiterhin entschlossen gegen Sicherheitsbedrohungen vorgehen kann. Im Berichtszeitraum erzielten die beiden gesetzgebenden Organe eine Einigung über die Fonds, mit denen viele der Maßnahmen im Rahmen der Sicherheitsunion unterstützt werden; dies

---

1 Mitteilung der Kommission – EU-Strategie für eine Sicherheitsunion (COM(2020) 605 final).
2 Auch im Hinblick auf lebensrettende Arzneimittel, Medizinprodukte und Impfstoffe.
3 Bericht 2021 über die Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität in der EU (SOCTA), Europol.
4 Siehe Anhang 2 (Fahrplan für die Umsetzung).
5 COM(2021) 277 final.

betraf insbesondere den aufgestockten Fonds für die innere Sicherheit (ISF) und das Instrument für Grenzmanagement und Visa (BMVI) im Rahmen des Fonds für integriertes Grenzmanagement (IBMF).

Der Erfolg der Strategie für eine Sicherheitsunion hängt von der Qualität ihrer Umsetzung ab.[6] Dies erfordert ein uneingeschränktes Engagement der nationalen Behörden und eine ständige Zusammenarbeit zwischen allen Akteuren, die sich mit der inneren und äußeren Sicherheit Europas befassen, einschließlich der EU-Agenturen. Durch eine verstärkte Zusammenarbeit zwischen den mit Sicherheitsthemen befassten Akteuren wird ein inklusiver, gesamtgesellschaftlicher Ansatz vorangetrieben.

In diesem zweiten Fortschrittsbericht zur EU-Strategie für eine Sicherheitsunion, der sich auf den Zeitraum seit dem ersten Bericht[7] vom 9. Dezember 2020 bezieht, werden die Fortschritte bei allen vier Säulen der Strategie dargestellt: ein zukunftsfähiges Sicherheitsumfeld, die Bewältigung sich wandelnder Bedrohungen, der Schutz der Europäerinnen und Europäer vor Terrorismus und organisierter Kriminalität und eine starke europäische Sicherheitsgemeinschaft. Darin wird dargelegt, wie die betreffende Arbeit voranschreitet, auch unter Beleuchtung des spezifischen Beitrags der EU-Agenturen.

II. Ein zukunftsfähiges Sicherheitsumfeld

1. Schutz und Widerstandsfähigkeit kritischer Infrastruktur

Der Schutz und die Widerstandsfähigkeit kritischer physischer und digitaler Infrastrukturen sind für das Funktionieren moderner Gesellschaften und die europäische Lebensweise von größter Bedeutung. Nie ist diese Aussage zutreffender als in Zeiten einer Notlage im Bereich der öffentlichen Gesundheit. Bedrohungen, Vorfälle und Angriffe in Bezug auf kritische Infrastrukturen können zu weitreichenden Beeinträchtigungen führen.

In Pandemiezeiten ist Widerstandsfähigkeit wichtiger denn je

In einer Zeit, in der die Gesundheitsinfrastruktur bereits unter Druck steht, können Cybervorfälle, die sich gegen Krankenhäuser, medizinische Einrichtungen und umfassende Gesundheitsdienstleistungen richten, besonders dramatische Folgen haben.

Irland wurde kürzlich von einer Reihe schwerwiegender Cyberangriffe auf sein Gesundheitssystem getroffen, wobei Hacker sowohl das Gesundheitsministerium als auch die irische Gesundheitsorganisation, Health Service Executive, angegriffen haben.

Die nationalen Datenbanken des Frühwarn- und Reaktionssystems (EWRS)[8], die die Reaktion des Gesundheitssektors unterstützen, waren Ziel von Eindringungsversuchen und Ransomware-Angriffen.[9]

---

6 Anhang 1 gibt einen Überblick über den Stand der Umsetzung der Rechtsvorschriften im Bereich Sicherheit.

7 Mitteilung der Kommission an das Europäische Parlament und den Rat – Erster Fortschrittsbericht zur EU-Strategie für die Sicherheitsunion (COM(2020) 797 final).

8 Das EWRS ist ein EU-weites Schnellwarnsystem zur Meldung schwerwiegender grenzüberschreitender Gesundheitsgefahren, das gemäß dem Beschluss Nr. 1082/2013/EU eingerichtet wurde (https://ec.europa.eu/health/security/surveillance_early-warning_de).

9 Die Datensicherheit des EWRS, für die das Europäische Zentrum für die Prävention und die Kontrolle von Krankheiten (ECDC) zuständig ist, war nicht betroffen, wird aber verstärkt.

Der Cyberangriff auf die Europäische Arzneimittel-Agentur hat gezeigt, dass der unrechtmäßige Zugriff auf Dokumente im Zusammenhang mit COVID-19-Arzneimitteln und -Impfstoffen dramatische Auswirkungen haben kann, wenn diese Dokumente im Internet veröffentlicht werden.

In einem anderen Bereich, außerhalb des Gesundheitsbereichs, der den Alltag der Bürgerinnen und Bürger berührt, zeigte der Ransomware-Angriff auf die Colonial Pipeline in den USA ebenfalls, wie wichtig der Schutz kritischer physischer Infrastrukturen und die damit einhergehende Cybersicherheit sind.[10]

Das Ausmaß der potenziellen Risiken zeigt, dass die Abwehrbereitschaft auf nationaler und EU-Ebene dringend verbessert werden muss, indem robuste Kapazitäten aufgebaut werden, um solche Bedrohungen zu verhindern, zu erkennen und zu mindern und Offline- und Online-Krisen zu bewältigen.

Die EU-Rechtsvorschriften in diesem Bereich, insbesondere die Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie)[11] und die Richtlinie über europäische kritische Infrastrukturen (ECI-Richtlinie)[12], waren eine gute Grundlage für die Reaktion auf die jüngsten Vorfälle. Im Falle des Ransomware-Angriffs auf die irische Gesundheitsorganisation nutzten nationale Cybersicherheitsexperten im Rahmen der NIS-Richtlinie eingerichtete Foren[13], um sowohl auf technischer als auch auf politischer Ebene Informationen auszutauschen. So konnten die irischen Behörden Unterstützung erhalten, und andere Mitgliedstaaten waren in der Lage, ihre Abwehrbereitschaft im Hinblick auf solche Angriffe zu verbessern.

Gleichzeitig zeigt die zunehmende Häufigkeit und Intensität von Bedrohungen, dass der derzeitige Rechtsrahmen seinen Zweck nicht erfüllt. Die Evaluierung[14] der Umsetzung der NIS-Richtlinie ergab, dass ihr Anwendungsbereich weder den heutigen Grad der Digitalisierung und Verflechtung noch die wechselseitige Abhängigkeit wichtiger wirtschaftlicher und gesellschaftlicher Sektoren widerspiegelt. Darüber hinaus unterliegen einige öffentliche und private Einrichtungen, die zu wesentlichen Sektoren gehören, entweder nicht der Richtlinie oder müssen nicht harmonisierten Verpflichtungen bezüglich Cybersicherheit und die Meldung von Sicherheitsvorfällen nachkommen. Bei der Evaluierung[15] der Umsetzung der ECI-Richtlinie hat sich herausgestellt, dass in dieser Richtlinie im Gegensatz zur Resilienz der Betreiber der Schutz von Anlagen nur in einer sehr begrenzten Anzahl von Sektoren im Mittelpunkt steht. Bei beiden Evaluierungen wurden unterschiedliche Ansätze sowie Mängel auf nationaler Ebene festgestellt.

---

[10] Die Colonial Pipeline, eine wichtige Pipeline, über die 45 % des an der Ostküste der USA verbrauchten Öls transportiert werden, war im Mai 2021 Ziel eines Cyberangriffs mit Ransomware, durch den die Öllieferungen tagelang unterbrochen waren.

[11] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.

[12] Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern.

[13] Netzwerk der Reaktionsteams für Computersicherheitsverletzungen (Computer Security Incident Response Teams – CSIRTs) und Kooperationsgruppe.

[14] SWD(2020) 345 final, Part II.

[15] SWD(2019) 310 final.

Im Dezember 2020 schlug die Kommission daher zwei wichtige Rechtsakte vor: eine Richtlinie über die **Resilienz kritischer Einrichtungen** (CER-Richtlinie)[16] und eine überarbeitete Richtlinie über Maßnahmen **für ein hohes gemeinsames Cybersicherheitsniveau in der Union** (überarbeitete NIS-Richtlinie)[17]. Beide Richtlinien haben einen breiten Anwendungsbereich und decken dieselben zehn wesentlichen Bereiche ab: Verkehr, Energie, Banken, Finanzmarktinfrastrukturen, Gesundheit, Trinkwasser, Abwasser, digitale Infrastruktur, öffentliche Verwaltung und Raumfahrt. Für diese Sektoren werden in der CER-Richtlinie Maßnahmen zur Schaffung eines Rahmens für die physische Resilienz vorgeschlagen, der Mindeststandards festlegt und somit Flexibilität ermöglicht, um nationalen Besonderheiten Rechnung zu tragen. Mit der vorgeschlagenen überarbeiteten NIS-Richtlinie soll ein horizontaler Standard für die Anforderungen an die Cybersicherheit im Binnenmarkt festgelegt und der Schwerpunkt verstärkt auf die Sicherheit der Lieferkette gelegt werden. Dadurch werden neue Instrumente für eine koordinierte Behandlung von Schwachstellen bzw. die Offenlegung von Schwachstellen sowie für eine wirksamere Reaktion auf Sicherheitsvorfälle und ein effektiveres Krisenmanagement eingeführt. Außerdem werden die Verpflichtungen in Bezug auf die Meldung von Sicherheitsvorfällen durch präzisere Bestimmungen den Meldeprozess, den Inhalt und den Zeitplan betreffend gestrafft.

Angesichts der sich ständig wandelnden Bedrohungen unserer kritischen Infrastrukturen ersucht die Kommission die beiden gesetzgebenden Organe, hohe Ambitionen an den Tag zu legen und eine reibungslose Annahme dieser beiden Vorschläge unter Wahrung ihrer Kohärenz und Komplementarität sicherzustellen. Sämtliche Fortschritte bei der Annahme dieser Vorschläge müssen auch im Einklang mit dem Vorschlag der Kommission aus dem Jahr 2020 über die Betriebsstabilität digitaler Systeme des Finanzsektors[18] stehen, mit dem die strategische Autonomie Europas im Finanzdienstleistungsbereich gestärkt werden und Europa auf diese Weise mehr Kompetenzen zur Regulierung und Beaufsichtigung des Finanzsystems im Interesse der Finanzstabilität erhalten soll.

Initiativen im Energiesektor
Um spezifischere Schwachstellen anzugehen, sind sektorspezifische Initiativen erforderlich. In diesem Zusammenhang sind wichtige Entwicklungen im Energiesektor hervorzuheben. Im Rahmen der Überwachung der Auswirkungen der COVID-19-Krise im Energiesektor wurde im Mai 2021 eine Studie abgeschlossen, in der die für die Sicherheit der Energieversorgung und die Energiewende entscheidenden Energieversorgungsketten ermittelt und Maßnahmen zur Verbesserung der Widerstandsfähigkeit im Fall von Pandemien und anderen Bedrohungsszenarien vorgeschlagen wurden. Die Ergebnisse dieser Studie werden in andere relevante Arbeitsbereiche einfließen, einschließlich in die Arbeit der NIS-Kooperationsgruppe für den Energiesektor. Das Thematische Netz für den Schutz kritischer Energieinfrastrukturen (Thematic Network on Critical Energy Infrastructure Protection) setzte seine Arbeit in Bezug auf die Herausforderungen für den Schutz kritischer

[16] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Resilienz kritischer Einrichtungen (COM(2020) 829 final).
[17] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 (COM(2020) 823 final).
[18] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Betriebsstabilität digitaler Systeme des Finanzsektors und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014 und (EU) Nr. 909/2014 (COM(2020) 595 final).

Energieinfrastrukturen fort und befasste sich mit Themen wie Risikobewertungen, Informationsaustausch und Finanzierung von Sicherheitsmaßnahmen.[19]

Im Januar 2021 leitete die Kommission zusammen mit der Agentur für die Zusammenarbeit der Energieregulierungsbehörden (ACER) das förmliche Verfahren für die Festlegung eines speziellen Netzkodex zur **Cybersicherheit für grenzüberschreitende Stromflüsse** ein. Dieser Netzkodex wird im Einklang mit dem in der NIS-Richtlinie festgelegten horizontalen Rahmen gemeinsame Mindestanforderungen für Planung, Überwachung, Berichterstattung und Krisenmanagement enthalten. Im Hinblick auf die **Risikovorsorge im Elektrizitätssektor** haben die Mitgliedstaaten im April 2021 eine Konsultation zur Kohärenz ihrer Entwürfe von Risikovorsorgeplänen auf den Weg gebracht. Diese Pläne umfassen Maßnahmen zur Vorbeugung und Eindämmung von Stromversorgungskrisen und beruhen auf nationalen Szenarien für Stromversorgungskrisen, die von den einzelnen Mitgliedstaaten ermittelt wurden, sowie auf den vom Europäischen Netz der Fernleitungsnetzbetreiber im September 2020 ermittelten regionalen Szenarien für Stromversorgungskrisen. Diese Szenarien schließen ebenfalls Cyberangriffe, Pandemien und extreme Wetterereignisse ein.

2. Cybersicherheit

Der digitale Wandel der Gesellschaft, der durch die COVID-19-Krise verstärkt wurde, bringt neue Herausforderungen mit sich, die innovative Antworten erfordern. In den letzten Monaten ist die Zahl der Cyberangriffe weiter gestiegen, wobei die von einer Vielzahl von Quellen sowohl innerhalb als auch außerhalb der EU stammenden Angriffe immer komplexer werden. Umfassende Datenschutzverletzungen und jüngste Cyberangriffe wie die massive Cyberattacke auf SolarWinds[20] verdeutlichen, wie hoch die Risiken für die Gesellschaft sind, wenn es uns nicht gelingt, die Cybersicherheit grundlegend zu verändern. Die EU muss sich darum bemühen, ihre Regierungen, Bürgerinnen und Bürger und Unternehmen vor Cyberbedrohungen zu schützen und gleichzeitig ein offenes und globales Internet zu gewährleisten. Wichtige Schritte wurden unternommen, um die Vision zu verwirklichen, dass alle Unionsbürgerinnen und -bürger in der Lage sind, ihr digitales Leben unter Nutzung eines globalen und offenen Internets auf sichere Weise zu führen.

Im Dezember 2020 legten die Kommission und die Hohe Vertreterin eine neue EU-Strategie für Cybersicherheit[21] vor. Als Schlüsselelement für die Gestaltung der digitalen Zukunft Europas, den Aufbauplan für Europa und die EU-Strategie für eine Sicherheitsunion soll diese Cybersicherheitsstrategie die kollektive Abwehrfähigkeit gegen Cyberbedrohungen stärken und dazu beitragen, dass alle Bürgerinnen und Bürger und Unternehmen die Vorzüge vertrauenswürdiger und zuverlässiger Dienste und digitaler Instrumente uneingeschränkt nutzen können. Der Cyberraum sollte global, offen, stabil und sicher bleiben. Die Strategie stützt sich auf drei Hauptsäulen: 1) Resilienz, technologische Souveränität und Führungsrolle, 2) Aufbau operativer Kapazitäten zur Prävention, Abschreckung und Reaktion und 3)

---

[19] Die Gespräche mit den Betreibern wurden auf die Mitgliedstaaten ausgeweitet, wobei zwischen März und Juni 2021 eine technische Runde bilateraler Gespräche stattfand.

[20] SolarWinds, ein großes US-amerikanisches IT-Unternehmen, war Ziel eines Cyberangriffs, von dem auch die Kunden des Unternehmens betroffen waren. Indem der Angriff monatelang unentdeckt blieb, erhielten Hacker Zugang zu Tausenden von Unternehmen und Regierungsstellen, die Produkte von SolarWinds einsetzten.

[21] Gemeinsame Mitteilung an das Europäische Parlament und den Rat – Die Cybersicherheitsstrategie der EU für die digitale Dekade (JOIN(2020) 18 final).

Förderung eines globalen offenen Cyberraums durch verstärkte Zusammenarbeit. Sie befasst sich erstmals mit der Cybersicherheit der Organe, Einrichtungen und sonstigen Stellen der EU. Der Rat hat Schlussfolgerungen zur Cybersicherheitsstrategie angenommen[22], mit denen die wichtigsten strategischen Initiativen zur Umsetzung gebilligt werden. Die Umsetzung dieser Strategie läuft derzeit, und ein detaillierter Überblick über den Stand der Umsetzung findet sich in einem spezifischen Durchführungsbericht[23].

