Rat der
Europäischen Union

Brüssel, den 10. Dezember 2021
(OR. en)

14874/21

JAI 1390	**DROIPEN 155**
COSI 247	**COPEN 448**
ENFOPOL 503	**FREMP 294**
ENFOCUSTOM 192	**JAIEX 133**
IXIM 287	**CFSP/PESC 1223**
CT 171	**COPS 465**
CRIMORG 161	**HYBRID 79**
FRONT 434	**DISINFO 44**
ASIM 102	**TELECOM 458**
VISA 249	**DIGIT 186**
CYBER 327	**COMPET 899**
DATAPROTECT 284	**RECH 558**
CATS 79	

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	8. Dezember 2021
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2021) 799 final
Betr.:	MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT Dritter Fortschrittsbericht über die Umsetzung der EU-Strategie für eine Sicherheitsunion

Die Delegationen erhalten in der Anlage das Dokument COM(2021) 799 final.

Anl.: COM(2021) 799 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 8.12.2021
COM(2021) 799 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

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

I. Einleitung

Mit der Sicherheitsunion soll sichergestellt werden, dass die EU ihrer Rolle bei der Gewährleistung der Sicherheit der Bürgerinnen und Bürger unter Achtung der Werte, die die europäische Lebensweise bestimmen, in vollem Umfang gerecht wird. Bei allen vier strategischen Prioritäten der Strategie für eine Sicherheitsunion[1] sind Umsetzungsfortschritte zu verzeichnen: i) ein zukunftsfähiges Sicherheitsumfeld, ii) Umgang mit sich wandelnden Bedrohungen, iii) Schutz der Europäerinnen und Europäer vor Terrorismus und organisierter Kriminalität und iv) eine starke europäische Sicherheitsgemeinschaft.

Aufgrund sich verändernder Technologien und internationaler Entwicklungen treten ständig neue Bedrohungen und Herausforderungen für die europäische Sicherheit auf, wobei die COVID-19-Pandemie die größten Schwachstellen hervorgehoben hat. Im zweiten Bericht über die Sicherheitsunion[2] sind die besonderen Herausforderungen, die sich aufgrund der COVID-19-Pandemie für die Sicherheit ergeben, aufgeführt.

In diesem dritten Bericht liegt der Schwerpunkt auf den Entwicklungen, die mit den größten neuen Bedrohungen der letzten sechs Monate in Zusammenhang stehen. Es wird insbesondere hervorgehoben, dass die Zusammenarbeit nicht nur innerhalb der EU, sondern auch auf internationaler Ebene mit einem breiten Spektrum von Interessenträgern und Partnern zu intensivieren ist.

Die Strategie für eine Sicherheitsunion wird vor dem Hintergrund zunehmend grenz- und sektorübergreifender Bedrohungen vorangetrieben. Die digitale Welt wird nach wie vor für böswillige Zwecke genutzt. Cyberangriffe mit Ursprung innerhalb oder außerhalb Europas, einschließlich Ransomware-Angriffe, zielen immer häufiger auf staatliche Kernfunktionen wie das Gesundheitswesen und wichtige Infrastrukturen, Industrien und öffentliche Stellen sowie Einzelpersonen ab. Die ausländische Manipulation von Informationen und die Einmischung aus dem Ausland nehmen zu und sind in einigen Fällen bereits mit Cyberaktivitäten, insbesondere Hacking und Leaking, einhergegangen. Es findet nach wie vor grenzüberschreitende organisierte Kriminalität jeder Art statt, wobei eine wirksame Reaktion von Partnerschaften außerhalb der EU abhängt. Internationale Entwicklungen erfordern Wachsamkeit im Zusammenhang mit potenzieller Radikalisierung und Terrorismus sowie hybriden Angriffen, einschließlich – während dieses Berichtszeitraums – an den Außengrenzen der EU.

Um diesen immer komplexer werdenden globalen und grenzüberschreitenden Bedrohungen zu begegnen, verstärkt die EU nicht nur ihre eigene Reaktion, sondern auch die Zusammenarbeit mit internationalen Partnern. Dies ist ein Themenschwerpunkt dieses Berichts.

Zeitgleich werden auch die Arbeiten zur Erhöhung der Sicherheit im Schengen-Raum intensiviert. Eine enge Zusammenarbeit zwischen den Mitgliedstaaten ist für die allgemeine Sicherheit des Schengen-Raums von entscheidender Bedeutung. Die Kommission hat ein umfangreiches neues Paket mit Maßnahmen zur Stärkung der polizeilichen Zusammenarbeit und Erhöhung der Sicherheit des Schengen-Raums ausgearbeitet, um weitere Verbesserungen in dieser Hinsicht zu erzielen.

---

1 COM(2020) 605.
2 COM(2021) 440.

Die EU-Agenturen werden durch ihre operativen Tätigkeiten zur Unterstützung der nationalen Behörden der Mitgliedstaaten und durch die Bereitstellung von Fachwissen, Informationen und Lageeinschätzungen zu den vordringlichsten Bedrohungen umfassend in diese Arbeit einbezogen.

Weitere Einzelheiten und aktuelle Informationen zum gesamten Spektrum der Initiativen im Rahmen der Sicherheitsunion sind im Anhang dieser Mitteilung enthalten.

II. Ein zukunftsfähiges Sicherheitsumfeld

Digitale Infrastrukturen, Technologien und Online-Systeme ermöglichen es uns, Unternehmen zu gründen, Produkte zu konsumieren und Dienstleistungen in Anspruch zu nehmen. Diese zunehmende Digitalisierung unserer Umwelt macht uns jedoch auch anfälliger für Angriffe. Sowohl der von **Europol** im November 2021 veröffentlichten Bewertung der Bedrohungslage im Bereich der organisierten Kriminalität im Internet[3] als auch dem von der Agentur der Europäischen Union für Cybersicherheit (**ENISA**) im Oktober 2021 veröffentlichten Jahresbericht zur Bedrohungslage zufolge nehmen Umfang, Häufigkeit und Komplexität von Cyberkriminalität und Cyberangriffen zu. Die Regierungen in Europa waren im vergangenen Jahr mit mindestens 198 Cybersicherheitsvorfällen konfrontiert, wodurch die öffentliche Verwaltung nun der am stärksten betroffene Sektor ist. Hochqualifizierte und gut ausgestattete böswillige Akteure von innerhalb, aber auch außerhalb der EU nutzen den grenzenlosen Charakter des globalen, offenen Internets sowie die Lücken der derzeitigen Rechtsrahmen aus. Cyberangriffe und Cyberkriminalität sind häufig miteinander verbunden (was sich an zahlreichen Vorfällen zeigt, bei denen Kriminelle Schwachstellen angreifen, um Geld zu erpressen) und eine ständige Bedrohung, die immer wieder neu auftritt. Cyberkriminelle können schlichtweg durch die zunehmenden Möglichkeiten der Monetarisierung ihrer Aktivitäten motiviert sein, doch andere böswillige staatliche oder nichtstaatliche Verhaltensweisen werden neben finanziellen Gewinnen durch komplexere geopolitische und ideologische Erwägungen geleitet. Von der **ENISA** erhobene Daten haben gezeigt, dass staatlich unterstützte Hacker auch bei Angriffen, die sich gegen Lieferketten des öffentlichen und privaten Sektors richteten, ein „neues Ausmaß an Komplexität und Wirkung“ erreicht haben.[4]

Es ist daher besonders wichtig, bei EU-Maßnahmen ein hohes Maß an Ehrgeiz aufrechtzuerhalten, und zwar sowohl hinsichtlich des angestrebten Sicherheitsniveaus als auch in Bezug auf das Arbeitstempo, in dem dieses erreicht werden soll. Der Europäische Rat befasste sich auf seiner Tagung im Oktober 2021[5] mit der deutlichen Zunahme böswilliger Cyberaktivitäten. Er bekräftigte das Eintreten der EU für einen offenen, freien, stabilen und sicheren Cyberraum und betonte, dass angesichts der zunehmenden Cybersicherheitsbedrohungen eine wirksame Koordinierung und Vorsorge erforderlich seien. Er betonte ferner, dass die Maßnahmen zur Bekämpfung der Cyberkriminalität, insbesondere von Ransomware-Angriffen, und die Zusammenarbeit mit Partnerländern, auch im Rahmen von multilateralen Foren, verstärkt werden müssten.

---

3 Bewertung der Bedrohungslage im Bereich der organisierten Kriminalität im Internet, 11. November 2021.
4 ENISA-Jahresbericht zur Bedrohungslage, 27. Oktober 2021.
5 Schlussfolgerungen des Europäischen Rates, 21. und 22. Oktober 2021.

Einige Beispiele jüngster Cyber-/Ransomware-Vorfälle im Berichtszeitraum

- Juli: Rund 500 Supermärkte in Schweden waren aufgrund eines sehr aggressiven Cyberangriffs mit Auswirkungen auf Organisationen in der ganzen Welt zur Schließung gezwungen.
- Juli: Berichten aus **Estland** zufolge wurden von einem Hacker mit Sitz in Tallinn 286 438 Ausweisfotos aus staatlichen Datenbanken heruntergeladen, wodurch eine Schwachstelle auf einer von der estnischen Informationssystembehörde verwalteten Plattform aufgedeckt wurde.
- August: Die Region Latium in **Italien** war Opfer eines Ransomware-Angriffs, bei dem IT-Verwaltungssysteme, einschließlich des Registrierungsportals für COVID-19-Impfungen, lahmgelegt wurden. Nach dem Angriff konnten mehrere Tage lang keine neuen Impftermine gebucht werden.
- September: In **Deutschland** wurde ein Cyberangriff bestätigt, bei dem Hacker in die Server- und Dateisysteme des Statistischen Bundesamts, das unter der Leitung des Bundeswahlleiters steht, eindringen konnten.
- September: In den **Niederlanden** behinderte ein Cyberangriff die Einführung des COVID-Passes.
- Oktober: Ein Krankenhaus in **Belgien** war aufgrund eines Ransomware-Angriffs gezwungen, alle geplanten Beratungstermine abzusagen.
- November: Bei einem Cyberangriff auf die europäische Elektronikhandelskette MediaMarkt forderten Hacker 50 Mio. USD in Bitcoin.

Interne Stärkung der Resilienz der EU

Im Europäischen Parlament und im Rat wird derzeit über die Vorschläge der Kommission aus dem Jahr 2020 **zum Schutz und zur Resilienz kritischer physischer und digitaler Infrastrukturen** verhandelt. Am 19. Oktober 2021 nahm das Parlament sein Verhandlungsmandat für den Entwurf einer Richtlinie über die Resilienz kritischer Einrichtungen und am 10. November 2021 für den Entwurf einer Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) an. Im Rat wurde am 3. Dezember eine allgemeine Ausrichtung zur NIS-2-Richtlinie festgelegt. Dies wird den Weg für einen raschen, kohärenten und ehrgeizigen Abschluss der Verhandlungen im Jahr 2022 ebnen.

