EUROPÄISCHE
KOMMISSION

Straßburg, den 1.4.2025
COM(2025) 148 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN

ProtectEU – eine Europäische Strategie für die innere Sicherheit

1. ProtectEU – eine Europäische Strategie für die innere Sicherheit

Sicherheit ist der Grundstein, auf dem alle unsere Freiheiten aufbauen. Demokratie, Rechtsstaatlichkeit, Grundrechte, das Wohlergehen der Europäerinnen und Europäer, Wettbewerbsfähigkeit und Wohlstand – all dies hängt von unserer Fähigkeit ab, eine grundlegende Sicherheitsgarantie zu bieten. Im neuen Zeitalter der Sicherheitsbedrohungen, in dem wir uns gerade befinden, hängt die Fähigkeit der EU-Mitgliedstaaten, die Sicherheit ihrer Bürgerinnen und Bürger zu gewährleisten, mehr denn je von einem **einheitlichen europäischen Vorgehen zum Schutz unserer inneren Sicherheit** ab. In einer sich wandelnden geopolitischen Landschaft muss Europa weiterhin sein beständiges Versprechen von Frieden einlösen.

Die ersten Schritte zum Aufbau eines europäischen Sicherheitsapparats wurden bereits unternommen. In den letzten zehn Jahren haben wir die Union mit verbesserten kollektiven Mechanismen für Maßnahmen in den Bereichen Strafverfolgung und justizielle Zusammenarbeit, Grenzsicherheit, Bekämpfung der schweren und organisierten Kriminalität sowie von Terrorismus und gewaltorientiertem Extremismus und Schutz der physischen und digitalen kritischen Infrastrukturen der EU ausgestattet. Die ordnungsgemäße Umsetzung bereits verabschiedeter Rechtsvorschriften und erarbeiteter politischer Maßnahmen ist nach wie vor von entscheidender Bedeutung.

Angesichts der Art der heutigen Bedrohungen und der untrennbaren Verbindung zwischen der inneren und der äußeren Sicherheit der EU müssen wir noch weiter gehen.

Die Bedrohungslage ist ernst. Die Grenzen zwischen **hybriden Bedrohungen** und offener Kriegsführung verschwimmen. Russland führt eine hybride Online- und Offline-Kampagne gegen die EU und ihre Partner, um den gesellschaftlichen Zusammenhalt und demokratische Prozesse zu stören und zu untergraben und die Solidarität der EU mit der Ukraine auf die Probe zu stellen. Feindselige ausländische Staaten und staatlich unterstützte Akteure versuchen, unsere kritischen Infrastrukturen und Lieferketten zu infiltrieren und zu unterbrechen, sensible Daten zu stehlen und sich für größtmögliche Störungen in der Zukunft zu positionieren. Sie nutzen Straftaten wie Dienstleistungen und Kriminelle als Bevollmächtigte. Darüber hinaus macht uns unsere Abhängigkeit von Drittländern in Bezug auf Lieferketten anfälliger für hybride Kampagnen feindseliger Staaten.

Wie in der kürzlich von Europol vorgelegten Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität in der EU (EU Serious and Organised Crime Threat Assessment, SOCTA)[1] hervorgehoben, breiten sich mächtige **Netze der organisierten Kriminalität** in Europa aus, werden online gefördert und wirken sich auf unsere Wirtschaft und Gesellschaft aus. Hat die organisierte Kriminalität erst einmal in einer Gemeinschaft oder in einem Wirtschaftszweig Fuß gefasst, wird ihre Ausrottung zu einem harten Kampf: Ein Drittel der gefährlichsten kriminellen Netze ist seit mehr als zehn Jahren aktiv. Kryptowährungen und parallele Finanzsysteme helfen ihnen, ihre Erlöse aus Straftaten zu waschen und zu verbergen.

Die **terroristische Bedrohung in Europa ist weiterhin akut**. Regionale Krisen außerhalb der EU haben einen Dominoeffekt und bieten terroristischen Akteure aus dem gesamten ideologischen Spektrum neue Motivation, neue Mitglieder zu rekrutieren, zu mobilisieren oder ihre Kapazitäten auszubauen. Sie richten ihre Radikalisierungs- und Rekrutierungsbemühungen speziell auf die schwächsten Teile unserer Gesellschaft und insbesondere auf bestimmte junge

[1] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

Menschen aus. Sie motivieren Einzeltäter zu Anschlägen und fördern den Anstieg des systemfeindlichen Extremismus, dessen Ziel es ist, die demokratische Rechtsordnung zu stören.

Der rasante **technologische Fortschritt** liefert uns wichtige Werkzeuge zur Verbesserung unseres Sicherheitsapparats. Allerdings kommt es immer häufiger zu Cyberangriffen und Informationsmanipulation aus dem Ausland unter Einsatz neuer Technologien wie künstlicher Intelligenz (KI). Kinder, junge und ältere Menschen sind im Internet besonders gefährdet, und die Verbreitung von Hass im Internet gefährdet die Meinungsfreiheit und den sozialen Zusammenhalt.

Unser Leben ist weniger sicher geworden, was sich bei den Europäerinnen und Europäern zunehmend bemerkbar macht – ihre **Wahrnehmung von Sicherheit in der EU** ist so stark geschwächt, dass sich 64 % auf die Frage nach der Zukunft eher besorgt bezüglich der Sicherheit in der EU äußern[2]. Auch Unternehmen sind zunehmend betroffen; Fehlinformationen und Desinformation, Kriminalität und illegale Aktivitäten sowie Cyberspionage gehören zu den zehn größten Risiken, die im Global Risks Report (Bericht über weltweite Risiken) 2025 des Weltwirtschaftsforums[3] ermittelt wurden.

Europäerinnen und Europäer sollten **ihr Leben frei von Angst führen können**, sei es auf der Straße, zu Hause, an öffentlichen Orten, in der U-Bahn oder im Internet. Der Schutz der Menschen, insbesondere derjenigen, die am anfälligsten für Angriffe sind, die in der Regel in unverhältnismäßig hohem Maße Kinder, Frauen und Minderheiten einschließlich jüdischer und muslimischer Gemeinschaften betreffen, steht im Mittelpunkt der Sicherheitsarbeit der EU. Dies ist für den Aufbau widerstandsfähiger und von Zusammenhalt geprägter Gesellschaften von entscheidender Bedeutung.

Die Kommission ist im Begriff, eine **Europäische Strategie für die inneren Sicherheit** aufzustellen, um Bedrohungen in den kommenden Jahren besser begegnen zu können. Mit einem verschärften rechtlichen Instrumentarium, einer engeren Zusammenarbeit und einem verstärkten Informationsaustausch werden wir unsere Widerstandsfähigkeit und unsere kollektive Fähigkeit verbessern, Sicherheitsbedrohungen vorherzusehen, zu verhindern, zu erkennen und wirksam darauf zu reagieren. Ein einheitlicher Ansatz für die innere Sicherheit kann die Mitgliedstaaten dabei unterstützen, die Macht der Technologie zu nutzen, um die Sicherheit zu stärken – und nicht zu schwächen – und gleichzeitig einen sicheren digitalen Raum für alle zu fördern. Darüber hinaus wird durch solch einen einheitlichen Ansatz auch die einheitliche Reaktion der Mitgliedstaaten auf globale politische und wirtschaftliche Veränderungen, die sich auf die innere Sicherheit der Union auswirken, unterstützt.

Diese Strategie, die auf der Achtung der Rechtsstaatlichkeit und der Grundrechte beruht, ist an **drei Grundsätzen** ausgerichtet.

Erstens: Ziel ist eine Veränderung der Sicherheitskultur. Wir brauchen **einen gesamtgesellschaftlichen Ansatz** mit Einbeziehung aller Bürgerinnen und Bürger und Interessenträger, einschließlich Zivilgesellschaft, Forschung, Wissenschaft und privater Einrichtungen. Bei den im Rahmen der Strategie ergriffenen Maßnahmen wird somit nach Möglichkeit ein integrierter Multi-Stakeholder-Ansatz verfolgt.

Zweitens: **Die Sicherheitserwägungen müssen in alle Rechtsvorschriften, Strategien und Programme der EU**, einschließlich des auswärtigen Handelns der EU, **integriert und durchgängig darin berücksichtigt werden**. Rechtsvorschriften, Strategien und Programme müssen unter Berücksichtigung von Sicherheitsaspekten ausgearbeitet, überprüft und

[2] Flash Eurobarometer FL550: EU Challenges and Priorities (Flash-Eurobarometer-Umfrage 550 zu Herausforderungen und Prioritäten in der EU).
[3] https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf, S. 17.

umgesetzt werden, wobei sicherzustellen ist, dass die notwendigen Sicherheitserwägungen berücksichtigt werden, um ein kohärentes und umfassendes Sicherheitskonzept zu fördern.

Drittens: Ein sicheres, geschütztes und widerstandsfähiges Europa erfordert **erhebliche Investitionen seitens der EU, ihrer Mitgliedstaaten und des Privatsektors**. Die in dieser Strategie festgelegten Prioritäten und Maßnahmen erfordern ausreichende personelle und finanzielle Ressourcen, um ihre Umsetzung zu gewährleisten. Wie in der Mitteilung mit dem Titel „Der Weg zum nächsten Mehrjährigen Finanzrahmen“[4] dargelegt, wird Europa zur Stärkung seiner Autonomie die öffentlichen Ausgaben für Sicherheit erhöhen und die Forschung und Investitionen im Bereich Sicherheit fördern müssen.

Diese Strategie ergänzt die **Strategie der Union zur Krisenvorsorge**[5], in der ein integrierter gefahrenübergreifender Ansatz für die Vorsorge für Konflikte, vom Menschen verursachte Katastrophen bzw. Naturkatastrophen und Krisen dargelegt wird, sowie das **Gemeinsame Weißbuch zur europäischen Verteidigung – Bereitschaft 2030**[6], durch das die Entwicklung und der Erwerb von Verteidigungsfähigkeiten in der gesamten EU zur Abschreckung feindlicher ausländischer Akteure unterstützt werden sollen. Die Kommission wird zudem einen **Europäischen Schutzschild für die Demokratie** zur Stärkung der demokratischen Resilienz in der EU vorschlagen. Zusammen bilden diese Initiativen die Vision für eine sichere, geschützte und widerstandsfähige EU.

Eine neue europäische Governance im Bereich der inneren Sicherheit

Die Kommission wird eng mit den Mitgliedstaaten und den EU-Agenturen zusammenarbeiten, um das Konzept der EU für die innere Sicherheit sowohl auf strategischer als auch auf operativer Ebene zu verbessern.

Dies soll erreicht werden durch:

- **konsequente Ermittlung der potenziellen Auswirkungen neuer und überarbeiteter Initiativen der Kommission auf die Sicherheit und Vorsorge von Anfang an und während des gesamten Verhandlungsprozesses;**
- **regelmäßige Sitzungen der Projektgruppe der Kommission zur inneren Sicherheit in Europa, unterstützt durch sektorübergreifende strategische Zusammenarbeit innerhalb der Kommission;**
- **Präsentationen der Bedrohungsanalysen im Zusammenhang mit der inneren Sicherheit zur Unterstützung der Arbeit des Sicherheitskollegs;**
- **Gespräche mit den Mitgliedstaaten im Rat über die sich entwickelnden Herausforderungen im Bereich der inneren Sicherheit auf der Grundlage der Bedrohungsanalyse und des Austauschs über die wichtigsten politischen Prioritäten;**
- **regelmäßige Berichterstattung an das Europäische Parlament und den Rat zur Verfolgung und Unterstützung der systematischen Umsetzung wichtiger Sicherheitsinitiativen.**

2. Integrierte Lageerfassung und Bedrohungsanalyse

Wir werden die EU mit neuen Möglichkeiten zum Austausch und zur Zusammenführung von Informationen ausstatten und eine regelmäßige Analyse der Bedrohungslage in Bezug auf die

[4] COM (2025) 46 final.
[5] JOIN(2025) 130 final.
[6] JOIN(2025) 120 final.

innere Sicherheit in der EU vorlegen, die zu einer umfassenden Risiko- und Bedrohungsanalyse beiträgt.

Sicherheit beginnt mit **wirksamer Antizipation**. Die EU muss sich auf eine umfassende, ausreichend autonome und aktuelle Lageerfassung und Bedrohungsanalyse stützen. Verwertbare nachrichtendienstliche Erkenntnisse, die die Mitgliedstaaten durch das Einheitliche Analyseverfahren (Single Intelligence Analysis Capacity, SIAC) als zentrale Stelle für die Zusammenführung dieser Erkenntnisse der Mitgliedstaaten weiter verbessern sollten, sind für die Bewertung und Abwehr von Bedrohungen von entscheidender Bedeutung und dienen als Grundlage für politische und gesetzgeberische Maßnahmen[7]. Wir müssen auf EU-Ebene wirksamer und kooperativer auf **nachrichtendienstliche Analysen** und **Gefahrenabschätzungen** zurückgreifen.

Aufbauend auf den verschiedenen Risiko- und Gefahrenabschätzungen, die auf EU-Ebene und für bestimmte Sektoren vorgenommen werden[8], wird die Kommission **regelmäßige Analysen der Bedrohungslage in Bezug auf die innere Sicherheit in der EU** erstellen, um die wichtigsten sicherheitsbezogenen Herausforderungen zu ermitteln und daraus politische Prioritäten abzuleiten. Diese sollen dazu beitragen, eine flexible und reaktionsschnelle Politik der inneren Sicherheit zu entwickeln, die den sich wandelnden Bedrohungen erfolgreich entgegenwirkt, Menschen und Unternehmen besser vor Angriffen schützt und gezielte politische Maßnahmen zeitnah ermöglicht. Diese Analysen der Bedrohungslage in Bezug auf die innere Sicherheit in der EU sollen auch zu der **umfassenden (sektorübergreifenden, alle Gefahren umfassenden) Risiko- und Gefahrenabschätzung für die EU** beitragen, die von der Kommission und der Hohen Vertreterin – wie in der Strategie der Union zur Krisenvorsorge dargelegt – vorgenommen wird.

Vertrauen und eine sichere Handhabung sind für den Informationsaustausch unerlässlich, und dies erfordert eine zuverlässige und sichere Infrastruktur. Die Organe, Einrichtungen und sonstigen Stellen der EU müssen sicherstellen, dass sie in der Lage sind, **sichere Kommunikationskanäle** für den Austausch sensibler Informationen und Verschlusssachen untereinander und mit den Mitgliedstaaten zu nutzen. Investitionen in **interoperable sichere Systeme** und zuverlässige Technologien werden die Autonomie der EU stärken und die Fähigkeit der EU verbessern, Krisen zu bewältigen und operationale Resilienz zu gewährleisten. In diesem Zusammenhang fordert die Kommission die beiden gesetzgebenden Organe nachdrücklich auf, die Verhandlungen über die **vorgeschlagene Verordnung über die Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der Union** abzuschließen, insbesondere um einen gemeinsamen Rahmen für den Umgang mit nicht als Verschlusssache eingestuften sensiblen Informationen und Verschlusssachen sicherzustellen[9].

Um ihre eigene operative Sicherheit und Lageerfassung zu gewährleisten, wird die Kommission ihren Rahmen für die Governance im Bereich der institutionellen Sicherheit überarbeiten und ein **Integriertes Sicherheitseinsatzzentrum (Integrated Security Operations Centre, ISOC)** einrichten, um Menschen, materielle Vermögenswerte und Operationen an allen

[7] Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness, S. 23.
[8] Zu den sektorspezifischen Gefahrenabschätzungen, die in diese Bedrohungsanalyse einfließen sollen, gehören die SOCTA, der Tendenz- und Lagebericht über den Terrorismus in der EU (EU Terrorism Situation & Trend Report, TE-SAT), der Gemeinsame Cyberbewertungsbericht (Joint Cyber Assessment Report, JCAR) sowie künftige Bewertungen der Bedrohungen, Risiken und Methoden der Geldwäsche und der Terrorismusfinanzierung, die von der Kommission und der Behörde zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung durchgeführt werden.
[9] COM(2022) 119 final.

Standorten der Kommission zu schützen. Die Kommission wird auch ihre operativen und analytischen Kapazitäten zur Ermittlung und Eindämmung hybrider Bedrohungen ausbauen.

Im Einklang mit der Strategie der Union zur Krisenvorsorge werden Vorsorge- und Sicherheitserwägungen in die Rechtsvorschriften, Strategien und Programme der EU einbezogen und durchgängig darin berücksichtigt. Bei der Ausarbeitung oder Überprüfung von Rechtsvorschriften, Strategien oder Programmen unter Berücksichtigung von Vorsorge- und Sicherheitsaspekten wird die Kommission konsequent die potenziellen Auswirkungen der bevorzugten politischen Option auf Vorsorge und Sicherheit ermitteln. Zu diesem Zweck werden politische Entscheidungsträger in der Kommission regelmäßig geschult.

Zur Unterstützung der Mitgliedstaaten wird die Kommission die sich entwickelnden Herausforderungen im Bereich der inneren Sicherheit und die wichtigsten politischen Prioritäten mit dem Rat erörtern und ihn regelmäßig über den neusten Stand bei der Umsetzung der Strategie in Kenntnis setzen. Darüber hinaus wird die Kommission das Europäische Parlament und die einschlägigen Interessenträger auf dem Laufenden halten und sie an allen einschlägigen Maßnahmen beteiligen.