Eine wichtige Initiative, die in den politischen Leitlinien der Kommission angekündigt wurde und in der Cybersicherheitsstrategie weiterverfolgt wird, ist der Aufbau einer **Gemeinsamen Cyber-Einheit**. Nach Konsultation der Mitgliedstaaten hat die Kommission zusammen mit diesem Bericht eine Empfehlung angenommen, in der der Prozess, die Etappenziele und der Zeitplan für den Aufbau der Gemeinsamen Cyber-Einheit genauer festgelegt werden sollen.[24] Die Gemeinsame Cyber-Einheit soll alle Cybersicherheitsgemeinschaften zusammenbringen, d. h. zivile, Strafverfolgungs-, Diplomatie- und Cyberabwehrgemeinschaften. Als Plattform für eine sichere und schnelle operative und technische Zusammenarbeit zwischen Stellen der EU und Behörden der Mitgliedstaaten baut die Gemeinsame Cyber-Einheit auf bestehenden Strukturen, Ressourcen und Fähigkeiten auf und bewirkt einen zusätzlichen Nutzen. Sie wird in einem vierstufigen Prozess aufgebaut, der die Ermittlung der verfügbaren operativen Kapazitäten der EU, die Ausarbeitung von Plänen zur Reaktion auf Sicherheitsvorfälle und von Krisenreaktionsplänen auf nationaler und EU-Ebene sowie die Ausweitung der Tätigkeiten zur Begründung der Zusammenarbeit mit privaten Einrichtungen umfasst. Die Gemeinsame Cyber-Einheit soll bis zum 30. Juni 2023 voll funktionsfähig sein.

Mit dem Ziel, die **Detektionsfähigkeiten** weiter zu verbessern und KI-gestützte Instrumente zu nutzen, um die EU vor Cyberangriffen zu schützen, erhöhen die Mitgliedstaaten – dank der Mittel im Rahmen der Aufbau- und Resilienzfazilität – derzeit ihre Investitionen in **Sicherheitseinsatzzentren** (Security Operation Centres – SOC). Die Kommission ergänzt die Anstrengungen der Mitgliedstaaten durch Mittelzuweisungen aus dem Programm „Digitales Europa“.

Cybersicherheit von 5G-Netzen

Im Rahmen der Cybersicherheitsstrategie hat die Kommission angesichts ihrer zentralen Rolle bei der Verwirklichung des digitalen Wandels der Wirtschaft und der Gesellschaft der EU drei Hauptziele für die künftige Arbeit in Bezug auf die Cybersicherheit von 5G-Netzen festgelegt: i) Gewährleistung der fortschreitenden EU-weiten Konvergenz der Risikominderungsansätze, ii) Unterstützung des kontinuierlichen Wissensaustauschs und Kapazitätsaufbaus und iii) Förderung der Resilienz der Lieferketten und anderer strategischer Sicherheitsziele der EU. Diese Ziele beruhen auf einem Bericht über 5G-Cybersicherheit[25], in dem die gemeinsame intensive Arbeit der Mitgliedstaaten und der Kommission mit Unterstützung der Agentur der Europäischen Union für Cybersicherheit (ENISA) überprüft wurde und in dem bestätigt wurde, dass seit der Einigung über das EU-Instrumentarium für Maßnahmen zur Risikominderung[26] erhebliche Fortschritte erzielt wurden. Weitere

[22] Cybersicherheit: Rat nimmt Schlussfolgerungen zur Cybersicherheitsstrategie der EU an – Consilium (europa.eu)
[23] JOIN(2021) 14 final.
[24] C(2021) 4520 final.
[25] SWD(2020) 357 final.
[26] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

Einzelheiten zum Stand der Umsetzung des EU-Instrumentariums sind dem Durchführungsbericht zur Cybersicherheitsstrategie[27] zu entnehmen.

Ein Cybersicherheitsökosystem
Um zur Schaffung eines vernetzten, europaweiten Cybersicherheitsökosystems im Bereich der Industrie und Forschung beizutragen, wurde im Mai 2021 eine Verordnung zur Einrichtung des **Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit** und des **Netzwerks nationaler Koordinierungszentren**[28] erlassen. Mit dieser Verordnung sollen die europäischen Cybersicherheitskapazitäten gestärkt, Forschungsexzellenz gefördert und die Wettbewerbsfähigkeit der Industrie der Union in diesem Bereich verbessert werden.[29] Die Kommission arbeitet bereits mit den rumänischen Behörden zusammen, um die Einrichtung des Zentrums in Bukarest vorzubereiten. Im Rahmen des Aktionsplans für Synergien zwischen der zivilen, der Verteidigungs- und der Weltraumindustrie[30] bemüht sich die Kommission um eine stärkere gegenseitige Bereicherung zwischen der Arbeit des Zentrums, dem Europäischen Verteidigungsfonds und dem EU-Weltraumprogramm im Bereich der Cybersicherheit und Cyberverteidigung.

Mit dem Rechtsakt zur Cybersicherheit[31] wurde ein EU-weiter **Rahmen für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen** eingeführt. In der EU tätige Unternehmen profitieren davon, dass sie ihre IKT-Produkte, -Prozesse und -Dienste nur einmal zertifizieren lassen können, wobei diese Zertifikate in der gesamten Europäischen Union anerkannt werden. Die Kommission hat die ENISA bereits gebeten, drei Schemata für die Cybersicherheitszertifizierung auszuarbeiten: das europäische Schema für Common Criteria, das europäische Schema für Cloud-Computing-Dienste und das europäische Schema für 5G-Netze.[32]

Internationale Dimension
Die Cybersicherheitsstrategie enthält Vorschläge, um böswillige Cyberaktivitäten weiter zu verhindern, davon abzuschrecken und darauf zu reagieren, indem verantwortungsvolles staatliches Handeln der internationalen Partner der EU im Cyberraum[33] gefördert, der Rahmen für eine gemeinsame diplomatische Reaktion der Union auf böswillige Cyberaktivitäten („Cyber Diplomacy Toolbox“)[34] gestärkt, die Koordinierung und Zusammenarbeit der EU im Bereich der Cyberabwehr ausgeweitet und die Cyberabwehrfähigkeiten durch den EU-Politikrahmen für die Cyberabwehr[35] ausgebaut

---

27 JOIN(2021) 14 final.
28 Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021.
29 Dazu entscheidet das Kompetenzzentrum insbesondere über die Mittelverwaltung für die Cybersicherheit aus den Programmen „Digitales Europa“ und „Horizont Europa“ sowie aus den Mitgliedstaaten.
30 COM(2021) 70 final vom 22.2.2021.
31 Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit).
32 Der Stand der Schemata wird im fortlaufenden Arbeitsprogramm der Union beschrieben werden.
33 Insbesondere durch Vorantreiben des Vorschlags für ein Aktionsprogramm zur Schaffung einer ständigen Infrastruktur für konkrete Maßnahmen zur Förderung eines verantwortungsvollen staatlichen Handelns im Cyberraum.
34 Beschluss (GASP) 2020/1127 des Rates, Beschluss (GASP) 2020/1537 des Rates und Beschluss (GASP) 2020/651 des Rates als Teil des Dokuments 9916/17.
35 Siehe Ratsdokument 14413/18.

werden. Die Hohe Vertreterin bereitet derzeit in Absprache mit der Kommission und im Einklang mit den Zielen des Strategischen Kompasses eine Überprüfung dieser Rahmen vor. Im Mai organisierte der Europäische Auswärtige Dienst (EAD) eine szenariobasierte Diskussion mit den Mitgliedstaaten und internationalen Partnern, um das gegenseitige Verständnis diplomatischer Optionen zur Verhinderung und Abschreckung von und zur Reaktion auf böswillige Cyberaktivitäten zu verbessern und Möglichkeiten für eine weitere Stärkung der internationalen Zusammenarbeit zu ermitteln.

Außerhalb Europas wird die Cybersicherheit in den östlichen Nachbarländern, in Afrika, Asien, Lateinamerika und der Karibik durch spezielle Kooperationsprojekte unterstützt, um europäisches Fachwissen für den Aufbau von Cyberkapazitäten zu mobilisieren und die Sicherheit und Widerstandsfähigkeit kritischer Infrastrukturen und Netzwerke zu erhöhen.[36] Mit dem Pakt für die zivile GSVP (Gemeinsame Sicherheits- und Verteidigungspolitik)[37] wurde die Cybersicherheit ebenfalls als einer der vorrangigen Bereiche für zivile GSVP-Missionen aufgenommen.

Um zu verhindern, dass Technologien für digitale Überwachung außerhalb der EU unter Verletzung der Menschenrechte eingesetzt werden, unterstützt die neue Ausfuhrverordnung[38] eine umfassende Modernisierung der EU-Vorschriften über die Ausfuhr von Gütern mit doppeltem Verwendungszweck[39]. Die neue Verordnung bietet der EU die Grundlage für die Durchführung wirksamer Ausfuhrkontrollen von Technologien für digitale Überwachung und zur Bewältigung von Sicherheitsrisiken im Zusammenhang mit dem weltweiten Handel mit neu entstehenden Technologien.

3. Schutz des öffentlichen Raums

In den letzten Jahren war der öffentliche Raum in der EU Ziel beispielloser Terroranschläge auf die Öffentlichkeit. Zu den aufkommenden Risiken für den öffentlichen Raum gehört die zunehmende Verbreitung von **Drohnen**. Unbemannte Luftfahrzeugsysteme können von böswilligen Akteuren genutzt werden, um Überwachungen vorzunehmen, den Betrieb kritischer Infrastrukturen zu unterbrechen oder Ziele von hohem Wert anzugreifen. Im April verabschiedete die Kommission einen **Rahmen für das europäische Konzept des Verkehrsmanagements unbemannter Luftfahrzeuge** (U-Space)[40], um den Behörden die Unterscheidung zwischen kooperativen und nicht kooperativen, potenziell böswilligen Drohnen zu erleichtern. Darüber hinaus unterstützt die Kommission die Erarbeitung von Leitfäden durch die Agentur der Europäischen Union für Flugsicherheit, finanziert innovative Projekte und Studien zur Drohnenabwehr und baut Brücken zwischen verschiedenen betroffenen Sektoren (Strafverfolgung, Luftfahrt, kritische Infrastruktur, Gefängnisse, Zoll/Grenzen, persönlicher Schutz, Organisatoren von Massenveranstaltungen) und anderen Interessenträgern. Für ein besser koordiniertes Vorgehen bei der Erprobung verschiedener Technologien zur Drohnenabwehr wurde ein einschlägiges europäisches Programm aufgelegt.

---

[36] Beispiele hierfür sind unter anderem die Projekte „Cyber4Dev“, „EU4Digital“ und „EU CyberNet“.

[37] Dokument 14305/18 vom 19. November 2018.

[38] Verordnung des Europäischen Parlaments und des Rates über eine Unionsregelung für die Kontrolle der Ausfuhr, der Vermittlung, der technischen Unterstützung der Durchfuhr und der Verbringung betreffend Güter mit doppeltem Verwendungszweck (Neufassung), 19. Mai 2021.

[39] Hierbei handelt es sich um Waren, Software oder Technologie, die sowohl für zivile als auch für militärische Anwendungen verwendet werden können.

[40] Durchführungsverordnungen C/2021/2671, C/2021/2672 und C/2021/2673 der Kommission.

Die Erarbeitung von Leitlinien zur Ermittlung und Reduzierung von Schwachstellen im öffentlichen Raum und zur Gewährleistung der eingebauten Sicherheit wird fortgesetzt. Im Rahmen des Instruments für die finanzielle Unterstützung der polizeilichen Zusammenarbeit, der Kriminalprävention und Kriminalitätsbekämpfung und des Krisenmanagements läuft ein mit 20 Mio. EUR ausgestattetes Programm, mit dem der **Schutz vor terroristischer Bedrohung von Gotteshäusern und anderen öffentlichen Räume**n verbessert werden soll, wobei der Schwerpunkt auf großen Sportstätten liegt. Im März hielt die Kommission eine Konferenz über die neuen Projekte ab, die 2021 starten sollen. Des Weiteren unterstützt die Kommission nationale, regionale und städtische Behörden und Betreiber öffentlicher Räume beim Austausch bewährter Verfahren, beim Aufbau von Netzwerken und bei der EU-weiten Zusammenarbeit[41] im Rahmen der EU-Städteagenda und durch Aktivitäten im Rahmen des Europäischen Fonds für regionale Entwicklung[42].

Der 2018 angenommene Aktionsplan für **Sicherheit im Schienenverkehr**[43] enthält konkrete Maßnahmen zur Verbesserung der Sicherheit im Schienenpersonenverkehr und wurde inzwischen vollständig umgesetzt. Die EU-Plattform für die Sicherheit im Schienenpersonenverkehr[44] hat eine Reihe von Best-Practice-Dokumenten zu Risikobewertung, Insider-Bedrohungen und Detektionstechnologien angenommen, um eine engere Zusammenarbeit zwischen den Mitgliedstaaten zu fördern und die Leistung im Bereich der Sicherheit im Schienenverkehr zu verbessern.

III. Bewältigung sich wandelnder Bedrohungen

1. Cyberkriminalität

Die Auswirkungen der Pandemie auf die Cyberkriminalität[45]

Kriminelle haben sich die aus Telearbeit und der verstärkten Nutzung von Online-Diensten ergebenden Veränderungen schnell zunutze gemacht und ihre illegalen Aktivitäten an die krisenbedingten Umstände angepasst. Die Zahl der cyber- und pandemiebezogenen Betrugsfälle, bei denen Malware, Ransomware und Phishing-Angriffe eingesetzt werden, nahm während der Pandemie zu, wobei die Angriffe sich gegen Einzelpersonen, Unternehmen und insbesondere den Gesundheitssektor richteten.

Das Pandemieszenario eröffnete neue Betrugsmöglichkeiten – Lieferengpässe wurden von

[41] So hat die Kommission beispielsweise im Rahmen der EU-Städteagenda der Partnerschaft für die Sicherheit im öffentlichen Raum thematisches und technisches Fachwissen durch Leitlinien und Unterstützung zur Verfügung gestellt, um Hilfestellung bei der Umsetzung von deren Aktionsplan zu leisten. Interreg-Programme für grenzübergreifende Zusammenarbeit, die aus dem Europäischen Fonds für regionale Entwicklung kofinanziert werden, unterstützen im Sicherheitsbereich tätige Akteure in benachbarten Grenzregionen dabei, wirksamer zusammenzuarbeiten.

[42] https://ec.europa.eu/jrc/en/protection-public-spaces-from-terrorist-attacks/newsletter-protection-public-spaces

[43] COM(2018) 470 final.

[44] Die EU-Plattform für die Sicherheit im Schienenpersonenverkehr setzt sich aus den für die Sicherheit im Schienenverkehr zuständigen Behörden der Mitgliedstaaten und interessierten Akteuren zusammen. Da das Mandat der Plattform im Juni 2021 ausgelaufen ist, wird die Umsetzung der Ergebnisse des Aktionsplans für Sicherheit im Schienenverkehr durch eine mit diesem Thema befasste Arbeitsgruppe innerhalb der Sachverständigengruppe zur Gefahrenabwehr im Landverkehr (LANDSEC) fortgesetzt.

[45] Bericht 2021 über die Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität in der EU (SOCTA), Europol.

gefälschten Webshops ausgenutzt, die nicht vorhandene Waren anboten und verkauften, darunter auch persönliche Schutzausrüstung und Selbsttestkits. Da sich der Vertrieb von Arzneimitteln vom physischen auf den Online-Markt verlagert hatte, wurden sogar betrügerische Angebote von COVID-19-Impfstoffen im Darknet gefunden.

Der Anstieg der weltweiten wirtschaftlichen Verluste im Zusammenhang mit Cyberkriminalität (die 2021 voraussichtlich 5,4 Billionen EUR jährlich erreichen werden) macht deutlich, dass sichere Anwendungen und Infrastrukturen entwickelt werden müssen, mit denen eine ständig zunehmende Bedrohung antizipiert und rasch darauf reagiert werden kann. Der von der Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust) im Mai veröffentlichte Justizmonitor für Cyberkriminalität (Cybercrime Judicial Monitor) bietet einen Überblick über gesetzgeberische Entwicklungen und die Rechtsprechung in der EU in den Bereichen Cyberkriminalität und durch den Cyberraum ermöglichte Kriminalität.[46]

Da eine starke Cybersicherheit von entscheidender Bedeutung ist, um der Flut von Cyberkriminalität Einhalt zu gebieten, ist es äußerst wichtig, dass die Mitgliedstaaten die bestehenden Rechtsvorschriften vollständig umsetzen. Die Kommission prüft kontinuierlich, ob die **Richtlinie über Angriffe auf Informationssysteme**[47] ordnungsgemäß umgesetzt wurde. Zusätzlich zu den bereits eingeleiteten Vertragsverletzungsverfahren[48] leitete die Kommission neue Verfahren wegen Mängeln bei der Umsetzung der Richtlinie ein (siehe Anhang 1 dieses Berichts). Erforderlichenfalls wird die Kommission weitere Verfahren einleiten. Parallel dazu unterstützte die Kommission die Mitgliedstaaten bei der Umsetzung der Richtlinie, indem sie am 23. Februar 2021 einen Workshop über bewährte Verfahren für die Erfassung, Erstellung und Veröffentlichung statistischer Daten bezüglich Meldungen, Strafverfolgungen und Verurteilungen wegen Cyberstraftaten im Sinne der Richtlinie veranstaltete. Für die Zerschlagung krimineller Netzwerke und die Unterbindung krimineller Aktivitäten, wie die gegenwärtige Zunahme von Ransomware-Angriffen, ist eine vollständige Umsetzung der Richtlinie über Angriffe auf Informationssysteme entscheidend. Die Verpflichtung der EU zur Zusammenarbeit mit gleich gesinnten Ländern in diesem Bereich, um der eskalierenden gemeinsamen Bedrohung durch kriminelle Ransomware-Netze zu begegnen, wurde sowohl auf dem NATO[49] als auch auf dem G7-Gipfel[50], die beide im Juni stattfanden, öffentlich betont.

