EUROPÄISCHE
KOMMISSION

Brüssel, den 24.7.2020
COM(2020) 605 final

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

EU-Strategie für eine Sicherheitsunion

I. Einleitung

Die Kommission hat in ihren politischen Leitlinien klargestellt, dass wir für den Schutz unserer Bürgerinnen und Bürger nichts unversucht lassen dürfen. Innere und äußere Sicherheit sind nicht nur das Fundament für die persönliche Sicherheit, sondern auch für den Schutz der Grundrechte und eine Voraussetzung für das Vertrauen in unsere Wirtschaft, unsere Gesellschaft und unsere Demokratie sowie für deren Eigendynamik. Europäerinnen und Europäer erleben heute ein sich wandelndes Sicherheitsumfeld, geprägt durch immer neue Bedrohungen, aber auch durch Faktoren wie den Klimawandel, demografische Trends und die politische Instabilität jenseits unserer Grenzen. Globalisierung, Freizügigkeit und digitaler Wandel bringen nach wie vor Wohlstand, erleichtern unser Leben und fördern Innovation und Wachstum. Diese Vorteile gehen jedoch mit Risiken und Kosten einher. Terrorismus, organisiertes Verbrechen sowie Drogen- und Menschenhandel sind eine konkrete Gefahr und bedrohen unmittelbar die Bürgerinnen und Bürger sowie unsere europäische Lebensweise. Cyberangriffe und Cyberkriminalität nehmen weiter zu. Zudem werden die Sicherheitsbedrohungen immer komplexer: Gründe und begünstigende Umstände sind die Möglichkeit, grenzüberschreitend zu arbeiten, und die Vernetzung, das Verschwimmen der Grenzen zwischen der physischen und der virtuellen Welt, die gezielte Ansprache anfälliger Gruppen sowie die Nutzung sozialer und wirtschaftlicher Unterschiede. Angriffe können zu jedem Moment erfolgen und wenig oder gar keine Spuren hinterlassen;, und sowohl staatliche als auch nichtstaatliche Akteure können eine Vielzahl hybrider Bedrohungen einsetzen[1] Ereignisse außerhalb der EU können sich zudem massiv auf die Sicherheit innerhalb der EU auswirken.

Durch die COVID-19-Krise hat sich auch unser Verständnis von Sicherheitsbedrohungen und einer entsprechenden Sicherheitspolitik gewandelt. Die Krise hat besonders deutlich zu Tage gebracht, wie wichtig es ist, sowohl in physischen als auch in digitalen Umgebungen die Sicherheit zu gewährleisten. Sie hat auch verdeutlicht, wie wichtig eine offene strategische Autonomie für unsere Lieferketten bei kritischen Produkten, Dienstleistungen, Infrastrukturen und Technologien ist. Es ist deshalb umso notwendiger, jeden Sektor und jede Einzelperson in ein gemeinsames Vorhaben einzubinden, damit die EU vor allem besser vorbereitet und widerstandsfähiger ist, ihr aber auch bessere Instrumente zu Verfügung stehen, wenn sie handeln muss.

Einzeln können die Mitgliedstaaten den Schutz der Bürgerinnen und Bürger nicht gewährleisten. Nie kam es mehr darauf an, dass wir zusammenarbeiten und unsere Stärken bündeln, und nie hatte die EU ein größeres Potenzial, um mehr zu erreichen. Sie kann mit gutem Beispiel vorangehen, indem sie ihr Krisenmanagementsystem insgesamt verbessert und innerhalb wie außerhalb ihrer Grenzen zur globalen Stabilität beiträgt. Zwar sind für die Sicherheit in erster Linie die Mitgliedstaaten verantwortlich, doch hat sich in den letzten Jahren ein immer größeres Verständnis dafür herausgebildet, dass die Sicherheit eines Mitgliedstaates die Sicherheit aller ist. Die EU kann multidisziplinäre und integrierte