Die Empfehlung der Kommission zum Aufbau einer **Gemeinsamen Cyber-Einheit** (Joint Cyber Unit – JCU) bildet eine Schlüsselkomponente für die Verbesserung der unmittelbaren Reaktions- und Erholungsfähigkeit der EU. Die JCU würde die Mitgliedstaaten und die einschlägigen Organe, Einrichtungen und sonstigen Stellen der EU zusammenbringen, um eine Struktur für eine koordinierte Zusammenarbeit auf operativer Ebene zu schaffen. Sie würde dazu beitragen, die verschiedenen Akteure, die für Cybersicherheitseinsätze in den EU-Cybersicherheitsgemeinschaften (Resilienz, Strafverfolgung, Cyberdiplomatie und Cyberabwehr) zuständig sind, miteinander zu vernetzen. Am 19. Oktober kam der Rat überein[6], das Potenzial der JCU-Initiative als Ergänzung zur Empfehlung der Kommission für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen zu prüfen. Es wurde ein Vorbereitungsprozess eingeleitet, und die **ENISA** hat mehrere Workshops

[6] Schlussfolgerungen des Rates zur Prüfung des Potenzials der Initiative für eine Gemeinsame Cyber-Einheit als Ergänzung zur koordinierten Reaktion der EU auf große Cybersicherheitsvorfälle und -krisen, 12534/2021 (https://data.consilium.europa.eu/doc/document/ST-12534-2021-INIT/de/pdf).

organisiert, um die in der Empfehlung der Kommission festgelegten Ergebnisse und nächsten Schritte unter Berücksichtigung des Diskussionspapiers des slowenischen Ratsvorsitzes zum weiteren Vorgehen für die JCU[7] zu erörtern.

Zusätzlich zu diesen übergeordneten Vorschlägen ergänzen sektorspezifische Rechtsvorschriften, mit denen konkreten Schwachstellen Rechnung getragen wird, diese Arbeit. Außerdem sind im Berichtszeitraum Fortschritte im Finanz-, Gesundheits-, Meeres- und Energiesektor sowie beim Verbraucherschutz zu verzeichnen.

Die Verhandlungen über den **Rechtsakt über die Betriebsstabilität digitaler Systeme des Finanzsektors**, mit dem die allgemeine Betriebsstabilität der digitalen Systeme von Finanzinstituten verbessert werden soll, kommen voran. Der Rat hat am 24. November eine allgemeine Ausrichtung festgelegt, während das Europäische Parlament beabsichtigt, sein Verhandlungsmandat noch vor Jahresende anzunehmen. Sobald diese Maßnahmen angenommen sind, werden die EU und ihre Mitgliedstaaten einen soliden und zukunftsfähigen Rechtsrahmen für eine wirksamere Bewältigung dieser Herausforderungen haben, sofern das erforderliche Maß an Ehrgeiz im Endergebnis der Verhandlungen zum Ausdruck kommt.

Die Pandemie hat den wesentlichen Charakter des Gesundheitssektors und die Notwendigkeit eines soliden Rahmens für die **Gesundheitssicherheit** deutlich gemacht. Die Vorschläge für eine Europäische Gesundheitsunion zielen darauf ab, den Schutz, die Prävention, die Vorsorge und die Reaktion auf Gefahren für die menschliche Gesundheit auf EU-Ebene zu verbessern, und zeigen, wie ambitioniert und entschlossen die EU diesen wichtigen Sektor schützen will. Es wurde bereits eine Einigung über die Aktualisierung der Mandate der wichtigsten Agenturen erzielt, was in Kürze auch in Bezug auf grenzüberschreitende Gesundheitsgefahren der Fall sein dürfte. Die Einrichtung der Europäischen Behörde für die Krisenvorsorge und -reaktion bei gesundheitlichen Notlagen (HERA) im September 2021 hat dieser Arbeit ebenfalls eine neue Dimension verliehen und wird durch einen neuen Rahmen von zeitlich begrenzten Sofortmaßnahmen unterstützt, die bei Bedarf eingeleitet werden.

Cyberbedrohungen und hybride Bedrohungen im maritimen Bereich, die sich gegen kritische **maritime Infrastrukturen** wie Häfen, Unterwasserkabel und -rohrbahnen, Energieplattformen und Meeresengen, in denen sich der Seeverkehr konzentriert, richten, können erhebliche Störungen hervorrufen. Die EU-Strategie für maritime Sicherheit und ihr Aktionsplan[8] werden derzeit im Hinblick auf eine mögliche Aktualisierung geprüft, durch die neu auftretende Cyberbedrohungen und hybride Bedrohungen wirksamer angegangen werden könnten.

In ihrer jüngsten Mitteilung „Steigende **Energie**preise: eine ‚Toolbox' mit Gegenmaßnahmen und Hilfeleistungen"[9] kündigte die Kommission an, bis Ende 2022 Maßnahmen ergreifen zu wollen, um die Widerstandsfähigkeit des Energiesystems an neue Bedrohungen wie Cyberangriffe oder extreme Wetterereignisse anzupassen. So plant sie unter anderem neue

---

[7] Der slowenische Ratsvorsitz erstellte ebenfalls ein Diskussionspapier (13019/21) zum weiteren Vorgehen für die JCU mit konkreten Schritten zur Verbesserung des gemeinsamen Lagebewusstseins innerhalb und zwischen allen relevanten Cybergemeinschaften vorgestellt werden.

[8] Bericht über die Umsetzung des überarbeiteten Aktionsplans im Rahmen der EU-Strategie für maritime Sicherheit, SWD(2020) 252.

[9] COM(2021) 660.

Vorschriften zur Cybersicherheit des Elektrizitätssystems, eine Empfehlung zu den Resilienzaspekten sauberer Energie sowie die Einrichtung einer für die Widerstandsfähigkeit der Energieinfrastruktur zuständigen ständigen europäischen Gruppe mit Vertretern von Betreibern und Behörden.

Sicherheitslücken sind auch in vielen intelligenten Produkten und drahtlosen Geräten vorhanden. Insbesondere Kinder können Sicherheitsrisiken ausgesetzt sein, weil **elektronische Produkte** wie vernetztes Spielzeug und Smartwatches angreifbar sind. Um dieses Problem anzugehen, hat die Kommission im Oktober 2021 im Rahmen der Funkanlagenrichtlinie einen delegierten Rechtsakt zum Schutz der Privatsphäre und der Netze sowie zum Schutz vor Betrug bei vernetzten elektronischen Produkten erlassen.[10] Mit diesem würden den Herstellern Anforderungen auferlegt, die das Cybersicherheitsniveau der in der EU in Verkehr gebrachten Produkte erhöhen würden, und die Mitgliedstaaten in die Lage versetzen, Korrekturmaßnahmen zu ergreifen, wenn unsichere Produkte auf dem Markt gefunden werden.

Stärkung der Widerstandsfähigkeit der EU durch internationale Zusammenarbeit

Sicherheitsbedrohungen sind globaler Natur, und der Aufbau starker internationaler Partnerschaften ist für ihre wirksame Bewältigung von entscheidender Bedeutung. Die EU und ihre Mitgliedstaaten intensivieren daher ihre Maßnahmen, um staatlich und nichtstaatlich finanzierte Angreifer abzuhalten, abzuschrecken und abzuwehren, unter anderem durch eine klarere Zuweisung von Verantwortung. Im Juli 2021 gaben die EU[11], die Vereinigten Staaten, die NATO und andere Weltmächte Erklärungen ab, in denen sie böswillige Cyberaktivitäten stark verurteilten und das Hoheitsgebiet China für den Hackerangriff auf Microsoft Exchange Server Anfang 2021 verantwortlich machten. Diese böswillige Cyberaktivität gefährdete weltweit mehr als 100 000 Server. Am 24. September 2021 gab der Hohe Vertreter im Namen der EU eine Erklärung[12] zur Achtung der demokratischen Prozesse der EU ab, in der er eine Reihe böswilliger Cyberaktivitäten anprangerte, die Russische Föderation nachdrücklich ermahnte, die Normen für verantwortungsvolles staatliches Verhalten im Cyberraum einzuhalten, und alle Beteiligten aufforderte, diese Aktivitäten unverzüglich einzustellen.

Die Diskussionen über globale Sicherheitsherausforderungen gewinnen auf **multilateraler** Ebene an Fahrt. Auf der **G7**-Tagung der Innen- und Sicherheitsminister im September 2021 wurde eine Reihe von Themen erörtert, die von Online-Material zu sexuellem Kindesmissbrauch über Ransomware bis hin zur Bekämpfung von Terrorismus, schwerer Kriminalität und Korruption reichten. Die G7-Partner tauschten sich über übereinstimmende Standpunkte aus und verpflichteten sich, unter Sicherstellung des Schutzes personenbezogener Daten und der Grundrechte den Informationsaustausch (einschließlich biometrischer und biografischer Daten) zu verstärken.

---

[10] COM(2021) 7672.

[11] Erklärung des Hohen Vertreters im Namen der EU, in der China nachdrücklich aufgefordert wird, Maßnahmen gegen vom chinesischen Hoheitsgebiet ausgehende böswillige Cyberaktivitäten zu ergreifen, 19. Juli 2021.

[12] Erklärung des Hohen Vertreters im Namen der Europäischen Union zur Achtung der demokratischen Prozesse der EU, 24. September 2021.

Die EU nahm im August auch an der **G20**-Tagung der Digitalminister unter der italienischen Präsidentschaft teil. Sie einigten sich auf eine Erklärung[13], in der betont wurde, dass die Datensicherheit für die breite Öffentlichkeit und Unternehmen sowie die Sicherheit des digitalen Umfelds für alle gewährleistet werden müssen. Auch eine Reihe von G20-Grundsätzen für ein sicheres und förderliches digitales Umfeld für Kinder wurde vereinbart.

Die EU ist nach wie vor starker Befürworter einer Multi-Stakeholder-Zusammenarbeit, da sie ihrer Ansicht nach wesentlich zur Aufrechterhaltung eines offenen, stabilen und sicheren Cyberraums beiträgt. Im November 2021 gab Präsidentin von der Leyen im Rahmen des Pariser Friedensforums 2021 den Beschluss bekannt, den **Pariser Aufruf für Vertrauen und Sicherheit im Cyberraum** zu unterstützen und sich den über 80 Staaten, 700 Unternehmen und 350 Organisationen der Zivilgesellschaft anzuschließen, die sich zur Zusammenarbeit bei der Bewältigung der Herausforderungen, aber auch der Ergreifung der Chancen, die der Cyberraum mit sich bringt, verpflichten.

Die EU arbeitet auch bilateral mit einer Reihe von Drittländern zusammen, unter anderem im Rahmen regelmäßiger Sicherheits- und Cyberdialoge. Die Zusammenarbeit zwischen der EU und den Vereinigten Staaten in Sicherheitsfragen hat in den vergangenen Monaten an Fahrt gewonnen und ist ein wichtiges Beispiel für die Zusammenarbeit mit gleich gesinnten Ländern, um die Sicherheitsagenda voranzubringen.