Bekämpfung des sexuellen Missbrauchs von Kindern
Der sexuelle Missbrauch von Kindern ist ein zunehmend besorgniserregender Bereich, in dem Straftaten häufig online und offline miteinander verknüpft sind.

[46] Eurojust, Cybercrime Judicial Monitor, sechste Ausgabe, Mai 2021, abgerufen am 7. Juni 2021.
[47] Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates.
[48] Im Jahr 019 wurden Vertragsverletzungsverfahren gegen Bulgarien, Italien, Portugal und Slowenien eingeleitet.
[49] Kommuniqué des Gipfeltreffens der NATO in Brüssel, 14. Juni 2021.
[50] Kommuniqué des G7-Gipfeltreffens, „Our Shared Agenda for Global Action to Build Back Better“, 13. Juni 2021.

Die COVID-19-Pandemie und der sexuelle Missbrauch von Kindern

Aus zahlreichen Berichten geht hervor, dass die Pandemie den Missbrauch vor allem von Kindern, die mit den Tätern zusammenleben, verschärft hat.[51] Während der Pandemie wurde auch ein erheblicher Anstieg „selbst erzeugten" visuellen Materials verzeichnet, das zum Teil durch Missbrauch von Kindern im Internet entstanden ist, wobei der Täter das Kind lockt oder unter Druck setzt, um dieses Material zu produzieren.[52]

Entsprechend der **EU-Strategie für eine wirksamere Bekämpfung des sexuellen Missbrauchs von Kindern**[53] und der **EU-Kinderrechtsstrategie**[54] arbeitet die Kommission nun an den ermittelten spezifischen Initiativen, um proaktive und die verschiedenen Interessenträger einbeziehende Maßnahmen in allen relevanten Bereichen zu fördern, darunter Prävention, Unterstützung bei der Strafverfolgung und Hilfe für die Opfer.

Im April erzielten das Europäische Parlament und der Rat eine vorläufige politische Einigung über den Vorschlag der Kommission für **einstweilige Rechtsvorschriften**, mit denen sichergestellt werden soll, dass Anbieter von Online-Diensten ihre freiwillige Vorgehensweise fortsetzen können, um sexuellen Missbrauch von Kindern im Internet aufzudecken und zu melden und Material über sexuellen Kindesmissbrauch aus ihren Systemen zu entfernen, sofern ihre Vorgehensweise rechtmäßig ist. Diese einstweiligen Regelungen werden zu gegebener Zeit durch längerfristige Rechtsvorschriften mit detaillierten Schutzmaßnahmen ersetzt, um sexuellen Missbrauch von Kindern wirksamer zu bekämpfen. Die Initiative war Gegenstand einer öffentlichen Konsultation und einer Folgenabschätzung.

Die Kommission überprüft derzeit die Umsetzung der **Richtlinie zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie**[55]. Zur Weiterverfolgung der im Jahr 2019 gegen 23 Mitgliedstaaten eingeleiteten Vertragsverletzungsverfahren setzt die Kommission ihre Bewertung fort und dürfte im zweiten Halbjahr 2021 weitere Maßnahmen einleiten. Die Kommission geht des Weiteren davon aus, in den kommenden Monaten eine Reihe von Verfahren abschließen zu können, da mehrere Mitgliedstaaten ihre nationalen Rechtsvorschriften angepasst haben, damit diese der Richtlinie vollumfänglich entsprechen.

Zur Unterstützung der Strafverfolgungsbehörden und zur Förderung einer Multi-Stakeholder-Koordinierung hat die Kommission die Arbeit zur Einrichtung eines **Präventionsnetzes** aus Praktikern und Forschern aufgenommen, um die Zusammenarbeit und den Austausch

---

[51] Siehe Europol-Bericht vom 19. Juni 2020 und NetClean (14. April 2021). Laut Berichten des US-amerikanischen National Centre for Missing and Exploited Children war die Zahl der Meldungen sexuellen Kindesmissbrauchs weltweit im April 2020 viermal so hoch wie im April 2019. Siehe auch WePROTECT Global Alliance, World Childhood Foundation, Unicef, UNDOC, WHO, ITU, End Violence Against Children und UNESCO, April 2020.

[52] Siehe Berichte der Internet Watch Foundation vom 12. Januar 2021 und die Bewertung Europols der Bedrohungslage im Bereich der schweren und organisierten Kriminalität vom 12. April 2021.

[53] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – EU-Strategie für eine wirksamere Bekämpfung des sexuellen Missbrauchs von Kindern (COM(2020) 607 final).

[54] COM(2021) 142 final.

[55] Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates 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.

bewährter Verfahren zwischen allen einschlägigen Akteuren zu verstärken. Damit sollen die weltweiten Standards für den Schutz von Kindern vor sexuellem Missbrauch verbessert werden, indem die Zusammenarbeit über die WePROTECT Global Alliance zur Beendigung der sexuellen Ausbeutung von Kindern im Internet sowie durch spezielle Finanzmittel gefördert wird.

Online-Ermittlungen und elektronische Daten
Um Cyberkriminelle vor Gericht zu bringen, ist es von entscheidender Bedeutung, den Zugang zu digitalen Beweismitteln sicherzustellen, die Ermittlungsansätze liefern können. Einige Mitgliedstaaten haben zwar einen Rahmen für die **Vorratsdatenspeicherung** zur Speicherung und Nutzung elektronischer Kommunikationsmetadaten für Strafverfolgungszwecke geschaffen, doch werfen diese Maßnahmen wichtige Fragen im Zusammenhang mit ihrem möglichen Eingriff in die Grundrechte, einschließlich des Rechts auf Privatsphäre und des Schutzes personenbezogener Daten, auf. Der Gerichtshof der Europäischen Union hat wichtige Klarstellungen und Orientierungshilfen geliefert.[56] Im März erließ der Gerichtshof ein weiteres Urteil[57] zu den nationalen Rechtsvorschriften Estlands und bestätigte die frühere Rechtsprechung. Ebenfalls im März rief der Europäische Rat[58] dazu auf, „das Potenzial von Daten und digitalen Technologien zum Vorteil der Gesellschaft, der Umwelt und der Wirtschaft besser zu nutzen, wobei die entsprechenden Rechte in Bezug auf den Datenschutz und die Privatsphäre sowie andere Grundrechte zu wahren sind und die für die Strafverfolgungs- und Justizbehörden für die Ausübung ihrer gesetzlichen Befugnisse zur Bekämpfung von schwerer Kriminalität erforderliche Vorratsdatenspeicherung sicherzustellen ist“. In Reaktion auf diese jüngsten Entwicklungen kündigte die Kommission in ihrer EU-Strategie zur Bekämpfung der organisierten Kriminalität[59] an, dass sie im Einklang mit den Urteilen des Gerichtshofs mögliche Ansätze und Lösungen analysieren und umreißen wird, die den Erfordernissen der Strafverfolgung und der Justiz in einer Weise entsprechen, die operativ sinnvoll, technisch möglich und rechtlich solide ist und bei der auch die Grundrechte in vollem Umfang gewahrt bleiben. Derzeit konsultiert die Kommission die Mitgliedstaaten, um das weitere Vorgehen zu planen.

Eine weitere zentrale Komponente für eine wirksamere Bekämpfung der Cyberkriminalität und für eine effizientere Strafverfolgung sind Rechtsvorschriften über den **grenzüberschreitenden Zugang zu elektronischen Beweismitteln**. Seit dem ersten Fortschrittsbericht über die EU-Strategie für eine Sicherheitsunion haben die Verhandlungen mit den beiden gesetzgebenden Organen über den Kommissionsvorschlag[60] neue Schwungkraft gewonnen, da das Europäische Parlament seinen Standpunkt im Dezember 2020 angenommen hat. Auf dieser Grundlage haben das Europäische Parlament und der Rat Trilog-Gespräche aufgenommen. Die schnelle Verabschiedung effizienter Maßnahmen im

---

[56] In seinen Urteilen in der Rechtssache C-623/17, Privacy International, und den verbundenen Rechtssachen C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., vom 6. Oktober 2020 bestätigte der EuGH seine frühere Rechtsprechung, dass elektronische Kommunikationsdaten vertraulich sind und Verkehrs- und Standortdaten grundsätzlich nicht allgemein und unterschiedslos gespeichert werden dürfen. Gleichzeitig nannte der EuGH bestimmte Situationen, in denen die Vorratsdatenspeicherung auf der Grundlage klarer und verhältnismäßiger Verpflichtungen, die gesetzlich festgelegt sind und strengen materiell- und verfahrensrechtlichen Garantien unterliegen, zulässig ist.

[57] Urteil des Gerichtshofs vom 2. März 2021, Prokuratuur, C-746/18.

[58] Erklärung der Mitglieder des Europäischen Rates vom 25.3.2021, SN 18/21.

[59] EU-Strategie zur Bekämpfung der organisierten Kriminalität 2021–2025, COM(2021) 170 final vom 14.4.2021.

[60] COM(2018) 225 final und COM(2018) 226 final.

Einklang mit dem Ziel der Vorschläge wird den Strafverfolgungs- und Justizbehörden dabei helfen, rasch Zugang zu elektronischen Beweismitteln zu erhalten, die für strafrechtliche Ermittlungen benötigt werden.

Vertrauensdienste und die elektronische Identifizierung spielen eine Schlüsselrolle, wenn es darum geht, Cyberkriminalität einzudämmen und sichere grenzüberschreitende Transaktionen über das Internet zu ermöglichen. Der am 3. Juni vorgeschlagene **Rahmen für die europäische digitale Identität** zielt darauf ab, allen Bürgerinnen und Bürgern, Einwohnern und Unternehmen in der EU vertrauenswürdige digitale Identitäten zur Verfügung zu stellen. Der Rahmen sieht höchste verfügbare Sicherheitsstandards vor, um Bedrohungen durch Betrug und Identitätsdiebstahl zu begegnen und den Bürgerinnen und Bürgern und anderen Inhabern solcher Identitäten eine vollständige, benutzerfreundliche Kontrolle darüber zu gewährleisten, welche ihrer Daten für eine bestimmte Transaktion bereitgestellt werden. Der Rahmen stützt sich auf eine gemeinsame technische Architektur, die auf dem neuesten Stand der Technik beruht.

Die Frist für die Anwendung der Verordnung zur Erhöhung der **Sicherheit von Personalausweisen und Aufenthaltsdokumenten** endet am 2. August 2021. Die meisten Mitgliedstaaten liegen im Zeitplan und werden Personalausweise und Aufenthaltsdokumente im neuen Format ausstellen.[61]

Internationale Dimension
Angesichts des globalen Charakters der Cyberkriminalität sind Anstrengungen auf internationaler Ebene unerlässlich, um wirksamere Ansätze ausfindig zu machen.

Die Verhandlungen über das Zweite Zusatzprotokoll zum **Budapester Übereinkommen des Europarats über Computerkriminalität** zielen darauf ab, die bestehenden Vorschriften für den grenzüberschreitenden Zugang zu elektronischen Beweismitteln für strafrechtliche Ermittlungen zu verbessern. Im Mai 2021 haben die Vertragsparteien des Übereinkommens die Beratungen abgeschlossen, und der Protokollentwurf wird nun in den zuständigen Ausschüssen des Europarats geprüft. Noch in diesem Jahr wird ein förmlicher Abschluss erwartet, der die anschließende Unterzeichnung und Ratifizierung des Protokolls ermöglicht. Die Kommission arbeitet mit dem Europäischen Parlament und dem Rat zusammen, damit die Mitgliedstaaten das Protokoll so bald wie möglich unterzeichnen und ratifizieren können.

Das Protokoll enthält ebenfalls Bestimmungen, die Behörden den Zugang zu Domänennamen-Registrierungsdaten (auch als „**WHOIS-Informationen**“ bezeichnet) für strafrechtliche Ermittlungen erleichtern. In diesem Zusammenhang beteiligt sich die Kommission auch an der Entwicklung und Umsetzung von Multi-Stakeholder-Strategien für die Erhebung von und den Zugang zu Domänennamen-Registrierungsdaten auf Ebene der Zentralstelle für die Vergabe von Internet-Namen und -Adressen (Cooperation for Assigning Names and Numbers – ICANN). Diese Verfahren sollten im Einklang mit den einschlägigen Bestimmungen der vorgeschlagenen überarbeiteten NIS-Richtlinie stehen, die Bestimmungen enthält, mit denen sichergestellt wird, dass rechtmäßige Zugangsinteressenten, darunter Strafverfolgungsbehörden, genaue Domänennamen-Registrierungsdaten abrufen und offenlegen können.

[61] Eine begrenzte Zahl von Mitgliedstaaten hat Verzögerungen gemeldet, die hauptsächlich auf die Pandemie zurückzuführen sind; es gibt aber auch andere Gründe für erhebliche Verzögerungen, zum Beispiel vor Gericht angefochtene Vergabeverfahren.

Eine wichtige Maßnahme für die internationale Zusammenarbeit ist das Projekt „Global Action on Cybercrime Extended“ (GLACY+). Damit sollen die Länder bei der Anwendung der Rechtsvorschriften über Cyberkriminalität und elektronische Beweismittel auf der Grundlage des Budapester Übereinkommens weltweit unterstützt und ihre Kapazität für die wirksame Zusammenarbeit im Einklang mit den internationalen Menschenrechtsnormen und der Rechtsstaatlichkeit gestärkt werden. Mit dem Projekt werden 16 vorrangige Länder unterstützt.[62] Außerdem soll das Projekt Akteure im Bereich der Strafverfolgung mit politischen Entscheidungsträgern und Gesetzgebern in Kontakt bringen, um eine stärkere politische Unterstützung für das Budapester Übereinkommen zu gewährleisten.

2. Moderne Strafverfolgung

Neue Technologien bieten erhebliche Chancen im Bereich der Sicherheit. Um die Sicherheit zu verbessern, ist es unerlässlich, Künstliche Intelligenz, Big Data und Hochleistungsrechentechnik in die Sicherheitspolitik einzubeziehen, ohne den wirksamen Schutz der Grundrechte zu schwächen.

Künstliche Intelligenz kann den Strafverfolgungsbehörden Instrumente an die Hand geben, die sie bei der Bekämpfung von Kriminalität und Terrorismus unterstützen; dadurch können die Behörden mit den sich rasch entwickelnden Technologien, welche von Kriminellen eingesetzt und bei ihren grenzüberschreitenden Aktivitäten genutzt werden, Schritt halten. In der jüngsten Mitteilung der Kommission für einen europäischen Ansatz bei Künstlicher Intelligenz[63] wird dargelegt, wie KI als strategisches Instrument sowohl zur Bewältigung aktueller Bedrohungen als auch zur Antizipierung künftiger Risiken und Chancen einen wesentlichen Beitrag zur Strategie für eine Sicherheitsunion leisten kann. Im April legte die Kommission einen Vorschlag für eine Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz[64] vor, mit der Europa zum globalen Drehkreuz für vertrauenswürdige KI werden soll. Ein wesentlicher Teil dieser Vorschläge konzentriert sich auf Hochrisiko-KI-Systeme, die erhebliche Risiken für die Gesundheit und Sicherheit oder die Grundrechte des Einzelnen in sich bergen. Die Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz sieht vor, dass eine biometrische Fernidentifizierung in Echtzeit in öffentlich zugänglichen Räumen für die Zwecke der Strafverfolgung grundsätzlich verboten ist, mit eng umrissenen Ausnahmen. Diese Arten von Hochrisiko-Systemen müssen eine Reihe horizontaler verbindlicher Anforderungen an vertrauenswürdige KI erfüllen, einschließlich Rückverfolgbarkeit, Transparenz, menschliche Aufsicht und Präzision. Die Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz hätte erhebliche Auswirkungen auf die Strafverfolgung und die Grenzkontrollen. Ziel ist es, einen ausgewogenen Rahmen für die Aufsicht über die von den

---

[62] So wird der Europarat beispielsweise durch das Europäische Nachbarschaftsinstrument bei der Durchführung des Projekts „CyberSouth“ unterstützt, mit dem die Rechtsvorschriften und institutionellen Kapazitäten in Bezug auf Cyberkriminalität und elektronische Beweismittel in der südlichen Nachbarschaft im Einklang mit den Menschenrechten und der Rechtsstaatlichkeit gestärkt werden sollen. Ein ähnliches Projekt – CyberEast – wird vom Europarat in der Region der Östlichen Partnerschaft durchgeführt. Ein weiteres im Rahmen des Instruments für Heranführungshilfe finanziertes Projekt des Europarats betrifft den Westbalkan und die Türkei. Es hat das Ziel, die Kapazitäten der Behörden im Westbalkan und in der Türkei weiter zu stärken, um Erträge aus Cyberkriminalität zu ermitteln, zu beschlagnahmen und einzuziehen, Geldwäsche im Internet zu verhindern und elektronische Beweismittel zu sichern.