[1] Hybride Bedrohungen werden unterschiedlich definiert, es geht jedoch immer darum, die Verbindung von Zwang und Unterwanderung und von konventionellen und unkonventionellen Methoden (diplomatischer, militärischer, wirtschaftlicher oder technologischer Natur) zu erfassen, auf die staatliche oder nichtstaatliche Akteure in koordinierter Weise zurückgreifen können, um bestimmte Ziele zu verfolgen (ohne dabei die Schwelle eines offiziell erklärten Kriegs zu erreichen). Siehe JOIN(2016) 18 final.

Maßnahmen ergreifen, um die Sicherheitsakteure in den Mitgliedstaaten mit den von ihnen benötigten Instrumenten und Informationen zu unterstützen.[2]

Die EU kann auch dafür Sorge tragen, dass die Sicherheitspolitik weiter in unseren gemeinsamen europäischen Werten – Einhaltung und Aufrechterhaltung von Rechtsstaatlichkeit, Gleichheit[3] und Grundrechten sowie Gewährleistung von Transparenz, Rechenschaftspflicht und demokratischer Kontrolle – verankert ist, und so die richtige Vertrauensbasis für politische Maßnahmen schaffen. Sie kann eine wirksame und echte Sicherheitsunion aufbauen, in der die Rechte und Freiheiten des Einzelnen gut geschützt sind. Sicherheit und Achtung der Grundrechte sind keine widersprüchlichen Ziele, sondern stehen miteinander in Einklang und ergänzen einander. Unsere Werte und Grundrechte müssen die Grundlage der Sicherheitspolitik bilden; dabei müssen die Grundsätze der Notwendigkeit, der Verhältnismäßigkeit und der Rechtmäßigkeit unter Wahrung der Rechenschaftspflicht und Rechtsbehelfe gewährleistet sein, und es müssen wirksame Maßnahmen zum Schutz des Einzelnen, vor allem von besonders schutzbedürftigen Personen, möglich sein.

Es gibt bereits einschlägige rechtliche, praktische und unterstützende Instrumente, die allerdings gestärkt und besser angewandt werden müssen. In Bezug auf einen besseren Informationsaustausch und die nachrichtendienstliche Zusammenarbeit mit den Mitgliedstaaten sowie das Verengen des Handlungsspielraums für Terroristen und Straftäter wurden bereits – trotz Fragmentierung – große Fortschritte erzielt.

Die Arbeiten müssen aber auch über die Grenzen der EU hinausgehen. Beim Schutz der Union und ihrer Bürger geht es nicht mehr nur um die Gewährleistung der Sicherheit innerhalb der EU-Grenzen, sondern auch um die Bewältigung der externen Dimension der Sicherheit. Der Ansatz der EU für die äußere Sicherheit im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik (GASP) und der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) wird ein wesentlicher Bestandteil der Bemühungen der EU um mehr Sicherheit in der EU bleiben. Die Zusammenarbeit mit Drittländern und auf globaler Ebene zur Bewältigung gemeinsamer Herausforderungen ist für eine wirksame und umfassende Reaktion von zentraler Bedeutung, denn die Stabilität und Sicherheit in der Nachbarschaft spielt für die Sicherheit der EU eine zentrale Rolle.

Die neue Strategie, die auf den Arbeiten des Europäischen Parlaments[4], des Rates[5] und der Kommission[6] aufbaut, zeigt, dass eine echte und effiziente Sicherheitsunion einen starken Kern aus Instrumenten und politischen Maßnahmen benötigt, um die Sicherheit in der Praxis gewährleisten zu können, wobei gleichzeitig klar sein muss, dass Sicherheitsfragen

---

[2] Beispielsweise durch die Dienste des Weltraumprogramms der EU, etwa des Programms Copernicus, das Erdbeobachtungsdaten und Anwendungen für die Grenzüberwachung, die maritime Sicherheit, die Strafverfolgung, die Bekämpfung der Piraterie, die Abschreckung von Drogenschmugglern und das Notfallmanagement liefert.