Zentrale Maßnahmen

Die Kommission wird

- **regelmäßige Bedrohungsanalysen für Herausforderungen in Bezug auf die innere Sicherheit in der EU erstellen und vorlegen.**

Die Mitgliedstaaten werden nachdrücklich aufgefordert,

- **den Austausch nachrichtendienstlicher Erkenntnisse mit dem SIAC zu verbessern und für einen besseren Informationsaustausch mit den Agenturen und Einrichtungen der EU zu sorgen.**

Das Europäische Parlament und der Rat werden aufgefordert,

- **die Verhandlungen über die vorgeschlagene Verordnung über die Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der Union abzuschließen.**

3. Verstärkte Sicherheitskapazitäten der EU

Wir werden neue Instrumente für die Strafverfolgung entwickeln, beispielsweise ein umgestaltetes Europol, sowie bessere Mittel zur Koordinierung und Gewährleistung eines sicheren Datenaustauschs und eines rechtmäßigen Zugangs zu Daten bereitstellen.

Um sich wandelnde Bedrohungen wirksam zu bewältigen, muss die EU ihre Sicherheitskapazitäten ausbauen und Innovationen fördern. Als Hauptakteure im Kampf gegen Bedrohungen der inneren Sicherheit benötigen Strafverfolgungs- und Justizbehörden die richtigen operativen Instrumente und Fähigkeiten, um rasch und wirksam handeln zu können. Es ist wichtig, dass diese Behörden in der Lage sind, grenzüberschreitend und diensteübergreifend zu kommunizieren und zu koordinieren, um eine wirksame Prävention, Aufdeckung, Ermittlung und strafrechtliche Verfolgung zu gewährleisten.

Agenturen und Einrichtungen der EU für innere Sicherheit

Die Agenturen und Einrichtungen der EU in den Bereichen Justiz, Inneres und Cybersicherheit spielen eine Schlüsselrolle in der Sicherheitsarchitektur der EU – eine Rolle, die mit der Ausweitung ihrer Zuständigkeiten weiter wächst.

Europol ist heute – 25 Jahre nach seiner Gründung – wichtiger denn je für den EU-Sicherheitsrahmen. Es unterstützt komplexe grenzüberschreitende Ermittlungen, erleichtert den Informationsaustausch, entwickelt innovative Instrumente für die Polizeiarbeit und bietet fortgeschrittenes Fachwissen für die Strafverfolgung. Mehrere Faktoren hindern Europol jedoch daran, sein operatives Potenzial zur Unterstützung von Ermittlungstätigkeiten und operativen Tätigkeiten zur Bekämpfung der grenzüberschreitenden Kriminalität voll auszuschöpfen: Sie reichen von unzureichenden Ressourcen bis hin zu dem Umstand, dass das derzeitige Mandat von Europol neue Sicherheitsbedrohungen wie Sabotage, hybride Bedrohungen oder Informationsmanipulation nicht abdeckt. Aus diesem Grund wird die Kommission **eine ehrgeizige Überarbeitung des Mandats von Europol** vorschlagen, um Europol zu einer wirklich operativen Polizeiagentur zu machen, die die Mitgliedstaaten besser unterstützt. Ziel ist es, das technologische Fachwissen und die Kapazitäten von Europol zur Unterstützung der nationalen Strafverfolgungsbehörden zu stärken, die Koordinierung mit anderen Agenturen und Einrichtungen sowie mit den Mitgliedstaaten zu verbessern, strategische Partnerschaften mit Partnerländern und dem Privatsektor zu intensivieren und eine verstärkte Aufsicht über Europol sicherzustellen.

Darüber hinaus wird die Kommission darauf hinarbeiten, **die Wirksamkeit und Komplementarität der EU-Agenturen und -Einrichtungen für die innere Sicherheit weiter zu verbessern und die nahtlose Zusammenarbeit** zwischen ihnen **zu stärken**.

Das Mandat der **Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust)** wird im Hinblick auf eine wirksamere justizielle Zusammenarbeit überprüft und gestärkt, wobei die Komplementarität und Zusammenarbeit mit Europol verbessert werden. Dazu gehört auch die Verbesserung der Effizienz von Eurojust sowie ihrer Fähigkeit, proaktiv Unterstützung und Analysen für die Justizbehörden der Mitgliedstaaten bereitzustellen. Darüber hinaus wird die Kommission angesichts der einzigartigen Zuständigkeit der **Europäischen Staatsanwaltschaft (EUStA)** für die Ermittlung und Verfolgung von Straftaten zum Nachteil der finanziellen Interessen der Union prüfen, wie die Fähigkeit der EUStA zum Schutz der Unionsmittel am besten gestärkt werden kann. Dazu gehört auch die Stärkung der Zusammenarbeit zwischen der EUStA und Europol.

Ein effizienter und sicherer Informationsaustausch zwischen den Agenturen ist für die Zusammenarbeit von entscheidender Bedeutung. Europol und die Europäische Agentur für die Grenz- und Küstenwache (Frontex) müssen gemäß der gemeinsamen Erklärung vom Januar 2024 rasch Informationen austauschen, auch zu operativen Zwecken[10]. Die **Agentur der Europäischen Union für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA)** spielt eine zentrale Rolle bei der Gewährleistung der sicheren Speicherung und Verfügbarkeit von Daten für eine bessere Koordinierung und einen effizienteren Informationsaustausch zwischen den Agenturen. Die **Agentur der Europäischen Union für Grundrechte** stellt Fachwissen zum Schutz der Grundrechte bei der Entwicklung und Umsetzung von Sicherheitsstrategien zur bereit.

Die **EU-Behörde zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung (Anti-Money Laundering Authority, AMLA)** wurde ermächtigt, Informationen nach dem Treffer/Kein-Treffer-Verfahren mit Informationen abzugleichen, die von Europol, der EUStA, von Eurojust und vom Europäischen Amt für Betrugsbekämpfung (OLAF) zur Verfügung gestellt werden, um gemeinsame Analysen grenzüberschreitender Fälle durchzuführen.

[10] https://www.europol.europa.eu/cms/sites/default/files/documents/europol-frontex_joint_statement_signed_31.1.2024.pdf.

Die **Agentur der Europäischen Union für Cybersicherheit (ENISA)** spielt eine zentrale Rolle bei der Umsetzung der europäischen Rechtsvorschriften zur Cybersicherheit. Bei der anstehenden **Überarbeitung des Rechtsakts zur Cybersicherheit** wird die Kommission das Mandat der ENISA prüfen und eine Modernisierung vorschlagen, um den EU-Mehrwert dieser Agentur zu stärken.

Die Zusammenarbeit zwischen den Zollbehörden und anderen Strafverfolgungsbehörden wird durch die vorgeschlagene Einrichtung der **EU-Zollbehörde** und der **EU-Zolldatenplattform** im Rahmen des EU-Zollreformpakets verstärkt. Informationen aus der künftigen Plattform und damit zusammenhängende Daten von Europol, Eurojust, der EUStA, dem OLAF, der AMLA und Frontex werden im Rahmen der jeweiligen Zuständigkeiten die gemeinsame Analyse verbessern und zu kohärenteren operativen Tätigkeiten, insbesondere an den Außengrenzen, beitragen. Die Kommission fordert die beiden gesetzgebenden Organe auf, die Verhandlungen über die EU-Zollreform rasch abzuschließen, und wird sie dabei weiterhin unterstützen.

Die Verbesserung der Komplementarität zwischen der EUStA, dem OLAF, Europol, Eurojust, der AMLA und der vorgeschlagenen EU-Zollbehörde wird auch auf den Ergebnissen der laufenden Überprüfung der **Betrugsbekämpfungsarchitektur der EU** aufbauen. Die innere Sicherheit kann von diesem ganzheitlichen Ansatz profitieren, bei dem der Schwerpunkt auf einer besseren Nutzung sowohl strafrechtlicher als auch administrativer Mittel, der Interoperabilität der IT-Systeme und der verbesserten Zusammenarbeit liegt.

Kritische Kommunikation

Heutzutage werden **kritische Kommunikationssysteme**[11] in den meisten Fällen isoliert auf nationaler Ebene betrieben. Dies bedeutet, dass Ersthelfer beim Grenzübertritt in andere Mitgliedstaaten häufig nicht mit ihren Kollegen kommunizieren können. In einigen Mitgliedstaaten bestehen zudem Beschränkungen hinsichtlich der Kommunikation zwischen verschiedenen Arten von Ersthelfern (z. B. Polizei und Sanitätern). Die Standards der meisten Systeme entsprechen nicht den derzeitigen Anforderungen in Bezug auf Funktionalität und Resilienz, wodurch die Reaktionsfähigkeit der Ersthelfer, insbesondere über Grenzen hinweg, erheblich eingeschränkt wird.

Um die Reaktionsfähigkeit der EU auf Krisen zu verbessern, wird die Kommission Rechtsvorschriften zur Schaffung eines **Europäischen Systems für kritische Kommunikation (European Critical Communication System, EUCCS)** vorschlagen, um die kritischen Kommunikationssysteme der nächsten Generation in der EU miteinander zu verknüpfen. Das EUCCS soll sich auf drei strategische Säulen stützen: operative Mobilität, ausgeprägte Resilienz und strategische Autonomie. Die EUCCS-Initiative, in deren Rahmen harmonisierte Anforderungen festgelegt werden sollen, soll dazu beitragen, die kritischen Kommunikationssysteme der Mitgliedstaaten zu modernisieren, damit sie nahtlos funktionieren können. Außerdem soll die Systemabdeckung durch das künftige multiorbitale System IRIS[212] ausgeweitet werden. Durch EU-finanzierte Projekte sollen die technischen Kapazitäten für das EUCCS aufgebaut werden, wobei in erster Linie auf europäische Technologieanbieter zurückgegriffen wird, um die strategische Autonomie der EU in diesem sensiblen Sektor zu fördern.

[11] Dies trifft auf die Netze zu, die von Strafverfolgungsbehörden, Grenzschutzbeamten, Zollbehörden, Katastrophenschutzbehörden, Feuerwehrleuten, Sanitätern und anderen wichtigen Akteuren im Bereich der öffentlichen Sicherheit genutzt werden.

[12] EU-Infrastruktur für Resilienz, Interkonnektivität und Sicherheit durch Satelliten (EU Infrastructure for Resilience, Interconnectivity and Security by Satellite).

Rechtmäßiger Zugang zu Daten

Strafverfolgungsbehörden und Justizbehörden müssen in der Lage sein, Straftaten zu untersuchen und dagegen vorzugehen. Heute haben fast alle Formen der schweren und organisierten Kriminalität einen digitalen Fußabdruck[13]. Etwa 85 % der strafrechtlichen Ermittlungen hängen nunmehr von der Fähigkeit der Strafverfolgungsbehörden ab, auf digitale Informationen zuzugreifen[14].

Die **hochrangige Gruppe für den Zugang zu Daten für eine wirksame Strafverfolgung** hob in ihrem abschließenden Bericht[15] hervor, dass die Strafverfolgungs- und Justizbehörden in den letzten zehn Jahren gegenüber Kriminellen an Boden verloren haben, da sich Kriminelle Instrumente und Produkte zunutze machen, die in anderen Rechtsordnungen von Anbietern bereitgestellt werden, die Maßnahmen ergriffen haben, wodurch ihnen die Möglichkeit genommen wird, bei rechtmäßigen Ersuchen in Einzelfällen zusammenzuarbeiten. Die systematische Zusammenarbeit zwischen Strafverfolgungsbehörden und privaten Parteien, einschließlich Diensteanbietern, ist daher für künftige Bemühungen zur Zerschlagung der gefährlichsten kriminellen Netze und Einzelpersonen in der Union und darüber hinaus von entscheidender Bedeutung.

Da die Digitalisierung immer weiter um sich greift und Kriminellen eine ständig wachsende Zahl neuer Instrumente bietet, ist ein Rahmen für den Zugang zu Daten, der den Erfordernissen der Durchsetzung unserer Gesetze und des Schutzes unserer Werte entspricht, unerlässlich. Gleichzeitig ist es für die Wahrung der Cybersicherheit und den Schutz vor neu auftretenden Sicherheitsbedrohungen ebenso wichtig sicherzustellen, dass digitale Systeme vor unbefugtem Zugriff geschützt sind. Bei solchen Zugangsrahmen müssen auch die Grundrechte gewahrt werden und es muss mitunter für einen angemessenen Schutz der Privatsphäre und der personenbezogenen Daten gesorgt werden.

In den letzten Jahren hat die EU Maßnahmen **zur Bekämpfung der Online-Kriminalität sowie zur Erleichterung des Zugangs zu digitalen Beweismitteln für alle Straftaten** ergriffen; dazu wurden Vorschriften für elektronische Beweismittel angenommen, die im August 2026 vollständig in Kraft treten[16]. Diese werden durch internationale Instrumente für den Austausch von Informationen und Beweismitteln ergänzt. Die Kommission wird in Kürze die Unterzeichnung und den Abschluss des neuen **Übereinkommens der Vereinten Nationen über Cyberkriminalität** vorschlagen.

Um den Empfehlungen der hochrangigen Gruppe[17] nachzukommen, wird die Kommission im ersten Halbjahr 2025 einen **Fahrplan** vorlegen, **in dem die** von ihr vorgeschlagenen **rechtlichen und praktischen Maßnahmen zur Gewährleistung eines rechtmäßigen und wirksamen Zugangs zu Daten dargelegt werden**. Im Rahmen der Folgemaßnahmen zu diesem Fahrplan wird die Kommission einer Bewertung der Auswirkungen der **Vorschriften über die Vorratsdatenspeicherung** auf EU-Ebene und der Ausarbeitung eines

[13] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.
[14] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52019PC0070.
[15] Concluding report of the High-Level Group on access to data for effective law enforcement, 15.11.2024, abrufbar unter https://home-affairs.ec.europa.eu/document/download/4802e306-c364-4154-835b-e986a9a49281_en?filename=Concluding%20Report%20of%20the%20HLG%20on%20access%20to%20data%20for%20effective%20law%20enforcement_en.pdf.
[16] Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren (ABl. L 191 vom 28.7.2023, S. 118).
[17] Schlussfolgerungen des Rates zum Zugang zu Daten für eine wirksame Strafverfolgung (12. Dezember 2024), abrufbar unter https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/de/pdf.

Technologiefahrplans für Verschlüsselung Vorrang einräumen, um technologische Lösungen zu ermitteln und zu bewerten, die es den Strafverfolgungsbehörden ermöglichen, auf rechtmäßige Weise und unter Wahrung der Cybersicherheit und der Grundrechte auf verschlüsselte Daten zuzugreifen.

Operative Zusammenarbeit

Die Kommission wird mit den Mitgliedstaaten, den Agenturen und Einrichtungen der EU sowie Partnerländern zusammenarbeiten, um die operative Zusammenarbeit zu stärken, die für einen wirksameren Ansatz zur Bekämpfung der grenzüberschreitenden organisierten Kriminalität und des Terrorismus von wesentlicher Bedeutung ist.

Als wichtigster EU-Rahmen für gemeinsame Maßnahmen zur Bekämpfung der schweren und organisierten Kriminalität hat die **Europäische multidisziplinäre Plattform gegen kriminelle Bedrohungen (European Multidisciplinary Platform Against Criminal Threats, EMPACT)** beachtliche operative Ergebnisse erzielt. Der nächste EMPACT-Zyklus 2026-2029 bietet die Gelegenheit, diesen Rahmen noch weiter zu stärken. Um die gefährlichsten kriminellen Netze zu zerschlagen und kriminelle Einzelpersonen an ihrem Tun zu hindern, muss die Union ihr Vorgehen straffen und den Fokus auf die dringendsten Prioritäten legen, wobei die Mitgliedstaaten stärker in die Pflicht genommen werden müssen und eine wirksame Nutzung der Ressourcen sicherzustellen ist.

Zu diesem Zweck wird die Kommission mit den Ratsvorsitzen und den Mitgliedstaaten zusammenarbeiten, um **das Potenzial von EMPACT zu maximieren und die wichtigsten Prioritäten für den nächsten EMPACT-Zyklus 2026-2029 anzugehen**. In diesen prioritären Bereichen besteht Bedarf an nachrichtendienstlichen Erkenntnissen über die gefährlichsten kriminellen Netze, an gemeinsamen Ermittlungen und operativen Taskforces sowie einer entschlossenen justiziellen Reaktion, einschließlich des Grundsatzes „Follow the money". Darüber hinaus muss die Union gegen die kriminelle Rekrutierung und Infiltration vorgehen und die behördenübergreifende und internationale Zusammenarbeit und Ausbildung im Bereich der Strafverfolgung stärken.

Die Kommission wird auch andere Formen der **grenzüberschreitenden operativen Zusammenarbeit im Bereich der Strafverfolgung zwischen den Mitgliedstaaten und assoziierten Schengen-Ländern** unterstützen. Der Schengen-Raum, in dem es keine Kontrollen an den Binnengrenzen gibt, erfordert eine enge Zusammenarbeit und einen Informationsaustausch zwischen den Strafverfolgungsbehörden der Mitgliedstaaten, um ein hohes Maß an innerer Sicherheit zu gewährleisten. Auch heute stehen Strafverfolgungsbeamte bei der Überwachung oder Durchführung dringender grenzüberschreitender Maßnahmen nach wie vor vor Herausforderungen[18], und auch die Abwehr hybrider Bedrohungen erfordert auch eine verstärkte grenzüberschreitende Zusammenarbeit. Es sollte eine **hochrangige Gruppe zur Zukunft der operativen Zusammenarbeit im Bereich der Strafverfolgung** eingerichtet werden, um eine gemeinsame strategische Vision zu entwickeln.