[63] Mitteilung der Kommission für einen europäischen Ansatz bei Künstlicher Intelligenz (Fostering a European approach to Artificial Intelligence) (COM(2021) 205 final).

[64] COM(2021) 206 final.

Strafverfolgungsbehörden eingesetzten Hochrisikosysteme während ihres gesamten Lebenszyklus zu schaffen und eine Reihe von Sicherheitsmaßnahmen zum Schutz der Grundrechte einzuführen.

Der europäische Raum für Sicherheitsdaten für Innovationen im Rahmen des **Programms „Digitales Europa“** zielt darauf ab, das Vertrauen in die Nutzung von KI durch Strafverfolgungsbehörden zu stärken, indem hochwertige Datensätze zum Trainieren, Testen und Validieren von Algorithmen erstellt, zugänglich gemacht und gemeinsam genutzt werden, was eine wesentliche Voraussetzung für den Aufbau von KI-Ökosystemen für Exzellenz und Vertrauen ist. Wie wichtig die Schaffung gemeinsamer Datenräume ist, wurde vom Europäischen Rat im März anerkannt.

Hochleistungsrechnen (HPC) ist entscheidend, damit Schlüsseltechnologien wie KI und Datenanalyse das enorme Potenzial von Big Data nutzen können. Supercomputing-Simulationen sind von zentraler Bedeutung für die Verbesserung der Sicherheit von Produkten und Dienstleistungen (insbesondere durch Modellierung) sowie für die nationale Sicherheit, die Verteidigung und die technologische Autonomie. Bei Anwendungen, die von Cybersicherheitssimulationen bis zu nuklearen Simulationen reichen, spielen Supercomputer eine wichtige Rolle, und die Kombination von HPC und KI wird in den Bereichen Verteidigung und Sicherheit bahnbrechende Veränderungen bringen. Die Eröffnung des Hauptsitzes des Gemeinsamen Unternehmens für europäisches Hochleistungsrechnen[65] (GU EuroHPC) im Mai war ein wichtiger Schritt, um einen schnellen Zugang zu den Hochleistungsrechenressourcen des EuroHPC zu ermöglichen, wenn dies für Sicherheit und Verteidigung essenziell ist.

Die Rolle der Verschlüsselung

Die **Verschlüsselung** ist eine entscheidende Technologie, wenn es um Sicherheit geht, und ist für die Sicherheit digitaler Systeme und Transaktionen sowie für den Schutz der Grundrechte – einschließlich des Rechts auf freie Meinungsäußerung, der Privatsphäre und des Datenschutzes – unerlässlich. Wie die jüngsten Operationen gegen EncroChat[66] und Sky ECC[67] zeigen, nutzen Kriminelle die verschlüsselte Kommunikation, und die Strafverfolgungsbehörden der EU müssen ihre Kapazitäten für den Umgang mit verschlüsselten Informationen im Rahmen strafrechtlicher Ermittlungen kontinuierlich ausbauen, wobei sie die geltenden Rechtsvorschriften einhalten müssen. Im Dezember 2020 wurde die neue Entschlüsselungsfunktion von Europol in Betrieb genommen. Diese Initiative soll die Achtung der Grundrechte sicherstellen und eine Einschränkung oder Schwächung der Verschlüsselung vermeiden und steht den nationalen Strafverfolgungsbehörden aller

---

[65] Das Gemeinsame Unternehmen EuroHPC wurde 2018 gegründet, um die EU in die Lage zu versetzen, eine weltweite Spitzenposition beim Hochleistungsrechnen zu erlangen. Derzeit wird auf EU-Ebene über eine neue Verordnung beraten, die voraussichtlich in den nächsten Monaten in Kraft treten wird.

[66] Im Jahr 2020 führten europaweite Ermittlungen zur Zerschlagung einer Krypto-Telefonlösung, die von Gruppen der organisierten Kriminalität genutzt wurde.

[67] Am 10. März 2021 unterstützte Eurojust gemeinsame Operationen der Justiz- und Strafverfolgungsbehörden Belgiens, Frankreichs und der Niederlande, um die Nutzung verschlüsselter Kommunikation durch in großem Stil agierende organisierte kriminelle Gruppen zu sperren. Den Ermittlern gelang es, die kriminelle Nutzung des Kommunikationsdienstes Sky ECC zu überwachen. Dadurch erhielten sie wertvolle Einblicke in Hunderte Millionen von Nachrichten, die zwischen Kriminellen ausgetauscht wurden, und hatten somit Zugang zu wichtigen Informationen über mehr als hundert geplante groß angelegte kriminelle Operationen, wodurch potenzielle lebensbedrohliche Situationen und mögliche Opfer verhindert wurden.

Mitgliedstaaten zur Verfügung, um die Sicherheit von Gesellschaften und Bürgerinnen und Bürgern zu gewährleisten.

Im Dezember 2020 rief der Rat dazu auf, in einen aktiven Dialog mit der Technologiebranche zu treten und einen Regelungsrahmen zu entwickeln, der es den nationalen Behörden ermöglichen würde, ihre operativen Aufgaben zu erfüllen und gleichzeitig die Privatsphäre, die Grundrechte und die Sicherheit der Kommunikation zu schützen.[68] In der EU-Strategie zur Bekämpfung der organisierten Kriminalität[69] hat die Kommission ihre Absicht dargelegt, im Jahr 2022 einen Vorschlag für ein künftiges Vorgehen in Bezug auf den rechtmäßigen und gezielten Zugriff auf verschlüsselte Informationen im Rahmen von strafrechtlichen Ermittlungen und Strafverfolgungen zu unterbreiten, das nicht zu einer allgemeinen Schwächung der Verschlüsselung oder zu einer willkürlichen Überwachung führt. Ein erster Schritt ist eine sorgfältige Bestandsaufnahme der Art und Weise, wie die Mitgliedstaaten mit Verschlüsselung umgehen, begleitet von einem Prozess mit mehreren Interessenträgern zur Untersuchung und Bewertung rechtlicher, ethischer und technischer Optionen.

Justizielle Zusammenarbeit
Eine angemessene Reaktion auf die Herausforderungen im Hinblick auf Sicherheit erfordert auch die **Modernisierung der justiziellen Zusammenarbeit** zwischen den EU-Staaten durch den Einsatz digitaler Technologien. Derzeit wird an einem Gesetzgebungsvorschlag zur Digitalisierung der grenzüberschreitenden justiziellen Zusammenarbeit in der EU gearbeitet. Damit soll ein digitaler Kommunikationskanal zwischen den zuständigen Behörden der Mitgliedstaaten und gegebenenfalls den EU-Agenturen eingerichtet werden. Ziel ist es, die Kommunikation zwischen den Behörden in Papierform aufzugeben und einen schnellen, sicheren und effizienten Datenaustausch zu gewährleisten. Eine öffentliche Konsultation[70] ergab, dass der Ansatz von der Öffentlichkeit und den Interessenträgern unterstützt wird.

3. Bekämpfung illegaler Online-Inhalte

In der EU-Strategie für eine Sicherheitsunion wurde hervorgehoben, dass die Sicherheit sowohl des Online-Umfelds als auch des physischen Umfelds ständige Anstrengungen zur Bekämpfung illegaler Online-Inhalte erfordert; hierbei wurden im Berichtszeitraum entscheidende Fortschritte erzielt. Die lange erwartete Verordnung zur Bekämpfung der **Verbreitung terroristischer Online-Inhalte**[71] wurde vom Europäischen Parlament und vom Rat angenommen und wird ab Juni 2022 uneingeschränkt gelten. Dann können die Mitgliedstaaten Entfernungsanordnungen gegenüber bestimmten Hostingdiensteanbietern, die in der EU Dienstleistungen anbieten, erlassen und diese verpflichten, innerhalb einer Stunde Material zu entfernen, das zur Begehung terroristischer Straftaten anstiftet oder solche befürwortet, Aktivitäten einer terroristischen Vereinigung unterstützt oder Anweisungen oder Techniken für die Begehung terroristischer Straftaten zur Verfügung stellt. Außerdem sieht

---

[68] Entschließung des Rates zur Verschlüsselung – Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung, 13084/1/20 REV 1.

[69] Mitteilung der Kommission über eine EU-Strategie zur Bekämpfung der organisierten Kriminalität 2021–2025 (COM(2021) 170 final).

[70] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12547-Digitalisierung-der-Justiz-in-der-EU_de

[71] Verordnung (EU) 2021/784 des Europäischen Parlaments und des Rates vom 29. April 2021 zur Bekämpfung der Verbreitung terroristischer Online-Inhalte.

diese Richtlinie Schutzvorkehrungen vor, um die Rechenschaftspflicht und die Transparenz in Bezug auf Maßnahmen zur Entfernung terroristischer Inhalte zu stärken und vor irrtümlicher Entfernung legitimer Äußerungen im Internet zu schützen.

Die von der Kommission im Dezember 2020 vorgeschlagene Verordnung über einen Binnenmarkt für digitale Dienste sieht Maßnahmen zur Bekämpfung illegaler Waren, illegaler Dienstleistungen und online verbreiteter illegaler Inhalte vor. Diese Verordnung ermöglicht Nutzern die Meldung illegaler Online-Inhalte und bietet vertrauenswürdigen Hinweisgebern einen privilegierten Kanal, um illegale Inhalte mit Priorität zu melden. Darüber hinaus müssen Online-Plattformen den zuständigen Strafverfolgungsbehörden den Verdacht auf bestimmte schwere Straftaten melden, und sehr große Online-Plattformen sind verpflichtet, jährliche Risikobewertungen durchzuführen und Risikominderungsmaßnahmen im Hinblick auf erhebliche systemische Risiken der Verbreitung illegaler Inhalte zu ergreifen. Der Vorschlag für eine Verordnung über einen Binnenmarkt für digitale Dienste stützt sich auf freiwillige Initiativen wie den **Verhaltenskodex zur Bekämpfung illegaler Hassrede im Internet**, die wertvolle Instrumente zur Bekämpfung bestimmter Formen illegaler Inhalte darstellen.

Die Herausforderungen im Umgang mit illegalen Online-Inhalten, darunter auch Material über den sexuellen Missbrauch von Kindern, standen im Mittelpunkt der Beratungen auf dem Ministertreffen des EU-Internetforums im Januar 2021, an der die EU-Mitgliedstaaten und Technologieunternehmen teilnahmen. Im Rahmen des EU-Internetforums hat die Kommission einen Prozess angestoßen, der Experten aus Industrie, Wissenschaft, Behörden und Organisationen der Zivilgesellschaft umfasst, um technische Lösungen zu ermitteln, die es Unternehmen ermöglicht, sexuellen Missbrauch von Kindern im Internet in elektronischen Nachrichten mit Ende-zu-Ende-Verschlüsselung aufzudecken, unter gleichzeitiger Wahrung der Grundrechte, einschließlich der Privatsphäre und der Vertraulichkeit der Kommunikation. Darüber hinaus wird derzeit an der Entwicklung einer EU-Liste gewalttätiger rechtsextremistischer Gruppen und Symbole gearbeitet, um Technologieunternehmen bei ihrer Entscheidung über die Moderation von Inhalten zu unterstützen, da in diesbezüglichen Debatten davon die Rede war, wie schwierig die Identifizierung von Material mit extremistischen Inhalten sei.

4. Hybride Bedrohungen

Geopolitische Spannungen, auch in Bezug auf neue Technologien, führen zu zunehmenden globalen Sicherheitsbedrohungen, einer Fragmentierung und einem beständigen Kampf der Narrative. Staatliche und nichtstaatliche Akteure missbrauchen zunehmend Technologien, um ihre Ziele zu verfolgen, unsere Gesellschaften, unsere Wirtschaft und unsere Sicherheit zu bedrohen und die Menschenrechte und Grundfreiheiten zu beeinträchtigen. Die Pandemie hat die EU und ihre Mitgliedstaaten anfälliger für hybride Bedrohungen gemacht, unter anderem durch die verstärkte Verbreitung von Desinformation und manipulativer Einflussnahme.

Gesundheit und Resilienz gegenüber hybriden Bedrohungen

Durch die Pandemie sind die Schwächen der Krisenvorsorge- und Krisenreaktionsmechanismen auf EU-Ebene deutlich geworden. Sowohl die öffentlichen als auch die privaten Kapazitäten im Bereich der Vorsorge und des Krisenmanagements, insbesondere in Bezug auf medizinische Gegenmaßnahmen, sind im Vergleich zu anderen globalen Akteuren (wie den USA oder China) fragmentiert, verstreut und suboptimal. Eine solche Fragmentierung bietet einen fruchtbaren Boden für hybride Bedrohungen durch

staatliche oder nichtstaatliche Akteure. Wie in der Mitteilung „Schaffung einer europäischen Gesundheitsunion: Die Resilienz der EU gegenüber grenzüberschreitenden Gesundheitsgefahren stärken“[72] und der Mitteilung „Erste Lehren aus der COVID-19-Pandemie“[73] dargelegt, würde die künftige EU-Behörde für die Krisenvorsorge und -reaktion bei gesundheitlichen Notlagen (HERA) eine entscheidende Rolle bei der Stärkung der allgemeinen Resilienz spielen und einen soliden Rahmen für Vorsorge, Überwachung, Risikobewertung, Frühwarnung und Reaktion der EU auf alle schwerwiegenden grenzüberschreitenden Gesundheitsgefahren gewährleisten.

Derzeit wird in engem Zusammenhang mit dem Protokoll der **EU für das operative Vorgehen bei der Abwehr hybrider Bedrohungen (EU-Playbook)** eine Überprüfung der Krisenbewältigungsmechanismen der EU durchgeführt. Ein erster Schritt in diesem Prozess war die Stärkung und Erweiterung des hybriden Netzes der Kontaktstellen in allen Kommissionsdienststellen, dem Europäischen Auswärtigen Dienst und der Europäischen Verteidigungsagentur. Ein weiteres Element für die durchgängige Einbeziehung des Aspekts der hybriden Bedrohungen in die Politikgestaltung ist die Bewertung hybrider Bedrohungen bei politischen Initiativen im Rahmen der besseren Rechtsetzung.

Die Umsetzung des Gemeinsamen Rahmens für die Bekämpfung hybrider Bedrohungen von 2016 und der Gemeinsamen Mitteilung über Stärkung der Resilienz und Ausbau der Kapazitäten zur Abwehr hybrider Bedrohungen von 2018 wird fortgesetzt, und der Stand der Umsetzung wird im fünften Jahresbericht[74] über die Abwehr hybrider Bedrohungen dargelegt. In dem Bericht werden die Fortschritte bei der Einrichtung einer zugangsbeschränkten Online-Plattform beschrieben, in der Mitgliedstaaten und EU-Organe Instrumente und Maßnahmen auf EU-Ebene zur Abwehr hybrider Bedrohungen, Maßnahmen zur Verbesserung der Lageerfassung, insbesondere durch die EU-Analyseeinheit für hybride Bedrohungen, und die Ermittlung sektorspezifischer Referenzwerte für die Resilienz einfach ausfindig machen können.

Die Abwehr zunehmend komplexer und destruktiver hybrider Bedrohungen und Cyberbedrohungen ist nach wie vor ein Kernbereich der **Zusammenarbeit zwischen der EU und der NATO**. Dies spiegelt sich auch im jüngsten Kommuniqué des Gipfeltreffens der NATO in Brüssel[75] wider. Die Zusammenarbeit wurde kontinuierlich fortgesetzt und baut auf den Erfolgen und der beständigen Dynamik der vorangegangenen Berichtszeiträume auf. Die wichtigsten Ergebnisse wurden im sechsten gemeinsamen Fortschrittsbericht der EU und der NATO[76] vorgestellt. Die Zahl der Mitglieder im Europäischen Kompetenzzentrum für die Abwehr hybrider Bedrohungen in Helsinki (Hybrid CoE) nahm weiter zu, wobei inzwischen 30 EU-Mitgliedstaaten und NATO-Verbündete dem Zentrum beigetreten sind. Im Berichtszeitraum beförderte das Hybrid CoE eine Reihe themenbezogener Debatten, Workshops und Übungen.

[72] COM(2020) 724 final.
[73] COM(2021) 380 final.
[74] SWD(2021) 729 final.
[75] Kommuniqué des Gipfeltreffens der NATO in Brüssel, 14. Juni 2021.
[76] Sechster Fortschrittsbericht über die Umsetzung des vom Rat der EU und vom NATO-Rat am 6. Dezember 2016 und 5. Dezember 2017 gebilligten gemeinsamen Pakets von Vorschlägen, 3. Juni 2021.