[3] Eine Union der Gleichheit: Strategie für die Gleichstellung der Geschlechter 2020-2025, COM(2020) 152.

[4] Beispielsweise die Arbeit des Sonderausschusses Terrorismus (TERR) des Europäischen Parlaments, der im November 2018 Bericht erstattet hat.

[5] Sie beginnen bei den Schlussfolgerungen des Rates vom Juni 2015 zur „erneuerten Strategie der inneren Sicherheit der Europäischen Union“ und reichen bis zu den Ergebnissen der Ratstagung im Dezember 2019.

[6] „Umsetzung der Europäischen Sicherheitsagenda im Hinblick auf die Bekämpfung des Terrorismus und die Weichenstellung für eine echte und wirksame Sicherheitsunion“, COM(2016) 230 final vom 20.4.2016. Siehe die jüngste Bewertung der Umsetzung der Rechtsvorschriften im Bereich der inneren Sicherheit: Implementation of Home Affairs legislation in the field of internal security (Umsetzung der Rechtsvorschriften im Bereich Inneres im Bereich der inneren Sicherheit) - 2017-2020 (SWD(2020) 135).

Auswirkungen auf alle Bereiche der Gesellschaft und der öffentlichen Politik haben. Die EU muss ein sicheres Umfeld für alle gewährleisten, unabhängig von Rasse, ethnischer Herkunft, Religion, Glauben, Geschlecht, Alter oder sexueller Orientierung.

Die hier dargelegte Strategie erstreckt sich auf den Zeitraum 2020-2025 und konzentriert sich auf den Aufbau von Fähigkeiten und Kapazitäten zur Gewährleistung eines zukunftsfähigen Sicherheitsumfelds. Sie skizziert ein gesamtgesellschaftliches Sicherheitskonzept, mit dem wirksam und koordiniert auf eine sich rasch wandelnde Bedrohungslandschaft reagiert werden kann. Außerdem werden strategische Prioritäten und die entsprechenden Maßnahmen festgelegt, um digitale und physische Risiken auf integrierte Weise im gesamten Gefüge der Sicherheitsunion anzugehen, wobei der Schwerpunkt auf den Bereichen liegt, in denen die EU einen zusätzlichen Nutzen bringen kann. Ziel ist es, einen Sicherheitsgewinn zu bieten, damit jeder in der EU geschützt wird.

II. Eine sich rasch wandelnde Bedrohungslage in Europa

Innere und äußere Sicherheit ist eine Voraussetzung für die persönliche Sicherheit, den Wohlstand und das Wohlergehen der Bürgerinnen und Bürger. Die Bedrohung dieser Sicherheit hängt davon ab, in welchem Maße das Leben und die Existenzgrundlagen der Bürgerinnen und Bürger gefährdet sind. Je größer die Anfälligkeit, desto größer ist das Risiko, dass sie ausgenutzt werden kann. Sowohl die Anfälligkeit als auch die Gefahren entwickeln sich ständig weiter, sodass die EU flexibel handeln muss.

In unserem täglichen Leben brauchen wir eine Vielzahl von Dienstleistungen in Bereichen Energie, Verkehr, Finanzen und Gesundheit. Für die Erbringung dieser Dienstleistung ist sowohl eine physische als auch eine digitale Infrastruktur erforderlich, was sie anfälliger macht und das Potenzial für Störungen erhöht. Während der COVID-19-Pandemie haben die neuen Technologien es vielen Unternehmen und öffentlichen Diensten ermöglicht, ihren Betrieb aufrechtzuerhalten bzw. ihre Arbeit fortzusetzen, indem sie beispielsweise über Telearbeit miteinander verbunden blieben oder die Logistik der Lieferketten weiter funktionierte. Dies hat jedoch auch zu einer außergewöhnlichen Zunahme böswilliger Angriffe geführt, bei denen versucht wurde, die Störungen bzw. Unterbrechungen aufgrund der Pandemie und den Übergang zur digitalen Heimarbeit für kriminelle Zwecke auszunutzen.[7] Engpässe in der Warenversorgung haben neue Einfallstore für das organisierte Verbrechen geschaffen. Die Folgen hätten fatal sein können, wenn unerlässliche Gesundheitsdienste zurzeit der stärksten Belastung gestört worden wären.