Zusammenarbeit zwischen der EU und den Vereinigten Staaten in Sicherheitsfragen

Auf dem Gipfeltreffen zwischen der EU und den Vereinigten Staaten am 15. Juni 2021 wurde erneut die Entschlossenheit bekräftigt, gemeinsame Herausforderungen im Bereich der Sicherheit gemeinsam anzugehen. Darauf folgte eine Reihe von Initiativen:

– Am 29. September 2021 fand die erste Sitzung des **EU-US-Handels- und Technologierats (TTC)** statt. In der diesbezüglichen Erklärung von Pittsburgh[14] wurde die Bedeutung der Überprüfung von Investitionen zur Abwendung von Risiken für die nationale Sicherheit, die Bedeutung der Zusammenarbeit in Bereichen, die mit der Ausfuhrkontrolle beim Handel mit Gütern mit doppeltem Verwendungszweck in Zusammenhang stehen, die Bedeutung des Ausbaus widerstandsfähiger und nachhaltiger Lieferketten sowie die Bedeutung der Bekämpfung der ausländischen Manipulation von Informationen und der Einmischung aus dem Ausland hervorgehoben. Der TTC umfasst eine Arbeitsgruppe für **Informations- und Kommunikationstechnologie und -dienste, Sicherheit und Wettbewerbsfähigkeit**, die sich mit Themen wie Sicherheit, Vielfalt, Interoperabilität und Widerstandsfähigkeit entlang der IKT-Lieferkette befassen wird, einschließlich sensibler und kritischer Bereiche wie 5G, Unterwasserkabel, Datenzentren und Cloud-Infrastruktur.

[13] https://www.g20.org/wp-content/uploads/2021/08/DECLARATION-OF-G20-DIGITAL-MINISTERS-2021_FINAL.pdf

[14] Erste gemeinsame Erklärung des EU-US-Handels- und Technologierats (europa.eu).

– Am 21. September 2021 fand ein **Cyberdialog zwischen der EU und den Vereinigten Staaten** statt. Es herrschte Einigkeit darüber, dass die Zusammenarbeit und Koordinierung bei den UN-Diskussionen über Cyberangelegenheiten verstärkt werden müssen, um für die Verhinderung von, Abschreckung vor und Abwehr von böswilligen Cyberaktivitäten zu sorgen, und dass eine wirksame Zusammenarbeit mit anderen Ländern erforderlich ist, insbesondere um die allgemeine Widerstandsfähigkeit zu erhöhen.
– Die EU nahm im Oktober 2021 an der **Initiative des Weißen Hauses zur Bekämpfung von Ransomware**[15] teil, an der sich auch hochrangige Sachverständige und Regierungsvertreter aus 30 Ländern beteiligten. Bei den Diskussionen ging es um die Widerstandsfähigkeit von Netzwerken, den Missbrauch virtueller Währungen zur Wäsche von Lösegeld, den Informationsaustausch zur Unterstützung der Ermittlung und Strafverfolgung grenzüberschreitend tätiger Ransomware-Krimineller sowie die diplomatischen Bemühungen zur Unterstützung gemeinsamer Ziele bei der Bekämpfung von Ransomware. Eine **für Ransomware zuständige EU-US-Arbeitsgruppe**, deren Schwerpunkt auf der operativen Zusammenarbeit der Strafverfolgungsbehörden liegt, ist am 25. Oktober 2021 zum ersten Mal zusammengetreten.
– Am Rande des G20-Treffens im Oktober 2021 führte die EU mit den Vereinigten Staaten und anderen Teilnehmern Gespräche über kurzfristige **Versorgungsstörungen** und Möglichkeiten für eine langfristige Widerstandsfähigkeit, um Engpässe zu vermeiden und die Märkte offen zu halten.[16]

Zur wirksamen Bekämpfung von **Cyberkriminalität** werden weltweit – auf nationaler, EU-[17] und internationaler Ebene – Anstrengungen unternommen, um den grenzüberschreitenden Zugang zu elektronischen Beweismitteln für strafrechtliche Ermittlungen zu verbessern. Kompatible Vorschriften auf internationaler Ebene sind besonders wichtig, um Rechtskollisionen zu vermeiden, wenn ein grenzüberschreitender Zugang zu elektronischen Beweismitteln angestrebt wird.

In diesem Bereich wurden mit dem förmlichen Abschluss der Verhandlungen über das Zweite Zusatzprotokoll zum Übereinkommen über Computerkriminalität (**Budapester Übereinkommen**) im Rahmen des Europarates mit der Annahme des Textes durch das Ministerkomitee des Europarates am 17. November 2021 erhebliche Fortschritte erzielt. Die Kommission hat Vorschläge angenommen, mit denen die Mitgliedstaaten ermächtigt werden sollen, das Protokoll[18] im Interesse der Union rasch zu unterzeichnen und zu ratifizieren, und arbeitet nun eng mit dem Europäischen Parlament und dem Rat zusammen, damit die Unterzeichnung und Ratifizierung durch die Mitgliedstaaten so bald wie möglich erfolgen kann. Mit dem Protokoll erhalten Fachkräfte weltweit Instrumente zur Verbesserung der Zusammenarbeit im Bereich Cyberkriminalität und elektronische Beweismittel und es wird

[15] Gemeinsame Erklärung der Minister und Vertreter des Treffens im Rahmen der Initiative zur Bekämpfung von Ransomware (Oktober 2021).
[16] Erklärung des Vorsitzes zu den Grundsätzen für die Widerstandsfähigkeit der Versorgungskette vom 31. Oktober 2021, Weißes Haus.
[17] Über das „Paket über elektronische Beweismittel“ (COM(2018) 225 und COM(2018) 226) wird im Europäischen Parlament und im Rat noch verhandelt. Es würde den nationalen Strafverfolgungs- und Justizbehörden in der EU die Möglichkeit geben, mithilfe von Europäischen Herausgabeanordnungen und Europäischen Sicherungsanordnungen unabhängig vom Standort der Niederlassung des Anbieters oder des Speicherorts der Informationen und unter Wahrung strenger Garantien in kurzer Zeit elektronische Beweismittel von Diensteanbietern für strafrechtliche Ermittlungen zu erlangen.
[18] COM(2021) 718 und COM(2021) 719.

anerkannt, dass eine wirksame grenzüberschreitende Zusammenarbeit für die Zwecke der Strafjustiz solide Garantien für den Schutz der Grundrechte erfordert. Das Protokoll enthält auch Garantien für den Schutz der Privatsphäre und personenbezogener Daten.

Parallel dazu wird derzeit ein neues Übereinkommen der Vereinten Nationen über Cyberkriminalität ausgearbeitet, das rechtlich mit den bestehenden Instrumenten, insbesondere dem Budapester Übereinkommen, in Einklang stehen sollte. Die Kommission wird für eine wirksame Beteiligung der Europäischen Union an den Verhandlungen sorgen, die im Januar 2022 beginnen.

III. Umgang mit sich wandelnden Bedrohungen

Die größten sich wandelnden Bedrohungen, die im Berichtszeitraum beobachtet wurden, sind **hybride** Bedrohungen und die kontinuierliche **technologische Weiterentwicklung**. Das Ausmaß, der sich wandelnde Charakter und der modus operandi von Sicherheitsbedrohungen und hybriden Bedrohungen stellen heute eine ständige Herausforderung dar, da die Vielfalt der von böswilligen Akteuren eingesetzten Instrumente immer größer wird. Sicherheitsherausforderungen ergeben sich auch zunehmend aus neuen technologischen Entwicklungen, die der Gesellschaft zwar neue Möglichkeiten eröffnen, doch häufig auch von böswilligen Akteuren und Kriminellen ausgenutzt werden.

Zur wirksamen Bewältigung der sich wandelnden Bedrohungen ist Präsidentin von der Leyen[19] zufolge ein umfassender Ansatz auf der Grundlage einer gemeinsamen Bewertung der Bedrohungslage erforderlich. Der vom Hohen Vertreter im November 2021 vorgestellte **Strategische Kompass**, auf den sich die Mitgliedstaaten im März 2022 verständigen sollen, wird als Leitdokument für die Sicherheits- und Verteidigungspolitik der EU dienen. Auf der Grundlage der ersten je durchgeführten umfassenden EU-Bedrohungsanalyse aus dem Jahr 2020 wird im Strategischen Kompass dargelegt, wie die strategische Autonomie der EU gestärkt und die EU ein stärkerer globaler Partner werden kann. Es werden konkrete Ziele und Ergebnisse für die nächsten fünf bis zehn Jahre festgelegt, die sich auf eine rasche Krisenreaktion, auf den Schutz unserer Bürgerinnen und Bürger vor sich schnell verändernden Bedrohungen, auf Investitionen in erforderliche Kapazitäten und auf die Zusammenarbeit mit Partnern zur Verwirklichung gemeinsamer Ziele beziehen.

Die Erfahrungen mit der COVID-19-Pandemie haben gezeigt, dass **die ausländische Manipulation von Informationen und die Einmischung aus dem Ausland** eine ernste und wachsende Sicherheitsbedrohung darstellen. Sie kann die in den EU-Verträgen verankerten Werte, insbesondere die demokratischen Einrichtungen und Prozesse, gefährden und die Grundrechte und Grundfreiheiten untergraben. Die EU trägt aktiv zur Ermittlung, Analyse und Aufdeckung ausländischer Manipulationen von Informationen und Einmischungen aus dem Ausland bei und arbeitet eng mit Drittländern und internationalen Partnern (insbesondere der G7 und der NATO) zusammen, um Kapazitäten aufzubauen. Nach dem Aktionsplan für Demokratie in Europa[20] arbeitet der Europäische Auswärtige Dienst nun in enger Zusammenarbeit mit der Europäischen Kommission an einem Instrumentarium für die Bekämpfung der ausländischen Manipulation von Informationen und der Einmischung aus dem Ausland. Die Kommission legte am 25. November eine Reihe von Initiativen zur Stärkung der Demokratie und der Integrität der Wahlen vor. Dazu zählen ein Vorschlag für

[19] Rede der Präsidentin Ursula von der Leyen zur Lage der Union 2021 vom 15. September 2021.
[20] COM(2020) 790.

eine Verordnung über die Transparenz[21] politischer Werbung und zwei Vorschläge zur Aktualisierung der Richtlinien über die Wahlrechte „mobiler EU-Bürger“[22].

Eine bemerkenswerte Entwicklung in Bezug auf hybride Angriffe auf die EU im Sommer 2021 war der Versuch, die EU durch die Instrumentalisierung von Migranten an den EU-Außengrenzen zu destabilisieren.

Der hybride Angriff von Belarus auf die EU

- Im Sommer 2021 sah sich Belarus nach der erzwungenen Landung eines Passagierflugzeugs im Mai 2021 mit Sanktionen konfrontiert. Als Reaktion darauf erleichterte das Regime es irregulären Migranten, die Grenzen Litauens, Lettlands und Polens zu erreichen. Diese Maßnahme zeigt einen entschlossenen Versuch, im Rahmen umfassenderer konzertierter Bemühungen um eine Destabilisierung der EU eine anhaltende Krisensituation zu schaffen.
- Im Rahmen der Maßnahmen von Belarus wurde nicht nur das erhebliche persönliche Risiko der Migranten in Kauf genommen, sondern auch Informationsmanipulation zu ihrer Instrumentalisierung betrieben. Die EU hat die ausländische Manipulation von Informationen und die Einmischung aus dem Ausland überwacht, analysiert und offengelegt und ihre Erkenntnisse mit den Mitgliedstaaten und internationalen Partnern (NATO und G7) über das Schnellwarnsystem ausgetauscht.
- In der Gemeinsamen Mitteilung vom 23. November zur Reaktion auf staatlich geförderte Instrumentalisierung von Migranten an der EU-Außengrenze[23] wird die starke und breitgefächerte Reaktion der EU auf diese Ereignisse dargelegt.
- Diese Reaktion umfasste bislang unter anderem folgende Maßnahmen: EU-Finanzhilfen; operative Unterstützung der betroffenen Mitgliedstaaten durch die EU-Agenturen **Frontex** und **EASO**; diplomatische Kontaktaufnahme zu Herkunfts- und Transitländern, um zu verhindern, dass ihre Bürgerinnen und Bürger in die Falle geraten; Anwendung von Sanktionen gegen Personen, die illegale Grenzübertritte an den Außengrenzen der Union erleichtern.[24] Es wurde ein Vorschlag für eine Verordnung unterbreitet, um die Handlungen von Verkehrsunternehmen, die Menschenhandel oder die Schleusung von Menschen in die EU erleichtern, zu beschränken.[25] Es wurden außerordentliche Asyl- und Rückführungsmaßnahmen vorgeschlagen, um die betroffenen Mitgliedstaaten dabei zu unterstützen, unter uneingeschränkter Achtung der Werte und Standards der EU auf die derzeitige Krise zu reagieren.[26] Die vorgeschlagene Überarbeitung des Schengener Grenzkodex wird dieses Instrumentarium ebenfalls ergänzen, indem die Instrumentalisierung im EU-Rechtsrahmen definiert wird.