Mit dem Pakt für die zivile GSVP[77] wurden hybride Bedrohungen ebenfalls als einer der vorrangigen Bereiche für zivile GSVP-Missionen aufgenommen. Ein entsprechendes Minikonzept für die zivile GSVP-Unterstützung bei der Abwehr hybrider Bedrohungen[78] wurde ausgearbeitet. In dem Dokument wird vorgeschlagen, 1) dem Schutz von Missionen gegen hybride Angriffe Vorrang einzuräumen und 2) gegebenenfalls den Aufnahmestaat bei der Stärkung der Resilienz gegenüber hybriden Bedrohungen zu unterstützen.

Ein wesentlicher Teil hybrider Bedrohungen ist **Desinformation**. Im Europäischen Aktionsplan für Demokratie[79] wurden mehrere Maßnahmen genannt, um die Reaktion auf die ausländische Manipulation von Informationen und die Einmischung aus dem Ausland zu verstärken.[80] Der Europäische Rat begrüßte das Konzept des Aktionsplans für Demokratie und hat gleichfalls dazu aufgerufen, die Maßnahmen der EU auszubauen.[81] Für den Erfolg dieser Maßnahmen arbeitet der EAD eng mit der Kommission zusammen und stützt sich dabei auf das Schnellwarnsystem der EU, um die Gemeinschaft der Experten zusammenzubringen, mit dem Ziel, einen starken, robusten, flexiblen und umfassenden Rahmen zur Bekämpfung der ausländischen Manipulation von Informationen und der Einmischung aus dem Ausland zu schaffen. Unterstützt wird diese Vorgehensweise auch durch den Verhaltenskodex zur Bekämpfung von Desinformation im Internet, der im Mai durch Leitlinien dahin gehend gestärkt wurde, wie teilnehmende Online-Diensteanbieter und andere relevante Interessenträger ihre Maßnahmen verstärken sollten, um Lücken und Mängel im Kodex zu beheben und eine transparentere, sicherere und vertrauenswürdigere Online-Umgebung zu schaffen.[82]

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

1. Terrorismus und Radikalisierung

Die Anschläge Ende des Jahres 2020 haben gezeigt, dass es nach wie vor wichtig ist, Terrorismus und seine Ursachen zu bekämpfen. In der im Dezember 2020 angenommenen neuen **EU-Agenda für Terrorismusbekämpfung**[83] wird dargelegt, wie der Kampf gegen Terrorismus und gewaltbereiten Extremismus verstärkt und die Resilienz der EU gegen terroristische Bedrohungen erhöht werden kann. Die Umsetzung schreitet gut voran. Des Weiteren bewertet die Kommission derzeit die Richtlinie (EU) 2017/541 zur Terrorismusbekämpfung, die Mindestvorschriften für die strafrechtliche Verfolgung von

---

77 Dokument 14305/18 vom 19. November 2018.
78 Dokument 8077/20 vom 20. Mai 2020.
79 COM(2020) 790 final.
80 Drei Kernbereiche sind: 1) weitere Präzisierung der Terminologie, die die Herausforderung beschreibt, 2) Entwicklung einer gemeinsamen Methodik und eines gemeinsamen Rahmens zur Erhebung systematischer Beweise für die ausländische Manipulation von Informationen und die Einmischung aus dem Ausland und 3) Weiterentwicklung des Instrumentariums der EU zur Bekämpfung der ausländischen Manipulation von Informationen und der Einmischung aus dem Ausland, damit die Instrumente zweckdienlicher werden und den Tätern Kosten auferlegt werden können.
81 Erklärung des Europäischen Rates vom März 2021 und Schlussfolgerungen des Rates vom Dezember 2020.
82 COM(2021) 262 final. In den Leitlinien wird auch speziell auf die COVID-19-Infodemie eingegangen.
83 Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Eine Agenda für Terrorismusbekämpfung: antizipieren, verhindern, schützen und reagieren (COM(2020) 795 final).

terroristischen Straftaten und Straftaten im Zusammenhang mit Terrorismus und die Festlegung von Sanktionen sowie Maßnahmen zum Schutz, zur Unterstützung und zur Hilfe der Opfer von Terrorismus enthält.

Ende 2020 vergab die Kommission einen neuen Rahmenvertrag an ein Konsortium zur politischen Unterstützung des **Aufklärungsnetzwerks gegen Radikalisierung** (RAN), mit dem die Arbeit der in diesem Netzwerk zusammengeschlossenen Akteure aus der Praxis ergänzt und politische Entscheidungsträger bei allgemeinen Präventionsfragen weiterhin unterstützt werden sollen. Ziel ist, das Wissen und die Kapazitäten der Mitgliedstaaten im Bereich der strategischen Kommunikation und die Faktengrundlage für die weitere Politikentwicklung, konkrete Ansätze und Interventionen zu verbessern.

Darüber hinaus arbeitet die Kommission mit den Mitgliedstaaten zusammen, um extremistische Ideologien zu bekämpfen, die zu gewaltbereitem Extremismus führen können. 2021 konzentriert sich diese Arbeit auf die zwischen allen Arten gewaltbereiter extremistischer Ideologien (darunter linker, rechter und islamistischer Extremismus) bestehenden Verbindungen und auf Radikalisierung, die zur Selbstausgrenzung führt. In den letzten Monaten wurden in diesem Bereich mehrere Sensibilisierungsinitiativen durchgeführt. Die Tätigkeiten des RAN wurden durch einen speziellen Vertrag, der im Januar 2021 in Kraft trat, auf den Westbalkan ausgeweitet.

Eine weitere Priorität besteht darin, den Erwerb von Stoffen durch Terroristen zu verhindern, die als Waffen eingesetzt werden können. Der Aktionsplan von 2017 in Bezug auf **chemische, biologische, radiologische und nukleare Stoffe (CBRN-Stoffe)** wurde durch eine im Juni 2021 abgeschlossene Studie über die Durchführbarkeit der Beschränkung des Zugangs zu einigen hochgefährlichen Chemikalien vorangebracht. Die Kommission hat außerdem vorbereitende Arbeiten für im nächsten Jahr stattfindende grenzüberschreitende Übungen und Workshops zum Thema Sicherheit von radioaktiven und biologischen Quellen in Krankenhäusern und Laboratorien aufgenommen. Die Umsetzung des CBRN-Aktionsplans wird durch aus dem Fonds für die innere Sicherheit kofinanzierte Projekte unterstützt, in dessen Rahmen Initiativen wie das Projekt „Safe Stadium“[84] ausgewählt wurden, die sich mit dem Schutz und der Vorsorge im Hinblick auf Angriffe mit CBRN-Stoffen in großen Sportarenen wie Fußballstadien befassen. Am 1. Februar 2021 traten neue Rechtsvorschriften über die Vermarktung und Verwendung von Ausgangsstoffen für Explosivstoffe in Kraft. Derzeit läuft die Umsetzung, und die Kommission unterstützt alle Beteiligten weiterhin bei der Erfüllung ihrer Verpflichtungen.

Ein Teil der inhärenten Verbindung zwischen der äußeren und der inneren Sicherheit der Union ist die Zusammenarbeit bei Bedrohungen, zum Beispiel durch CBRN-Stoffe. Mithilfe der Außenfinanzierungsinstrumente der EU werden Anstrengungen zur Verbesserung der globalen und regionalen Governance und Zusammenarbeit bei der Erkennung und Eindämmung von CBRN-Risiken unterstützt, wobei auf den positiven Erfahrungen aufgebaut wird, die beispielsweise im Rahmen der Initiative der Europäischen Union für Exzellenzzentren für chemische, biologische, radiologische und nukleare Risiken (CBRN-Risiken) und des Ausfuhrkontrollprogramms für Güter mit doppeltem Verwendungszweck

[84] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/31077817/101034226/ISFP

gewonnen wurden. Bislang haben 34 Länder einen nationalen CBRN-Aktionsplan ausgearbeitet, wobei zehn Länder einen solchen Plan offiziell verabschiedet haben.

Gesundheit und Terrorismus

Mit dem EU4Health-Programm[85] werden Maßnahmen zur Prävention von, Vorsorge für und Reaktion auf grenzüberschreitende Gesundheitsgefahren unterstützt.

Die **Krisenvorsorge im Gesundheitswesen im Falle von Terroranschlägen**[86] wird im Rahmen des dritten EU-Gesundheitsprogramms kofinanziert; hierbei handelt es sich um eine gemeinsame Maßnahme mit den Gesundheitsbehörden der EU, die im Mai 2021 auf den Weg gebracht wurde. Ihr Ziel ist, Unionsbürgerinnen und -bürger vor vorsätzlichen Gesundheitskrisen zu schützen, indem die Lücken bei der Krisenvorsorge im Gesundheitswesen geschlossen werden und die sektorübergreifende Arbeit (Gesundheit, Sicherheit und Katastrophenschutz) für die Reaktion auf einen biologischen und/oder chemischen Terroranschlag gestärkt wird.

Mit dem Gesundheitsprogramm 2017–2021 wurden Vorsorge- und Reaktionskapazitäten des Gesundheitssektors gegen chemische und biologische Bedrohungen unterstützt. Die gemeinsame Maßnahme „**Strengthened International Health Regulations and Preparedness in the EU**“[87] umfasst ein Netz von Referenzlaboratorien, die sich mit hochpathogenen Erregern befassen und dem 41 Laboratorien angeschlossen sind.

Maßnahmen gegen die Bedrohung durch aus Syrien und Irak zurückkehrende **ausländische terroristische Kämpfer** spielen nach wie vor eine wichtige Rolle bei der Terrorismusbekämpfung und sind weiterhin ein vorrangiges Ziel der Radikalisierungsprävention. Wie in den strategischen Orientierungen für ein koordiniertes EU-Konzept für die Radikalisierungsprävention („Strategic Orientations on a coordinated EU approach to prevention of radicalisation“) für 2021 vereinbart, arbeitet die Kommission an vier wesentlichen Prioritäten: Rückkehrer im Kindesalter, Stärkung und Sicherung des Rückkehrprozesses (Rückführung, Strafverfolgung und Wiedereingliederung), Kompetenzen der an der Wiedereingliederung von Rückkehrern im Kindesalter beteiligten Fachkräften und Rückkehrerinnen. In Bezug auf die Gefängnisse und Lager für Binnenvertriebene im Nordosten Syriens prüfen der EAD und die Kommission im Einvernehmen mit den Mitgliedstaaten neue Wege zur Ausweitung der Hilfe in der Region, um die Lebensbedingungen zu verbessern und der Radikalisierung Einhalt zu gebieten.

Die Kommission hat kürzlich die Aktualisierung der Datenanalyse zur Terrorismusbekämpfung und zur Prävention und Bekämpfung von gewaltbereitem Extremismus abgeschlossen. Diese ergab, dass Umfang und Schnelligkeit der Finanzhilfen aus EU-Außenfinanzierungsinstrumenten bei solchen Maßnahmen beeindruckend waren.[88]

---

[85] Eingerichtet durch die Verordnung (EU) 2021/522 des Europäischen Parlaments und des Rates.

[86] Gemeinsame Maßnahme zur Krisenvorsorge im Gesundheitswesen im Falle von Terroranschlägen, https://ec.europa.eu/chafea/health/funding/joint-actions/documents/ja-2019-presentation-03_en.pdf.

[87] Gemeinsame Maßnahme „Strengthened International Health Regulations and Preparedness in the EU“ (SHARP), https://sharpja.eu/wp7/.

[88] Die EU leistet umfangreiche Unterstützung für alle Initiativen des Globalen Forums „Terrorismusbekämpfung“, einschließlich des Instituts für Justiz und Rechtsstaatlichkeit, und für den Globalen Fonds für Engagement und Widerstandsfähigkeit der Allgemeinheit (GCERF), um Maßnahmen zur Prävention und Bekämpfung von gewaltbereitem Extremismus in einer Reihe von Ländern, die für die EU von strategischer Bedeutung sind, zu fördern.

Am Stichtag 1. Januar 2021 liefen insgesamt 99 Maßnahmen zur Antizipierung und Prävention von, zur Reaktion auf und zum Schutz vor Terrorismus in Ländern außerhalb der EU mit einem Gesamtvolumen von 501 Mio. EUR (8 % mehr als im Vorjahr), die den Prioritäten der EU-Agenda für die Terrorismusbekämpfung und den Schlussfolgerungen des Rates zur Terrorismusbekämpfung Rechnung tragen.

Gestützt auf das Fachwissen des Netzwerks von EU-Experten für Terrorismusbekämpfung und Sicherheit wurden weitere Schritte unternommen, um Partnerschaften zur Terrorismusbekämpfung aufzubauen und zu stärken und die Zusammenarbeit mit Ländern in der Nachbarschaft und darüber hinaus zu fördern. In den letzten Monaten ist die Umsetzung des Gemeinsamen Aktionsplans zur Terrorismusbekämpfung für den westlichen Balkan vorangekommen, mit einigen Verzögerungen aufgrund der Pandemie und der internen politischen Dynamik der Partner.

Die EU hat ihren Sanktionsrahmen für die Terrorismusbekämpfung im Berichtszeitraum weiterhin genutzt. Im Februar 2021 schloss der Rat die Überprüfung der EU-Terroristenliste[89] ab, und im April 2021 wurde im Rahmen der eigenständigen Sanktionsregelung der EU zur Bekämpfung des Terrorismus (ISIL (Da'esh)/Al-Qaida) dieser Liste ein neuer Eintrag hinzugefügt[90].

Schließlich organisierten Eurojust und das Europäische Netzwerk im Mai 2021 gemeinsam den 6. EU-Tag gegen Straflosigkeit, wobei der Schwerpunkt auf wesentlichen internationalen Verbrechen lag, die in Syrien von terroristischen Organisationen und dem syrischen Regime begangen werden. Grundlage war die seit dem letzten Jahr geleistete Arbeit zur Unterstützung der kumulativen Strafverfolgung ausländischer terroristischer Kämpfer wegen der von ihnen begangenen völkerrechtlichen Verbrechen und Straftaten im Zusammenhang mit Terrorismus. Der Tag hat zudem gezeigt, dass eine verstärkte justizielle Zusammenarbeit zwischen den Mitgliedstaaten von entscheidender Bedeutung für die Ermittlung und Verfolgung von Kriegsverbrechern ist, die sich in der EU aufhalten.

2. Bekämpfung der organisierten Kriminalität

Im Bericht von 2021 über die Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität (SOCTA 2021)[91] werden die anhaltende Bedrohung durch die organisierte Kriminalität und ihre zunehmende Komplexität beleuchtet. Die organisierte Kriminalität operiert grenzübergreifend: 65 % der organisierten kriminellen Gruppen setzen sich aus Mitgliedern verschiedener Nationalitäten zusammen, und sieben von zehn sind in mehr als drei Ländern aktiv. Die Landschaft der organisierten Kriminalität in der EU ist durch ein vernetztes Umfeld gekennzeichnet, in dem verschiedene Gruppen untereinander und mit Anbietern krimineller Dienste zusammenarbeiten. 60 % der kriminellen Netzwerke wenden Gewalt im Rahmen ihrer kriminellen Geschäfte an, doch fast alle kriminellen

[89] Beschluss (GASP) 2021/142 des Rates vom 5. Februar 2021 zur Aktualisierung der Liste der Personen, Vereinigungen und Körperschaften, für die die Artikel 2, 3 und 4 des Gemeinsamen Standpunkts 2001/931/CFSP gelten.

[90] Beschluss (GASP) 2021/613 des Rates und Durchführungsverordnung (EU) 2021/612 des Rates vom 15. April 2021 zur Durchführung der Verordnung (EU) 2016/1686 zur Verhängung zusätzlicher restriktiver Maßnahmen gegen ISIL (Da'esh) und Al-Qaida und die mit ihnen verbundenen natürlichen oder juristischen Personen, Organisationen und Einrichtungen.

[91] https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment

Aktivitäten weisen inzwischen eine Online-Komponente irgendeiner Art auf. Die Gefahr einer Unterwanderung der legalen Wirtschaft durch die organisierte Kriminalität nimmt ebenfalls zu: Schätzungen zufolge nutzen mehr als 80 % legale Unternehmensstrukturen für kriminelle Aktivitäten.

Kriminelle, welche die durch die Pandemie verursachten wirtschaftlichen Schwachstellen ausnutzen

Aufgrund der Erfahrungen aus früheren Krisen kann davon ausgegangen werden, dass eine instabile Wirtschaftslage mit zunehmender Armut und sozialer Ungleichheit ein Nährboden für organisierte und schwere Kriminalität ist.

Unternehmen, die in Branchen tätig sind, welche unter besonders hohem wirtschaftlichem Druck leiden – wie Hotellerie, Gastronomie und Tourismus –, sind anfälliger für eine kriminelle Unterwanderung.[92]

Im Jahr 2020 erhielt und bearbeitete das bei Europol angesiedelte Europäische Zentrum für schwere und organisierte Kriminalität (ESOCC) mehr als 35 183 operative Beiträge in den sieben vom Zentrum abgedeckten Bereichen[93], was mehr als der Hälfte (57 %) der operativen Beiträge von Europol entspricht. Das ESOCC unterstützte die Mitgliedstaaten bei 837 Operationen, was einem Anstieg um 41 % gegenüber 2019 entspricht. Diese Zahlen spiegeln die Zunahme der Aktivitäten organisierter krimineller Gruppen und die wachsende Nachfrage der Mitgliedstaaten nach Unterstützung durch Europol in diesem Bereich wider. Das ESOCC organisierte und koordinierte 11 operative Taskforces, welche die Koordinierung nachrichtendienstlicher und ermittlungsrelevanter Maßnahmen im Hinblick auf 60 hochrangige Ziele, d. h. mutmaßliche Mitglieder krimineller Organisationen, die ein besonders hohes Risiko darstellen, übernahmen, wobei 21 dieser Mitglieder festgenommen wurden.