Da digitale Technologien unserem Leben auf immer vielfältigere Weise zugutekommen, hat auch die Frage der **Cybersicherheit** von Technologien an strategischer Bedeutung gewonnen.[8] Haushalte, Banken, Finanzdienstleister und Unternehmen (insbesondere kleine und mittlere Unternehmen) sind von Cyberangriffen besonders stark betroffen. Der potenzielle Schaden wird durch die Interdependenz der physischen und digitalen Systeme noch weiter vervielfacht: Jede physische Beeinträchtigung zieht digitale Systeme in Mitleidenschaft, denn Cyberangriffe auf Informationssysteme und digitale Infrastrukturen

[7] Europol: Beyond the pandemic. How COVID-19 will shape the serious and organised crime landscape in the EU (Jenseits der Pandemie. Wie COVID-19 das Umfeld der schweren und organisierten Kriminalität in der EU prägen wird) (April 2020).

[8] Empfehlung der Kommission zur Cybersicherheit von 5G-Netzen, C(2019) 2335; Mitteilung „Sichere 5G-Einführung in der EU – Umsetzung des EU-Instrumentariums“, COM(2020) 50.

können grundlegende Dienste völlig lahmlegen.[9] Die zunehmende Bedeutung des Internets der Dinge und der verstärkte Einsatz künstlicher Intelligenz werden neuen Nutzen, aber auch neue Risiken mit sich bringen.

Unsere Welt ist ohne digitale Infrastrukturen, Technologien und Online-Systeme nicht mehr denkbar. Sie ermöglichen es uns, Unternehmen zu gründen, Produkte zu konsumieren und Dienstleistungen in Anspruch zu nehmen. Und alle beruhen auf Kommunikation und Interaktion. Durch die Online-Abhängigkeit wurde einer Welle der **Cyberkriminalität** ausgelöst.[10] Das Phänomen „Cybercrime as a service“ und die cyberkriminelle Schattenwirtschaft ermöglichen einen einfachen Online-Zugang zu Produkten und Dienstleistungen der Cyberkriminalität. Straftäter passen sich rasch an neue Technologien an und nutzen sie für ihre Zwecke. So haben nachgeahmte und verfälschte Medikamente die legale Lieferkette für Arzneimittel infiltriert.[11] Die exponentielle Zunahme von Darstellungen des sexuellen Missbrauchs von Kindern im Internet[12] hat gezeigt, welche sozialen Folgen Veränderungen krimineller Muster haben können. Eine kürzlich durchgeführte Umfrage ergab, dass die meisten Menschen in der EU (55 %) besorgt darüber sind, dass Straftäter und Betrüger auf ihre Daten zugreifen könnten.[13]

Auch das **globale Umfeld** verstärkt diese Bedrohungen. Die selbstbewusste Industriepolitik von Drittländern sowie der fortlaufende, durch das Internet begünstigte Diebstahl geistigen Eigentums verändern die strategischen Paradigmen für den Schutz und die Förderung europäischer Interessen. Die Zunahme der Anwendungen mit doppeltem Verwendungszweck verdeutlichen dies ebenfalls, da ein starker ziviler Technologiesektor nun auch bedeutende Vorteile für die Fähigkeiten im Bereich Verteidigung und Sicherheit bringt. Industriespionage hat erhebliche Auswirkungen auf die Wirtschaft, die Beschäftigung und das Wachstum in der EU: Der Cyberdiebstahl von Geschäftsgeheimnissen kostet die EU geschätzte 60 Mrd. EUR pro Jahr.[14] Dies erfordert ein gründliches Nachdenken darüber, was Abhängigkeiten und die zunehmende Gefährdung durch Cyberbedrohungen für die Fähigkeit der EU bedeuten, Einzelpersonen und Unternehmen gleichermaßen zu schützen.