[21] COM(2021) 731.
[22] COM(2021) 732, COM(2021) 733.
[23] JOIN(2021) 32 final.
[24] Beschluss (GASP) 2021/1990 des Rates zur Änderung des Beschlusses 2012/642/GASP über restriktive Maßnahmen gegen Belarus und Verordnung (EU) 2021/1985 des Rates zur Änderung der Verordnung (EG) Nr. 765/2006 über restriktive Maßnahmen gegen Belarus (ABl. L 405 vom 16.11.2021, S. 1 und 10).
[25] COM(2021) 753.
[26] COM(2021) 752.

Wie im fünften Jahresbericht[27] dargelegt, wird die Umsetzung des Gemeinsamen Rahmens für die Abwehr hybrider Bedrohungen von 2016 und der Gemeinsamen Mitteilung zur Stärkung der Resilienz und zum Ausbau der Kapazitäten zur Abwehr hybrider Bedrohungen von 2018 fortgesetzt. Überlegungen zu hybriden Bedrohungen werden als Bestandteil der Folgenabschätzungen neuer politischer Initiativen der EU im Rahmen des Instrumentariums für eine bessere Rechtsetzung durchgängig in die Politikgestaltung einbezogen. Das Netz der Kontaktstellen für hybride Bedrohungen, zu dem nun Referenten aus allen Kommissionsdienststellen, aus dem Europäischen Auswärtigen Dienst und aus der Europäischen Verteidigungsagentur gehören, wurde gestärkt.

Die Verbesserung des Lagebewusstseins und die Stärkung der Resilienz sind ebenfalls von entscheidender Bedeutung für die Abwehr hybrider Bedrohungen. Die im Rahmen des Europäischen Auswärtigen Dienstes tätige **Analyseeinheit für hybride Bedrohungen** innerhalb des EU-Zentrums für Informationsgewinnung und Lageerfassung (EU INTCEN) hat bereits über 100 schriftliche Berichte über hybride Bedrohungen erstellt, darunter sechs Analysen von Trends bei hybriden Bedrohungen. Um Instrumente zur Bewertung des Stands der Abwehrbereitschaft in Sektoren zu entwickeln, die anfällig für hybride Bedrohungen sind, haben die Kommissionsdienststellen und der Europäische Auswärtige Dienst **erstmals sektorspezifische Referenzwerte festgelegt**, was einen ersten Schritt darstellt, um die Fortschritte beim Schutz der Mitgliedstaaten und der EU-Organe vor hybriden Bedrohungen zu verfolgen.

Hybride Bedrohungen sind – auf der Grundlage der Gemeinsamen Erklärungen von Warschau und Brüssel von 2016 und 2018 – auch ein Schwerpunkt der **Zusammenarbeit zwischen der EU und der NATO**, die während der COVID-19-Pandemie weiter intensiviert wurde.[28] Angesichts der sich ständig wandelnden Bedrohungen für die EU-Mitgliedstaaten und die NATO-Bündnispartner laufen derzeit Verhandlungen über eine dritte gemeinsame Erklärung der EU und der NATO.

Chemische, biologische, radiologische und nukleare Risiken

Bedrohungen biologischen, chemischen und unbekannten Ursprungs können grenzüberschreitende Gesundheitsgefahren darstellen und als hybride Bedrohungen oder für terroristische Zwecke genutzt werden. Diese Bedrohungen kontinuierlich zu analysieren sowie die Beschaffung und Herstellung einschlägiger medizinischer Gegenmaßnahmen zu fördern wird ein Bestandteil des Mandats der HERA sein. Die EU finanziert (mit 5 Mio. EUR aus dem Gesundheitsprogramm) außerdem eine gemeinsame Maßnahme, die speziell darauf ausgerichtet ist, die Abwehrbereitschaft und Reaktion im Hinblick auf biologische und chemische Terrorangriffe zu verbessern.[29]

Technologische Herausforderungen

---

[27] SWD(2021) 729.

[28] Siehe 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.

[29] Die Arbeit des Konsortiums JA TERROR wird sich konkret auf die Bereitstellung von Wissen und Informationen für alle relevanten Sektoren konzentrieren, um die Gesundheitsvorsorge zu unterstützen und die sektorübergreifende Reaktion (Gesundheit, Sicherheit und Katastrophenschutz) auf biologische oder chemische Terroranschläge zu stärken. In der Gruppe befinden sich Interessenträger aus 18 europäischen Ländern (14 Mitgliedstaaten, ein EWR-Mitgliedstaat, ein Bewerberland, ein mögliches Bewerberland und das Vereinigte Königreich). Angesichts der gemeinsamen Ziele wird auch die HERA eng mit diesem Konsortium zusammenarbeiten.

Böswillige Akteure und Kriminelle können sich Technologien wie Verschlüsselung oder künstliche Intelligenz zunutze machen. Hier besteht die Herausforderung für die politischen Entscheidungsträger in Europa und darüber hinaus darin, das richtige Gleichgewicht zwischen dem Schutz der Rechte und Freiheiten des Einzelnen, der Gewährleistung der Cybersicherheit und der Gewährleistung, dass die Strafverfolgungsbehörden ihre Aufgaben erfüllen können, zu finden.

Wie im dritten Bericht der Beobachtungsstelle für Verschlüsselung[30] hervorgehoben wird, stehen die Strafverfolgungs- und Justizbehörden vor zahlreichen Herausforderungen, wenn es darum geht, Kommunikation rechtmäßig abzufangen und Beweismittel für strafrechtliche Ermittlungen zu sammeln. In der diesjährigen Strategie zur Bekämpfung der organisierten Kriminalität hat die Kommission ihre Absicht dargelegt, im Jahr 2022 einen Vorschlag für das künftige Vorgehen in Bezug auf den rechtmäßigen und gezielten Zugriff auf **verschlüsselte Informationen** für strafrechtliche Ermittlungen und Strafverfolgungsmaßnahmen zu unterbreiten. Die Kommission führt derzeit eine Bestandsaufnahme der bestehenden Rechtsvorschriften, der Rechtsprechung, der operativen Verfahren und des Bedarfs in den Mitgliedstaaten durch, um ein umfassenderes Verständnis der rechtlichen Rahmenbedingungen, der derzeitigen Praktiken und der Bedürfnisse der Strafverfolgungsbehörden, Justizbehörden und Cybersicherheitsgemeinschaften zu erlangen.

Der Rat „Justiz und Inneres“ und der Rat „Telekommunikation“ haben den Vorschlag der Kommission für ein Gesetz über **künstliche Intelligenz** erörtert. Der slowenische Ratsvorsitz hat Workshops, einschließlich spezieller Workshops zum Thema Strafverfolgung, organisiert, um die komplexesten Fragen zu klären. Im Juni 2021 veröffentlichten der Europäische Datenschutzausschuss und der Europäische Datenschutzbeauftragte eine gemeinsame Stellungnahme zum Vorschlag der Kommission[31], in der ein allgemeines Verbot der Verwendung von KI für biometrische Fernidentifizierungssysteme im öffentlichen Raum gefordert wird. Das Europäische Parlament hat am 6. Oktober 2021 eine Entschließung angenommen[32], in der auf das Risiko biometrischer Echtzeit-Fernidentifizierungssysteme und diskriminierender Algorithmen bei KI-Anwendungen hingewiesen und betont wird, dass eine menschliche Aufsicht und starke rechtliche Befugnisse erforderlich sind, insbesondere im Strafverfolgungs- und grenzüberschreitenden Kontext.

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

Terrorismus

Aus dem von Europol im Juni 2021 veröffentlichten Tendenz- und Lagebericht über den Terrorismus in der EU[33] geht hervor, dass die Mitgliedstaaten der Auffassung sind, dass der Dschihad-Terrorismus nach wie vor die größte terroristische Bedrohung in der EU darstellt. Im Bericht wird bestätigt, dass die häufigsten Dschihad-Angriffe in der EU, in der Schweiz und im Vereinigten Königreich Anschläge auf Zivilpersonen an öffentlichen Orten waren.

---

30 Dritter Bericht der Beobachtungsstelle für Verschlüsselung vom 2. Juli 2021.

31 Gemeinsame Stellungnahme 5/2021 des EDSA und EDSB zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz).

32 Entschließung des Europäischen Parlaments vom 6. Oktober 2021 zu dem Thema: Künstliche Intelligenz im Strafrecht und ihre Verwendung durch die Polizei und Justizbehörden in Strafsachen.

33 Europol, Tendenz- und Lagebericht über den Terrorismus in der EU (TE-SAT), 22. Juni 2021.

Alle im Jahr 2020 ausgeübten Dschihad-Angriffe wurden von Einzelpersonen, die allein handelten, verübt. Es wird auch darauf hingewiesen, dass mehrere im Jahr 2020 festgenommene Verdächtige Online-Kontakt mit Anhängern terroristischer Gruppen außerhalb der EU hatten. Die selbsterklärte Terrorgruppe Islamischer Staat und das Al-Qaida-Netzwerk stifteten weiter einzelne Akteure zu Anschlägen in westlichen Ländern an[34], was aufzeigt, wie eng die äußere und die innere Sicherheit miteinander verknüpft sind. Im August erklärte der Rat „Justiz und Inneres“: „Die EU und ihre Mitgliedstaaten werden alles in ihrer Macht Stehende tun, um sicherzustellen, dass die Lage in Afghanistan nicht zu neuen Sicherheitsbedrohungen für EU-Bürgerinnen und -Bürger führt.“[35] Es wurden bereits Schritte unternommen, um sicherzustellen, dass alle verfügbaren Instrumente genutzt werden, um auf mögliche Bedrohungen zu reagieren.