Als Beitrag zur Bewältigung der zunehmenden Herausforderungen nahm die Kommission im April die **EU-Strategie zur Bekämpfung der organisierten Kriminalität 2021–2025**[94] an. Darin werden vorrangige Maßnahmen zur Stärkung der Strafverfolgung und der justiziellen Zusammenarbeit, zur Gewährleistung wirksamer Ermittlungen für die Zerschlagung von Strukturen der organisierten Kriminalität und die Bekämpfung von Straftaten mit hoher Priorität, zum Ausschluss von Gewinnen aus der organisierten Kriminalität und zur Rüstung der Strafverfolgung und der Justiz für das digitale Zeitalter festgelegt. Außerdem stellte die Kommission die „Europäische multidisziplinäre Plattform gegen kriminelle Bedrohungen“ (EMPACT)[95] bereit. Darin wird dargelegt, wie EMPACT ihr Potenzial voll ausschöpfen und

[92] Auf der Grundlage des Beitrags der ersten Sitzung der Arbeitsgruppe zu kriminellen Bedrohungen und Strafverfolgungsmaßnahmen im Zusammenhang mit COVID-19; Europol 2020, „Enterprising criminals: Europe’s fight against the global networks of financial and economic crime“.

[93] Schleusung von Migranten, Hochrisikogruppen der organisierten Kriminalität, Umweltkriminalität, organisierte Eigentumskriminalität, Drogen, Menschenhandel sowie Waffen- und Sprengstoffhandel.

[94] COM(2021) 170 final.

[95] EMPACT ist das EU-Instrument für die polizeiliche Zusammenarbeit; Ziel ist es, den wichtigsten Bedrohungen für die Sicherheit der EU zu begegnen, indem die Zusammenarbeit zwischen den zuständigen Dienststellen der Mitgliedstaaten, den Organen, Einrichtungen und sonstigen Stellen der EU sowie Drittländern und Organisationen intensiviert wird. Das Instrument bringt verschiedene Interessenträger zusammen, um die Zusammenarbeit zwischen den Mitgliedstaaten, den Organen, Einrichtungen und sonstigen Stellen der EU sowie Drittländern und Organisationen, gegebenenfalls einschließlich des Privatsektors, zu verbessern und zu stärken (SWD(2021) 74 final).

zu einem Vorzeigeinstrument für die multidisziplinäre und behördenübergreifende operative Zusammenarbeit bei der Bekämpfung der organisierten Kriminalität werden kann. Darüber hinaus ist die Kommission eng in die laufende Vorbereitung des nächsten EMPACT-Zyklus einbezogen, der den Zeitraum 2022 bis 2025 abdecken wird.

Bekämpfung des Menschenhandels

Menschenhandel ist ein äußerst profitables Verbrechen, das Kriminellen auf Kosten der Opfer und der Gesellschaft insgesamt enorme Gewinne einbringt. Im April nahm die Kommission die Strategie der EU zur Bekämpfung des Menschenhandels 2021–2025[96] an. Da Menschenhandel häufig von organisierten Gruppen betrieben wird, steht diese Strategie in engem Zusammenhang mit der EU-Strategie zur Bekämpfung der organisierten Kriminalität. Im Rahmen der Strategie zur Bekämpfung des Menschenhandels werden rechtliche, politische und operative Initiativen vorgeschlagen, die von der Prävention bis zur Verurteilung von Straftätern reichen, wobei gleichzeitig der Opferschutz in allen Phasen, insbesondere unter Berücksichtigung von Frauen und Kindern als Opfer sowie Menschenhandel zum Zwecke der sexuellen Ausbeutung, betont wird. Der Schwerpunkt liegt auf der Verringerung der Nachfrage, die den Menschenhandel fördert, auf der Zerschlagung des kriminellen Modells, um die Ausbeutung der Opfer zu stoppen, auf dem Schutz, der Unterstützung und der Befähigung der Opfer und auf der Berücksichtigung der internationalen Dimension dieser Form der Kriminalität. Diese Themen waren das Ergebnis eines Berichts von Eurojust, der 18 Empfehlungen zur Unterstützung der Mitgliedstaaten enthält, wobei sich die Unterstützung nicht nur auf die Ermittlung, Strafverfolgung und justizielle Zusammenarbeit in Fällen des Menschenhandels bezieht, sondern auch auf die Identifizierung, die Rettung und den Schutz von Opfern.[97]

Bekämpfung illegaler Drogen

Nach der Annahme der EU-Drogenstrategie 2021–2025 werden die Beratungen über den entsprechenden Aktionsplan fortgesetzt, damit der Rat diesen spätestens zum Ende des portugiesischen Vorsitzes annehmen kann. An die Rechtsvorschriften zu neuen **psychoaktiven Substanzen**, die im November 2018 in vollem Umfang in Kraft traten, schloss sich ein delegierter Rechtsakt an, mit dem zwei neue psychoaktive Substanzen in die Drogendefinition aufgenommen wurden.[98]

Im Eurojust-Bericht über den Drogenhandel vom April 2021[99] wird hervorgehoben, dass die Produktion synthetischer Drogen und deren Verkäufe über das Darknet zugenommen haben; beides bringt rechtliche Herausforderungen für die Staatsanwaltschaften in der EU mit sich. Der Bericht enthält Empfehlungen zur Verstärkung der Finanzermittlungen, der Vermögensabschöpfung und der justiziellen Zusammenarbeit, auch mit Drittländern. Im März 2021 legte Eurojust anlässlich des jährlichen Dialogs zwischen der EU und den USA über Drogen zentrale Fragen und Beispiele für eine erfolgreiche justizielle Zusammenarbeit in Fällen des Drogenhandels zwischen den Mitgliedstaaten und den USA vor. Das erste Treffen des Dialogs EU-China über Drogen fand am 22. Januar 2021 statt und umfasste die

[96] Mitteilung der Kommission – Die Strategie der EU zur Bekämpfung des Menschenhandels 2021–2025 (COM(2021) 171 final).
[97] Der Bericht ist abrufbar unter https://www.eurojust.europa.eu/eurojust-report-trafficking-human-beings.
[98] Delegierte Richtlinie C(2021) 1570 final; der Zeitraum für die Prüfung durch das Europäische Parlament und den Rat endet Mitte Mai.
[99] Der Bericht ist abrufbar unter https://www.eurojust.europa.eu/eurojust-report-drug-trafficking.

Zusammenarbeit bei der Drogenbekämpfung. Die EU nahm an der 64. Tagung der Suchtstoffkommission der Vereinten Nationen teil und wiederholte ihre Forderung nach einer beschleunigten Umsetzung der umfassenden Verpflichtungen, die die internationale Gemeinschaft zur Bewältigung der weltweiten Drogensituation eingegangen ist.

Bekämpfung des illegalen Handels mit Feuerwaffen

Die kodifizierte Feuerwaffen-Richtlinie[100] trat im April 2021 in Kraft, und die Kommission hat in der Folge Vorschriften für den systematischen elektronischen Austausch von Informationen im Zusammenhang mit Versagungen von Genehmigungen für den Erwerb und den Besitz bestimmter Feuerwaffen[101] erlassen. Diese sollen ab dem 31. Januar 2022 gelten und es den zuständigen nationalen Behörden ermöglichen, zu erfahren, ob einem Antragsteller, der einen Waffenschein beantragt, in einem anderen Mitgliedstaat eine ähnliche Genehmigung verweigert wurde. Dadurch soll die Wahl des günstigsten Gerichtsstands zur Umgehung von Waffenbesitzverboten verhindert werden.

Die Kommission unterstützt ferner ein Pilotprojekt zur Echtzeitverfolgung von EU-weiten Vorfällen im Zusammenhang mit Feuerwaffen, um ein stets aktuelles Bild zu erhalten. Zur Unterstützung der Arbeit der Strafverfolgungsbehörden leitet die Kommission die Maßnahme zur Einrichtung und Entwicklung von Kontaktstellen für Feuerwaffen auf nationaler Ebene.

Im Hinblick auf die internationale Zusammenarbeit hat die Kommission die konstruktive Beteiligung der Türkei an den operativen Tätigkeiten von EMPACT im Zusammenhang mit der Bedrohung durch umbaubare Schreckschuss- und Signalwaffen aktiv unterstützt. Sie trug auch dazu bei, das Thema des illegalen Handels mit Feuerwaffen wieder auf die Agenda der Zusammenarbeit mit den Ländern des Nahen Ostens und Nordafrikas zu setzen. Darüber hinaus hatte die Kommission einen großen Anteil bei der operativen Zusammenarbeit mit Südosteuropa, unter anderem durch die Vorbereitung einer gemeinsamen Operation der Mitgliedstaaten und der Partner im Westbalkan sowie durch regionale Treffen mit den Kommissionen für Kleinwaffen und leichte Waffen.

Das EU-Programm „Global Illicit Flows“[102] (globale illegale Ströme) ist weiterhin ein wirksamer Mechanismus zur Koordinierung der transregionalen Maßnahmen gegen die organisierte Kriminalität und zur Stärkung der Kapazitäten von mehr als 80 Partnerländern weltweit, um den Handel mit illegalen Waren zu unterbinden, wobei der Schwerpunkt auf Betäubungsmitteln und Feuerwaffen liegt. Außerdem konnten EU-Agenturen und EU-Mitgliedstaaten mithilfe des Programms die Reichweite ihrer Strafverfolgung ausdehnen.

Bekämpfung der Finanzkriminalität

Im Rahmen der Bekämpfung der Gefahr der Unterwanderung der legalen Wirtschaft durch die organisierte Kriminalität sind die Mitgliedstaaten verpflichtet, die Richtlinie von 2019 zur Erleichterung der Nutzung von Finanz- und sonstigen Informationen für die Verhütung,

---

[100] Richtlinie (EU) 2021/555 des Europäischen Parlaments und des Rates vom 24. März 2021 über die Kontrolle des Erwerbs und des Besitzes von Waffen (kodifizierter Text).

[101] Delegierte Verordnung der Kommission zur Festlegung detaillierter Vorkehrungen gemäß der Richtlinie(EU) 2021/555 des Europäischen Parlaments und des Rates für den systematischen elektronischen Austausch von Informationen im Zusammenhang mit Versagungen von Genehmigungen für den Erwerb und den Besitz bestimmter Feuerwaffen (C(2021) 3400 final).

[102] https://illicitflows.eu/

Aufdeckung, Untersuchung oder Verfolgung bestimmter Straftaten[103] bis August 2021 umzusetzen. Die Kommission wird die Umsetzung und wirksame Anwendung der Richtlinie genau überwachen.

Im Mai und Juni 2021 fanden zwei Konsultationssitzungen mit den Mitgliedstaaten zur Überarbeitung des Beschlusses des Rates über Vermögensabschöpfungsstellen[104] und der Richtlinie über die Sicherstellung und Einziehung[105] statt. In den Beratungen wurden der Mehrwert dieser Instrumente für eine verbesserte Vermögensabschöpfung in der Union und die Bedeutung einer wirksamen Verwaltung eingezogener Vermögenswerte, unter uneingeschränkter Achtung der Grundrechte, sowie die Notwendigkeit einer besseren Zusammenarbeit während des gesamten Prozesses der Vermögensabschöpfung hervorgehoben.

Seit dem 3. Juni 2021 gelten neue Rechtsvorschriften für die Überwachung von Barmitteln, die in die Union oder aus der Union verbracht werden[106], und seit Mai sind wesentliche Durchführungsvorschriften zur Festlegung diesbezüglicher Verfahren und technischer Vorschriften[107] in Kraft. Weitere Durchführungsvorschriften zur Festlegung von Kriterien für den gemeinsamen Risikomanagementrahmen bei Barmittelbewegungen werden derzeit erarbeitet.

Am 1. Juni 2021 hat die Europäische Staatsanwaltschaft (EUStA) ihre Ermittlungs- und Strafverfolgungstätigkeit aufgenommen. Die EUStA hat nun damit begonnen, Straftaten zum Nachteil der finanziellen Interessen der Union zu untersuchen und strafrechtlich zu verfolgen. Zu den von der EUStA untersuchten und verfolgten Straftaten zählt der Mehrwertsteuerbetrug im Zusammenhang mit dem Hoheitsgebiet von zwei oder mehr Mitgliedstaaten mit einem Gesamtschaden von mindestens 10 Mio. EUR. Jedes Jahr gehen den Mitgliedstaaten durch Betrug Mehrwertsteuereinnahmen in Milliardenhöhe verloren.

Bekämpfung der Umweltkriminalität

Die **Richtlinie** 2008/99/EG über den **strafrechtlichen Schutz der Umwelt** ist das wichtigste Rechtsinstrument der EU für den strafrechtlichen Schutz der Umwelt. Derzeit laufen umfassende Konsultationen zur Überarbeitung des Textes, um die Anwendung zu verbessern und die Funktion der Strafverfolgungskette (Aufdeckung, Ermittlung, Strafverfolgung, Strafgerichtsbarkeit) zu stärken. Die Arbeit zur Bekämpfung der Umweltkriminalität wird

[103] 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.

[104] Beschluss 2007/845/JI des Rates vom 6. Dezember 2007 über die Zusammenarbeit zwischen den Vermögensabschöpfungsstellen der Mitgliedstaaten auf dem Gebiet des Aufspürens und der Ermittlung von Erträgen aus Straftaten oder anderen Vermögensgegenständen im Zusammenhang mit Straftaten.

[105] Richtlinie 2014/42/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Sicherstellung und Einziehung von Tatwerkzeugen und Erträgen aus Straftaten in der Europäischen Union.

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

[107] Durchführungsverordnung (EU) 2021/776 der Kommission vom 11. Mai 2021 zur Festlegung von Mustern für bestimmte Formulare sowie von technischen Vorschriften für den wirksamen Informationsaustausch gemäß der Verordnung (EU) 2018/1672 des Europäischen Parlaments und des Rates über die Überwachung von Barmitteln, die in die Union oder aus der Union verbracht werden.

auch im Rahmen des Forums für den Vollzug des Umweltrechts und Umweltordnungspolitik (Environmental Compliance and Governance Forum)[108] vorangetrieben, in dessen Sitzungen im Januar und Juni 2021 die Überarbeitung der Richtlinie und die Bekämpfung der Umweltkriminalität im Allgemeinen im Mittelpunkt standen.

Bekämpfung des illegalen Handels mit Kulturgütern

Die EU-Rechtsvorschriften über die Einfuhr von Kulturgütern zielen darauf ab, die Einfuhr illegal aus ihrem Ursprungsland ausgeführter Kulturgüter zu unterbinden. Derzeit werden Durchführungsbestimmungen für ein zentrales elektronisches System für die Einfuhr von Kulturgütern (Import of Cultural Goods – ICG) erlassen, das die Speicherung und den Austausch von Informationen zwischen den Mitgliedstaaten und die Erfüllung der Einfuhrförmlichkeiten ermöglicht. Die allgemeine Verbotsvorschrift durch die Verordnung[109] trat am 28. Dezember 2020 in Kraft; somit können die Zollbehörden der Mitgliedstaaten Sendungen kontrollieren, die möglicherweise unzulässig aus ihrem Ursprungsland ausgeführte Kulturgüter enthalten, und entsprechend tätig werden.

V. Eine starke europäische Sicherheitsgemeinschaft

1. Zusammenarbeit und Informationsaustausch

In der EU-Strategie für eine Sicherheitsunion wird dargelegt, wie das Handeln der EU einen wesentlichen Beitrag zur Bewältigung zunehmend komplexer sowie grenz- und sektorübergreifender Sicherheitsbedrohungen leisten kann, indem die im Sicherheitsbereich tätigen Akteure in den Mitgliedstaaten mit den benötigten Instrumenten und Informationen unterstützt werden.

Europol spielt in dieser Hinsicht eine zentrale Rolle. Mit dem im Dezember letzten Jahres angenommenen Vorschlag der Kommission zur Modernisierung und Stärkung des **Mandats von Europol**[110] wird auf spezifische Sachzwänge eingegangen, denen sich Europol heute gegenübersieht, wie zum Beispiel die Beziehungen Europols zum Privatsektor. Darüber hinaus schlägt die Kommission vor, Europol die Erstellung von Ausschreibungen von Terroristen und anderen Straftätern im Schengener Informationssystem auf der Grundlage von Informationen aus Drittstaaten zu ermöglichen. Dadurch kann Europol die Mitgliedstaaten bei der Bekämpfung von schwerer Kriminalität und Terrorismus besser unterstützen. Die Kommission sieht einer raschen Formulierung der Standpunkte des Europäischen Parlaments und des Rates entgegen, damit Trilog-Gespräche unter dem slowenischen Ratsvorsitz aufgenommen werden können.