Die COVID-19-Krise hat auch deutlich gemacht, wie soziale Unterschiede und Unsicherheiten zu Sicherheitsdefiziten führen. Dies erhöht das Potenzial für komplexe und

---

[9] Im März 2020 war das Universitätskrankenhaus im tschechischen Brünn Opfer eines Cyberangriffs, sodass Patienten verlegt und Operationen verschoben werden mussten (siehe hierzu Europol: Pandemic Profiteering. How criminals exploit the COVID-19 crisis - Profit aus der Pandemie: Wie Kriminelle die COVID-19-Krise ausnutzen). Künstliche Intelligenz kann für digitale, politische und physische Angriffe sowie für Überwachungszwecke missbraucht werden. Die Erhebung von Daten über das Internet der Dinge kann für die Überwachung von Personen (mithilfe von intelligenten Uhren, virtuellen Assistenten usw.) genutzt werden.

[10] Prognosen zufolge werden die jährlichen Kosten durch Datenschutzverletzungen von 3 Billionen US-Dollar im Jahr 2015 auf 5 Billionen im Jahr 2024 steigen (Juniper Research, The Future of Cybercrime & Security (die Zukunft der Cyberkriminalität und der Sicherheit)).

[11] Nach Schätzungen einer Studie von 2016 (Legiscript) operieren weltweit nur 4 % der Internetapotheken legal, wobei die 30 000 bis 35 000 illegalen Online-Apotheken in erster Linie Verbraucher aus der EU anvisieren.

[12] EU-Strategie für eine wirksamere Bekämpfung des sexuellen Missbrauchs von Kindern, COM(2020) 607.

[13] Agentur der Europäischen Union für Grundrechte (2020), Your rights matter: Security concerns and experiences, Fundamental Rights Survey (Ihre Rechte sind wichtig: Sicherheitsbedenken und -erfahrungen, Umfrage zu den Grundrechten), Luxemburg, Amt für Veröffentlichungen.

[14] The scale and impact of industrial espionage and theft of trade secrets through cyber (Ausmaß und Auswirkungen der Industriespionage und des Diebstahls von Geschäftsgeheimnissen über das Internet), 2018.

hybride Angriffe seitens staatlicher und nichtstaatlicher Akteure. Die Schwachstellen werden dabei durch eine Mischung aus Cyberangriffen, Beschädigungen kritischer Infrastruktur[15], Desinformationskampagnen und Radikalisierung des politischen Diskurses ausgenutzt.[16]

Gleichzeitig entwickeln sich schon länger bestehende Bedrohungen weiter. Die Zahl der **Terroranschläge** in der EU war 2019 rückläufig. Von dschihadistischen Angriffen, begangen oder inspiriert von Da'esh und Al-Qaida sowie ihren Unterorganisationen, geht jedoch nach wie vor eine große Gefahr für die Bürgerinnen und Bürger der EU aus.[17] Parallel dazu nimmt auch die Bedrohung durch den gewalttätigen Rechtsextremismus zu.[18] Rassistisch motivierte Angriffe sollten Anlass zu ernster Besorgnis geben: Die tödlichen antisemitischen Terroranschläge in Halle sind eine Mahnung, dass im Einklang mit der Erklärung des Rates von 2018 die Gegenmaßnahmen verstärkt werden müssen.[19] Jeder fünfte Mensch in der EU hat große Befürchtungen, dass es in den nächsten 12 Monaten zu einem Terroranschlag kommen könnte.[20] In ihrer überwiegenden Mehrheit waren die Terroranschläge der letzten Zeit „Low-tech"-Anschläge, die von Einzeltätern gegen Einzelpersonen im öffentlichen Raum verübt wurden, wobei die terroristische Propaganda im Internet mit dem Livestreaming der Anschläge von Christchurch an neuer Bedeutung gewonnen hat.[21] Die Bedrohung durch radikalisierte Personen ist nach wie vor hoch – und könnte sich durch aus dem Ausland zurückkehrende terroristische Kämpfer und aus dem Gefängnis entlassene Extremisten verstärken.[22]