Angesichts der Entwicklungen in Afghanistan hat der EU-Koordinator für die Terrorismusbekämpfung in Abstimmung mit der Kommission, dem Europäischen Auswärtigen Dienst, dem Ratsvorsitz und einschlägigen EU-Agenturen einen **Aktionsplan zur Terrorismusbekämpfung für Afghanistan**[36] ausgearbeitet. Der Aktionsplan enthält 23 Empfehlungen für Maßnahmen, die in vier Bereiche unterteilt sind: 1) Sicherheitskontrollen – Unterwanderung verhindern; 2) verhindern, dass Afghanistan zu einem sicheren Zufluchtsort terroristischer Vereinigungen wird; 3) Überwachung und Bekämpfung von Propaganda und Mobilisierung (z. B. Rolle des Aufklärungsnetzwerks gegen Radikalisierung) und 4) Bekämpfung der organisierten Kriminalität als Quelle der Terrorismusfinanzierung. Die Mitgliedstaaten begrüßten den Aktionsplan auf der Tagung des Rates „Justiz und Inneres“ vom 8. Oktober 2021. Ein erster Erfolg war ein freiwilliges Verfahren für verstärkte Sicherheitskontrollen bei Einreisenden aus Afghanistan, das am 22. November 2021 vom Ständigen Ausschuss der EU für die innere Sicherheit gebilligt wurde. Bei einer Fachsitzung mit Mitgliedern der von den Taliban erklärten afghanischen Übergangsregierung am 28. November 2021 in Doha[37] forderte die EU Afghanistan nachdrücklich auf, entschlossene Maßnahmen zur Bekämpfung aller Formen des Terrorismus zu ergreifen.

Die Kommission arbeitet weiter an der Umsetzung der Agenda für Terrorismusbekämpfung. Am 18. November 2021 wurde eine **Evaluierung der Richtlinie zur Terrorismusbekämpfung**[38] angenommen[39], deren Ergebnis im Großen und Ganzen positiv war. Es bestehen jedoch Probleme, die die Funktionsweise der Richtlinie einschränken, so gibt es z. B. Schwierigkeiten beim Nachweis des terroristischen Vorsatzes oder in einigen Mitgliedstaaten Herausforderungen bei der Einstufung rechtsextremer Gewalttaten als terroristische Handlungen.

Zuletzt bestehen auch nach wie vor Hindernisse für eine wirksame Zusammenarbeit und Koordinierung zwischen den Mitgliedstaaten in Bezug auf **den Schutz und die Unterstützung der Opfer des Terrorismus**. Die Kommission prüft derzeit die Umsetzung der Richtlinie in nationales Recht weiter und hat seit Juli 2021 Vertragsverletzungsverfahren gegen 24 Mitgliedstaaten wegen unzureichender Umsetzung der Richtlinie eingeleitet. Im

---

34 Europol, Tendenz- und Lagebericht über den Terrorismus in der EU (TE-SAT), 22. Juni 2021.
35 Erklärung zur Lage in Afghanistan, 11385/21, 31. August 2021.
36 Afghanistan: Aktionsplan zur Terrorismusbekämpfung, 29. September 2021.
37 Dieser Dialog bedeutet nicht, dass die EU die Übergangsregierung anerkennt, sondern ist Teil des operativen Engagements der EU – im Interesse der EU und des afghanischen Volkes.
38 Richtlinie (EU) 2017/541 vom 15. März 2017 zur Terrorismusbekämpfung (ABl. L 88 vom 15.3.2017, S. 6).
39 COM (2021) 701 final.

Rahmen des Pilotprojekts des EU-Kompetenzzentrums für Terroropfer[40] wurden die Mitgliedstaaten und die nationalen Opferschutzorganisationen bei der praktischen Anwendung der EU-Vorschriften über Opfer des Terrorismus unterstützt. Zu den Ergebnissen dieses Pilotprojekts gehören das EU-Handbuch zu Opfern des Terrorismus, nationale Handbücher und nationale Schulungsmaßnahmen mit mehr als 750 Teilnehmern.

Die Kommission unterstützt fortwährend die Bemühungen der Mitgliedstaaten um einen besseren Schutz des öffentlichen Raums. Es wurde eine zweite digitale Herbstschule zum Thema Schutz des öffentlichen Raums veranstaltet, und Interessenträger werden über bewährte Verfahren auf dem Laufenden gehalten.[41]

Um Terrorismus besser zu verhindern, muss die Bekämpfung der Radikalisierung, sowohl offline als auch online, fortgesetzt werden. Im Oktober 2021 feierte das **Aufklärungsnetzwerk gegen Radikalisierung (RAN)** das zehnte Jahr der Radikalisierungsprävention, wobei im Mittelpunkt einer Konferenz der sich wandelnde Charakter der Herausforderungen in diesem Bereich stand. In Bezug auf die Bekämpfung der Online-Radikalisierung organisierte **Europol** am 5. November 2021 in Zusammenarbeit mit der Kommission eine Planübung, um die Umsetzung des EU-Krisenprotokolls[42] zu testen. Bei der Übung, die im Rahmen des EU-Internetforums stattfand, wurde die Zusammenarbeit zwischen Regierungsbehörden und der Tech-Industrie getestet, um die virale Verbreitung terroristischer und gewaltverherrlichender extremistischer Online-Inhalte einzudämmen.

Da die Sicherheit unserer Partner und Nachbarn für die Gewährleistung der eigenen inneren Sicherheit Europas von entscheidender Bedeutung ist, stehen der Europäische Auswärtige Dienst und die Kommission in einem regelmäßigen engen **Dialog über Terrorismusbekämpfung** mit wichtigen Drittländern und internationalen Organisationen, um die Zusammenarbeit in Fragen der Sicherheit und der Terrorismusbekämpfung zu verbessern. Dabei werden Abkommen geschlossen, um den Austausch von Informationen und personenbezogenen Daten zu erleichtern, was wiederum eine stärkere operative Zusammenarbeit über Europol ermöglicht.

Dialoge mit Drittländern/internationalen Organisationen über Terrorismusbekämpfung im Zeitraum Juli bis Dezember 2021

Zentralasien – Politischer und sicherheitspolitischer Dialog auf hoher Ebene (Juli 2021)
- Neuseeland – Gemischter Kooperationsausschuss, Strategischer Dialog EU-NZ (Juli 2021)
- Malediven – Treffen hoher Beamter – Fachbereich Terrorismusbekämpfung (September 2021)
- Bosnien und Herzegowina – Dialog über Terrorismusbekämpfung (Oktober 2021)
- Türkei – Dialog über Terrorismusbekämpfung (25. November 2021)
- EU-NATO – Dialog über Terrorismusbekämpfung (15. November 2021)

Europol-Abkommen mit Drittländern über den Austausch personenbezogener

[40] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/protecting-victims-rights/eu-centre-expertise-victims-terrorism_en.

[41] Siehe den Newsletter zum Schutz des öffentlichen Raums: https://europa.eu/!jV87NK.

[42] Das von den Justiz- und Innenministern im Oktober 2019 angenommene EU-Krisenprotokoll ist ein freiwilliger Mechanismus, der es den EU-Mitgliedstaaten und Online-Plattformen ermöglicht, im Falle eines Terroranschlags rasch und koordiniert auf die Verbreitung terroristischer Inhalte im Internet zu reagieren und gleichzeitig strenge Datenschutz- und Grundrechtsgarantien zu wahren.

Daten

- Abschluss eines Abkommens zwischen Europol und Neuseeland am 28. September 2021
- Abhaltung einer ersten Verhandlungsrunde mit Israel am 22. November 2021

Europol-Abkommen über strategische Zusammenarbeit

- Unterzeichnung eines Abkommens über strategische Zusammenarbeit zwischen Europol und Armenien am 16. September 2021

Mit dem Westbalkan ist die Zusammenarbeit bei der Terrorismusbekämpfung und der Radikalisierungsprävention im Rahmen des Gemeinsamen Aktionsplans 2018 zur Terrorismusbekämpfung für den westlichen Balkan[43] besonders intensiv. Die Arbeiten zur Umsetzung der sechs Durchführungsvereinbarungen mit den einzelnen Partnern im Westbalkan werden kontinuierlich fortgesetzt. Auf dem Gipfeltreffen EU-Westbalkan im Oktober 2021 in Slowenien wurde betont, wie wichtig es ist, entschlossene Maßnahmen zu ergreifen, um Terrorismus und Radikalisierung, schwere und organisierte Kriminalität, insbesondere Menschenhandel, Schleuserkriminalität, Geldwäsche, Drogenanbau und -handel, sowie Korruption, unerlaubten Handel mit Feuerwaffen, Cyberbedrohungen und hybride Bedrohungen anzugehen.

Am 20. Juli 2021 legte die Kommission ein ehrgeiziges Paket von Legislativvorschlägen zur Stärkung der **EU-Vorschriften zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung (AML/CFT)**[44] vor, einschließlich Maßnahmen in Bezug auf Kryptowerte, mit denen für eine Angleichung an die neuesten internationalen Standards, die von der Arbeitsgruppe „Bekämpfung der Geldwäsche und der Terrorismusfinanzierung“ (FATF) ausgearbeitet wurden, gesorgt werden soll. So werden beispielsweise alle Anbieter von Krypto-Dienstleistungen in den Anwendungsbereich der EU-Rechtsvorschriften zur Bekämpfung der Geldwäsche einbezogen, gemäß denen sie verdächtige Transaktionen ihrer Kunden melden müssen. Die Kommission schlägt ferner vor, die Bereitstellung anonymer Krypto-Geldbörsen durch Anbieter von Krypto-Dienstleistungen zu verbieten. Das Paket ist Teil der Zusage der Kommission, Einzelpersonen in der EU und das EU-Finanzsystem vor Terrorismusfinanzierung zu schützen. Das Ziel besteht darin, die Aufdeckung verdächtiger Transaktionen und Aktivitäten zu erleichtern und die Schlupflöcher zu schließen, die Kriminelle dazu nutzen, Erträge aus Straftaten über das Finanzsystem zu waschen oder damit terroristische Aktivitäten zu finanzieren.

Neue Vorschriften zu Zollkontrollen betreffend Barmittel, die in die Union oder aus der Union verbracht werden[45] und zur Einfuhr von Kulturgütern[46] sind inzwischen in der

[43] Im Oktober 2018 unterzeichneten die Kommission und Vertreter Albaniens, Bosnien und Herzegowinas, des Kosovos*, Montenegros, Nordmazedoniens und Serbiens einen Gemeinsamen Aktionsplan zur Terrorismusbekämpfung für den westlichen Balkan.

[44] COM(2021) 421 final, COM(2021) 420 final, COM(2021) 423 final, COM(2021) 422 final.

[45] Verordnung (EU) 2018/1672 über die Überwachung von Barmitteln, die in die Union oder aus der Union verbracht werden (ABl. L 284 vom 12.11.2018, S. 6).

[46] Verordnung (EU) 2019/880 des Europäischen Parlaments und des Rates vom 17. April 2019 über das Verbringen und die Einfuhr von Kulturgütern (ABl. L 151 vom 7.6.2019, S. 1).

Umsetzungsphase[47] (letztere in der Teilumsetzung, solange die Einrichtung eines dazugehörigen zentralen IT-Systems noch aussteht). Diese Vorschriften werden nicht nur zur Bekämpfung von Geldwäsche und zum Schutz des Kulturerbes beitragen, sondern auch zur verstärkten Bekämpfung der Terrorismusfinanzierung.

Organisierte Kriminalität

Die von Europol während der COVID-19-Pandemie beobachteten Kriminalitätstrends zeigen, dass trotz Lockdowns und Beschränkungen weiterhin schwere und organisierte Verbrechen verübt werden, die Täter sich anpassen und alle Umstände ausgenutzt werden, um einen Gewinn zu erzielen. Während die legalen Volkswirtschaften geschwächt wurden, ist die kriminelle Wirtschaft stärker geworden. Die internationale Zusammenarbeit bei der Strafverfolgung zeigt täglich das globale Ausmaß organisierter krimineller Netze und wie stark Kriminelle untereinander vernetzt sind. Es ist internationales Engagement bei der Bekämpfung der organisierten Kriminalität, einschließlich weiterer Schritte zur Entwicklung von Partnerschaften und der Zusammenarbeit mit Ländern in der unmittelbaren Nachbarschaft und darüber hinaus, erforderlich, um diese grenzüberschreitende Herausforderung zu bewältigen.