Ein effizienter Datenaustausch zwischen den Strafverfolgungsbehörden ist auch für eine wirksame grenzüberschreitende Zusammenarbeit wesentlich. Sobald die **Interoperabilitätsarchitektur** eingerichtet ist, wird sie Strafverfolgungsbehörden und Europol einen effektiven Zugang zu wichtigen Informationen ermöglichen. Gleichzeitig sollten die EU und ihre Mitgliedstaaten dem bilateralen und multilateralen Informationsaustausch durch die

[18] Siehe Arbeitsunterlage der Kommissionsdienststellen „Assessment of the effect given by the Member States to Council Recommendation (EU) 2022/915 of 9 June 2022 on operational law enforcement cooperation (5909/25)".

rechtliche und technische Umsetzung der **Prüm-II-Verordnung**[19] in Zusammenarbeit mit eu-LISA und Europol Vorrang einräumen. Dies wird einen sicheren automatisierten Austausch von Fingerabdrücken, DNA-Profilen, Fahrzeugzulassungsdaten, Gesichtsbildern und Polizeiakten über EU-Router ermöglichen. Auf nationaler Ebene müssen die Mitgliedstaaten die **Richtlinie über den Informationsaustausch**[20] umsetzen, um die Kanäle für den Informationsaustausch für einen nahtlosen grenzüberschreitenden Informationsfluss zu verbessern und gleichzeitig ihre Integration mit Systemen auf Unionsebene wie der SIENA[21] sicherzustellen.

Eine wirksame grenzüberschreitende Zusammenarbeit setzt auch die Förderung einer **gemeinsamen EU-Strafverfolgungskultur** voraus. Gemeinsame Schulungen, Kompetenzzentren und Mobilitätsprogramme sind für die Erreichung dieses Ziels von entscheidender Bedeutung. Die Kommission wird prüfen, wie die EU Schulungen für die Behörden der Mitgliedstaaten am besten unterstützen kann, wobei sie auf die **Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (CEPOL)** zurückgreift.

Verstärkte Sicherheit an den Grenzen

Die Stärkung der Widerstandsfähigkeit und Sicherheit der Außengrenzen ist von entscheidender Bedeutung, wenn es darum geht, hybriden Bedrohungen wie dem Einsatz von Migration als Waffe entgegenzuwirken, das Eindringen bedrohlicher Akteure und die Einfuhr bedrohlicher Waren in die EU zu verhindern und grenzüberschreitende Kriminalität und Terrorismus wirksam zu bekämpfen. **Das Schengener Informationssystem (SIS) soll** 2026 dahingehend **erweitert werden**, dass die Mitgliedstaaten Ausschreibungen über an Terrorismus beteiligte Drittstaatsangehörige, einschließlich ausländischer terroristischer Kämpfer, und über Drittstaatsangehörige, die an anderen schweren Straftaten beteiligt sind, auf der Grundlage von Daten eingeben können, die von Drittstaaten an Europol weitergegeben werden.

Durch die verbesserte **Interoperabilität** der großen EU-Informationssysteme erhalten die Mitgliedstaaten wesentliche Informationen über Personen aus Drittstaaten, die Außengrenzen überschreiten oder überschreiten wollen, was den Behörden dabei hilft, die Voraussetzungen für die Genehmigung der Einreise in das Hoheitsgebiet der Mitgliedstaaten zu bewerten[22]. Die Kommission wird weiterhin eng mit den Mitgliedstaaten und eu-LISA zusammenarbeiten, um diese Systeme, insbesondere das **Einreise-/Ausreisesystem (Entry/Exit System, EES), das Europäisches Reiseinformations- und -genehmigungssystem (European Travel Information and Authorisation System, ETIAS) und das überarbeitete Visa-**

[19] Verordnung (EU) 2024/982 des Europäischen Parlaments und des Rates vom 13. März 2024 über die automatisierte Abfrage und den Austausch von Daten für die polizeiliche Zusammenarbeit und zur Änderung der Beschlüsse 2008/615/JI und 2008/616/JI des Rates sowie der Verordnungen (EU) 2018/1726, (EU) 2019/817 und (EU) 2019/818 des Europäischen Parlaments und des Rates (Prüm-II-Verordnung) (ABl. L. 2024/982 vom 5.4.2024).

[20] Richtlinie (EU) 2023/977 des Europäischen Parlaments und des Rates vom 10. Mai 2023 über den Informationsaustausch zwischen den Strafverfolgungsbehörden der Mitgliedstaaten und zur Aufhebung des Rahmenbeschlusses 2006/960/JI des Rates (ABl. L 134 vom 22.5.2023, S. 1).

[21] Netzanwendung für den sicheren Datenaustausch (Secure Information Exchange Network Application).

[22] Insbesondere wird das EES es den Mitgliedstaaten ermöglichen, Drittstaatsangehörige an den Außengrenzen des Schengen-Raums zu identifizieren und ihre Ein- und Ausreisen zu erfassen, was eine systematische Identifizierung von Aufenthaltsüberziehern ermöglicht. Vor der Ankunft eines Drittstaatsangehörigen an den Außengrenzen können die Mitgliedstaaten anhand des ETIAS und des VIS vorab prüfen, ob die Anwesenheit eines Drittstaatsangehörigen im Gebiet der EU ein Sicherheitsrisiko darstellt.

Informationssystem (VIS), rasch umzusetzen und ihren reibungslosen Betrieb und ihre Sicherheitsvorteile zu gewährleisten.

Um die Grenzsicherheit weiter zu verbessern und die Zusammenarbeit in der EU angesichts sich wandelnder Bedrohungen zu stärken, **wird die Kommission eine Stärkung von Frontex vorschlagen**. Die Personalausstattung von Frontex sollte im Laufe der Zeit auf 30 000 erhöht werden. Die Agentur sollte mit fortschrittlichen Technologien für die Überwachung und Lageerfassung ausgestattet werden, einschließlich nachrichtendienstlicher Erkenntnisse, die für die integrierte europäische Grenzverwaltung relevant sind, und Zugang zu robusten staatlichen Erdbeobachtungsdiensten der EU für die Grenzkontrolle erhalten, die bis 2027 eingeführt werden sollen. Dies sollte die Fähigkeit zur Aufdeckung, Verhütung und Bekämpfung grenzüberschreitender Kriminalität an den Außengrenzen weiter verbessern und die Unterstützung der Mitgliedstaaten bei der Durchführung von Rückführungen verstärken, insbesondere in Bezug auf Drittstaatsangehörige, die ein Sicherheitsrisiko darstellen.

Dokumenten- und Identitätsbetrug fördert die Schleuserkriminalität, den Menschenhandel, kriminelle Bewegungen im Verborgenen sowie den illegalen Warenhandel. Sobald der **Detektor für Mehrfachidentitäten (multiple-identity detector, MID)**[23] einsatzbereit ist, wird er die Fähigkeit der nationalen Behörden verbessern, Personen mit Mehrfachidentitäten zu ermitteln und Identitätsbetrug zu bekämpfen. Die Kommission wird sondieren, wie die Sicherheit von Reise- und Aufenthaltsdokumenten, die EU-Bürgerinnen und -Bürgern und Drittstaatsangehörigen ausgestellt werden, verbessert werden kann. Ferner wird die Kommission prüfen, wie die europäische Brieftasche für die Digitale Identität, die bis Ende 2026 im Zuge des europäischen Rahmens für eine digitale Identität eingeführt werden soll, dazu beitragen kann, die Sicherheit von Reisedokumenten zu erhöhen und die Identitätsüberprüfung zu verbessern. Dies wird die Vorschläge zum digitalen Reiseausweis und zur digitalen EU-Reise-App[24] ergänzen.

Reiseinformationen sind für die Behörden von entscheidender Bedeutung, um Bewegungen von Kriminellen, Terroristen und anderen Personen, von denen eine Sicherheitsbedrohung ausgeht, zu erkennen und zu untersuchen. Zwar gibt es einen EU-Rahmen für Informationen im Bereich des gewerblichen Luftverkehrs[25], die Verarbeitung von Daten anderer Verkehrsträger zu Strafverfolgungszwecken ist jedoch fragmentiert. Somit können Kriminelle und Terroristen verschiedene Verkehrsträger für illegale Aktivitäten nutzen, ohne entdeckt zu werden. Die Kommission wird mit den Mitgliedstaaten und dem Verkehrssektor zusammenarbeiten, um **den Rahmen für Reiseinformationen zu stärken**; dazu wird eine Unionsregelung geprüft, mit der Betreiber von Privatflügen zur Erhebung und Übermittlung von Fluggastdatensätzen verpflichtet werden, und es werden die Vorschriften für die Verarbeitung von Fluggastdatensätzen bewertet und Möglichkeiten zur Straffung der Verarbeitung von Informationen im Seeverkehr sondiert. Für den Straßenverkehr wird die Kommission eine erweiterte Nutzung von Systemen zur **automatischen Nummernschildererkennung** prüfen und die Möglichkeiten für Synergien mit dem SIS erhöhen.

[23] Der MID ist eine der Interoperabilitätskomponenten, die durch die Verordnung (EU) 2019/818 und die Verordnung (EU) 2019/817 eingeführt wurden.
[24] https://ec.europa.eu/commission/presscorner/detail/de/ip_24_5047.
[25] Fluggastdatensätze (passenger name record, PNR) und vorab übermittelte Fluggastdaten (advance passenger information, API) gemäß der Richtlinie (EU) 2016/681 („PNR-Richtlinie“) und der Verordnungen (EU) 2025/12 und (EU) 2025/13 („API-Verordnungen“).

Vorausschau, Innovation und auf Fähigkeiten ausgerichteter Ansatz

Die Kommission wird **einen umfassenden vorausschauenden Ansatz für die innere Sicherheit auf EU-Ebene** entwickeln, der sich auf die auf nationaler Ebene ermittelten bewährten Verfahren stützt. Dieser Ansatz wird die Politikgestaltung unterstützen und Investitionen in einschlägige EU-finanzierte Sicherheitsforschung und -innovation lenken.

Durch die Schaffung von Lösungen zur Bekämpfung neu auftretender Bedrohungen, auch durch den Missbrauch von Technologie[26], **spielen Forschung und Innovation eine entscheidende Rolle in Bezug auf die innere Sicherheit**. Die EU muss weiterhin über EU-finanzierte Sicherheitsforschung und -innovation[27] in die Entwicklung innovativer Instrumente und Lösungen investieren, um Sicherheitsbedrohungen unter Einhaltung der EU-Vorschriften und der Grundrechte zu begegnen. Die Kommission sollte den Übergang von der Forschung zur Einführung unterstützen, um die wirksame Nutzung dieser modernen Fähigkeiten sicherzustellen, wobei der Schwerpunkt auf **modernen Technologien** wie künstlicher Intelligenz liegen sollte. Dieser Ansatz sollte Schulungen zur Verbesserung der Nutzung von KI-Systemen und anderen technischen Kapazitäten durch Strafverfolgungs- und Justizbehörden umfassen. Darüber hinaus sollte gegebenenfalls das Potenzial von Technologien mit doppeltem Verwendungszweck in beide Richtungen (von zivil zu militärisch und von militärisch zu zivil) genutzt werden[28].

Das **europäisches Innovationszentrum für innere Sicherheit**[29], ein Netz von Innovationslaboren, die die neuesten innovativen Neuerungen und wirksamen Lösungen zur Unterstützung der Arbeit der Akteure der inneren Sicherheit in der EU und den Mitgliedstaaten bereitstellen, wird dazu beitragen, die Forschung in die Praxis und die Politik zu integrieren. Um die Wirksamkeit von Europol zu verbessern, muss das Instrumentenarchiv von Europol gestärkt werden, damit fortschrittliche Technologien ermittelt, entwickelt, gemeinsam beschafft und operativ angewendet werden können. Darüber hinaus wird die Kommission in ihrer Gemeinsamen Forschungsstelle einen **Campus für Sicherheitsforschung und -innovation** einrichten, in dem Forscher zusammenkommen, um den Zyklus von Forschungsergebnissen zu Innovation, Entwicklung und erfolgreicher Umsetzung zu verkürzen und gleichzeitig die Kosten für Entwicklung, Erprobung und Validierung zu senken.

Unser **Europäischer Forschungsraum** ist auf Kooperation ausgerichtet und daher anfällig für Einflussnahme aus dem Ausland und Desinformation. Nach der Annahme der Empfehlung des Rates zur Forschungssicherheit[30] ergreifen die Kommission und die Mitgliedstaaten Maßnahmen zur Stärkung der einschlägigen Akteure, unter anderem durch die Einrichtung eines Kompetenzzentrums für Forschungssicherheit.

Zentrale Maßnahmen

Die Kommission wird im Jahr 2026 Folgendes annehmen:

- **einen Legislativvorschlag zur Umwandlung von Europol in eine wirklich operative Strafverfolgungsbehörde;**
- **einen Legislativvorschlag zur Stärkung von Eurojust;**

[26] Siehe den Bericht der Gemeinsamen Forschungsstelle der Europäischen Kommission mit dem Titel „Emerging risks and opportunities for EU internal security stemming from new technologies", abrufbar unter https://publications.jrc.ec.europa.eu/repository/handle/JRC139674.
[27] Study on strengthening EU-funded security research and innovation – 20 years of EU-Funded Civil Security Research and Innovation – 2025, abrufbar unter https://data.europa.eu/doi/10.2837/0004501.
[28] Wie im Niinistö-Bericht dargelegt.
[29] EU Innovation Hub for Internal Security | Europol.
[30] ABl. C/2024/3510, 30.5.2024.

- **einen Legislativvorschlag zur Stärkung der Rolle und der Aufgaben von Frontex;**
- **einen Legislativvorschlag zur Einrichtung eines Europäischen Systems für kritische Kommunikation.**

Die Kommission wird

- **im Jahr 2025 einen Fahrplan für das weitere Vorgehen in Bezug auf den rechtmäßigen und wirksamen Zugang zu Daten für Strafverfolgungszwecke vorlegen;**
- **im Jahr 2025 eine Folgenabschätzung im Hinblick auf die Aktualisierung der Vorschriften über die Vorratsdatenspeicherung auf EU-Ebene, soweit erforderlich, vornehmen;**
- **im Jahr 2026 einen Technologiefahrplan für Verschlüsselung zur Ermittlung und Bewertung technologischer Lösungen zur Ermöglichung des rechtmäßigen Zugangs der Strafverfolgungsbehörden zu Daten vorlegen;**
- **an der Einsetzung einer hochrangigen Gruppe zur Stärkung der operativen Zusammenarbeit im Bereich der Strafverfolgung arbeiten;**
- **im Jahr 2026 einen Campus für Sicherheitsforschung und -innovation in der Gemeinsamen Forschungsstelle einrichten.**

Die Kommission wird in Zusammenarbeit mit den Mitgliedstaaten und den einschlägigen EU-Agenturen

- **die EMPACT-Architektur stärken;**
- **auf die rasche Einführung der Interoperabilitätsarchitektur und die Umsetzung der Prüm-II-Verordnung hinwirken;**
- **den Rahmen für Reiseinformationen stärken.**

Die Mitgliedstaaten werden nachdrücklich aufgefordert,

- **die Richtlinie über den Informationsaustausch umzusetzen und vollständig anzuwenden.**

4. Widerstandsfähigkeit gegen hybride Bedrohungen und andere feindselige Handlungen

Wir werden die Widerstandsfähigkeit gegen hybride Bedrohungen stärken, indem wir den Schutz kritischer Infrastrukturen verbessern, die Cybersicherheit erhöhen, Verkehrsknotenpunkte und Häfen sichern und Online-Bedrohungen bekämpfen.

Feindselige Handlungen, die die Sicherheit der EU untergraben, werden immer häufiger und komplexer, wobei böswillige Akteure ihr Arsenal erheblich erweitert haben. Hybride Kampagnen, die sich gegen die EU, ihre Mitgliedstaaten und Partner richten, haben zugenommen und umfassen Sabotageakte gegen kritische Infrastrukturen, Brandstiftung, Cyberangriffe, Einmischung in Wahlen, Informationsmanipulation und Einflussnahme aus dem Ausland, einschließlich Desinformation, sowie die Nutzung von Migration als Waffe. Aufgrund ihrer politischen und operativen Rolle und der Art der von ihnen bearbeiteten Informationen bleiben auch die Organe, Einrichtungen und sonstigen Stellen der Union (im Folgenden „Einrichtungen der Union“) nicht verschont.

Die EU muss **ihre Widerstandsfähigkeit stärken**, die derzeit vorhandenen Instrumente wirksam einsetzen und neue Wege finden, um diesen sich wandelnden Bedrohungen, die von staatlichen und nichtstaatlichen Akteuren ausgehen, sowohl jetzt als auch in Zukunft zu begegnen.

Kritische Infrastrukturen

Bedrohungen **kritischer Infrastrukturen**, einschließlich hybrider Bedrohungen wie Sabotage und böswillige Cyberaktivitäten, stellen ein großes Problem dar, vor allem in Bezug auf Infrastrukturen, die die Mitgliedstaaten verbinden – seien es Energieverbindungsleitungen, grenzüberschreitende Kommunikationskabel oder der Verkehr. Seit dem Angriffskrieg Russlands gegen die Ukraine haben die Sabotageakte gegen kritische Infrastrukturen zugenommen, insbesondere im Jahr 2024; zahlreiche Mitgliedstaaten sind betroffen. Die Zusammenarbeit zwischen Strafverfolgungsbehörden, Sicherheits- und Cybersicherheitsdiensten, Militär und Katastrophenschutzbehörden sowie privaten Akteuren ist von entscheidender Bedeutung, wenn es darum geht, solche Handlungen vorherzusehen, aufzudecken, zu verhindern und wirkungsvoll auf sie zu reagieren.

Die Verringerung von Schwachstellen und die Stärkung der Widerstandsfähigkeit kritischer Einrichtungen sind unerlässlich, um die ununterbrochene Erbringung wesentlicher Dienste für Wirtschaft und Gesellschaft sicherzustellen. Die rechtzeitige Umsetzung und ordnungsgemäße Anwendung der **Richtlinie über die Resilienz kritischer Einrichtungen**[31] und der **Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie)**[32] durch alle Mitgliedstaaten sind in diesem Zusammenhang somit von wesentlicher Bedeutung.