Die Krise hat ebenfalls gezeigt, wie sich bestehende Bedrohungen unter neuen Umständen weiterentwickeln können. **Organisierte kriminelle Gruppen** haben die Engpässe in der Warenversorgung für die Schaffung neuer illegaler Märkte genutzt. Der Handel mit illegalen Drogen ist nach wie vor der größte kriminelle Markt in der EU, auf dem jährlich ein geschätzter Umsatz von 30 Mrd. EUR (Endkundenpreis) erwirtschaftet wird.[23]. Der Menschenhandel geht ebenfalls weiter: Schätzungen zufolge werden mit den verschiedenen Formen der Ausbeutung weltweit jährliche Profite von insgesamt 30 Mrd. EUR erzielt.[24] Der internationale Handel mit nachgeahmten Arzneimitteln erreichte einen Wert von

---

15 Kritische Infrastrukturen sind für wichtige gesellschaftliche Funktionen, die Gesundheit, die Sicherheit, das wirtschaftliche und das soziale Wohlergehen von wesentlicher Bedeutung; ihre Störung oder Zerstörung hat erhebliche Auswirkungen (Richtlinie 2008/114/EG des Rates).

16 97 % der EU-Bürgerinnen und Bürger waren bereits mit Falschmeldungen konfrontiert, 38 % haben täglich mit ihnen zu tun. Siehe JOIN(2020) 8 final.

17 13 EU-Mitgliedstaaten meldeten insgesamt 119 vollendete, fehlgeschlagene oder vereitelte Terroranschläge mit insgesamt zehn Todesopfern und 27 Verletzten (Europol, Tendenz- und Lagebericht der Europäischen Union über den Terrorismus, 2020).

18 2019 wurden sechs rechtsgerichtete Terroranschläge gezählt (einer vollendet, einer fehlgeschlagen, vier vereitelt, drei betroffene Mitgliedstaaten), 2018 dagegen nur einer, wobei in Vorfällen, die nicht als Terroranschläge eingestuft wurden, noch weitere Menschen zu Tode kamen (Europol, 2020).

19 Siehe auch die Erklärung des Rates zur Bekämpfung von Antisemitismus und zur Entwicklung eines gemeinsamen Sicherheitskonzepts für einen besseren Schutz jüdischer Gemeinschaften und Einrichtungen in Europa.

20 EU-Grundrechteagentur: Your rights matter: Security concerns and experiences, 2020.

21 Im Zeitraum von Juli 2015 bis Ende 2019 fand Europol terroristische Inhalte auf 361 Plattformen (Europol 2020).

22 Europol: A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism (Rezension bewährter Verfahren aus Übersee, um der Radikalisierung in Gefängnissen entgegenzuwirken und Rückfälle bei terroristischen Tätern zu verhindern), 2019.

23 Bericht der Europäischen Beobachtungsstelle für Drogen und Drogensucht und von Europol über die Drogenmärkte in der EU (2019).