Die **EU und Interpol** arbeiten bereits seit Langem eng zusammen. Interpol ist ein wichtiger Partner für die EU im Bereich der inneren und äußeren Sicherheit, einschließlich der Bekämpfung von Terrorismus und organisierter Kriminalität, sowie beim integrierten Grenzmanagement. Die Kommission hat Verhandlungen vorgeschlagen, um die operative und strategische Zusammenarbeit durch ein Kooperationsabkommen[111] weiter zu verbessern.

---

[108] Compliance Assurance - Legislation - Environment - European Commission (europa.eu)

[109] Verordnung (EU) 2019/880 des Europäischen Parlaments und des Rates vom 17. April 2019 über das Verbringen und die Einfuhr von Kulturgütern.

[110] COM(2020) 791 final und COM(2020) 796 final.

[111] COM(2021) 177 final.

Auf operativer Ebene laufen die Vorbereitungen für die vollständige Umsetzung der Überarbeitung des **Schengener Informationssystems** (SIS) mit dem Ziel, alle erforderlichen Tests bis Ende 2021 abzuschließen. Im März 2021 wurde Europol an das SIRENE[112]-Mail-Relais angeschlossen. Ende 2020 hatten die meisten Mitgliedstaaten die neue SIS-Suchfunktion für Fingerabdrücke[113] eingeführt.

Die Arbeit zur Änderung der Rechtsvorschriften wurde aufgenommen, um die Möglichkeit von **Eurojust** zu verbessern, Verbindungen zwischen parallelen Verfahren in Fällen von grenzüberschreitendem Terrorismus zu erkennen.[114] Gleichzeitig wurden von Eurojust weiterhin operative Folgemaßnahmen und Koordinierungstätigkeiten auf der Grundlage von Informationen unternommen, die über das europäische Justizielle Terrorismusregister (CTR) übermittelt werden. Dieses Register wurde mit dem Ziel eingerichtet, Verbindungen zwischen Gerichtsverfahren im Bereich der Terrorismusbekämpfung in den Mitgliedstaaten ausfindig zu machen. Aus den bisherigen Erfahrungen mit dem CTR geht hervor, dass die an Eurojust übermittelten Informationen erheblich zugenommen haben, und es wurden bereits einige Verbindungen zwischen Verfahren festgestellt, die den nationalen Behörden zuvor nicht bekannt waren. Des Weiteren konnte durch das CTR der Informationsaustausch in Verfahren im Bereich der Terrorismusbekämpfung erheblich verbessert werden.

Mit den Vorbereitungen für die Einrichtung der **Kooperationsplattform für gemeinsame Ermittlungsgruppen (GEG)** wurde begonnen. Konsultationen mit den Mitgliedstaaten, dem Sekretariat des GEG-Netzes, Eurojust, Europol und OLAF über die Gestaltung der Kooperationsplattform sind im Gange. Seit April 2021 leistet Eurojust auch finanzielle Unterstützung für GEG außerhalb des regulären Finanzierungssystems für dringende und/oder unvorhergesehene Maßnahmen.[115]

Fluggastdatensätze (PNR-Daten) sind eine wichtige Informationsquelle zur Identifizierung von Personen, die ein Sicherheitsrisiko darstellen. Auf der Grundlage der Informationen, die zur Vorbereitung einer Überarbeitung der Rechtsvorschriften[116] gesammelt wurden, unterstützt die Kommission die Mitgliedstaaten dabei, die Nutzung von PNR-Daten zu verbessern und die Zusammenarbeit zu vertiefen[117]. Die meisten nationalen PNR-Zentralstellen sind inzwischen voll funktionsfähig, und die Verarbeitung von PNR-Daten ist ein wichtiges Instrument für die nationalen Strafverfolgungsbehörden bei der Bekämpfung von Terrorismus und schwerer Kriminalität, auch wenn die Zahl der Fluggäste während der Pandemie zurückgegangen ist.

Auch auf internationaler Ebene wurde die Arbeit intensiviert. Am 30. Dezember 2020 wurde das Handels- und Kooperationsabkommen zwischen der EU und dem Vereinigten

---

[112] Supplementary Information Request at the National Entries (Antrag auf Zusatzinformationen bei der nationalen Eingangsstelle). Jedes EU-Land, das das SIS betreibt, hat ein nationales SIRENE-Büro eingerichtet, das für den Austausch von Zusatzinformationen und die Koordinierung der Tätigkeiten im Zusammenhang mit SIS-Ausschreibungen zuständig ist.

[113] Automatisiertes Fingerabdruck-Identifizierungssystem.

[114] Beschluss 2005/671/JI des Rates und Verordnung (EU) 2018/1727 des Europäischen Parlaments und des Rates.

[115] https://www.eurojust.europa.eu/eurojust-launches-new-scheme-urgent-jit-funding

[116] COM(2020) 305 final über die Überprüfung der Richtlinie (EU) 2016/681.

[117] Slowenien ist der letzte Mitgliedstaat, dessen nationale Maßnahmen zur Umsetzung der PNR-Richtlinie von der Kommission derzeit geprüft werden, während alle anderen Mitgliedstaaten die Richtlinie vollständig umgesetzt haben.

Königreich[118] unterzeichnet und ist seit Mai in Kraft. Es umfasst den Austausch von PNR-Daten und deren Verwendung zum Zwecke der Bekämpfung von Terrorismus und schwerer Kriminalität. Die Kommission nahm Berichte[119] über die gemeinsame Evaluierung der bestehenden internationalen PNR-Abkommen mit den USA und Australien sowie über die gemeinsame Überprüfung der Durchführung des Abkommens zwischen der EU und Australien an. Insgesamt bestätigten diese Berichte den Nutzen der Verwendung von PNR-Daten, ihre Wirksamkeit bei der Erreichung der angestrebten Zwecke und die Einmaligkeit der durch die PNR-Daten verfügbaren Informationen. Im Januar 2021 nahm der Rat den Standpunkt der Union[120] an, in dem die Annahme neuer Richtlinien und Empfehlungen für die Verarbeitung und den Schutz von Fluggastdatensätzen durch die Internationale Zivilluftfahrt-Organisation (ICAO) begrüßt wird. Am 28. Februar 2021 trat der ICAO-Beschluss in Kraft und ist für alle ICAO-Mitglieder verbindlich;[121] er stellt nun eine solide Grundlage für die weltweite Verarbeitung von Fluggastdatensätzen unter uneingeschränkter Achtung der Grundrechte dar.

Derzeit laufen Verhandlungen über den Austausch personenbezogener Daten zwischen Europol und bestimmten Drittstaaten zur Bekämpfung von schwerer Kriminalität und Terrorismus. Die ersten beiden Verhandlungsrunden mit Neuseeland fanden in einer konstruktiven Atmosphäre statt. Auch bei den Verhandlungen mit der Türkei wurden Fortschritte erzielt, und es fanden konstruktive Gespräche mit Tunesien statt. Mit einer Reihe weiterer Länder sind Sondierungsgespräche auf fachlicher Ebene im Gange.

Im März 2021 erteilte der Rat der Kommission das Mandat, Verhandlungen über Abkommen zwischen der EU und 13 Drittstaaten[122] über die Zusammenarbeit zwischen Eurojust und den für die justizielle Zusammenarbeit in Strafsachen zuständigen Behörden aufzunehmen. Diese internationalen Abkommen werden einen wichtigen Eckpfeiler der EU-Sicherheitsvorschriften darstellen und sollen weltweit zu einer besseren Bekämpfung der organisierten Kriminalität beitragen.

Seit 2012 gewährleistet das **Europäische Strafregisterinformationssystem (ECRIS)** den effizienten elektronischen Austausch von Strafregisterinformationen zwischen den Mitgliedstaaten, wobei jährlich mehr als vier Millionen Nachrichten ausgetauscht werden. Die Kommission hat einen Bericht über die Funktionsweise von ECRIS[123] angenommen und wertet derzeit die Ergebnisse mit den Mitgliedstaaten aus. An der Entwicklung und Umsetzung eines zentralisierten Systems zur Ermittlung der Mitgliedstaaten, in denen Informationen über Verurteilungen von Drittstaatsangehörigen vorliegen (ECRIS-TCN), wird derzeit gearbeitet, und das System soll 2023 in Betrieb genommen werden. Das neue System soll ECRIS ergänzen und den Austausch von Informationen über in der EU verurteilte Drittstaatsangehörige ermöglichen.

---

[118] ABl. L 444 vom 31.12.2020, S. 14.
[119] COM(2021) 17 final, COM(2021) 18 final und COM(2021) 19 final.
[120] ABl. L 37 vom 3.2.2021, S. 6.
[121] Die Mitgliedstaaten haben eine abweichende Regelung in Bezug auf einen Teil der einschlägigen Richtlinien und Empfehlungen (SARP) eingeführt.
[122] Ägypten, Algerien, Argentinien, Armenien, Bosnien und Herzegowina, Brasilien, Israel, Jordanien, Kolumbien, Libanon, Marokko, Türkei und Tunesien.
[123] COM(2020) 778 final, SWD(2020) 378 final vom 21. Dezember 2020.

2. *Der Beitrag starker Außengrenzen*

Ein effizientes Management der EU-Außengrenzen ist für die Gewährleistung der Sicherheit der Bürgerinnen und Bürger von zentraler Bedeutung. Die Schengen-Strategie[124] der Kommission umfasst Maßnahmen in diesem Bereich, die die Integrität des Schengen-Raums schützen und dessen Funktionsweise weiter verbessern. Derzeit wird an einer neuen Architektur der EU-Informationssysteme für Sicherheit, Grenz- und Migrationsmanagement gearbeitet, um die nationalen Behörden zu unterstützen. Es ist von entscheidender Bedeutung, dass die Mitgliedstaaten ohne Verzögerung die notwendigen Schritte unternehmen, um den vereinbarten Umsetzungszeitplan einzuhalten, damit dieses ehrgeizige Projekt verwirklicht werden kann.

Die Arbeit zur Anwendung der **Interoperabilitätsverordnungen** kommt voran, wobei die Verordnungen bis Ende 2023 in vollem Umfang anwendbar sein sollen. EU-LISA schließt derzeit die Beschaffung der verschiedenen Interoperabilitätskomponenten ab, und die Kommission arbeitet zusammen mit Experten an einem Leitfaden. Des Weiteren laufen die Vorbereitungen für die Inbetriebnahme des **Einreise-/Ausreisesystems** (EES), damit die Tests und Schulungen Anfang 2022 vor Inbetriebnahme des Systems im Mai 2022 abgeschlossen werden können. Außerdem schreiten die Vorbereitungen für das **Europäische Reiseinformations- und -genehmigungssystem** (ETIAS) voran, dessen Inbetriebnahme Ende 2022 geplant ist. Das Europäische Parlament und der Rat haben sich nun auch auf den Vorschlag geeinigt, mit dem die Verbindung zwischen ETIAS und den einschlägigen EU-Datenbanken sichergestellt werden soll.

Im Dezember 2020 haben das Europäische Parlament und der Rat eine vorläufige Einigung über den Vorschlag der Kommission zur Überarbeitung und Modernisierung des **Visa-Informationssystems** (VIS) erzielt. Zu den wichtigsten Vorteilen der vereinbarten Änderungen gehören eine gründlichere Hintergrundüberprüfung von Visumantragstellern, die Schließung von Sicherheitsdatenlücken durch einen besseren Informationsaustausch zwischen den Mitgliedstaaten, die Ausweitung des Visa-Informationssystems auf Visa für den längerfristigen Aufenthalt und Aufenthaltstitel sowie die Bekämpfung des Menschenhandels durch die Senkung des Alters für die Abnahme von Fingerabdrücken für Minderjährige. Zusammen mit den anderen neuen und modernisierten Informationssystemen dürfte das neue VIS bis Ende 2023 betriebsbereit und vollständig interoperabel sein.

Seit dem 1. Januar werden die ersten Teams der ständigen Reserve der **Europäischen Grenz- und Küstenwache** erfolgreich eingesetzt. Die ständige Reserve, die sich aus 10 000 Frontex- und nationalen Beamten zusammensetzt, wird die Grenzsicherheit erheblich verbessern, da sie in den kommenden Jahren allmählich wächst, um ihre volle Kapazität zu erreichen. Mit der kürzlich angenommenen Durchführungsverordnung über das Europäische Grenzüberwachungssystem (Eurosur)[125] sollen das Lagebewusstsein und die Reaktionsfähigkeit an den Außengrenzen weiter verbessert werden, um illegale Einwanderung und grenzüberschreitende Kriminalität aufzudecken, zu verhüten und zu bekämpfen.

---

[124] COM(2021) 277 final.

[125] Durchführungsverordnung (EU) 2021/581 der Kommission.

Zollkontrollen
Die Kommission erarbeitet derzeit eine neue Strategie für das Zollrisikomanagement, die darauf abzielt, den strukturierten Ansatz für das Zollrisikomanagement zu verbessern, Kontrollen wirksamer zu gestalten und die Risiken für die EU und ihre Bürgerinnen und Bürger zu verringern, bei gleichzeitiger Gewährleistung der Wettbewerbsfähigkeit rechtmäßiger EU-Unternehmen.

Im Rahmen der Strategie und des Aktionsplans der EU zur Stärkung des Zollrisikomanagements entwickelt die Kommission gegenwärtig auch das neue System für ein vorausschauendes Frachtrisikomanagement, das eine gemeinsame Risikoanalyse im Bereich Sicherheit und Gefahrenabwehr ermöglicht, bevor Waren in die EU gelangen oder für den Transport in die EU verladen werden.[126]

3. Intensivierung von Sicherheitsforschung und Innovation

Innovation sollte als strategisches Instrument für die EU betrachtet werden: Sie wirkt sich horizontal auf fast alle Aspekte der Sicherheitsgemeinschaft aus, indem sie neue Wege zur Bewältigung der technologischen Herausforderungen eröffnet, die strategische Abhängigkeit verringert und die Lieferketten stärkt. Aus diesem Grund werden bei der Gestaltung der wichtigsten Forschungsprojekte der EU die Sicherheitsdimension, die Bedürfnisse der EU und die Rolle des Privatsektors berücksichtigt.

Der Aufbau des **europäischen Innovationszentrums für innere Sicherheit** wird fortgesetzt. Im Rahmen des Programms „**Horizont Europa“** wird die Reaktion der EU auf Sicherheitsherausforderungen unterstützt, wobei für den Zeitraum 2021–2027 Finanzmittel in Höhe von 1,6 Mrd. EUR bereitgestellt werden. Im März 2021 nahm die Kommission den ersten Strategieplan für Horizont Europa an, und es wurden strategische Leitlinien für die ersten vier Jahre festgelegt: Die Sicherheitsforschung wird als Instrument für den Übergang von einem reaktiven Ansatz im Bereich der Sicherheit zu einem proaktiven Ansatz dienen, der auf Vorausschau und Prävention beruht. Ein neues Arbeitsprogramm für den Zeitraum 2021–2022 wurde vereinbart, mit dem die Umsetzung der Dimension der inneren Sicherheit der EU-Strategie für eine Sicherheitsunion, die Grenzmanagement- und Sicherheitsaspekte der Migrations- und Asylpolitik und die EU-Politik zur Verringerung des Katastrophenrisikos unterstützt wird.

Die Finanzierung durch EU-Mittel bietet weitere Möglichkeiten zur Intensivierung der europäischen Innovation an der Schnittstelle zwischen Verteidigung, Weltraum und ziviler Nutzung. Im Februar 2021 hat die Kommission den Aktionsplan für Synergien zwischen der **zivilen, der Verteidigungs- und der Weltraumindustrie**[127] auf den Weg gebracht. Es wurden drei Vorzeigeprojekte ermittelt (zu den Themen Drohnentechnologien, weltraumgestützte sichere Konnektivität und Weltraumverkehrsmanagement). Mit dem Aktionsplan wird die Sicherheitsbranche der EU durch modernste, innovative Lösungen unterstützt, die sich aus der gegenseitigen Bereicherung und aus effizienten Synergien zwischen der zivilen, der Verteidigungs- und der Weltraumindustrie ergeben.

---

[126] Release 1, das Luftkurier- und Luftpostdienste abdeckt, wurde im März in Betrieb genommen. Release 2 in Bezug auf allgemeine Luftfracht ist für März 2023 geplant. Das dritte Release, das sich auf den See-, Straßen- und Schienenverkehr bezieht, ist für 2024 geplant.

[127] COM(2021) 70 final.

Weltraumtechnologien, -daten und -dienste sind für die Sicherheit der Europäerinnen und Europäer unverzichtbar geworden und spielen eine wichtige Rolle für die Wahrung zahlreicher strategischer Interessen. Mit der im April erlassenen **Verordnung über die Einrichtung des Weltraumprogramms**[128], für das Haushaltsmittel in Höhe von 14,6 Mrd. EUR vorgesehen sind, wird eine neue Komponente für die staatliche Satellitenkommunikation eingeführt, die den Grundstein für eine sichere weltraumgestützte Konnektivität in der EU bildet.