Um rasche Fortschritte zu gewährleisten, wird die Kommission in Zusammenarbeit mit der **Gruppe für die Resilienz kritischer Einrichtungen und der NIS-Kooperationsgruppe** die Mitgliedstaaten bei der Ermittlung kritischer Einrichtungen[33] und dem Austausch bewährter Verfahren für nationale Strategien und Risikobewertungen in Bezug auf wesentliche Dienste unterstützen. Sollte es zu Störungen kritischer Infrastrukturen mit erheblichen grenzüberschreitenden Auswirkungen kommen, werden die Reaktionen auf EU-Ebene über den **europäischen Konzeptentwurf für eine koordinierte Reaktion auf Störungen kritischer Infrastrukturen von erheblicher grenzüberschreitender Bedeutung** koordiniert. Die Kommission fordert den Rat auf, den **europäischen Cyberkonzeptentwurf** rasch anzunehmen, mit dem die Koordinierung im Kontext des Krisenmanagements weiter gestärkt und so eine engere Zusammenarbeit der Behörden im Bereich der physischen und digitalen Resilienz erleichtert wird. Nach erfolgreichen Stresstests im Energiesektor im Jahr 2023 wird die Kommission **freiwillige Stresstests** in anderen für die innere Sicherheit wichtigen Sektoren fördern. Darüber hinaus wird die Kommission eine **unionsweite Übersicht über grenzüberschreitende und sektorübergreifende Risiken** für die Erbringung wesentlicher Dienste erstellen, um die Mitgliedstaaten bei ihren Risikobewertungen zu unterstützen und eine umfassende Risikobewertung auf EU-Ebene zu ermöglichen. Im Einklang mit der Strategie der Union zur Krisenvorsorge wird die Kommission gemeinsam mit den Mitgliedstaaten weitere Sektoren und Dienstleistungen ermitteln, die von den bestehenden Rechtsvorschriften nicht erfasst werden und für die möglicherweise Handlungsbedarf besteht.

Die **EU-NATO-Taskforce für die Resilienz kritischer Infrastrukturen** hat eine hervorragende Zusammenarbeit beim Austausch bewährter Verfahren und bei der Stärkung der

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

[32] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie).

[33] Zu den Sektoren, die unter die Richtlinie fallen, gehören Energie, Verkehr, Banken, Finanzmarktinfrastruktur, Gesundheit, Trinkwasser, Abwasser, digitale Infrastruktur, öffentliche Verwaltung, Raumfahrt sowie Produktion, Verarbeitung und Verteilung von Lebensmitteln.

Widerstandsfähigkeiten in den Bereichen Energie, Verkehr, digitale Infrastruktur und Weltraum gefördert. Diese Arbeit wird im Rahmen des **strukturierten Dialogs zwischen der EU und der NATO über Resilienz** fortgesetzt. Das **EU-Instrumentarium gegen hybride Bedrohungen** bietet den Mitgliedstaaten und Partnern solide Unterstützung bei der Vorbereitung auf hybride Bedrohungen und der Abwehr solcher Bedrohungen. **Teams für die rasche Reaktion auf hybride Bedrohungen**[34] bieten den Mitgliedstaaten, verschiedenen EU-Missionen und Partnern auf Ersuchen maßgeschneiderte kurzfristige Unterstützung. Darüber hinaus wird die Kommission die Zusammenarbeit der EU bei der Bekämpfung von Sabotage durch Expertentätigkeiten[35] vorantreiben, einschließlich eines **speziellen gemeinsamen Arbeitsprogramms** für die Experten zur Straffung des Informationsaustauschs und zur Festlegung von Gegenmaßnahmen.

Vorfälle, die **Seekabel** in Europa betreffen, verdeutlichen die Notwendigkeit strengerer Maßnahmen und klarerer Reaktionen. Wie im **EU-Aktionsplan für Kabelsicherheit**[36] dargelegt, werden die Kommission und die Hohe Vertreterin mit den Mitgliedstaaten, EU-Agenturen und Partnern wie der NATO zusammenarbeiten, um Bedrohungen von Unterseekabeln zu verhindern, aufzudecken, darauf zu reagieren und abzuwenden. Um eine umfassendes Lageerfassung der Bedrohungen zu erstellen, wird die Kommission gemeinsam mit den Mitgliedstaaten auf freiwilliger Basis einen integrierten Überwachungsmechanismus für Seekabel in den einzelnen Meeresbecken entwickeln und einrichten, beginnend mit einem regionalen Zentrum im nordischen/baltischen Raum.

Cybersicherheit

Anhaltende **böswillige Cyberaktivitäten**, die häufig Teil eines breiteren Spektrums multidimensionaler und hybrider Bedrohungen sind, erfordern kontinuierliche Aufmerksamkeit und Maßnahmen auf europäischer Ebene. In den letzten Jahren hat die Union eine Reihe von Cybersicherheitsgesetzen zur Stärkung der Cyberresilienz von NIS-2-Einrichtungen in kritischen Sektoren der EU sowie von Einrichtungen der Union[37], zur Verbesserung der Sicherheit digitaler Produkte (Cyberresilienz-Verordnung) und zur Schaffung eines Rahmens für die Unterstützung der Abwehrbereitschaft und der Reaktion auf Sicherheitsvorfälle (Cybersolidaritätsgesetz) angenommen. Im Januar 2025 hat die Kommission den **Europäischen Aktionsplan für die Cybersicherheit von Krankenhäusern und Gesundheitsdienstleistern**[38] angenommen, um im Hinblick auf Bedrohungen die Aufdeckung, Vorsorge und Krisenreaktion zu verbessern. Die vollständige Umsetzung dieses Aktionsplans ist von zentraler Bedeutung. Gleichzeitig müssen wir unsere Maßnahmen insbesondere in den Bereichen Informationsaustausch, Sicherheit der Lieferketten, Ransomware und Cyberangriffe sowie technologische Souveränität verstärken, um neuartigen Bedrohungen und Entwicklungen zu begegnen.

Darüber hinaus erfordert die Umsetzung, dass die Fachkräftelücke im Cybersicherheitsbereich geschlossen werden, wo aktuell 299 000 Fachleute fehlen. Die Kommission wird im Rahmen

[34] Strategischer Kompass der Union für Sicherheit und Verteidigung 2022, S. 22.
[35] EU-Sicherheitsberater, Europäisches Netz für die Beseitigung von Explosivstoffen, EU-Netz der Spezialeinheiten (ATLAS-Verbund), EU-Sicherheitsnetz für Hochrisikofälle, Beratergruppe für chemische, biologische, radiologische und nukleare Sicherheit, Gruppe für die Resilienz kritischer Einrichtungen.
[36] JOIN(2025) 9 final.
[37] Verordnung (EU, Euratom) 2023/2841 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union (ABl. L, 2023/2841, 18.12.2023).
[38] https://digital-strategy.ec.europa.eu/de/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers.

der Union der Kompetenzen[39] mit den Mitgliedstaaten zusammenarbeiten, um die Zahl der Fachkräfte im Bereich der Cybersicherheit zu erhöhen, insbesondere durch die neue EU-Akademie für Cyberkompetenzen. Der Strategieplan für die Bildung in MINT-Fächern[40] (d. h. Mathematik, Informatik, Naturwissenschaften und Technik) trägt dazu bei, die Talentpipeline und die europäische Reaktion auf den Bedarf des Arbeitsmarkts im Bereich der Cybersicherheit zu verbessern.

Parallel zur Stärkung ihrer Resilienz wird die EU den Rahmen für eine gemeinsame diplomatische Reaktion der Union auf böswillige Cyberaktivitäten (**Instrumentarium für die Cyberdiplomatie**) weiterhin in vollem Umfang nutzen, um Cyberbedrohungen, die von staatlichen und nichtstaatlichen Akteuren ausgehen, zu verhindern, abzuwenden und darauf zu reagieren.

Sicherheit der Lieferketten für Informations- und Kommunikationstechnologien

Das **Instrumentarium für die 5G-Cybersicherheit** bietet den einschlägigen Rahmen für den Schutz von 5G-Netzen, wird jedoch derzeit von den Mitgliedstaaten unzureichend umgesetzt. Es bestehen nach wie vor unannehmbare Sicherheitsrisiken, insbesondere im Hinblick auf die Ersetzung von Hochrisikoanbietern. Ein harmonisierter Ansatz für die Sicherheit der Lieferketten für Informations- und Kommunikationstechnologien (im Folgenden „IKT-Lieferketten“) kann der derzeitigen Fragmentierung des Binnenmarkts aufgrund unterschiedlicher Ansätze auf nationaler Ebene entgegenwirken, kritische Abhängigkeiten vermeiden und unsere IKT-Lieferketten von Hochrisikoanbietern entlasten, wodurch unsere kritischen Infrastrukturen gesichert werden.

Im Einklang mit diesem Ansatz wird die Kommission bei der bevorstehenden **Überarbeitung des Rechtsakts zur Cybersicherheit** die Sicherheit und Resilienz von IKT-Lieferketten und -Infrastrukturen umfassender prüfen. Überdies wird die Kommission vorschlagen, den **europäischen Rahmen für die Cybersicherheitszertifizierung** zu verbessern, um sicherzustellen, dass künftige Zertifizierungssysteme rechtzeitig angenommen werden können und den politischen Erfordernissen entsprechen.

Aufbauend auf bestehenden oder laufenden sektorspezifischen Bewertungen[41] wird die Kommission gemeinsam mit den Mitgliedstaaten eine **strategische Planung für koordinierte Bewertungen von Cybersicherheitsrisiken** ausarbeiten.

Cloud-Dienste und Telekommunikationsdienste sind aus Lieferketten für kritische Infrastrukturen, Unternehmen und Behörden nicht mehr wegzudenken. Die Kommission wird Maßnahmen ergreifen, um kritische Einrichtungen dazu anzuhalten, **Cloud-Dienste und Telekommunikationsdienste mit einem angemessenen Maß an Cybersicherheit** zu wählen, wobei nicht nur technische Risiken, sondern auch strategische Risiken und Abhängigkeiten zu berücksichtigen sind.

Ransomware und Cyberangriffe

Eine anhaltende große Herausforderung in der EU und weltweit ist **Ransomware** – in einem Bericht werden die jährlichen durch Ransomware verursachten Kosten bis 2031 auf mehr als 250 Mrd. EUR geschätzt[42]. Sowohl die **NIS-2-Richtlinie** als auch die **Cyberresilienz-Verordnung** werden einen beträchtlichen Beitrag zur Verbesserung der Sicherheitslage von

[39] COM(2025) 90 final.
[40] COM(2025) 89 final.
[41] Beispielsweise in den Bereichen 5G-Netze, Telekommunikation, Elektrizität, erneuerbare Energien und vernetzte Fahrzeuge.
[42] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

Einrichtungen leisten, sodass es für Ransomware-Netze kostspieliger wird, ihre Angriffe durchzuführen. Darüber hinaus wird die Kommission eng mit den Mitgliedstaaten zusammenarbeiten, um sicherzustellen, dass den Strafverfolgungsbehörden mehr Ransomware-Angriffe, insbesondere fortgeschrittene anhaltende Bedrohungen, und Lösegeldzahlungen gemeldet werden, um die Ermittlungen zu erleichtern.

Um Cyberangriffe zu verhindern und zu unterbinden, muss die EU den Informationsaustausch zwischen Strafverfolgungsbehörden, Cybersicherheitsbehörden und -einrichtungen sowie privaten Parteien unter der Ägide von Europol und der ENISA verstärken.

Europol und Eurojust sollten auf ihren Erfolgen bei der Bekämpfung von Ransomware-Operationen aufbauen und die Zusammenarbeit der Strafverfolgungsbehörden weiter unterstützen. Zu diesem Zweck sollten die Strafverfolgungsbehörden die Nutzung von Kooperationsmechanismen, einschließlich des **„International Ransomware Response Model“** (internationales Modell zu Bekämpfung von Ransomware) von Europol und der **Internationalen Initiative zur Bekämpfung von Ransomware**[43], maximieren, und die ENISA und Europol sollten zusammenarbeiten, um das Verzeichnis von Entschlüsselungsinstrumenten für Ransomware-Angriffe[44] zu erweitern.

Technologische Souveränität

Cybersicherheit und technologische Souveränität sind eng miteinander verknüpft, und technologische Abhängigkeiten müssen vorrangig angegangen werden. Die Union muss **die Entwicklung und den Einsatz neuer Technologien steuern**, wobei die Kommission daran arbeiten muss, die **Fähigkeiten in strategischen Technologien** wie KI, Quantentechnologie, fortgeschrittene Konnektivität, Cloud- und Edge-Computing und Internet der Dinge[45] durch künftige Initiativen wie den Aktionsplan „KI-Kontinent“, die Strategie für Quantentechnologie und andere[46] zu **verbessern**. Die Kommission wird weiterhin die rechtzeitige Einführung der neuesten verfügbaren international vereinbarten **Internetprotokolle** unterstützen, die für die Aufrechterhaltung eines skalierbaren und effizienten Internets mit mehr Cybersicherheit wesentlich sind. Darüber hinaus sind weitere Maßnahmen erforderlich, um **Herausforderungen im Zusammenhang mit Funkfrequenzen**, beispielsweise in Bezug auf Spoofing-Angriffe auf Signale der globalen Satellitennavigationssysteme, Stören (Jamming) oder Risiken und Abhängigkeiten in der Lieferkette, anzugehen, darunter der Einsatz von Quantenerfassungstechnologien und die Prüfung der Entwicklung von Kapazitäten zur Überwachung von Funkfrequenzen.

Der Einsatz von Lösungen der **Post-Quanten-Kryptografie** wird für den Schutz von sensibler Kommunikation und von gespeicherten Daten sowie von digitalen Identitäten im neuen Quantenzeitalter von entscheidender Bedeutung sein. Auf der Grundlage der Empfehlung von 2024 über einen Fahrplan für die koordinierte Umsetzung des Übergangs zur Post-Quanten-Kryptografie[47] arbeitet die Kommission mit den Mitgliedstaaten zusammen, um diesen Übergang zu fördern. In diesem Zusammenhang sollten die Mitgliedstaaten Hochrisikofälle in kritischen Einrichtungen ermitteln und für diese Hochrisikofälle so bald wie möglich, spätestens jedoch bis Ende 2030, eine quantensichere Verschlüsselung gewährleisten. Die

[43] https://counter-ransomware.org/.
[44] Erhältlich über das Projekt „No More Ransom“: https://www.nomoreransom.org/en/index.html.
[45] https://strategic-technologies.europa.eu/about_en#step-scope.
[46] Darunter das Gemeinsame Unternehmen EuropHPC (https://eurohpc-ju.europa.eu/index_en), die Leitinitiative zur Quantentechnik (Homepage | Leitinitiative zur Quantentechnik), 3C-Netze (COM(2024) 81 final) und der EU-Aktionsplan für Kabelsicherheit (JOIN(2025) 9 final).
[47] Empfehlung zu einem koordinierten Umsetzungsfahrplan für den Übergang zur Post-Quantum-Kryptographie | Gestaltung der digitalen Zukunft Europas.

Kommission arbeitet auch mit den Mitgliedstaaten und der Europäischen Weltraumorganisation zusammen, um die **europäische Quantenkommunikationsinfrastruktur (European Quantum Communication Infrastructure, EuroQCI)**[48] auf der Grundlage der Quantenschlüsselverteilung im Rahmen des EU-Programms für sichere Konnektivität **IRIS²** zu entwickeln und einzuführen. Beide Initiativen werden es den Einrichtungen letztlich ermöglichen, Daten zu übermitteln und Informationen sicher zu speichern.

Quantentechnologien werden auch in Bezug auf Sicherheitsanwendungen eine wichtige Rolle spielen: Im Rahmen der **Strategie für Quantentechnologie** wird ein **Fahrplan für die Quantenerfassung in Sicherheitsanwendungen** entwickelt werden. Ebenso arbeitet die Kommission derzeit daran, ihre internen sicherheitskritischen Systeme, einschließlich ihrer für Verschlusssachen genutzten IT-Systeme, quantensicher zu machen.

Ein unternehmensfreundlicher Rahmen für Cybersicherheit

Die bevorstehende Überarbeitung des Rechtsakts zur Cybersicherheit bietet die Gelegenheit, die **EU-Rechtsvorschriften zur Cybersicherheit** im Einklang mit dem Kompass für Wettbewerbsfähigkeit zu **vereinfachen**. Die Kommission wird eng mit den Mitgliedstaaten zusammenarbeiten, um eine rasche, kohärente und unternehmensfreundliche Umsetzung des in der NIS-2-Richtlinie, der Cyberresilienz-Verordnung und im Cybersolidaritätsgesetz festgelegten horizontalen Cybersicherheitsrahmens zu gewährleisten, um Einfachheit und Kohärenz zu fördern und eine Fragmentierung oder Duplizierung der Cybersicherheitsvorschriften im EU-Recht und im nationalen Recht zu vermeiden.

Um einen sicheren Zugang zu Online-Diensten zu ermöglichen und die digitale Sicherheit in der gesamten EU zu stärken, sieht der **Rahmen für eine europäische digitale Identität** vor, dass allen Bürgerinnen und Bürgern und Einwohnern der EU bis Ende 2026 vertrauenswürdige Brieftaschen für die Digitale Identität bereitgestellt werden. Durch die bevorstehende Einführung der **Europäischen Brieftasche für Unternehmen** sollen sichere grenzüberschreitende Interaktionen zwischen Unternehmen und öffentlichen Verwaltungen erleichtert werden. Beides sind Voraussetzungen für ein sicheres und effizienteres Funktionieren des datengesteuerten Binnenmarkts mit Instrumenten wie dem einheitlichen digitalen Zugangstor, der elektronischen Rechnungsstellung, der elektronischen Auftragsvergabe und dem digitalen Produktpass.