24 Bericht von Europol über das finanzielle Geschäftsmodell Menschenhandel (2015).

38,9 Mrd. EUR[25]. Gleichzeitig bedeuten niedrige Einziehungsquoten, dass Straftäter ihre kriminellen Tätigkeiten weiter ausdehnen können und in die legale Wirtschaft eindringen.[26]. Über den Online-Markt und durch die neuen Technologien wie den 3D-Druck haben Straftäter und Terroristen leichter Zugang zu Schusswaffen.[27] Die Nutzung künstlicher Intelligenz, neuer Technologien und der Robotik erhöht nochmals das Risiko, dass Kriminelle die Vorteile der Innovation für böswillige Zwecke nutzen.[28]

Diese Bedrohungen, die nicht nur in eine Risikokategorie fallen, treffen verschiedene Teile der Gesellschaft auf unterschiedliche Weise. Sie alle sind eine große Gefahr für Einzelpersonen und Unternehmen und erfordern ein umfassendes und kohärentes Handeln auf EU-Ebene. Wenn selbst kleine miteinander vernetzte Haushaltsgeräte wie ein Kühlschrank oder eine Kaffeemaschine eine Sicherheitslücke verursachen können, dürfen wir uns bei der Gewährleistung unserer Sicherheit nicht mehr allein auf die traditionellen staatlichen Akteure stützen. Die Wirtschaftsbeteiligten müssen mehr Verantwortung für die Cybersicherheit der Produkte und Dienstleistungen übernehmen, die sie in Verkehr bringen; zugleich müssen aber auch Einzelpersonen zumindest über ein Grundverständnis von Cybersicherheit verfügen, damit sie sich auch selbst besser schützen können.

III. Eine koordinierte Reaktion der EU für die gesamte Gesellschaft

Die EU hat bereits gezeigt, dass sie einen echten Mehrwert hat. Seit 2015 sorgt die Sicherheitsunion für neue Bande im Bereich der Sicherheitspolitik auf EU-Ebene. Doch die gesamte Gesellschaft muss noch aktiver miteinbezogen werden, unter anderem die Regierungen auf allen Ebenen, Unternehmen in allen Sektoren und Einzelpersonen in allen Mitgliedstaaten. Das zunehmende Bewusstsein über die Risiken von Abhängigkeiten[29] und den Bedarf einer belastbaren europäischen Industriestrategie[30] weisen die Richtung hin zu einer EU, die in den Bereichen Industrie, Technologie und Widerstandsfähigkeit der Lieferketten über einer kritische Masse verfügt. Belastbarkeit bedeutet hier auch, dass die uneingeschränkte Achtung der Grundrechte und der Werte der EU gewährleistet wird: Dies ist eine Voraussetzung für eine legitime, wirksame und nachhaltige Sicherheitspolitik. In der Strategie für eine Sicherheitsunion werden konkrete Bereiche festgelegt, an denen gearbeitet werden soll. Die Grundlage dafür bilden die folgenden gemeinsamen Ziele:

- ***Aufbau von Fähigkeiten und Kapazitäten zur Früherkennung und Verhütung von Krisen und zur raschen Krisenreaktion:*** Europa muss widerstandsfähiger werden, um künftigen Schocks vorzubeugen, sich vor ihnen zu schützen und ihnen standzuhalten.

[25] Amt der Europäischen Union für geistiges Eigentum und Bericht der OECD über den Handel mit nachgeahmten Arzneimitteln.

[26] Bericht „Abschöpfung und Einziehung von Vermögenswerten: Straftaten dürfen sich nicht auszahlen“, COM(2020) 217.

[27] 2017 wurden bei 41 % aller Terroranschläge Schusswaffen eingesetzt (Europol, 2018).

[28] Im Juli 2020 stellten die französischen und niederländischen Strafverfolgungs- und Justizbehörden zusammen mit Europol und Eurojust die gemeinsamen Ermittlungen zur Zerschlagung von EncroChat vor. Das verschlüsselte Telefonnetz wurde von kriminellen Netzwerken genutzt, die im großen Stil an gewalttätigen Überfällen, Korruption, versuchten Morden und Drogentransporten beteiligt waren.