Der Handel mit **illegalen Drogen** ist nach wie vor der größte kriminelle Markt in der EU. Der EU-Drogenaktionsplan für die Jahre 2021–2025 wurde Anfang Juli im Anschluss an die im Dezember 2020 veröffentlichte Strategie angenommen. Die Koordinatoren für die Drogenbekämpfung der EU-Mitgliedstaaten trafen am 22. September zusammen, um über die Prävention zu sprechen. Die **Europäische Beobachtungsstelle für Drogen und Drogensucht** (EMCDDA) stellte im Juni im Europäischen Drogenbericht 2021[48] ihre jüngste Analyse der Drogensituation in Europa vor und veröffentlichte im September einen Bericht, in dem die zunehmende Produktion von Methamphetamin in Afghanistan[49] hervorgehoben wird. **Europol** intensiviert die Zusammenarbeit mit den iranischen und türkischen Behörden, um die Gewinnung von Erkenntnissen über den Drogenhandel zu verbessern. Nach Angaben von Europol führt die Hauptroute für den Heroinhandel innerhalb der EU nach wie vor über den Balkan, während der Kokainhandel am häufigsten über Containerhäfen wie Antwerpen oder Rotterdam stattfindet. Europol baut derzeit eine neue Drogenplattform auf, um die EU-Mitgliedstaaten wöchentlich über die Entwicklungen zu informieren.

Die Zusammenarbeit mit internationalen Partnern ist bei der Drogenbekämpfung von entscheidender Bedeutung. Zu den jüngsten Kontakten gehörten ein Dialog zwischen der EU und den Vereinigten Staaten im September 2021, der Dialog zwischen der EU und dem Westbalkan über Drogen im Oktober und der EU-LAK-Mechanismus zur Koordinierung und Zusammenarbeit im Bereich der Drogenbekämpfung im Juni. Es sollen ein Dialog zwischen

[47] Durchführungsverordnung 2021/1079 der Kommission zur Umsetzung der Verordnung (EU) 2019/880 des über das Verbringen und die Einfuhr von Kulturgütern (von der Kommission am 24.6.2021 angenommen) und Durchführungsbeschluss der Kommission über Kriterien für den gemeinsamen Risikomanagementrahmen bei Barmittelbewegungen zu Zwecken der Verordnung 2018/1672 des Europäischen Parlaments und des Rates über die Überwachung von Barmitteln, die in die Union oder aus der Union verbracht werden (wird voraussichtlich im Dezember 2021 angenommen).

[48] https://www.emcdda.europa.eu/publications/edr/trends-developments/2021_en.

[49] https://www.emcdda.europa.eu/publications/ad-hoc-publication/methamphetamine-from-afghanistan-signals-indicate-europe-should-be-better-prepared_en.

der EU und Iran sowie ein Dialog zwischen der EU und Kolumbien über Drogen aufgenommen werden.

Aus dem EU-Aktionsplan gegen den **unerlaubten Handel mit Feuerwaffen** 2020–2025[50]geht klar hervor, dass die vollständige Umsetzung der Richtlinie über Feuerwaffen oberste Priorität hat. Im Bericht der Kommission vom Oktober 2021 wird die Anwendung der Richtlinie über die Kontrolle des Erwerbs und des Besitzes von Waffen[51] bewertet und festgestellt, dass durch die Feuerwaffen-Richtlinie bei den Kategorien von Feuerwaffen, ihrer Nachverfolgung sowie dem Austausch von Informationen und Verwaltungsverfahren Verbesserungen eingetreten sind. Bislang haben jedoch nur zehn Mitgliedstaaten die Richtlinie vollständig umgesetzt. In dem Bericht wird hervorgehoben, dass noch Raum für weitere Fortschritte bei der rechtlichen Kontrolle des Erwerbs, Besitzes und der Verbringung von Waffen für den zivilen Gebrauch besteht. Die Kommission wird daher eine Folgenabschätzung der möglichen Änderungen an der Feuerwaffen-Richtlinie durchführen. In der EU gibt es rund 35 Millionen illegale Feuerwaffen, und viele werden über unsere Grenzen geschmuggelt. Die Zusammenarbeit mit dem Westbalkan ist von entscheidender Bedeutung. Im September 2021 fand eine Ministerkonferenz EU-Westbalkan zu Feuerwaffen statt, auf der die enge Zusammenarbeit zwischen der EU und dem westlichen Balkan bei der Bekämpfung des unerlaubten Handels mit Feuerwaffen im Rahmen der Europäischen multidisziplinären Plattform gegen kriminelle Bedrohungen (**EMPACT**) hervorgehoben wurde. Seit der Annahme des Regionalen Fahrplans für eine umfassende Klein- und Leichtwaffenkontrolle im Jahr 2018 haben die Partner im Westbalkan stetige Fortschritte bei der Harmonisierung der Rechtsrahmen mit den Feuerwaffenvorschriften der EU und der Vereinten Nationen erzielt und die operative Zusammenarbeit und den Informationsaustausch mit der EU und ihren Agenturen intensiviert.

Der **illegale Handel mit Abfällen**[52] ist eine der schwersten Formen der Umweltkriminalität. Bis zu 30 % der Abfallverbringungen im Wert von jährlich 9,5 Mrd. EUR sind illegal. Die Kommission hat am 17. November 2021 die überarbeitete Verordnung über die Verbringung von Abfällen angenommen, durch die mit der Einsetzung einer EU-Gruppe für die Durchsetzung der Vorschriften über die Abfallverbringung, mit der Ermächtigung des Europäischen Amts für Betrugsbekämpfung (OLAF), länderübergreifende Ermittlungen der Mitgliedstaaten im Bereich des illegalen Abfallhandels zu unterstützen, und mit dem Erlass strengerer Vorschriften über Verwaltungssanktionen die Maßnahmen zur Bekämpfung des illegalen Abfallhandels weiter verstärkt werden.

Die **Korruptionsbekämpfung** ist von entscheidender Bedeutung, um eine starke Rechtsstaatlichkeit sicherzustellen und das Vertrauen der Bürgerinnen und Bürger in die öffentlichen Einrichtungen zu erhalten. Der enge Zusammenhang zwischen organisierter Kriminalität und Korruption sowie die Gefahr der Unterwanderung der legalen Wirtschaft und öffentlicher Einrichtungen stellen zentrale Herausforderungen dar. Im zweiten Bericht über die Rechtsstaatlichkeit, der am 20. Juli 2021 veröffentlicht wurde[53], wird hervorgehoben, dass die EU-Mitgliedstaaten zwar weiterhin zu den Ländern mit den weltweit besten Ergebnissen bei der Korruptionsbekämpfung zählen, in einigen Mitgliedstaaten jedoch nach wie vor Herausforderungen bestehen, insbesondere in Zusammenhang mit

[50] COM(2020) 608 final.
[51] COM(2021) 647 final.
[52] COM(2021) 709 final.
[53] COM(2021) 700 final.

strafrechtlichen Ermittlungen, Strafverfolgungsmaßnahmen und der Verhängung von Strafen für Korruption. Zahlreiche Mitgliedstaaten haben Maßnahmen zur Stärkung der Korruptionsprävention und Integritätsrahmen, einschließlich der Vorschriften über Interessenkonflikte, die Transparenz der Lobbyarbeit und den Drehtüreffekt, ergriffen, gleichzeitig jedoch sind die für die Korruptionsbekämpfung bereitgestellten Mittel in einigen Mitgliedstaaten unzureichend. In anderen Mitgliedstaaten bestehen Bedenken hinsichtlich der Wirksamkeit der Ermittlungen, Strafverfolgung und Urteilsfindung in Korruptionsfällen auf hoher Ebene fort.

Es ist auch von wesentlicher Bedeutung, **Betrug zum Nachteil des EU-Haushalts** zu verhindern. Das Europäische Parlament veröffentlichte am 26. Oktober zwei Berichte[54], in denen mit Besorgnis festgestellt wird, dass sich durch die COVID-19-Pandemie neue Chancen für Betrüger und die organisierte Kriminalität ergeben, und betont wird, dass Präventivmaßnahmen eine wichtige Rolle dabei zukommt, Korruptionsrisiken in Krisensituationen vorherzusehen und zu bekämpfen, und darauf hingewiesen wird, dass das finanzielle Umfeld der Union transparenter gestaltet werden muss. Im September 2021, weniger als vier Monate seit Aufnahme ihrer Tätigkeit, hat die Europäische Staatsanwaltschaft (EUStA) bereits bemerkenswerte Ergebnisse erzielt und in mutmaßlichen Betrugsfällen im Gesamtwert von schätzungsweise rund 4,5 Mrd. EUR Ermittlungen eingeleitet.[55] Am 15. Oktober 2021 leitete Europol die Operation Sentinel ein, eine neue EU-weite Operation zur Bekämpfung von Betrug, der sich auf Mittel im Rahmen der Initiative „Next Generation EU“ bezieht. An ihr sind die EUStA, Eurojust, das OLAF und 23 Mitgliedstaaten beteiligt. Die Tätigkeiten werden mindestens ein Jahr andauern und sich auf den proaktiven Austausch nachrichtendienstlicher Erkenntnisse, den Informationsaustausch und die Unterstützung der Koordinierung von Maßnahmen zur Bekämpfung von Betrug, insbesondere Betrug zulasten der Aufbau- und Resilienzfazilität, konzentrieren.

Die **Schleusung von Migranten** ist eine kriminelle Handlung, bei der schutzbedürftige Personen ausgenutzt werden. 50 % der Schleuser sind Polykriminelle, die auch an anderen kriminellen Aktivitäten beteiligt sind. Die Verhütung und Bekämpfung der Schleusung von Migranten ist eines der Hauptziele der EU-Strategie für eine Sicherheitsunion, der EU-Strategie zur Bekämpfung der organisierten Kriminalität, der EU-Strategie zur Bekämpfung des Menschenhandels (2021–2025) und des neuen Migrations- und Asylpakets, das eine kontinuierliche internationale Zusammenarbeit und Koordinierung erfordert. Aufbauend auf den Fortschritten, die mit dem ersten EU-Aktionsplan gegen die Schleusung von Migranten (2015–2020) erzielt wurden, hat die Kommission in Zusammenarbeit mit dem Hohen Vertreter einen neuen EU-Aktionsplan für den Zeitraum 2021–2025[56] angenommen.

---

[54] Bericht über die Bewertung von Präventivmaßnahmen zur Vorbeugung von Korruption, vorschriftswidrigen Ausgaben und der Zweckentfremdung von europäischen und nationalen Mitteln im Falle von Nothilfefonds und krisenbezogenen Ausgabenbereichen (2020/2222(INI)) und Bericht über die Auswirkungen der organisierten Kriminalität auf die Eigenmittel der EU und auf die Zweckentfremdung von EU-Mitteln mit besonderem Augenmerk auf der geteilten Mittelverwaltung (2020/2221(INI)).