Sicherheit im Internet

Einige der schwerwiegendsten hybriden Bedrohungen, die die Sicherheit der Menschen in Europa gefährden und auf den demokratischen Raum der EU abzielen, finden online statt. Zu diesen Bedrohungen gehören illegale Aktivitäten und illegale Online-Inhalte, Informationsmanipulation mit künstlicher Verstärkung, irreführende Informationen und Informationsmanipulation und Einflussnahme aus dem Ausland.

Die strikte Durchsetzung des **Gesetzes über digitale Dienste** ist von entscheidender Bedeutung, um ein sicheres und zugängliches Online-Umfeld mit rechenschaftspflichtigen Akteuren zu gewährleisten, das auch gegenüber hybriden Bedrohungen widerstandsfähig ist. Gemäß dem Gesetz über digitale Dienste sind Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen verpflichtet, Risikobewertungen durchzuführen und Maßnahmen zur Minderung systemischer Risiken zu ergreifen, die sich aus der Gestaltung, dem Betrieb oder der Nutzung ihrer Dienste ergeben. Solche Risiken können negative Auswirkungen auf gesellschaftliche Debatten und auf Wahlprozesse sowie auf die öffentliche

[48] https://digital-strategy.ec.europa.eu/de/policies/european-quantum-communication-infrastructure-euroqci.

Sicherheit umfassen, z. B. weitreichende Einmischung böswilliger ausländischer staatlicher Akteure etwa in Wahlprozesse. Die Schulung der zuständigen Behörden der Mitgliedstaaten in Bezug auf den Einsatz von Rechtsinstrumenten zur unverzüglichen Entfernung illegaler Online-Inhalte ist wichtig, insbesondere im Hinblick auf geschlechtsspezifische Cybergewalt. Im Gesetz über digitale Dienste ist ein Krisenreaktionsmechanismus vorgesehen, der aktiviert werden kann, wenn außergewöhnliche Umstände eintreten, die zu einer schwerwiegenden Bedrohung der öffentlichen Sicherheit oder der öffentlichen Gesundheit in der Union oder in wesentlichen Teilen der Union führen können. Zur Ergänzung dieses Mechanismus haben die Kommission und die als Koordinatoren für digitale Dienste benannten zuständigen nationalen Behörden auch einen freiwilligen **Rahmen für die Reaktion auf Vorfälle im Rahmen des Gesetzes über digitale Dienste** entwickelt. Die Koordinatoren für digitale Dienste haben zudem Maßnahmen zum Schutz der Integrität von Wahlen ergriffen, beispielsweise durch die Organisation von Wahlrundtischgesprächen und Stresstests[49]. Das Gesetz über digitale Dienste bildet zusammen mit der Verordnung über politische Werbung[50] einen von mehreren Strängen zur Wahrung der Demokratie und der Integrität demokratischer Prozesse, die durch feindselige Akteure, unter anderem mithilfe digitaler Instrumente und in sozialen Medien, angegriffen werden können.

Die Umsetzung des **Instrumentariums gegen Informationsmanipulation und Einflussnahme aus dem Ausland** ist eine weitere wichtige Komponente, die entscheidende Unterstützung auf EU-Ebene bietet. Die Förderung der digitalen Kompetenz, der Medienkompetenz und des kritischen Denkens ist ebenfalls von zentraler Bedeutung für diese Bemühungen[51].

Bekämpfung des Einsatzes von Migration als Waffe

Russland hat mit Hilfe und entschlossener Unterstützung von Belarus Migration gezielt als Waffe eingesetzt und künstlich illegale Migrationsströme in Richtung der EU-Außengrenzen ausgelöst, mit dem Ziel, unsere Gesellschaften zu destabilisieren und die Einheit der Europäischen Union zu untergraben. Dies gefährdet nicht nur die nationale Sicherheit und Souveränität der Mitgliedstaaten, sondern auch die Sicherheit und Integrität des Schengen-Raums und die Sicherheit der Union insgesamt. In seinen Schlussfolgerungen vom Oktober 2024 betonte der Europäische Rat, dass es Russland, Belarus oder anderen Ländern nicht gestattet werden darf, unsere Werte, einschließlich des Rechts auf Asyl, zu missbrauchen und unsere Demokratie zu untergraben.

Wie in der Mitteilung der Kommission über den Einsatz von Migration als Waffe aus dem Jahr 2024 dargelegt, hat die Union neben einer starken politischen Unterstützung finanzielle, operative und diplomatische Maßnahmen ergriffen, einschließlich der Zusammenarbeit mit Herkunfts- und Transitländern, um diesen Bedrohungen wirksam zu begegnen[52]. Dies bedeutet, dass der vom Rat geschaffene neue Rahmen genutzt werden muss, um Personen und Organisationen, die an Handlungen und politischen Maßnahmen wie dem Einsatz von Migration als Waffe durch Russland beteiligt sind, durch das Einfrieren von Vermögenswerten

[49] DSA Elections Toolkit for Digital Services Coordinators, 2025, abrufbar unter https://digital-strategy.ec.europa.eu/en/library/dsa-elections-toolkit-digital-services-coordinators.
[50] Verordnung (EU) 2024/900 des Europäischen Parlaments und des Rates vom 13. März 2024 über die Transparenz und das Targeting politischer Werbung (ABl. L, 2024/900, 20.3.2024).
[51] Aktionsplan für digitale Bildung (2021-2027) – Europäischer Bildungsraum.
[52] COM(2024) 570 final.

und Reiseverbote zu sanktionieren[53]. Die EU wird diesen Rahmen erforderlichenfalls weiterhin nutzen und die Mitgliedstaaten bei der Abwehr dieser Bedrohung unterstützen.

Verkehrssicherheit

Seehäfen, Flughäfen und Landinfrastrukturen sind wichtige Ein- und Ausreisestellen. Sie spielen eine wichtige Rolle für die Wirtschaft und Gesellschaft der EU und sind für die militärische Mobilität von wesentlicher Bedeutung. Diese Verkehrsknotenpunkte und -mittel sind jedoch auch bevorzugte Ziele für externe Bedrohungen und kriminelle Aktivitäten. Die jüngsten Vorfälle, darunter Verstöße gegen die Luftfrachtsicherheit und die Luftsicherheit und Angriffe auf die Eisenbahninfrastruktur, verdeutlichen die gravierenden Risiken. **Verkehrsunternehmen** können sowohl Ziele als auch Instrumente für böswillige Akteure sein. Die bestehenden Rechtsinstrumente der EU haben zu einer Verbesserung der Luftsicherheit geführt[54], doch die hohe Bedrohung der Zivilluftfahrt erfordert ein Mittel, um Vorfälle vorherzusehen und die betroffenen Mitgliedstaaten rasch zu konsultieren. Die Kommission wird mit den Mitgliedstaaten zusammenarbeiten, um die bestehenden Durchführungsvorschriften im Bereich der Luftsicherheit für den Austausch von Verschlusssachen über **Ereignisse im Bereich der Luftsicherheit** zu ändern. Darüber hinaus wird die Kommission **Regulierungsmaßnahmen** in Erwägung ziehen, um neuen Bedrohungen wie **Vorfällen im Bereich der Luftfrachtsicherheit** zu begegnen und die Luftsicherheitsstandards zu stärken. Dazu gehört auch die Stärkung der **Rechtsvorschriften zur Luftsicherheit**, um Sofortmaßnahmen zu ermöglichen und gleichzeitig den Raum der einmaligen Sicherheitskontrolle an EU-Flughäfen aufrechtzuerhalten.

Bei der Ausarbeitung der künftigen **Strategie für die Häfen der EU**, die auf der **Europäischen Hafenallianz** aufbaut, wird die Kommission prüfen, wie die Rechtsvorschriften im Bereich der maritimen Sicherheit weiter gestärkt werden können, um neuen Bedrohungen wirksam zu begegnen, die Häfen zu sichern und die Sicherheit der Lieferketten in der EU zu verbessern. Zu diesem Zweck wird die Kommission für eine konsequente Umsetzung sorgen und daran arbeiten, die nationalen Verfahren zu harmonisieren und die Zuverlässigkeitsüberprüfungen in den Häfen zu verstärken. Zusätzlich zu den Sicherheitsprotokollen für Luftfracht wird die Kommission mit den Mitgliedstaaten und dem Privatsektor zusammenarbeiten, um diese Protokolle zu erweitern, um die Seeverkehrsketten zu sichern.

Die vorgeschlagene EU-Zollbehörde wird Risiken auf der Grundlage von **Zollinformationen** im Zusammenhang mit Waren, die in die EU eingeführt, aus der EU ausgeführt oder durch die EU befördert werden, analysieren und bewerten, um die Mitgliedstaaten dabei zu unterstützen, die Ausnutzung internationaler Lieferketten durch böswillige Akteure zu verhindern. Im Einklang mit der EU-Strategie für maritime Sicherheit[55] wird der künftige **Europäischer Pakt für die Meere** eine Schlüsselrolle bei der Verbesserung der maritimen Sicherheit in den Meeresbecken rund um die EU und darüber hinaus spielen, unter anderem durch die Förderung der Ausweitung von Mehrzweckeinsätzen und -übungen auf See.

Widerstandsfähigkeit der Lieferketten

Europa muss weniger auf Technologien aus Drittländern zurückgreifen, da dies zu Abhängigkeit und Sicherheitsrisiken führen kann. Ziel der Kommission ist es, die Abhängigkeit von einzelnen ausländischen Anbietern zu verringern, unserer Lieferketten von

[53] Verordnung (EU) 2024/2642 des Rates vom 8. Oktober 2024 über restriktive Maßnahmen angesichts der destabilisierenden Aktivitäten Russlands, ST/8744/2024/INIT (ABl. L, 2024/2642, 9.10.2024).
[54] Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates vom 11. März 2008 über gemeinsame Vorschriften für die Sicherheit in der Zivilluftfahrt (ABl. L 97 vom 9.4.2008, S. 72).
[55] JOIN(2023) 8 final.

Hochrisikolieferanten zu entlasten und kritische Infrastrukturen und industrielle Kapazitäten auf EU-Boden zu sichern, wie im **Kompass für Wettbewerbsfähigkeit**[56] und im **Deal für eine saubere Industrie**[57] festgelegt. Die Kommission wird eine **Industriepolitik für die innere Sicherheit** fördern, indem sie mit der EU-Industrie in Schlüsselsektoren (z. B. Verkehrsknotenpunkte, kritische Infrastrukturen) zusammenarbeitet, um Sicherheitslösungen wie Detektionsgeräte, biometrische Technologien und Drohnen mit eingebauten Sicherheitsmerkmalen zu entwickeln. Bei der **Überarbeitung der EU-Vergabevorschriften** wird die Kommission prüfen, ob die Sicherheitserwägungen in der Richtlinie über die Vergabeverfahren im Verteidigungs- und Sicherheitsbereich aus dem Jahr 2009[58] ausreichen, um den Erfordernissen der Strafverfolgung und der Widerstandsfähigkeit kritischer Einrichtungen gerecht zu werden.

Die Kommission wird die Mitgliedstaaten bei der **Überprüfung ausländischer Direktinvestitionen** und der Beschaffung von Ausrüstung für Logistikknotenpunkte unterstützen, um dafür zu sorgen, dass kritische Infrastrukturen und Technologien weiterhin sicher sind.

Sobald das **Binnenmarkt-Notfall- und Resilienzgesetz** in Kraft getreten ist, wird es der EU dabei helfen, Krisen zu bewältigen, die kritische Lieferketten und den freien Waren-, Dienstleistungs- und Personenverkehr stören. Dieses Gesetz wird eine rasche Krisenkoordinierung sowie die Ermittlung krisenrelevanter Waren und Dienstleistungen ermöglichen und ein Instrumentarium zur Sicherstellung ihrer Verfügbarkeit bieten. Ferner wird die Kommission in enger Zusammenarbeit mit den Mitgliedstaaten die Einrichtung eines **behördenübergreifenden Warnmechanismus für die Sicherheit des Verkehrs und der Lieferketten** vorschlagen, um einen sicheren und rechtzeitigen Austausch einschlägiger Informationen zu gewährleisten, die für die Vorhersage und Abwehr von Bedrohungen erforderlich sind.

Außerdem wird die verstärkte Nutzung von Kriterien wie Nachhaltigkeit, Resilienz und europäische Präferenz im öffentlichen Beschaffungswesen in der EU mit der Umsetzung der Verordnung zu kritischen Rohstoffen und der Netto-Null-Industrie-Verordnung die Entwicklung von Leitmärkten fördern. Engere Handelsbeziehungen, beispielsweise durch Rohstoffpartnerschaften und Partnerschaften für sauberen Handel und Investitionen, werden zur Diversifizierung der Lieferketten beitragen.

Widerstandsfähigkeit und Vorsorge gegenüber chemischen, biologischen, radiologischen und nuklearen Bedrohungen

Der Angriffskrieg Russlands gegen die Ukraine hat das Risiko **chemischer, biologischer, radiologischer und nuklearer (CBRN) Bedrohungen** erhöht. Um dem potenziellen Erwerb und dem Einsatz von CBRN-Material als Waffe entgegenzuwirken, wird die Kommission die Mitgliedstaaten und Partnerländer durch spezielle Schulungen und Übungen unterstützen. Die Kommission wird außerdem die Fähigkeiten zur Vorsorge und Reaktion gegenüber CBRN-Bedrohungen durch die Priorisierung von Bedrohungen, Innovationsfinanzierung für Gegenmaßnahmen, rescEU-Kapazitäten und die Bevorratung medizinischer Gegenmaßnahmen im Rahmen eines neuen **Aktionsplans für eine bessere Vorsorge und Reaktion gegenüber CBRN-Bedrohungen** stärken. Darüber hinaus wird die **EU-Strategie für medizinische Gegenmaßnahmen** die Entwicklung medizinischer Gegenmaßnahmen von der Forschung bis

[56] COM(2025) 30 final.
[57] COM(2025) 85 final.
[58] Richtlinie 2009/81/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über die Koordinierung der Verfahren zur Vergabe bestimmter Bau-, Liefer- und Dienstleistungsaufträge in den Bereichen Verteidigung und Sicherheit (ABl. L 216 vom 20.8.2009).

hin zur Herstellung und zum Vertrieb unterstützen, um die EU vor Pandemien und CBRN-Bedrohungen zu schützen.

Aufbauend auf den Erfahrungen mit der COVID-19-Pandemie hat die EU den Rahmen für die Gesundheitssicherheit gestärkt[59]. Die Kommission benennt EU-Referenzlaboratorien für die öffentliche Gesundheit, um die Überwachungs- und Schnellerkennungskapazitäten der EU und der Mitgliedstaaten zu stärken. Ein Unionsplan für Vorsorge, Prävention und Reaktion im Bereich der Gesundheitssicherheit wird 2025 veröffentlicht.

Zentrale Maßnahmen

Die Kommission wird

- **im Jahr 2025 den Rechtsakt zur Cybersicherheit überprüfen und überarbeiten;**
- **Maßnahmen zur Gewährleistung der Cybersicherheit bei der Nutzung von Cloud-Diensten entwickeln;**
- **im Jahr 2025 eine Strategie für die Häfen der EU vorschlagen;**
- **im Jahr 2026 die EU-Vergabevorschriften für den Verteidigungs- und Sicherheitsbereich überarbeiten;**
- **im Jahr 2026 einen Aktionsplan für eine bessere Vorsorge und Reaktion gegenüber CBRN-Bedrohungen vorlegen.**

Die Kommission wird in Zusammenarbeit mit den Mitgliedstaaten

- **auf die Entwicklung und Einführung der EuroQCI hinarbeiten;**
- **für eine wirksame Durchsetzung des Gesetzes über digitale Dienste sorgen;**
- **Maßnahmen zur Bekämpfung des Einsatzes von Migration als Waffe ergreifen;**
- **ein System für Ereignisse im Bereich der Luftsicherheit einrichten;**
- **auf die Einrichtung eines behördenübergreifenden Warnmechanismus für die Sicherheit des Verkehrs und der Lieferketten hinarbeiten.**

Der Rat wird nachdrücklich aufgefordert,

- **die Empfehlung des Rates zum Cyberkonzeptentwurf der EU anzunehmen.**

Die Mitgliedstaaten werden nachdrücklich aufgefordert,

- **die Richtlinie über die Resilienz kritischer Einrichtungen sowie die NIS-2-Richtlinie umzusetzen und vollständig anzuwenden.**

5. Verschärftes Vorgehen gegen schwere und organisierte Kriminalität

Wir werden dazu beitragen, die organisierte Kriminalität auszumerzen, indem wir strengere Vorschriften zur Bekämpfung von Netzen der organisierten Kriminalität, auch in Bezug auf Ermittlungen, vorschlagen, die Anfälligkeit junger Menschen in der EU für die Rekrutierung für Straftatenverringern und Maßnahmen verstärken, um den Zugang zu kriminellen Instrumenten und Vermögenswerten zu unterbinden.

Die organisierte Kriminalität macht sich ein sich wandelndes Umfeld zunutze und breitet sich exponentiell aus. Sie profitiert von fortgeschrittenen Technologien, ist über mehrere Rechtsräume hinweg tätig und unterhält enge Verbindungen über die EU-Grenzen hinaus. Angesichts dieser komplexen, transnationalen Bedrohungen sind Koordinierung und Unterstützung auf EU-Ebene von entscheidender Bedeutung.

[59] Insbesondere durch die Verordnung (EU) 2022/2371 zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren.