4. Sicherheitskompetenzen und Sicherheitsbewusstsein

Für eine resilientere Gesellschaft mit besser gerüsteten Unternehmen und Verwaltungen und besser vorbereiteten Bürgern kommt es entscheidend darauf an, dass ein Bewusstsein für Sicherheitsbedrohungen und Kompetenzen im Umgang damit vorhanden sind. Am 9. Februar 2021 fand der 18. Safer Internet Day online in 170 Ländern statt, mit Jugendbotschaftern von „Better Internet for Kids“ und Vertretern der Industrieallianz. Der Aktionsplan der EU für digitale Bildung (2021–2027) enthält eine Maßnahme, mit der Lehrkräfte und Bildungspersonal bei der Förderung der digitalen Kompetenz und der Bekämpfung von Desinformation unterstützt werden sollen. Es werden Leitlinien erarbeitet, die im September 2022 in der gesamten EU eingeführt werden sollen.

Gute Kenntnisse des digitalen Umfelds und die Entwicklung entsprechender Kompetenzen im privaten und öffentlichen Sektor sind von grundlegender Bedeutung für eine resiliente und wettbewerbsfähige Gesellschaft. Im Rahmen des Programms „Digitales Europa“ wurde im Mai eine erste Aufforderung zur Einreichung von Vorschlägen für die Errichtung europäischer Zentren für digitale Innovation (European Digital Innovation Hubs – EDIHs)[129] veröffentlicht; Ziel ist, die ersten Zentren Anfang 2022 in Betrieb nehmen zu können. Die EDIHs unterstützen private und öffentliche Akteure, indem sie Zugang zu technischem Fachwissen und Experimentiereinrichtungen bieten und die breite Akzeptanz von Künstlicher Intelligenz, Hochleistungsrechnen (HPC) und Cybersicherheit sowie anderen digitalen Technologien seitens der Branche (insbesondere KMU und Mid Caps) und Organisationen des öffentlichen Sektors in Europa fördern.

In einer sich beständig verändernden Sicherheitslandschaft sollten Strafverfolgungsbeamte und Justizbedienstete stets auf dem neuesten Stand sein. Eine Bewertung der **Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (CEPOL)** wird im zweiten Halbjahr 2021 abgeschlossen. Ende 2020 hat die Kommission eine Strategie für die justizielle Aus- und Fortbildung auf europäischer Ebene für den Zeitraum 2021–2024[130] angenommen und im Mai 2021 zusammen mit dem portugiesischen Ratsvorsitz eine Konferenz für Interessenträger veranstaltet, um die Ausbildung von Richtern und Staatsanwälten zu fördern.

Das Sicherheitsbewusstsein steht auch im Mittelpunkt der im Juni 2020 angenommenen EU-Strategie für die **Rechte von Opfern** (2020–2025), mit der sichergestellt werden soll, dass

---

[128] Verordnung (EU) 2021/696 des Europäischen Parlaments und des Rates vom 28. April 2021 zur Einrichtung des Weltraumprogramms der Union und der Agentur der Europäischen Union für das Weltraumprogramm und zur Aufhebung der Verordnungen (EU) Nr. 912/2010, (EU) Nr. 1285/2013 und (EU) Nr. 377/2014 sowie des Beschlusses Nr. 541/2014/EU.

[129] https://digital-strategy.ec.europa.eu/en/activities/edihs

[130] COM(2020) 713 final.

sich alle Opfer von Straftaten unabhängig davon, wo und unter welchen Umständen die Straftat stattfindet, uneingeschränkt auf ihre Rechte berufen können. Die erste Plenarsitzung der Plattform für Opferrechte fand im Februar 2021 statt. Des Weiteren arbeitet die Kommission derzeit an der Evaluierung der Opferschutzrichtlinie und kann 2022 gegebenenfalls Änderungen der Rechtsvorschriften vorschlagen.

5. Die Rolle der EU-Agenturen

Die EU-Strategie für eine Sicherheitsunion beruht auf einem gesamtgesellschaftlichen Ansatz, bei dem alle Institutionen, Organisationen und Behörden, die beim Schutz der Bürgerinnen und Bürger der EU eine Rolle spielen, zusammengeführt werden. Neben der Unterstützung und dem Fachwissen, die sie den Mitgliedstaaten zur Verfügung stellen, spielen die EU-Agenturen eine entscheidende Rolle bei der Förderung der Zusammenarbeit und des Informationsaustauschs zwischen den nationalen Behörden der Mitgliedstaaten auf operativer Ebene. Angesichts der Vielzahl neuer und sich abzeichnender Bedrohungen in der derzeitigen Lage müssen Synergien und die Koordinierung der Tätigkeiten der EU-Agenturen weiter gefördert werden.

Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol)
Die Jahresberichte von Europol über die Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität (SOCTA), des Terrorismus (TE-SAT) und der organisierten Kriminalität im Internet (IOCTA) liefern wichtige Daten und Analysen zur Unterstützung politischer und operativer Maßnahmen im Bereich der Sicherheit. Des Weiteren trägt Europol dazu bei, die operative Wirksamkeit der Strafverfolgung insgesamt zu verbessern, indem sie ihre Zusammenarbeit mit Drittländern zur Bekämpfung von Kriminalität und Terrorismus im Einklang mit anderen außenpolitischen Maßnahmen und Instrumenten der EU ausweitet.

Das Operations- und Analysezentrum ist die Informationszentrale von Europol. Das Zentrum überwacht Operationen und Entwicklungen rund um die Uhr, arbeitet mit Drittländern und Organisationen zusammen und entsendet Experten vor Ort. Des Weiteren stellt es Analysen für die anderen Zentren und Organisationen von Europol bereit. Das bei Europol angesiedelte Europäische Zentrum für schwere und organisierte Kriminalität unterstützt die EU-Länder bei der Bekämpfung internationaler krimineller Netze, die an Drogen-, Waffen- und Sprengstoffhandel sowie Eigentums- und Umweltkriminalität beteiligt sind. Das Zentrum beherbergt auch das Europäische Zentrum zur Bekämpfung der Migrantenschleusung, das für die Beobachtung und Zerschlagung der komplexen und ausgefeilten kriminellen Netze, die in die Schleusung von Migranten verstrickt sind, zuständig ist. Das Europäische Zentrum für Finanz- und Wirtschaftskriminalität von Europol bietet dagegen Unterstützung bei hochkomplexen Fällen von Geldwäsche, Vorschussbetrug und Betrug, die sich gegen Einzelpersonen, Unternehmen und den öffentlichen Sektor richten.

Der Beitrag von Europol ist ebenfalls für die Koordinierung des EU-Konzepts zur Terrorismusbekämpfung von grundlegender Bedeutung. Europol hat die Mitgliedstaaten weiterhin bei Ermittlungen im Zusammenhang mit Terrorismus über das Europäische Zentrum zur Terrorismusbekämpfung (ECTC) unterstützt. Trotz der Beschränkungen infolge der Pandemie hat das ECTC im Jahr 2020 bei 776 Operationen zur Terrorismusbekämpfung Unterstützung geleistet (gegenüber 632 Operationen 2019). Die EU-Meldestelle für Internetinhalte bei Europol hat ebenfalls nach wie vor eine entscheidende Rolle bei der

Überwachung der Online-Aktivitäten terroristischer Gruppen und der von Plattformen ergriffenen Maßnahmen sowie bei der Weiterentwicklung des EU-Krisenreaktionsprotokolls gespielt. Europol ist entschlossen, die Mitgliedstaaten auch künftig beim Ausbau ihrer nationalen Kapazitäten zur Verhinderung terroristischer Online-Inhalte durch die Organisation von Tagen für die gezielte Meldung von Internetinhalten (Targeted Referral Action Days) zu unterstützen.

Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust)
In den ersten Monaten des Jahres 2021 unterstützte Eurojust mehrere grenzüberschreitende Ermittlungen und Strafverfolgungsmaßnahmen gegen auf Betrug spezialisierte Gruppen der organisierten Kriminalität. Außerdem stellte Eurojust die Beschlagnahme von Unternehmensvermögen oder die administrative Schließung von Unternehmen sicher, die für Betrug genutzt wurden.[131]

Ferner unterstützte Eurojust wichtige gemeinsame internationale Operationen zur Zerschlagung von cyberkriminellen Netzen. Diese Operationen richteten sich unter anderem gegen kriminelle Gruppen, die eine plattformübergreifende mobile Anwendung mit der Bezeichnung Mobdro betrieben, mit der das illegale Streaming von audiovisuellen Werken, einschließlich Fußballspielen, erleichtert wurde.[132] Gegenstand einer weiteren Operation war eine der gefährlichsten Schadsoftware (EMOTET), die eingesetzt wurde, um die betroffenen Rechner für Infektionen durch Dritte zu öffnen.[133] Des Weiteren arbeitete Eurojust mit Angehörigen der Rechtsberufe zusammen, um dazu beizutragen, rechtliche und operative Herausforderungen bei der Ermittlung und Verfolgung von Straftaten zu erfassen, die von rechtsextremistischen und terroristischen Gruppen sowie von Einzeltätern begangen werden, und um den Erfahrungsaustausch zu erleichtern.[134]

Zusammenarbeit zwischen den Agenturen
Auf operativer Ebene unterzeichneten Europol und Eurojust am 23. Dezember 2020 eine Beitragsvereinbarung[135], mit der ihre Partnerschaft bei der Unterstützung von Strafverfolgungs- und Justizbehörden beim grenzüberschreitenden Zugang zu elektronischen Beweismitteln ausgebaut wird. Eurojust und Europol haben darüber hinaus bilaterale Arbeitsvereinbarungen mit der **Europäischen Staatsanwaltschaft (EUStA)** zur Regelung ihrer künftigen Beziehungen geschlossen, um eine enge Zusammenarbeit für einen besseren Schutz der finanziellen Interessen der Union innerhalb der Grenzen der EU und darüber hinaus sicherzustellen. Dank einer engen Zusammenarbeit zwischen Europol, Eurojust und dem Europäischen Justiziellen Netz unterstützt das Projekt SIRIUS[136] sowohl die Strafverfolgungs- als auch die Justizbehörden der EU durch Schulungen und Leitlinien zur Verbesserung der Zusammenarbeit (hauptsächlich zwischen der EU und den USA) beim grenzüberschreitenden Zugang zu elektronischen Informationen. Im März einigten sich Eurojust und das Amt der Europäischen Union für geistiges Eigentum (EUIPO) darauf, ihre

131 https://www.eurojust.europa.eu/action-counter-italian-fuel-tax-fraud-worth-almost-eur-1-billion
132 https://www.eurojust.europa.eu/eurojust-supports-spanish-action-against-illegal-streaming-football-matches
133 https://www.eurojust.europa.eu/worlds-most-dangerous-malware-emotet-disrupted-through-global-action
134 https://www.eurojust.europa.eu/eurojust-expert-workshops-violent-right-wing-extremism-and-terrorism
135 Europol arbeitet mit Eurojust beim Projekt SIRIUS zusammen, das eine für Strafverfolgungs- und Justizbehörden zugängliche interaktive Plattform für den Wissensaustausch umfasst und das Ziel hat, Schulungen und Leitlinien auszuarbeiten und zu verbreiten, um die Zusammenarbeit – hauptsächlich zwischen der EU und den USA – beim grenzüberschreitenden Zugang zu elektronischen Informationen zu verbessern.
136 https://www.europol.europa.eu/activities-services/sirius-project

Zusammenarbeit zur Bekämpfung von Fälschungen und Online-Piraterie zu intensivieren.[137] Diese neue Vereinbarung markiert eine neue Ära der Zusammenarbeit zwischen Eurojust, Europol und dem EUIPO, die eine wirksame Unterstützung über den gesamten Lebenszyklus von Fällen – von der Strafanzeige bis zum Gerichtsurteil – ermöglichen wird.

Agentur der Europäischen Union für Cybersicherheit (ENISA)
Die ENISA hat den Rahmen für die **strukturierte Zusammenarbeit mit dem CERT-EU**[138] auf der Grundlage einer im März unterzeichneten Vereinbarung umgesetzt, um Synergien zu nutzen und Doppelarbeit bei der Wahrnehmung ihrer Aufgaben im Bereich der operativen Zusammenarbeit zu vermeiden. Dadurch sollen sowohl der EU-Krisenreaktionsmechanismus als auch der langfristige Kapazitätsaufbau wirksamer und effizienter werden. Unterstützt wird dies durch ein lokales Büro der Agentur in Brüssel, das die Zusammenarbeit mit anderen Organen, Einrichtungen und sonstigen Stellen der EU fördern soll.[139] Die ENISA trägt dazu bei, konkrete Schritte zur Umsetzung neuer Cybersicherheitsstrategien zu unternehmen. Im Mai übermittelte sie das erste mögliche Schema für Common Criteria für die Cybersicherheitszertifizierung[140], und im Juni leitete sie das Verfahren zur Einrichtung einer Ad-hoc-Arbeitsgruppe zur 5G-Cybersicherheitszertifizierung[141] ein.

Europäische Agentur für die Grenz- und Küstenwache (Frontex)
Frontex spielt eine entscheidende Rolle bei der Unterstützung der Mitgliedstaaten beim Management der Außengrenzen und bei Rückführungen und trägt zur Sicherheit der EU bei. Durch die neue Verordnung[142] wurde Frontex sowohl personell als auch finanziell zur größten EU-Agentur.

Europäische Beobachtungsstelle für Drogen und Drogensucht (EMCDDA)
Der Europäischen Beobachtungsstelle für Drogen und Drogensucht kommt eine wichtige Rolle zu, indem sie die Drogensituation in der EU kontinuierlich überwacht, um den EU-Organen und den Mitgliedstaaten die aktuellsten Informationen zur Verfügung zu stellen. Ein besonderer Schwerpunkt ihrer jüngsten Arbeit lag auf den Auswirkungen der Pandemie auf Drogenmärkte, Drogenkonsum, drogenbezogene gesundheitliche und soziale Folgen und Drogendienste.[143]

VI. Fazit

Die EU verfügt über die einzigartige Kapazität, auf heutige Sicherheitsbedrohungen und Herausforderungen im Bereich der Sicherheit zu reagieren, und stellt sich schrittweise entsprechend auf, um ihre Reaktionsfähigkeit zu stärken. Durch die EU-Strategie für eine Sicherheitsunion mit ihrem umfassenden und dynamischen Ansatz werden Schranken abgebaut, um zu gewährleisten, dass jedes Risiko im Kontext der breiteren Bedrohungslage

---

137 https://www.eurojust.europa.eu/stepping-cooperation-tackle-intellectual-property-crime
138 Das IT-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der EU (CERT-EU) setzt sich aus IT-Sicherheitsexperten der wichtigsten EU-Organe zusammen.
139 C(2021) 4626 final.
140 Crossing a bridge: the first EU cybersecurity certification scheme is availed to the Commission — ENISA (europa.eu)
141 Calling on you, 5G Experts! Join us on 5G Cybersecurity Certification — ENISA (europa.eu)
142 Verordnung (EU) 2019/1896 des Europäischen Parlaments und des Rates vom 13. November 2019 über die Europäische Grenz- und Küstenwache und zur Aufhebung der Verordnungen (EU) Nr. 1052/2013 und (EU) 2016/1624.
143 EMCDDA, Europäischer Drogenbericht 2021 vom 9. Juni 2021.

verstanden wird, das Fachwissen aller Interessenträger zum Aufbau einer sichereren und widerstandsfähigeren EU beiträgt und alle zur Verfügung stehenden Instrumente im Einklang mit den europäischen Werten und der Achtung der Grundrechte wirksam eingesetzt werden.

Die Kommission wird das Europäische Parlament und den Rat bei der Fertigstellung wichtiger anstehender Rechtsvorschriften im Bereich der Sicherheit unterstützen und dafür sorgen, dass die Ambitionen den Herausforderungen gerecht werden, mit denen die EU gegenwärtig und in Zukunft konfrontiert ist.

Um globale Sicherheitsherausforderungen anzugehen und die Beziehungen zu gleich gesinnten Ländern zu stärken, wird die EU ebenfalls die Zusammenarbeit mit internationalen Partnern in Bereichen wie der Bekämpfung von Terrorismus und Extremismus, böswilligen Cyberaktivitäten, hybriden Bedrohungen und anderen gemeinsamen Sicherheitsrisiken intensivieren. Dies spiegelt sich auch in der Erklärung wider, die auf dem jüngsten Gipfeltreffen zwischen der EU und den USA vereinbart wurde.[144]

Während die EU kontinuierlich Fortschritte bei der Verbesserung und Anpassung ihres Rechtsrahmens erzielt, um den verschiedenen Sicherheitsaspekten Rechnung zu tragen, müssen die Rechtsvorschriften ordnungsgemäß umgesetzt werden. Im Rahmen dieser gemeinsamen Verantwortung muss jeder Mitgliedstaat seine Aufgaben erfüllen, um die Sicherheit Europas insgesamt zu gewährleisten.

[144] Erklärung zum Gipfeltreffen EU-USA: Auf dem Weg zu einer erneuerten transatlantischen Partnerschaft, 15. Juni 2021.