[55] „Geschätzter Schaden für den EU-Haushalt in laufenden EUStA-Ermittlungen: fast 4,5 Mrd. EUR“, abrufbar unter: https://www.eppo.europa.eu/en/news/estimated-damages-eu-budget-ongoing-eppo-investigations-almost-eu45-billion.

[56] COM(2021) 591.

Themenschwerpunkte des EU-Aktionsplans gegen die Schleusung von Migranten (2021–2025)

- Entwicklung **operativer Partnerschaften zur Bekämpfung von Schleuserkriminalität** mithilfe konkreter Instrumente, die Teil umfassender, ausgewogener, maßgeschneiderter und für beide Seiten vorteilhafter Migrationspartnerschaften sind, wobei weiter auf Vertrauen und gegenseitige Zusammenarbeit gesetzt wird;
- Verbesserung der Umsetzung der Rechtsrahmen für die Sanktionierung von Schleusern und für den Schutz vor Ausbeutung;
- Stärkung der justiziellen Zusammenarbeit im Bereich der Schleuserkriminalität, indem die EU-Mitgliedstaaten aufgefordert werden, die Unterstützung von **Eurojust** bei grenzüberschreitenden Ermittlungen über gemeinsame Ermittlungsgruppen stärker und die Fokusgruppe der für Schleuserkriminalität zuständigen Staatsanwälte bestmöglich in Anspruch zu nehmen;
- Reaktion auf **sich ständig weiterentwickelnde Online-Praktiken** und -Instrumente, die Schleuserkriminalität erleichtern, durch eine verstärkte operative Zusammenarbeit und einen verstärkten Informationsaustausch zwischen nationalen Behörden und EU-Agenturen;
- Intensivierung der **Forschung und Datenerhebung** für ein besseres Verständnis der Migrationstendenzen, der Art und des Umfangs krimineller Netzwerke, der Auswirkungen von Maßnahmen zur Bekämpfung von Schleuserkriminalität und der Vorgehensweise krimineller Netzwerke.

Am 4. und 5. November 2021 hielt **Eurojust** seine Jahrestagung zum Thema Schleuserkriminalität ab, die auch die Gelegenheit bot, die diesbezügliche Zusammenarbeit mit dem Westbalkan und den Partnerländern des südlichen Mittelmeerraums, die am Programm „EuroMed Justice“ teilnehmen, zu vertiefen. In den letzten sechs Monaten des Jahres 2021 hat Eurojust auch mehrere große Operationen gegen die Schleusung von Migranten unterstützt.[57]

Im Anschluss an die **Strategie zur Bekämpfung des Menschenhandels**[58] führt die Kommission derzeit eine Evaluierung der Richtlinie zur Bekämpfung des Menschenhandels[59] durch, bei der sie auch die Möglichkeit der Einführung von EU-Mindestvorschriften prüft, mit denen die Inanspruchnahme von Diensten, die von Opfern des Menschenhandels erbracht werden, unter Strafe gestellt werden könnten. Am 18. Oktober 2021 fand der 15. EU-Tag zur Bekämpfung des Menschenhandels statt, um für dieses Verbrechen zu sensibilisieren. Am selben Tag veröffentlichte das Netz der JI-Agenturen einen gemeinsamen Bericht[60] über die Ermittlung und den Schutz von Opfern des Menschenhandels. Im November 2021 koordinierten bzw. unterstützten **Europol** und **Frontex** eine große internationale Aktion zur

[57] Siehe zum Beispiel folgende Pressemitteilung: https://www.eurojust.europa.eu/people-smuggling-network-netherlands-and-hungary-dismantled.

[58] COM(2021) 171.

[59] Richtlinie 2011/36/EU vom 5. April 2011 zur Verhütung und Bekämpfung des Menschenhandels und zum Schutz seiner Opfer (ABl. L 101 vom 15.4.2011).

[60] Gemeinsamer Bericht des Netzes der JI-Agenturen zur Ermittlung und zum Schutz von Opfern des Menschenhandels | Eurojust | Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (europa.eu).

Bekämpfung des Menschenhandels. Es beteiligten sich 29 Länder unter der Leitung von Österreich und Rumänien an den Aktionstagen, wobei mehr als 14 000 Strafverfolgungsbeamte Schleusungsrouten (Straßen und Flughäfen) ins Visier nahmen, was 212 Festnahmen und die Identifizierung weiterer 89 Personen mit Verdacht auf Menschenhandel zum Ergebnis hatte.

Der **sexuelle Missbrauch von Kindern** – sowohl online als auch offline – ist eines der schwersten Verbrechen, und seine Bekämpfung stellt für die EU und ihre Mitgliedstaaten eine ständige Priorität dar. Am 12. November 2021 haben die Innenminister erörtert, welche Strategien und Verfahren zur Sensibilisierung und Verhütung dieser Straftat zum Einsatz kommen sollen, welche Instrumente für eine erfolgreiche Ermittlung dieser Straftat unter uneingeschränkter Achtung der Grundrechte aller Betroffenen erforderlich sind, und welche Möglichkeiten für den Opferschutz mit starkem Fokus auf den Rechten des Kindes bestehen. Die befristeten Rechtsvorschriften, mit denen sichergestellt werden soll, dass Anbieter von Online-Diensten weiterhin in der Lage sind, sexuellen Missbrauch von Kindern im Internet auf freiwilliger Basis aufzudecken und zu melden[61] und Material über sexuellen Kindesmissbrauch aus ihren Systemen zu entfernen, traten am 3. August 2021 in Kraft. Die Kommission treibt die Umsetzung der in der EU-Strategie für eine wirksamere Bekämpfung des sexuellen Missbrauchs von Kindern und der umfassenden EU-Strategie für die Rechte des Kindes angekündigten Initiativen weiter voran und arbeitet außerdem an längerfristigen Rechtsvorschriften zur wirksameren Bekämpfung des sexuellen Missbrauchs von Kindern im Internet.

V. Eine starke europäische Sicherheitsgemeinschaft

Eine verstärkte polizeiliche Zusammenarbeit in der gesamten EU sowie starke Außengrenzen sind wesentliche Elemente einer EU ohne Kontrollen an den Binnengrenzen. Angesichts des grenzüberschreitenden Charakters der Kriminalitätsbekämpfung und der Erhöhung der Sicherheit müssen sich die Mitgliedstaaten zunehmend aufeinander verlassen. Es bestehen jedoch nach wie vor Hindernisse für den Datenaustausch zwischen den Strafverfolgungsbehörden in verschiedenen EU-Mitgliedstaaten, die zu blinden Flecken führen, die von Kriminellen und Terroristen, die in mehr als einem Mitgliedstaat in Aktion treten, ausgenutzt werden können.[62] Mit der Vorlage eines Pakets von Maßnahmen im Bereich der polizeilichen Zusammenarbeit will die Kommission die Mitgliedstaaten besser unterstützen.

Das **Paket von Maßnahmen im Bereich der polizeilichen Zusammenarbeit** umfasst folgende Vorschläge:

- **Vorschlag für eine Richtlinie über den Informationsaustausch zwischen den Strafverfolgungsbehörden der Mitgliedstaaten**[63]: Ziel ist es, i) den Strafverfolgungsbehörden einen gleichwertigen Zugang zu in einem anderen Mitgliedstaat verfügbaren Informationen zu erleichtern, ii) sicherzustellen, dass alle Mitgliedstaaten über eine effizient funktionierende einzige Anlaufstelle verfügen, und

[61] COM(2020) 568.

[62] Dem Bericht über die Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität (SOCTA) von Europol aus dem Jahr 2021 zufolge sind mehr als 70 % der organisierten kriminellen Gruppen in mehr als drei Mitgliedstaaten vertreten.

[63] COM(2021) 782.

iii) die Netzanwendung für sicheren Datenaustausch von Europol (SIENA) als Standard-Kommunikationskanal für den Austausch von strafverfolgungsrelevanten Informationen zwischen den Mitgliedstaaten einzurichten.

- **Vorschlag für eine Empfehlung des Rates zur operativen polizeilichen Zusammenarbeit**[64]: Ziel ist es, die operative grenzüberschreitende polizeiliche Zusammenarbeit durch die Annahme gemeinsamer EU-Mindeststandards für Kooperationsinstrumente in Bereichen wie grenzüberschreitende Nacheilen, gemeinsame Patrouillen und gemeinsame Einsätze zu verbessern.
- **Vorschlag für eine Verordnung zu Prüm II**[65]: Ziel ist es, den derzeitigen Prüm-Rahmen für den automatisierten Datenaustausch zu überarbeiten, indem u. a. i) die Kategorien von Polizeidaten und Gesichtsbildern hinzugefügt werden, ii) eine technische Lösung (ein zentraler Router) für einen effizienteren automatisierten Datenaustausch zwischen Strafverfolgungsbehörden bereitgestellt wird und iii) sichergestellt wird, dass den Strafverfolgungsbehörden der Mitgliedstaaten einschlägige Daten aus der Europol-Datenbank zur Verfügung stehen.

Europol spielt für die polizeiliche Zusammenarbeit bei der Bekämpfung von Terrorismus und organisierter Kriminalität eine wesentliche Rolle. Eine rasche Einigung über den Vorschlag zur Änderung der Europol-Verordnung[66] würde es Europol ermöglichen, die Mitgliedstaaten bei der Bekämpfung der organisierten Kriminalität und des Terrorismus besser zu unterstützen.

Die Zusammenarbeit zwischen den Strafverfolgungsbehörden auf internationaler Ebene ist für unsere innere Sicherheit von entscheidender Bedeutung. Im Rat wurde im Juli ein Verhandlungsmandat für ein Abkommen zwischen der EU und **Interpol** angenommen. Die Verhandlungen sollten im Dezember 2021 beginnen.

Um die Ermittlungen der Mitgliedstaaten zur Bekämpfung von Terrorismus und organisierter Kriminalität weiter zu unterstützen und die justizielle Zusammenarbeit zu erleichtern, hat die Kommission am 1. Dezember 2021 ein **Paket zur Digitalisierung der Justiz** angenommen.

Das **Paket zur Digitalisierung der Justiz** umfasst folgende Vorschläge:

- **Vorschlag in Bezug auf den digitalen Informationsaustausch in Fällen des grenzüberschreitenden Terrorismus**[67]: Ziel ist es, die Funktionsweise des im Oktober 2019 eingerichteten Justiziellen Terrorismusregisters zu verbessern, damit **Eurojust** die Koordinierung und Zusammenarbeit zwischen den nationalen Ermittlungs- und Strafverfolgungsbehörden bei terroristischen Straftaten stärker und proaktiver unterstützen kann.
- **Vorschlag zur Einrichtung einer Plattform für die Zusammenarbeit gemeinsamer Ermittlungsgruppen (GEG)**[68]: Ziel ist es, die Effizienz und Wirksamkeit von GEG weiter zu steigern. Die Plattform wird eine sichere elektronische Kommunikation und einen sicheren Austausch von Informationen und Beweismitteln zwischen den zuständigen nationalen Behörden sowie den Einrichtungen und sonstigen Stellen der

64 COM(2021) 780.
65 COM(2021) 784.
66 COM(2020) 796.
67 COM(2021) 757.
68 COM(2021) 756.

Union, die an den jeweiligen GEG beteiligt sind, ermöglichen.