Verhütung von Straftaten

Die Rekrutierung junger Menschen für die organisierte Kriminalität gibt in der EU zunehmend Anlass zur Sorge. Die Bekämpfung der organisierten Kriminalität erfordert die Bekämpfung ihrer **eigentlichen Ursachen** durch Bildung und Alternativen zu einem Leben in der Kriminalität im Rahmen eines gesamtgesellschaftlichen Ansatzes. Die Kommission wird die Einbeziehung von Sicherheitserwägungen in die Bildungs-, Sozial-, Beschäftigungs- und Regionalpolitik der EU unterstützen. Die EU wird **Strategien zur auf wissenschaftlichen Erkenntnissen beruhenden Kriminalprävention**[60] fördern, die auf die lokalen Gegebenheiten zugeschnitten sind.

Um die Nutzer von Online-Diensten, insbesondere Minderjährige, unter anderem vor sexuellen Missbrauchstätern, Menschenhändlern und der Rekrutierung für Straftaten oder gewalttätigen Extremismus zu schützen, sehen die Maßnahmen im Rahmen des **Gesetzes über digitale Dienste** vor, dass Anbieter von Online-Plattformen, die für Minderjährige zugänglich sind, Risiken bewältigen und gegen illegale Inhalte, einschließlich Hassreden, vorgehen müssen. Die Kommission plant, **Leitlinien zum Schutz von Minderjährigen** herauszugeben, um Anbieter von Online-Plattformen dabei zu unterstützen, ein hohes Maß an Privatsphäre, Sicherheit und Schutz für Minderjährige im Internet zu gewährleisten. Die Leitlinien werden eine Reihe von Empfehlungen für sämtliche in der Union angebotenen digitalen Dienste enthalten, um den Schutz Minderjähriger im Internet zu verbessern. Für das Jahr 2025 plant die Kommission außerdem die Einführung einer EU-weiten Lösung zur **Altersüberprüfung, die den Datenschutz gewährleistet**, um die Zeit bis zur Einführung der europäischen Brieftasche für die Digitale Identität Ende 2026 zu überbrücken. Außerdem wird die Kommission einen Aktionsplan gegen Cybermobbing vorlegen.

Darüber hinaus wird die Kommission weiterhin die freiwillige Zusammenarbeit verschiedener Interessenträger mit Online-Plattformen und anderen einschlägigen Akteuren unterstützen, unter anderem durch das EU-Internetforum und gezielte Verhaltenskodizes im Rahmen des Gesetzes über digitale Dienste wie den Verhaltenskodex für die Bekämpfung illegaler Hassreden im Internet von 2025. Ziel ist es, das Bewusstsein zu schärfen, gemeinsam auf aktuelle und neue Bedrohungen zu reagieren und bewährte Verfahren für Abhilfemaßnahmen zu entwickeln und auszutauschen.

Auf lokaler Ebene machen die Auswirkungen der organisierten Kriminalität deutlich, dass es regionaler Lösungen bedarf, um die Anfälligkeit für illegale Aktivitäten und deren Attraktivität zu verringern. Die EU-Agenda für Städte, die auf der EU-Initiative „Städte gegen Radikalisierung“ aufbaut, wird sich mit sicherheitspolitischen Herausforderungen in Städten befassen. Die Kommission wird die Mitgliedstaaten durch den Europäischen Fonds für regionale Entwicklung bei der Verbesserung der städtischen und regionalen Sicherheit unterstützen**.**

Eine solide Bildungs- und Kompetenzgrundlage ist die Basis für eine widerstandsfähige und von Zusammenhalt geprägte Gesellschaft. Im Rahmen der **Union der Kompetenzen** und des **Aktionsplans für Integration und Inklusion** wird die Union daran arbeiten, Menschen dabei zu unterstützen, widerstandsfähiger gegenüber Fehl- und Desinformation, Radikalisierung und Rekrutierung für kriminelle Handlungen zu werden.

Der Schutz von Kindern vor sämtlichen Formen von Gewalt, einschließlich Kriminalität, körperlicher oder psychischer Gewalt, online wie offline, ist ein zentrales Ziel der EU. Um den besonderen Bedürfnissen besonders gefährdeter Gruppen wie Kinder Rechnung zu tragen, die zunehmend von Rekrutierung und Radikalisierung, Kontaktaufnahme zu Missbrauchszwecken

[60] https://www.eucpn.org/.

(Grooming) und sexuellem Kindesmissbrauch, Cybermobbing, Desinformation und anderen Bedrohungen betroffen sind, wird die EU einen **Aktionsplan zum Schutz von Kindern vor Kriminalität** ausarbeiten, der sowohl den Online- als auch den Offline-Bereich umfasst. Dieser wird einen kohärenten und koordinierten Ansatz auf der Grundlage der verfügbaren Rahmenwerke und Instrumente, einschließlich des künftigen EU-Zentrums für die Prävention und Bekämpfung sexuellen Kindesmissbrauchs sowie anderer Einrichtungen und Agenturen der EU, umfassen sowie Vorschläge für Möglichkeiten für das weitere Vorgehen in Bereichen, in denen noch Lücken bestehen.

Zerschlagung krimineller Netze und ihrer Unterstützer

Der Kampf gegen kriminelle Netze mit hohem Gefahrenpotenzial sowie deren Rädelsführer und Unterstützer muss intensiviert werden. Wenngleich in jüngster Zeit bemerkenswerte Erfolge erzielt wurden[61], stehen veraltete Vorschriften und die uneinheitliche Definition des Begriffs „kriminelles Netz“ einer wirksamen strafrechtlichen Reaktion und grenzüberschreitenden Zusammenarbeit im Weg. Die Kommission wird veraltete Rechtsvorschriften in diesem Bereich überprüfen und einen neuen **Rechtsrahmen zur Bekämpfung der organisierten Kriminalität** vorschlagen, um die Reaktion zu verstärken.

Wie die EUStA und das OLAF bei der Bekämpfung **grenzüberschreitender Betrugsfälle und Straftaten zum Nachteil der finanziellen Interessen der EU** gezeigt haben, kann die verwaltungsrechtliche Durchsetzung die Strafverfolgung ergänzen, um schnellere Ergebnisse zu erzielen. Subventionsbetrüger konzentrieren sich auf Sektoren wie erneuerbare Energien, Forschungsprogramme und den Agrarsektor[62]. Die Kommission wird prüfen, wie der Einsatz straf- und verwaltungsrechtlicher Instrumente koordiniert und die Zusammenarbeit mit Europol, Eurojust und der EUStA verbessert werden kann. Die Kommission wird auch weiterhin die breitere Anwendung des **administrativen Ansatzes** unterstützen, um lokale und andere Verwaltungsbehörden in die Lage zu versetzen, kriminelle Unterwanderung zu unterbinden[63].

Die EU arbeitet an der Stärkung ihres Rechtsrahmens zur **Korruptionsbekämpfung**[64]. Das Europäische Parlament und der Rat sollten die Verhandlungen über den von der Kommission vorgeschlagenen aktualisierten Rahmen für die Korruptionsbekämpfung rasch abschließen. Die Kommission wird eine EU-Strategie zur Korruptionsbekämpfung vorlegen, um die Integrität zu fördern und die Koordinierung zwischen allen einschlägigen Behörden und Interessenträgern in diesem Bereich zu stärken.

Feuerwaffen sind ein Schlüsselfaktor für die zunehmende Gewalt durch organisierte kriminelle Gruppen. Die Kommission wird gemeinsame strafrechtliche Normen für den unerlaubten Handel mit Feuerwaffen vorschlagen. Ein neuer **EU-Aktionsplan gegen den unerlaubten Handel mit Feuerwaffen** wird sich auf den Schutz des legalen Marktes und die Eindämmung krimineller Aktivitäten konzentrieren, und zwar auf der Grundlage einer besseren Erkenntnisgewinnung und einer verstärkten internationalen Zusammenarbeit mit besonderem Schwerpunkt auf der Ukraine und dem Westbalkan.

---

[61] Einschließlich jüngster EMPACT-Fälle.

[62] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

[63] https://administrativeapproach.eu/sites/default/files/page/files/eu-jha-council-9-10-june-conclusions-administrative-approach-org-crime.pdf.

[64] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Bekämpfung der Korruption, zur Ersetzung des Rahmenbeschlusses 2003/568/JI des Rates und des Übereinkommens über die Bekämpfung der Bestechung, an der Beamte der Europäischen Gemeinschaften oder der Mitgliedstaaten der Europäischen Union beteiligt sind, sowie zur Änderung der Richtlinie (EU) 2017/1371 des Europäischen Parlaments und des Rates (COM(2023) 234 final, Brüssel, 3.5.2023).

Illegal gehandelte pyrotechnische Gegenstände, die für Straftaten eingesetzt werden, erfordern Maßnahmen zur Verbesserung der Prävention und Rückverfolgbarkeit. Die Kommission bewertet derzeit die Richtlinie über pyrotechnische Gegenstände und wird auch **strafrechtliche Sanktionen für den Handel mit pyrotechnischen Gegenständen** in Erwägung ziehen.

Verfolgung von Geldflüssen

Die **Verfolgung von Geldflüssen** (Grundsatz „Follow the money") ist für die Bekämpfung der organisierten Kriminalität und des Terrorismus von entscheidender Bedeutung, gestaltet sich aber nach wie vor sehr schwierig. Die Verbindung zwischen organisierter Kriminalität und Geldflüssen erfordert intensive und gemeinsame Anstrengungen, um den Zugang krimineller Netze zu Finanzierungsquellen zu unterbinden und Menschen, Unternehmen und öffentliche Haushalte besser zu schützen.

Die EU hat ihre Bemühungen mit den neuen Vorschriften zur Bekämpfung der Geldwäsche, einschließlich der Einrichtung der **AMLA**[65], verstärkt. Die Zusammenarbeit zwischen der AMLA, dem OLAF, der EUStA, Eurojust und Europol ist für die Durchführung wirksamer Finanzermittlungen von wesentlicher Bedeutung. Die Kommission wird die Einrichtung von **Partnerschaften** unterstützen – sowohl solcher, die die Zusammenarbeit zwischen den Behörden erleichtern, als auch solcher, an denen der Privatsektor beteiligt ist.

Um die finanziellen Motive der organisierten Kriminalität zu zerschlagen, sind die Beschlagnahme von Vermögenswerten und die Einziehung von Erlösen aus Straftaten unerlässlich. Die kürzlich verabschiedeten strengeren Vorschriften für die **Abschöpfung und Einziehung von Vermögenswerten**[66] sollten von den Mitgliedstaaten unverzüglich umgesetzt und in vollem Umfang angewendet werden. Auch die Bekämpfung paralleler Finanzsysteme, die genutzt werden, um den EU-Rahmen zur Bekämpfung der Geldwäsche zu umgehen, darunter kryptobasierte Systeme, erfordert innovative Maßnahmen, den Austausch bewährter Verfahren zwischen den Mitgliedstaaten und eine verstärkte Unterstützung durch Europol und Eurojust. Die Kommission wird die Machbarkeit eines neuen EU-weiten Systems zur Verfolgung von Gewinnen aus organisierter Kriminalität und Terrorismusfinanzierung prüfen und außerdem einen zeitnahen und erweiterten Informationsfluss von den **zentralen Meldestellen** an die Strafverfolgungsbehörden fördern. Die Kommission wird prüfen, wie Schlupflöcher geschlossen werden können, die Mitgliedstaaten beim Aufbau von Kapazitäten unterstützen und weiter an der Stärkung der Zusammenarbeit mit Drittländern arbeiten, die von Kriminellen für illegale Bankgeschäfte missbraucht werden.

Bekämpfung schwerer Straftaten

Neben der Zerschlagung krimineller Netze sind für die Bekämpfung schwerer Straftaten gezielte Anstrengungen erforderlich. Um unsere Fähigkeit zur Bekämpfung von **Online-Betrug** zu stärken, der erhebliche finanzielle Schäden verursacht[67], wird die Kommission Präventionsmaßnahmen und wirksamere Strafverfolgungsmaßnahmen unterstützen und mit den Mitgliedstaaten und Interessenträgern zusammenarbeiten, um Opfer zu unterstützen und zu schützen, unter anderem durch Hilfe bei der Wiedererlangung ihrer Gelder. Diese Bemühungen werden in einem **Aktionsplan zu Bekämpfung von Online-Betrug** formalisiert.

Aufbauend auf der EU-Strategie zur Bekämpfung des **sexuellen Missbrauchs von Kindern** 2020-2025[68] wird die Kommission die beiden gesetzgebenden Organe dabei unterstützen, die

[65] https://www.amla.europa.eu/index_en.
[66] Richtlinie (EU) 2024/1260 des Europäischen Parlaments und des Rates vom 24. April 2024 über die Abschöpfung und Einziehung von Vermögenswerten (ABl. L, 2024/1260, 2.5.2024).
[67] Global State of Scams Report 2024.
[68] COM(2020) 607 final.

beiden Legislativvorschläge[69] zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern im Internet und zur wirksameren Strafverfolgung von sexuellem Missbrauch und sexueller Ausbeutung von Kindern fertigzustellen Da die Übergangsvorschriften nur bis April 2026 gelten, muss unbedingt ein dauerhafter Rechtsrahmen geschaffen werden, und die Kommission fordert die beiden gesetzgebenden Organe auf, Verhandlungen über den Entwurf einer Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern aufzunehmen. Die beiden gesetzgebenden Organe werden ferner ersucht, die Verhandlungen über die Richtlinie zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie von Darstellungen sexuellen Missbrauchs von Kindern voranzubringen, in der Mindestvorschriften für die Definition von Straftaten und Sanktionen im Bereich der sexuellen Ausbeutung von Kindern festgelegt werden.

Die Hälfte der gefährlichsten kriminellen Netze in der EU ist in gewaltsamen **Drogenhandel** verwickelt. Obschon die EU kürzlich ihre Maßnahmen zur Bekämpfung dieser Art von Kriminalität verstärkt hat[70], insbesondere durch die Ausweitung des Mandats der **Drogenagentur der EU**, sind weitere Maßnahmen erforderlich. Die Kommission wird eng mit den Mitgliedstaaten zusammenarbeiten, um eine neue **EU-Drogenstrategie** vorzuschlagen. Außerdem wird sie den **Rechtsrahmen für Drogenausgangsstoffe** überarbeiten und einen **Europäischen Aktionsplan gegen den Drogenhandel** vorschlagen, um Routen zu unterbrechen und Geschäftsmodelle zu stören**.** Die **öffentlich-private Partnerschaft der Europäischen Hafenallianz** zur Stärkung des Schutzes von Häfen wird auf kleinere Häfen und Binnenhäfen ausgeweitet, um die Durchsetzung der Vorschriften zur Gefahrenabwehr im Seeverkehr sicherzustellen. In Anerkennung der schwerwiegenden lokalen Auswirkungen des Drogenhandels wird die Kommission weiterhin eine ausgewogene, evidenzbasierte und multidisziplinäre Drogenpolitik unterstützen, die für plötzliche Drogenzuströme, insbesondere synthetische Opioide, gerüstet ist.

Um die Ausbeutung von Menschen zu bekämpfen, wurden neue EU-Vorschriften angenommen[71] und es wird eine **neue Strategie der EU zur Bekämpfung des Menschenhandels** (2026-2030) auf den Weg gebracht, die alle Phasen von der Prävention bis zur Strafverfolgung abdeckt, wobei der Schwerpunkt auf der Unterstützung der Opfer sowohl auf EU-Ebene als auch auf internationaler Ebene liegt.

In Bezug auf die Bekämpfung der **Schleuserkriminalität** wird die Kommission gemeinsam mit wichtigen Partnern im Rahmen der neuen Globalen Allianz zur Bekämpfung der Schleuserkriminalität in Zusammenarbeit mit Europol, Eurojust und Frontex die Bemühungen, auch im Online-Bereich, anführen. Die Vorschläge der Kommission zur Bekämpfung der Schleuserkriminalität[72] sollten unverzüglich angenommen und umgesetzt werden. Darüber hinaus hat die Kommission nach der Annahme des **Instrumentariums für Verkehrsunternehmen**[73] ihre Kontakte zu ausländischen Behörden und Betreibern intensiviert und wird weiterhin mit der Luftfahrtindustrie und den Zivilluftfahrtorganisationen[74]

[69] COM(2022) 209 final und COM(2024) 60 final.
[70] COM(2023) 641 final.
[71] Richtlinie (EU) 2024/1712 vom 13. Juni 2024 zur Änderung der Richtlinie 2011/36/EU zur Verhütung und Bekämpfung des Menschenhandels und zum Schutz seiner Opfer (ABl. L, 2024/1712, 24.6.2024).
[72] COM(2023) 755 final und COM(2023) 754 final.
[73] Toolbox addressing the use of commercial means of transport to facilitate irregular migration to the EU.
[74] Einschließlich der Internationalen Zivilluftfahrt-Organisation.

zusammenarbeiten, um das Bewusstsein für die Schleusung von Migranten auf dem Luftweg zu schärfen[75].

Umweltkriminalität gefährdet langfristig die Umwelt, die öffentliche Gesundheit und die Wirtschaft. Die Kommission wird die Mitgliedstaaten bei der Umsetzung der Richtlinie über Umweltkriminalität[76] unterstützen und operative Netze und Maßnahmen in diesem Bereich stärken[77]. Eine konsequente Durchsetzung ist wesentlich. Überdies wird das kürzlich verabschiedete Übereinkommen des Europarats über den Schutz der Umwelt durch das Strafrecht[78] dazu beitragen, dass sowohl innerhalb als auch außerhalb Europas entschlossene und vergleichbare Anstrengungen zur Bekämpfung der Umweltkriminalität unternommen werden.