- **Vorschlag zur Digitalisierung der grenzüberschreitenden justiziellen Zusammenarbeit und des Zugang zur Justiz in Zivil-, Handels- und Strafsachen**[69]: Ziel des Vorschlags ist es, natürlichen und juristischen Personen einen wirksamen Zugang zur Justiz zu ermöglichen und die justizielle Zusammenarbeit zwischen den Mitgliedstaaten zu erleichtern, indem eine Rechtsgrundlage für den Einsatz moderner digitaler Technologien für die Kommunikation im Zusammenhang mit grenzüberschreitenden Gerichtsverfahren in Zivil-, Handels- und Strafsachen geschaffen wird.

Bessere Synergien zwischen Sicherheit und Verteidigung werden die Wirksamkeit unserer Maßnahmen zur Unterstützung der Mitgliedstaaten in diesen Bereichen erhöhen. Die Kommission hat mit der Umsetzung des im Februar 2021 angenommenen Aktionsplans für **Synergien zwischen der zivilen, der Verteidigungs- und der Weltraumindustrie**[70] begonnen. Sie arbeitet mit EU-Agenturen, insbesondere mit der Europäischen Verteidigungsagentur, zusammen, um auf Fähigkeiten ausgerichtete Ansätze in allen Sicherheitssektoren und Synergien durch eine bessere Koordinierung von EU-Programmen und -Instrumenten zu fördern. Darüber hinaus wird von der Kommission eine Arbeitsunterlage der Kommissionsdienststellen zum Thema „Verbesserung der Sicherheit durch Forschung und Innovation“ veröffentlicht. In diesem Dokument wird zum einen die strategische Rolle der Sicherheitsforschung bei der Unterstützung der Verwirklichung der verschiedenen Ziele der zivilen Sicherheitspolitik hervorgehoben und zum anderen werden die Maßnahmen veranschaulicht, die ergriffen werden, um eine optimale Übertragung von Innovationen aus der Forschung auf Instrumente und Dienste zu ermöglichen, die den europäischen und nationalen Sicherheitsbehörden zur Verfügung stehen.

Was die EU-Mittel für Sicherheit anbelangt, so wurde das Arbeitsprogramm des Fonds für die innere Sicherheit für den Zeitraum 2021–2022 am 26. November 2021 angenommen. Dies wird zu Maßnahmen in einer Reihe von Bereichen wie Informationsaustausch, grenzüberschreitende Zusammenarbeit, Prävention und Bekämpfung von organisierter Kriminalität, Terrorismus und Radikalisierung (sowohl offline als auch online) beitragen. Am 10. November 2021 nahm die Kommission Arbeitsprogramme für das Programm „Digitales Europa“ an. Hierzu gehört das mit 269 Mio. EUR ausgestattete Arbeitsprogramm zur Cybersicherheit, das von der Kommission im Namen des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (ECCC) mit dem Netzwerk nationaler Koordinierungszentren durchgeführt wird.[71] Im Rahmen dieses Programms werden Investitionen in den Aufbau fortschrittlicher Cybersicherheitsausrüstungen, -werkzeuge und -dateninfrastrukturen getätigt. Es wird die Entwicklung und optimale Nutzung der Kenntnisse und Fähigkeiten im Bereich der Cybersicherheit finanziert, es werden bewährte Verfahren gefördert und es wird die breite Einführung modernster Cybersicherheitslösungen in der gesamten europäischen Wirtschaft ermöglicht.

---

69 COM(2021) 759.

70 COM(2021) 70 final.

71 Bis das ECCC in der Lage ist, seinen eigenen Haushalt zu verwalten, wird die Europäische Kommission die Maßnahmen im Rahmen dieses Arbeitsprogramms in direkter Verwaltung im Namen des ECCC durchführen.

Eine zügige und vollständige Umsetzung der erlassenen Rechtsvorschriften ist für die Wirksamkeit der Sicherheitsunion von entscheidender Bedeutung. In ihren Vertragsverletzungsverfahren verfolgt die Europäische Kommission rechtliche Schritte gegen Mitgliedstaaten, die ihren Verpflichtungen aus dem EU-Recht, einschließlich der Rechtsvorschriften im Rahmen der Sicherheitsunion, nicht nachkommen. Am 2. Dezember beschloss die Kommission, Verfahren gegen verschiedene Mitgliedstaaten einzuleiten[72], weil sie bestimmte Elemente der EU-Vorschriften zur Terrorismusbekämpfung, zur Bekämpfung von Rassismus und Fremdenfeindlichkeit, zum Europäischen Haftbefehl, zum Austausch von Informationen aus dem Strafregister und zur strafrechtlichen Bekämpfung von gegen die finanziellen Interessen der Union gerichtetem Betrug nicht umgesetzt oder angewendet haben.

Die Rolle der Agenturen und Einrichtungen der EU

Die Agenturen und Einrichtungen der EU spielen nicht nur bei der Förderung der Zusammenarbeit und des Informationsaustauschs in der gesamten Union, sondern auch bei der Kriminalitätsbekämpfung nach wie vor eine entscheidende Rolle. Im Berichtszeitraum waren viele ihrer Tätigkeiten darauf ausgerichtet, nicht nur auf die operativen Erfordernisse infolge der Afghanistan-Krise, sondern auch auf andere dringende sicherheitsbezogene Herausforderungen wie hybride Bedrohungen, Ransomware und organisierte Kriminalität unverzüglich zu reagieren.

Beispiele für operative Tätigkeiten der EU-Agenturen

- Im Oktober 2021 trugen die von **Europol** und **Eurojust** koordinierten Kooperationsmaßnahmen entscheidend dazu bei, Ransomware-Angriffe auf kritische Infrastrukturen zu bekämpfen und eine Reihe von Angreifern zu ermitteln, die über 1800 Opfern in 71 Ländern Schaden zufügten.[73]
- Im Juli 2021 feierte **Europol** den fünften Jahrestag der Initiative „No More Ransom“, durch die mehr als sechs Millionen Unternehmen und Einzelpersonen ihre Dateien kostenlos wiedererlangen konnten und die Zahlung von fast einer Milliarde Euro an Cyberkriminelle verhindert wurde.
- Es wurde die Rolle der **ENISA** im Bereich der operativen Zusammenarbeit verstärkt, damit das CSIRTs Network[74], das CyCLONe[75] und alle in der EU tätigen Akteure zusammenarbeiten und auf Großangriffe reagieren können. Durch die Koordinierung der Sekretariate der beiden EU-Netzwerke CyCLONe und CSIRTs will die ENISA die technische und operative Ebene und alle an den Reaktionsmaßnahmen beteiligten EU-Akteure synchronisieren.

Die Zusammenarbeit zwischen den Agenturen spielt ebenfalls eine wichtige Rolle. Ein Beispiel hierfür ist die am 22. November geschlossene Vereinbarung zwischen **Frontex** und

[72] https://ec.europa.eu/commission/presscorner/detail/de/INF_21_6201

[73] https://www.eurojust.europa.eu/12-targeted-involvement-ransomware-attacks-against-critical-infrastructure.

[74] Das Netzwerk von Computer-Notfallteams (CSIRTs Network) ist ein Netzwerk, das aus den ernannten Reaktionsteams für Computersicherheitsverletzungen (Computer Security Incident Response Teams – CSIRTs) der EU-Mitgliedstaaten und dem IT-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der EU (Computer Emergency Response Team for the EU Institutions, bodies and agencies – CERT-EU) besteht.

[75] Netzwerk der Verbindungsorganisationen für Cyberkrisen (Cyber Crisis Liaison Organisation Network).

der Agentur der Europäischen Union für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (**eu-LISA**).

Die meisten Agenturen entwickeln derzeit eine externe Dimension ihrer Tätigkeiten. Die internationale Zusammenarbeit und diese externe Dimension sind der Schlüssel zur Bewältigung der Sicherheitsherausforderungen, mit der die Agenturen beauftragt sind. Die Umsetzung dieser externen Dimension erfolgt in enger Abstimmung und in Koordinierung mit anderen externen Akteuren und Programmen, einschließlich Maßnahmen im Bereich der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP), um Doppelarbeit zu vermeiden, die Zusammenarbeit zu ermöglichen und die Wirksamkeit zu erhöhen.

Die Rolle der EU-Agenturen bei der Reaktion auf die Lage in Afghanistan und der Region

- Die EU-Agenturen stellen eine ständige Überwachung der Lage in Afghanistan und der Region sicher und tragen zur Lageerfassung und zu einem dynamischen Informationsaustausch über Afghanistan im Rahmen des EU-Vorsorge- und Krisenmanagementnetzes für Migration (Blueprint Network) bei.
- Am 31. August veröffentlichte die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (**Europol**) einen Bericht über die möglichen Auswirkungen der Entwicklungen in Afghanistan auf die innere Sicherheit der EU in den Bereichen Terrorismus, organisierte Kriminalität und Schleuserkriminalität. Europol hat ferner eine interne Arbeitsgruppe aus Sachverständigen eingesetzt, um die Krise zu überwachen und relevante und verlässliche Informationen auszutauschen.
- Das Europäische Unterstützungsbüro für Asylfragen (**EASO**) veröffentlichte einen aktualisierten Herkunftsländerbericht mit Informationen über die Sicherheitslage in Afghanistan und leitete Unterstützungsmaßnahmen sowohl in Bezug auf die interne als auch die externe Dimension der Krise in die Wege.
- Die Europäische Agentur für die Grenz- und Küstenwache (**Frontex/EBCG**) ist nach wie vor dabei, die Lage zu überwachen und gemeinsame Operationen der Mitgliedstaaten mit Drittländern zu koordinieren, um die Grenzsicherheit, die operative Zusammenarbeit und den Informationsaustausch zu verbessern.

Neben den im vorliegenden Bericht beschriebenen operativen Maßnahmen haben die Agenturen und Einrichtungen der EU seit dem letzten Fortschrittsbericht über die Sicherheitsunion viele wertvolle Berichte und Leitlinien herausgegeben, die im Anhang aufgeführt sind.

VI. Fazit

Die EU beweist immer wieder aufs Neue, dass sie sich anpassen und neue Herausforderungen annehmen kann, wenn sie entstehen, und dies zeigt sich im Bereich der Sicherheit besonders deutlich. Sei es bei der Unterstützung der Mitgliedstaaten angesichts neuer hybrider Bedrohungen an den Außengrenzen der EU oder bei der Zusammenarbeit mit internationalen Partnern für eine koordinierte Reaktion auf die sich ständig wandelnden Bedrohungen, die sich aus neuen Technologien ergeben – die EU bleibt auf dem neuesten Stand, um ihre

Mitgliedstaaten zu schützen. Gleichzeitig wird konventionelleren Sicherheitsrisiken weiterhin mit Lösungen und Präventivmaßnahmen auf EU-Ebene begegnet.

Die Gewährleistung der Sicherheit Europas als Ganzes ist eine gemeinsame Verantwortung, bei der jeder Akteur seinen Beitrag leisten muss – vom Europäischen Parlament und vom Rat, die neue zweckdienliche und wirksame Vorschriften erlassen, über die Mitgliedstaaten, die diese rechtzeitig umsetzen, bis hin zu der Vielzahl von Behörden, Organisationen und Interessenträgern, die vor Ort die operative Arbeit leisten. Die Sicherheitsunion wird im Interesse der Bürgerinnen und Bürger der EU weiterhin die Koordinierung einer sehr großen Vielfalt von Instrumenten und Akteuren sicherstellen.