Strafrechtliche Reaktion

Kriminalität und Terrorismus können jeden treffen; daher ist es unerlässlich, die Rechte der **Opfer** zu schützen und zu wahren, um Schäden zu mindern und die allgemeine Sicherheit und das Vertrauen in die Behörden zu stärken. Aufbauend auf der Opferschutzrichtlinie wird die Kommission eine neue **Strategie für die Rechte von Opfern** auf den Weg bringen.

Die **Strafrechtssysteme in der EU** brauchen wirksame Instrumente, um neuen Bedrohungen zu begegnen. Dazu hat die Kommission ein **Hochrangiges Forum zur Zukunft der Strafjustiz in der EU** ins Leben gerufen. In diesem Forum kommen die Mitgliedstaaten, das Europäische Parlament, EU-Agenturen und -Einrichtungen sowie andere relevante Interessenträger zusammen. Ziel ist es zu erörtern, wie sichergestellt werden kann, dass unsere Strafrechtssysteme angesichts sich wandelnder Herausforderungen wirksam, fair und widerstandsfähig bleiben, während gleichzeitig die justizielle Zusammenarbeit und das gegenseitige Vertrauen gestärkt wird, auch durch Digitalisierung[79].

Zentrale Maßnahmen

Die Kommission wird

- **im Jahr 2026 einen Legislativvorschlags für modernisierte Vorschriften zur Bekämpfung der organisierten Kriminalität vorlegen;**
- **im Jahr 2025 einen Legislativvorschlags zur Überarbeitung des Rechtsrahmens für Drogenausgangsstoffe vorlegen;**
- **im Jahr 2025 einen Legislativvorschlags für gemeinsame strafrechtliche Standards bezüglich des unerlaubten Handels mit Feuerwaffen vorlegen;**
- **die Notwendigkeit einer Überarbeitung der Richtlinie über pyrotechnische Gegenstände und der Richtlinie über Explosivstoffen für zivile Zwecke bewerten;**
- **die Notwendigkeit einer weiteren Stärkung der Europäischen Ermittlungsanordnung und des Europäischen Haftbefehls bewerten;**
- **im Jahr 2026 eine neue Strategie der EU zur Bekämpfung des Menschenhandels vorlegen;**

[75] Die Kommission wird auch die Fertigstellung der Verordnung über Maßnahmen gegen Verkehrsunternehmen, die Menschenhandel oder die Schleusung von Migranten erleichtern oder daran beteiligt sind (COM(2021) 753 final) unterstützen.

[76] Richtlinie (EU) 2024/1203 des Europäischen Parlaments und des Rates vom 11. April 2024 über den strafrechtlichen Schutz der Umwelt (ABl. L, 2024/1203, 30.4.2024).

[77] Gemeinschaftsnetz für die Durchführung und Durchsetzung des Umweltrechts, Europäisches Netz der in Umweltsachen tätigen Staatsanwälte, EnviCrimeNet und Richterforum der Europäischen Union für Umwelt.

[78] Committee of experts on the protection of the environment through Criminal Law (PC-ENV) – Europäischer Ausschuss für Strafrechtsfragen.

[79] Insbesondere durch die Einrichtung der Kommunikation via Online-Datenaustausch im Rahmen der E-Justiz und des Europäischen Strafregisterinformationssystem für Drittstaatsangehörige.

- **im Jahr 2026 eine neue Strategie für die Rechte von Opfern vorlegen;**
- **bis 2027 einen EU-Aktionsplan zum Schutz von Kindern vor Kriminalität vorlegen;**
- **im Jahr 2025 einen Europäischen Aktionsplan gegen den Drogenhandel vorlegen;**
- **im Jahr 2026 einen EU-Aktionsplan gegen den unerlaubten Handel mit Feuerwaffen vorlegen;**
- **ab 2025 schrittweise die Europäische Hafenallianz ausweiten;**
- **im Jahr 2026 Leitlinien zum Schutz von Minderjährigen im Rahmen des Gesetzes über digitale Dienste annehmen;**
- **im Jahr 2026 einen EU-Aktionsplan gegen Cybermobbing vorlegen.**

Die Mitgliedstaaten werden nachdrücklich aufgefordert,

- **die neuen Vorschriften über die Abschöpfung und Einziehung von Vermögenswerten bis Ende 2026 vollständig umzusetzen und in vollem Umfang anzuwenden;**
- **den administrativen Ansatz bei der Bekämpfung der kriminellen Unterwanderung umzusetzen;**
- **öffentlich-private Partnerschaften zur Bekämpfung der Geldwäsche einzurichten;**
- **die Richtlinie zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt umzusetzen und vollständig anzuwenden.**

Das Europäische Parlament und der Rat werden ausdrücklich aufgefordert,

- **die Verhandlungen über die Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern und über die Richtlinie zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie von Darstellungen sexuellen Missbrauchs von Kindern aufzunehmen;**
- **die Verhandlungen über die Richtlinie zur Bekämpfung der Korruption abzuschließen.**

6. Bekämpfung von Terrorismus und gewaltorientiertem Extremismus

Wir werden eine umfassende Agenda zur Terrorismusbekämpfung einführen, um Radikalisierung zu verhindern, den Online- und den öffentlichen Raum zu sichern, Finanzierungskanäle zu blockieren und bei Angriffen zu reagieren.

Die Terrorgefahr in der EU ist nach wie vor hoch. Sie steht in engem Zusammenhang mit den Ausstrahlungseffekten geopolitischer Ereignisse, mit neuen Technologien und neuen Methoden der Terrorismusfinanzierung. Wir müssen dafür sorgen, dass die EU gut gerüstet ist, um Bedrohungen vorherzusehen, Radikalisierung (sowohl offline als auch online) zu verhindern, die Bürgerinnen und Bürger und den öffentlichen Raum vor Angriffen zu schützen und im Falle von Angriffen wirksam zu reagieren. Im Jahr 2025 wird eine **neue EU-Agenda zur Prävention und Bekämpfung von Terrorismus und gewaltbereitem Extremismus** vorgelegt, in der die künftigen Maßnahmen der EU dargelegt sind. Im Einklang mit der neuen Agenda werden die EU und der Westbalkan 2025 den neuen **Gemeinsamen Aktionsplan** zur Prävention und Bekämpfung von Terrorismus und gewaltorientiertem Extremismus unterzeichnen.

Prävention von Radikalisierung und Schutz von Menschen im Internet

Ähnlich wie beim Kampf gegen die organisierte Kriminalität beginnt die Bekämpfung von Terrorismus und gewaltbereitem Extremismus damit, **die eigentlichen Ursachen anzugehen**. Das **EU-Wissenszentrum zur Prävention von Radikalisierung** wird seine Unterstützung für

Praktiker und politische Entscheidungsträger mit einem neuen **umfassenden Präventionsinstrumentarium** verstärken, um eine frühzeitige Erkennung gefährdeter Personen, insbesondere unter Minderjährigen, und entsprechende Maßnahmen zu ermöglichen**.** Radikalisierung findet häufig in Gefängnissen statt. Um die Mitgliedstaaten bei der Bewältigung dieses Problems zu unterstützen, wird die Kommission neue Empfehlungen herausgeben.

Terroristen und gewalttätige Extremisten nutzen Online-Plattformen, um terroristische und andere schädliche Inhalte zu verbreiten, Gelder zu sammeln und neue Anhänger zu rekrutieren. Gefährdete Nutzer, insbesondere Minderjährige, werden im Internet in alarmierendem Ausmaß radikalisiert. Die **Verordnung zur Bekämpfung terroristischer Online-Inhalte** hat maßgeblich dazu beigetragen, der Verbreitung terroristischer Inhalte im Internet entgegenzuwirken, indem sie die rasche Entfernung abscheulichster und gefährlichster Inhalte ermöglicht hat[80]. Die Kommission bewertet derzeit ihre Funktionsweise und wird prüfen, wie dieser Rahmen am besten gestärkt werden kann.

Das **EU-Krisenprotokoll** für eine gemeinsame, rasche Reaktion der Strafverfolgungsbehörden und der Technologiebranche im Hinblick auf einen Terroranschlag wird geändert, um Skalierbarkeit und Flexibilität zu gewährleisten und so auf die zunehmende Online-Dimension terroristischer Anschläge reagieren zu können. Das EU-Internetforum wird auch weiterhin das wichtigste Forum für die freiwillige Zusammenarbeit mit der Technologiebranche bei der Bekämpfung terroristischer und anderer schädlicher Online-Inhalte sein. Darüber hinaus beteiligt sich die Kommission an internationalen Initiativen wie der Christchurch Call Foundation und dem Globalen Internetforum zur Bekämpfung des Terrorismus.

Bekämpfung der Terrorismusfinanzierung

Terroristen finanzieren ihre Aktivitäten über Crowdfunding-Kampagnen, Kryptowerte, Neo-Banken oder Online-Zahlungsplattformen. Die Strafverfolgungsbehörden müssen diese Finanzströme aufdecken und untersuchen. Dies erfordert Mittel, Instrumente und Fachwissen. Dem **Netzwerk der Finanzermittler zur Terrorismusbekämpfung** kommt dabei eine zentrale Rolle zu. Die Kommission wird die Schaffung eines **neuen EU-weiten Systems zur Verfolgung der Terrorismusfinanzierung** prüfen, das Transaktionen innerhalb der EU und SEPA-Transaktionen, Kryptowertetransfers sowie Online- und elektronische Zahlungen umfasst und das Abkommen zwischen der EU und den USA über das Programm zum Aufspüren der Finanzierung des Terrorismus ergänzt.

Der EU-Haushalt muss **vor Missbrauch zum Zwecke der Förderung radikaler/extremistischer Ansichten** in den Mitgliedstaaten geschützt werden. Die überarbeitete **Haushaltsordnung** sieht nun eine Verurteilung wegen „Aufstachelung zu Diskriminierung, Feindseligkeit oder Gewalt“ als Grund für den Ausschluss von der Finanzierung durch die EU vor. Die Kommission wird weiterhin prüfen, wie das Instrumentarium am besten genutzt werden kann, auch bei der Auswahl potenzieller Begünstigter. Der Schutz des EU-Haushalts hängt auch von einer engen Zusammenarbeit und einem intensiven Informationsaustausch mit den nationalen Behörden sowie den Agenturen und Einrichtungen der EU ab.

Schutz vor Angriffen

Neben Investitionen in die Prävention von Radikalisierung besteht eine wichtige Komponente des Schutzes von Bürgerinnen und Bürger darin, die Mittel für Terroristen und andere

[80] Bis zum 31. Dezember 2024 wurden 1 426 Anordnungen zur Entfernung terroristischer Inhalte oder zur Sperrung des Zugangs zu diesen Inhalten erlassen, wobei die überwiegende Mehrheit davon dschihadistische terroristische Inhalte, aber auch rechtsextremistische terroristische Inhalte betraf.

Kriminelle einzuschränken, mit denen sie Anschläge verüben. Es müssen Maßnahmen sowohl in Bezug auf die von Terroristen verwendeten Instrumente als auch zum Schutz der von Anschlägen bedrohten Ziele ergriffen werden.

Zusätzlich zu den Maßnahmen bezüglich Feuerwaffen wird die Kommission auch die **Vorschriften** über **Ausgangsstoffe für Explosivstoffe überprüfen**, um Chemikalien mit hohem Risiko einzubeziehen. Der **öffentliche Raum** bleibt das häufigste Ziel für Terroranschläge, insbesondere durch Einzeltäter. Um die Bürgerinnen und Bürger zu schützen, wird das **EU-Sicherheitsberaterprogramm** gestärkt, um auf Ersuchen der Mitgliedstaaten und mit Mitteln des EU-Haushalts im Rahmen des Fonds für die innere Sicherheit Schwachstellenanalysen für den öffentlichen Raum, für kritische Infrastrukturen und für Hochrisikoereignisse durchzuführen. Die EU wird bestrebt sein, die verfügbaren Mittel für den Schutz des öffentlichen Raums aufzustocken. Die Kommission bietet den Behörden der Mitgliedstaaten und privaten Akteuren Unterstützung durch spezielle Orientierungshilfen und Instrumente, darunter das Wissenszentrum für den Schutz des öffentlichen Raums[81]. Seit 2020 wurden bereits 70 Mio. EUR für den Schutz des öffentlichen Raums bereitgestellt.

Die Kommission wird in Zusammenarbeit mit den lokalen Behörden und privaten Partnern zudem die Einführung des Erfordernisses für Organisationen prüfen, Sicherheitsmaßnahmen an öffentlich zugänglichen Orten zu erwägen oder zu ergreifen.

Angesichts offensichtlicher Schwachstellen wird die **Strategie der EU zur Bekämpfung von Antisemitismus und zur Förderung jüdischen Lebens (2021-2030)** weiterhin als Richtschnur für die Maßnahmen der Kommission zum Schutz der jüdischen Gemeinschaft dienen. Die Kommission wird ebenso dafür sorgen, dass geeignete Instrumente zur Verfügung stehen, um die Mitgliedstaaten bei der Bekämpfung von **Hass gegen Muslime** zu unterstützen.

Der Einsatz von **Drohnen** zu Spionagezwecken und für Angriffe stellt eine zunehmende Herausforderung für die Sicherheit dar. Die Kommission wird eine **harmonisierte Testmethode für Drohnenabwehrsysteme** entwickeln, ein **Kompetenzzentrum für die Drohnenabwehr** einrichten und prüfen, ob die Rechtsvorschriften und Verfahren der Mitgliedstaaten einer Harmonisierung bedürfen[82].

Ausländische terroristische Kämpfer

Um ausländische terroristische Kämpfer zu identifizieren, die zurückkehren oder an den EU-Außengrenzen einreisen, werden Daten über Personen benötigt, die eine terroristische Bedrohung darstellen. Zu diesem Zweck wird die Kommission gemeinsam mit Europol ihre **Zusammenarbeit mit wichtigen Drittstaaten verstärken, um biografische und biometrische Daten über Personen, die eine terroristische Bedrohung darstellen könnten** – einschließlich ausländischer terroristischer Kämpfer – zu erhalten, die dann unter uneingeschränkter Einhaltung des geltenden Rechtsrahmens der EU und der Mitgliedstaaten in das Schengener Informationssystem eingegeben werden können. Daher ist es von entscheidender Bedeutung, dass die Mitgliedstaaten alle vorhandenen Instrumente nutzen. Dazu gehören die Eingabe aller relevanten Informationen in das **SIS**, die Verbesserung der biometrischen Kontrollen und die obligatorische systematische Kontrolle aller Personen an den EU-Außengrenzen[83]. Darüber hinaus werden die von Frontex entwickelten **gemeinsamen Risikoindikatoren** die Grenzkontrollbehörden der Mitgliedstaaten weiterhin dabei

[81] Knowledge Hub on the Protection of Public Spaces.
[82] Entsprechend den wichtigsten Maßnahmen in der Mitteilung zur Drohnenabwehr von 2023 (COM(2023) 659 final).
[83] In voller Übereinstimmung mit dem Schengener Grenzkodex und der Screening-Verordnung.

unterstützen, das Risiko verdächtiger Reisen potenzieller ausländischer terroristischer Kämpfer zu ermitteln und zu bewerten.

Um sicherzustellen, dass die Mitgliedstaaten weiterhin Zugang zu **Beweismitteln aus Kampfgebieten** haben, die vom Ermittlungsteam der Vereinten Nationen zur Förderung der Rechenschaftspflicht für von ISIL (Da'esh) begangene Verbrechen (United Nations Investigative Team to Promote Accountability for Crimes Committed by Da'esh/ISIL, UNITAD) für die Strafverfolgung ausländischer terroristischer Kämpfer gesammelt wurden, wird die Kommission gemeinsam mit Eurojust die Möglichkeit prüfen, diese Beweismittel in der Eurojust-Datenbank für Beweismittel für Kernverbrechen des Völkerstrafrechts zu speichern. Darüber hinaus werden die Justizbehörden der Mitgliedstaaten durch das neue **Justizielle Terrorismusregister** weiterhin dabei unterstützt, grenzüberschreitende Verbindungen in Terrorismusfällen schnell aufzudecken.

Zentrale Maßnahmen

Die Kommission wird

- **im Jahr 2025 eine neue EU-Agenda zur Prävention und Bekämpfung von Terrorismus und gewaltbereitem Extremismus annehmen;**
- **im Jahr 2025 mit dem Westbalkan einen neuen Gemeinsamen Aktionsplan zur Prävention und Bekämpfung von Terrorismus und gewaltorientiertem Extremismus unterzeichnen;**
- **ein neues umfassendes Präventionsinstrumentarium mit dem EU-Wissenszentrums entwickeln;**
- **im Jahr 2026 die Anwendung der Verordnung zur Bekämpfung terroristischer Online-Inhalte bewerten;**
- **im Jahr 2025 das EU-Krisenprotokoll ändern;**
- **im Jahr 2026 einen Legislativvorschlag zur Überarbeitung der Verordnung über die Vermarktung und Verwendung von Ausgangsstoffen für Explosivstoffe vorlegen;**
- **die Machbarkeit eines neuen EU-weiten Systems zur Verfolgung von Terrorismusfinanzierung prüfen.**

Die Mitgliedstaaten werden nachdrücklich aufgefordert,

- **die biometrischen Kontrollen zu verbessern und obligatorische systematische Kontrollen an den EU-Außengrenzen durchzuführen;**
- **das Europäischen Justizielle Terrorismusregister in vollem Umfang zu nutzen.**

7. Die EU als starker globaler Akteur im Bereich Sicherheit

Um die Sicherheit in der EU zu erhöhen, werden wir die operative Zusammenarbeit durch Partnerschaften mit wichtigen Regionen wie unseren Erweiterungs- und Nachbarschaftspartnern, Lateinamerika und dem Mittelmeerraum stärken. Die Sicherheitsinteressen der EU werden bei der internationalen Zusammenarbeit berücksichtigt, unter anderem durch die Nutzung von Werkzeugen und Instrumenten der EU.

Die letzten Jahre haben gezeigt, dass die äußere und die innere Sicherheit der EU untrennbar miteinander verbunden sind. Der Angriffskrieg Russlands gegen die Ukraine, der Konflikt im Gazastreifen, die Lage in Syrien und sich abzeichnende Konflikte weltweit haben schwerwiegende Ausstrahlungseffekte auf die innere Sicherheit der EU. Um den Auswirkungen der globalen Instabilität auf ihre innere Sicherheit entgegenzuwirken, **muss die EU ihre**

Sicherheitsinteressen aktiv verteidigen, indem sie Bedrohungen von außen angeht, die Menschenhandelsrouten unterbricht und Korridore von strategischem Interesse wie etwa Handelsrouten schützt. Gleichzeitig wird die EU ihren Partnerländern weiterhin ein starker Verbündeter sein und gemeinsam mit ihnen daran arbeiten, die globale Sicherheit zu erhöhen und die gegenseitige Widerstandsfähigkeit gegenüber Bedrohungen zu stärken.

In den letzten Jahren hat die EU bedeutende Schritte zur Verbesserung der sicherheitspolitischen Zusammenarbeit unternommen. Sie hat operative Abkommen über Strafverfolgung und justizielle Zusammenarbeit sowie andere Arten von Vereinbarungen mit Partnerländern geschlossen. Sie setzt sich aktiv für weitere internationale Abkommen im Einklang mit den Verhandlungsrichtlinien des Rates und für Initiativen zum Kapazitätsaufbau ein, die von den Agenturen und Einrichtungen der EU unterstützt werden. Von entscheidender Bedeutung für die Stärkung der Sicherheit mit Partnerländern ist auch das Instrument für Nachbarschaft, Entwicklungszusammenarbeit und internationale Zusammenarbeit – Europa in der Welt.

Die **regelbasierte multilaterale Ordnung** ist ein Eckpfeiler für die Stärkung der globalen Sicherheit. Sicherheitsdialoge, einschließlich thematischer Dialoge, sind zur Unterstützung dieser Bemühungen wesentlich. Die Umsetzung des **Strategischen Kompasses für Sicherheit und Verteidigung** und bilateraler und multilateraler Kooperationsrahmen wie Stabilisierungs- und Assoziierungsabkommen und Assoziierungsabkommen sowie die Zusammenarbeit mit Organisationen wie den Vereinten Nationen und der NATO sind für die Entwicklung wirksamer Sicherheitslösungen von zentraler Bedeutung. Die EU wird weiterhin ihren Beitrag in multilateralen Foren[84] leisten und ihre Zusammenarbeit mit einschlägigen internationalen und regionalen Organisationen und Rahmen wie der NATO, den Vereinten Nationen, dem Europarat, Interpol, der G7, der Organisation für Sicherheit und Zusammenarbeit in Europa und der Zivilgesellschaft intensivieren.

Regionale Zusammenarbeit

Die Fortsetzung der unerschütterlichen Unterstützung der **Ukraine** durch die EU und die Stärkung der Sicherheit und Widerstandsfähigkeit der **Erweiterungsländer der EU** sind vorrangige politische und geostrategische Erfordernisse. Die Unterstützung der Sicherheit der EU sollte einhergehen mit der **beschleunigten Integration der Bewerberländer** in die **Sicherheitsarchitektur der EU**, parallel zur Konsolidierung ihrer regionalen Zusammenarbeit. Die Kommission wird die Erweiterungspolitik der EU nutzen, um die Fähigkeit der Bewerberländer und möglichen Bewerberländer zu unterstützen, auf Bedrohungen zu reagieren, die operative Zusammenarbeit und den Informationsaustausch zu verstärken und die Angleichung an die Grundsätze, Rechtsvorschriften und Instrumente der EU sicherzustellen. Das Instrument für Heranführungshilfe (Instrument for Pre-accession Assistance, IPA III) sowie die Ukraine-Fazilität, die Reform- und Wachstumsfazilität für Moldau und die Reform- und Wachstumsfazilität für den Westbalkan sind für die Stärkung der Sicherheit sowohl in den Bewerberländer als auch in den möglichen Bewerberländern von entscheidender Bedeutung.

Die EU wird auch die **Nachbarschaftspartner** weiter in die Sicherheitsarchitektur der EU integrieren. Im Rahmen des **neuen Pakts für den Mittelmeerraum** und des anstehenden **Strategischen Ansatzes für den Schwarzmeerraum** wird die Union darauf hinarbeiten, die regionale Zusammenarbeit und bilaterale umfassende strategische Partnerschaften mit einer Sicherheitsdimension auszubauen, gegebenenfalls mit regelmäßigen hochrangigen Sicherheitsdialogen. Die operative Zusammenarbeit mit Nordafrika, dem **Nahen Osten und**

[84] Globales Forum „Terrorismusbekämpfung“, internationale Allianz gegen Da’esh, Globales Internetforum zur Bekämpfung des Terrorismus, Christchurch Call Foundation, Globale Koalition zur Bewältigung der Gefahren durch synthetische Drogen (Global Coalition to Address Synthetic Drug Threats).

den Golfstaaten wird verstärkt, vor allem in den Bereichen Terrorismusbekämpfung, Bekämpfung der Geldwäsche, des Handels mit Feuerwaffen sowie der Herstellung von und des Handels mit Drogen, insbesondere Captagon**.**

Um der Zunahme terroristischer und krimineller Aktivitäten und ihren potenziellen Ausstrahlungseffekten in **Subsahara-Afrika, insbesondere in der Sahelzone, am Horn von Afrika und in Westafrika**, entgegenzuwirken, wird die EU die Afrikanische Union, die regionalen Wirtschaftsgemeinschaften und die Länder in der Region stärker unterstützen. Im Einklang mit der EU-Strategie für maritime Sicherheit[85] wird die EU die Zusammenarbeit im **Golf von Guinea, im Roten Meer und im Indischen Ozean** bei der Bekämpfung von Menschenhandel und Piraterie verstärken, indem sie die innerafrikanische und regionale Zusammenarbeit unterstützt; dabei erhält sie Hilfe durch die koordinierten maritimen Präsenzen der EU und das Operationszentrum für den Kampf gegen den Drogenhandel im Atlantik.

Mit **Lateinamerika und der Karibik** wird die EU ihre operative Zusammenarbeit verstärken, um kriminelle Netze mit hohem Risikopotenzial zu zerschlagen und strafrechtlich zu verfolgen sowie illegale Aktivitäten zu stoppen und Schmuggelrouten zu unterbrechen, indem sie die Kooperationsrahmen, darunter der Lateinamerikanische Ausschuss für innere Sicherheit und der Mechanismus zur Koordinierung und Zusammenarbeit im Bereich der Drogenbekämpfung, verbessert. Zu den Prioritäten werden die Resilienz von Logistikknotenpunkten und Partnerschaften sowie der Grundsatz „Follow the money“ gehören. Die EU wird die Entwicklung der amerikanischen Polizeigemeinschaft (AMERIPOL) weiter unterstützen, damit diese zum regionalen Pendant von Europol wird und die justizielle Zusammenarbeit der Mitgliedstaaten und in der Region gestärkt wird. Die EU wird auch mit **Süd- und Zentralasien** bei gemeinsamen sicherheitspolitischen Herausforderungen im Zusammenhang mit Terrorismus, illegalem Warenhandel einschließlich Drogen, Menschenhandel und Schleuserkriminalität zusammenarbeiten.

Darüber hinaus wird die EU regionale Kooperationsrahmen in Drittstaaten unterstützen, um diese im Einklang mit dem Grundsatz der gemeinsamen Verantwortung für die gesamte kriminelle Lieferkette bei der Unterbindung des illegalen Handels an der Quelle weiter zu unterstützen. Weiter wird die EU ihren Teil dazu beitragen, die Sicherheit von Logistikknotenpunkten im Ausland zu verbessern, indem sie **gemeinsame Inspektionen in Häfen in Drittstaaten** koordiniert.

Operative Zusammenarbeit

Im Rahmen von **Global Gateway** werden nachhaltige und hochwertige Infrastrukturprojekte in den Bereichen Digitales, Klima und Energie, Verkehr, Gesundheit, Bildung und Forschung gefördert. Bei Investitionen im Rahmen von Global Gateway wird die Kommission jetzt Sicherheitserwägungen berücksichtigen, sofern dies angezeigt ist. Dazu gehören Initiativen, die für die strategische Autonomie der EU und ihrer Partnerländer von entscheidender Bedeutung sind, z. B. Infrastrukturprojekte, die Sicherheitsbewertungen und Risikominderungsmaßnahmen umfassen.

Die Kommission wird weitere **Abkommen zwischen der EU und Drittstaaten über die Zusammenarbeit mit Europol und Eurojust** anstreben, insbesondere mit lateinamerikanischen Ländern.

Darüber hinaus ist die proaktive Beteiligung von Nicht-EU-Ländern an **EMPACT** eines der wirksamsten Mittel zur Stärkung der operativen Zusammenarbeit. Die EU wird die Beteiligung von Drittstaaten, insbesondere von Ländern des Westbalkans, der östlichen Nachbarschaft, in

[85] JOIN(2023) 8 final.

Subsahara-Afrika, in Nordafrika, im Nahen Osten, in Lateinamerika und in der Karibik, in diesem Rahmen weiter fördern. Ein weiteres Instrument zur Intensivierung der Zusammenarbeit mit Drittstaaten bei der Kriminalitätsbekämpfung sind die von Europol koordinierten operativen Taskforces zwischen den Mitgliedstaaten, an denen auch Drittländer teilnehmen können. Die Kommission strebt außerdem den Abschluss der Verhandlungen über das internationale Abkommen **zwischen der EU und Interpol**[86] an, um einen einheitlicheren Ansatz für das Vorgehen gegen globale Sicherheitsbedrohungen und die Bekämpfung der grenzüberschreitenden Kriminalität zu gewährleisten.

Im Rahmen des „Team Europa"-Konzepts muss die Union Präsenz vor Ort zeigen. Spezialisierte Bedienstete der Union und der Mitgliedstaaten spielen eine entscheidende Rolle, wenn es darum geht, sicherzustellen, dass die Union in ihrem auswärtigen Handeln hinreichend fundiert, koordiniert und reaktionsfähig vorgeht. Um diesen Ansatz eine Stufe weiter zu bringen, wird die Kommission mit Unterstützung der Hohen Vertreterin für die Außen- und Sicherheitspolitik die **Verbindungsnetze** stärken und die Entsendung regionaler **Verbindungsbeamter von Europol und Eurojust** entsprechend den operativen Erfordernissen der Mitgliedstaaten erleichtern.

Die EU wird sich für eine engere operative Zusammenarbeit in den Bereichen Strafverfolgung und justizielle Zusammenarbeit einsetzen sowie den Informationsaustausch in Echtzeit und gemeinsame Aktionen durch **gemeinsame Ermittlungsgruppen** in Drittstaaten mit Unterstützung von Europol und Eurojust fördern. Die Kommission wird die Mitgliedstaaten auch bei der Einrichtung **gemeinsamer Verbindungszentren** unterstützen, in denen Fachleute und Bedienstete der örtlichen Strafverfolgungsbehörden in strategischen Drittstaaten zusammenkommen.

Instrumente der Gemeinsamen Außen- und Sicherheitspolitik (GASP)

Auch die **Missionen im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP)** werden entsprechend den vom Rat festgelegten Mandaten in vollem Umfang genutzt, um externe Bedrohungen für die innere Sicherheit der EU besser zu erkennen und zu bekämpfen. Zum Kapazitätsaufbau in Drittstaaten werden die Hohe Vertreterin für die Außen- und Sicherheitspolitik und die Kommission GSVP-Maßnahmen mit speziellen Finanzierungsinstrumenten unterstützen und alle geeigneten Finanzierungsmöglichkeiten ausloten.

Restriktive Maßnahmen der EU sind ein bewährtes Instrument der GASP, das auch im Kampf gegen den Terrorismus eingesetzt wird. Auf der Grundlage von Vorschlägen der Hohen Vertreterin für die Außen- und Sicherheitspolitik, der Mitgliedstaaten oder der Kommission könnte der Rat prüfen, wie die bestehenden eigenständigen restriktiven EU-Maßnahmen (EU-Terroristenliste) wirksamer, operativer und flexibler gestaltet werden könnten. Darüber hinaus könnte der Rat erwägen, im Einklang mit den Zielen der GASP zusätzliche restriktive Maßnahmen gegen kriminelle Netze zu prüfen.

Visumpolitik und Informationsaustausch

Durch die Kontrolle der Einreise in die EU und die Festlegung der entsprechenden Bedingungen ist die Visumpolitik der EU ein wichtiges Instrument für die Zusammenarbeit mit Drittstaaten und die Sicherung unserer Grenzen. Im Rahmen der anstehenden Strategie für eine EU-Visumpolitik wird die Kommission **Sicherheitserwägungen** vollständig **in die Visumpolitik der EU** einbeziehen. Die Kommission wird mit den beiden gesetzgebenden Organen zusammenarbeiten, um den Vorschlag zur Überarbeitung und Straffung des Visa-

[86] Beschluss (EU) 2021/1312 des Rates vom 19. Juli 2021 und Beschluss (EU) 2021/1313 des Rates vom 19. Juli 2021.

Aussetzungsmechanismus anzunehmen, insbesondere für bestimmte Fälle des Missbrauchs der Regelung für visumfreies Reisen[87]. Drittstaaten werden dazu angehalten, Informationen über Personen, die eine Sicherheitsbedrohung darstellen könnten, weiterzugeben, damit diese in EU-Informationssysteme und -Datenbanken eingegeben werden können.

Um politische Koordinierung und vorgelagerte Maßnahmen zu erzielen und eine effizientere, schnellere und reibungslosere Zusammenarbeit zu ermöglichen, wird die Kommission auf die Festlegung von **Regelungen für den Datenfluss** hinarbeiten und Möglichkeiten zur **Verbesserung des Informationsaustauschs** zu Strafverfolgungs- und Grenzmanagementzwecken mit vertrauenswürdigen Drittstaaten unter Einhaltung der Grundrechte und Datenschutzvorschriften ausloten.

Zentrale Maßnahmen

Die Kommission wird

- **internationale Abkommen zwischen der EU und vorrangigen Drittstaaten über die Zusammenarbeit mit Europol und Eurojust abschließen;**
- **die Beteiligung von Partnerländern an EMPACT zur Bekämpfung der organisierten Kriminalität und des Terrorismus fördern;**
- **die Agenturen und Einrichtungen der EU bei der Schaffung und Stärkung von Arbeitsvereinbarungen mit Partnerländern unterstützen;**
- **Sicherheitserwägungen in der EU-Visumpolitik durch die anstehende Strategie für eine EU-Visumpolitik weiter berücksichtigen;**
- **den Informationsaustausch zu Strafverfolgungs- und Grenzmanagementzwecken mit vertrauenswürdigen Drittländern stärken.**

In Zusammenarbeit mit der Hohen Vertreterin der Union für die Außen- und Sicherheitspolitik wird die Kommission

- **zivile Missionen im Rahmen der GSVP in vollem Umfang nutzen;**
- **bis 2027 gemeinsame Inspektionen in Häfen von Drittstaaten koordinieren.**

In Zusammenarbeit mit der Hohen Vertreterin der Union für die Außen- und Sicherheitspolitik und den Mitgliedstaaten wird die Kommission

- **die Verbindungsnetze und die Zusammenarbeit im Rahmen des Konzepts „Team Europa“ stärken;**
- **ab 2025 gemeinsame Einsatzteams und Verbindungszentren in Drittstaaten einrichten.**

Das Europäische Parlament und der Rat werden ausdrücklich aufgefordert,

- **die Verhandlungen über die Überarbeitung des Visa-Aussetzungsmechanismus abzuschließen.**

8. Fazit

In einer von Unsicherheit geprägten Welt muss die Fähigkeit der Union, Sicherheitsbedrohungen vorherzusehen, zu verhindern und darauf zu reagieren, verbessert werden.

[87] COM(2023) 642.

Es reicht nicht aus, erst dann auf Krisen zu reagieren, wenn sie auftreten. Wir müssen unser Bewusstsein schärfen und uns ein vollständiges Bild von den Bedrohungen machen, noch während sie entstehen. Und wir müssen sicherstellen, dass unsere Instrumente und Fähigkeiten der Aufgabe gerecht werden.

Das umfassende Maßnahmenpaket, so wie es in dieser Strategie dargelegt ist, wird dazu beitragen, eine stärkere Union in der Welt zu schaffen: eine Union, die in der Lage ist, ihre eigenen Sicherheitsbedürfnisse rechtzeitig wahrzunehmen, entsprechend zu planen und sich um diese Bedürfnisse zu kümmern; die wirksam auf Bedrohungen ihrer inneren Sicherheit reagieren und Täter zur Rechenschaft ziehen kann und die ihre offenen, freien und florierenden Gesellschaften und Demokratien schützt.

Dies erfordert eine Änderung unserer Denkweise in Bezug auf die innere Sicherheit. Wir werden uns für die Förderung einer neuen EU-Sicherheitskultur einsetzen, in der Sicherheitserwägungen in all unseren Rechtsvorschriften, Strategien und Programmen – von der Konzeption bis zur Umsetzung – berücksichtigt werden. Und in der die Zusammenarbeit über Politikbereiche hinweg es uns ermöglicht, neue Wege zu beschreiten.

Dies ist nicht die Aufgabe eines einzelnen Organs, einer einzelnen Regierung oder eines einzelnen Akteurs. Es ist ein gemeinsames Unterfangen Europas.