[29] Zu den Risiken bei Abhängigkeit vom Ausland gehören eine höhere Anfälligkeit für mögliche Bedrohungen, wie beispielsweise die Ausnutzung von Sicherheitslücken in der IT-Infrastruktur, durch die kritische Infrastruktur (z. B. für die Bereiche Energie, Verkehr, Bankwesen oder Gesundheit) beeinträchtigt oder die Kontrolle über industrielle Steuerungssysteme übernommen werden kann, oder erhöhte Fähigkeiten zum Datendiebstahl oder zur Spionage.

[30] Mitteilung der Kommission „Eine neue Industriestrategie für Europa“, COM(2020) 102 final.

Wir müssen über einen umfassenden und koordinierten Ansatz Fähigkeiten und Kapazitäten für die Früherkennung von Sicherheitskrisen und die rasche Krisenreaktion aufbauen, sowohl im Allgemeinen als auch durch sektorspezifische Initiativen (etwa in den Bereichen Finanzwesen, Energie, Justiz, Strafverfolgung, Gesundheitsversorgung, maritimer Sektor und Verkehr) und dabei bestehende Instrumente und Initiativen weiterentwickeln.[31] Die Kommission wird auch Vorschläge für ein umfassendes Krisenmanagementsystem in der EU vorlegen, das auch sicherheitsrelevant sein könnte.

- ***Ergebnisorientierung:*** Um unsere Arbeit auf die beste Wirkung auszurichten, muss einer leistungsorientierten Strategie eine sorgfältige Bedrohungs- und Risikobewertung zugrunde gelegt werden. Dabei müssen die richtigen Regeln und Instrumente festgelegt und angewandt werden. Als Grundlage für die Sicherheitspolitik der EU sind hier verlässliche, strategische Informationen erforderlich. Wo EU-Rechtsvorschriften nötig sind, ist eine Überwachung der Strategie angezeigt, damit die Umsetzung vollumfänglich und ohne Fragmentierung oder Lücken erfolgt, die ausgenutzt werden könnten. Bei der wirksamen Umsetzung der Strategie wird es auch darauf ankommen, eine angemessene Finanzierung im nächsten Programmplanungszeitraum 2021-2027 sicherzustellen, auch für die entsprechenden EU-Agenturen.
- ***Alle öffentlichen und privaten Akteure in einer gemeinsamen Aufgabe zusammenbringen:*** Wichtige Akteure sowohl im öffentlichen als auch im privaten Sektor geben sicherheitsrelevante Informationen bislang nur zögerlich weiter, sei es aus Angst vor einer Beeinträchtigung der nationalen Sicherheit oder aus Wettbewerbsgründen.[32] Die größte Wirkung können wir jedoch erzielen, wenn wir uns alle gegenseitig unterstützen können. Zunächst bedeutet dies eine intensivere Zusammenarbeit zwischen den Mitgliedstaaten unter Einbeziehung der Strafverfolgung, der Gerichte und anderer Behörden und mit den EU-Organen und Agenturen zum Aufbau des für gemeinsame Lösungen erforderlichen Verständnisses und Austauschs. Auch die Zusammenarbeit mit dem privaten Sektor ist von grundlegender Bedeutung, insbesondere, da ein Großteil der für die wirksame Bekämpfung von Kriminalität und Terrorismus entscheidenden digitalen und nicht digitalen Infrastruktur sich im Besitz der Industrie befindet. Auch Einzelpersonen können einen Beitrag leisten, indem sie sich etwa die Fähigkeiten und das Bewusstsein aneignen, um sich gegen Cyberkriminalität und Desinformation zu wappnen. Schließlich darf diese gemeinsame Aufgabe auch nicht an unseren Grenzen enden. Es gilt, engere Bande mit gleich gesinnten Partnern zu knüpfen.

IV. Schutz für jeden in der EU: strategische Prioritäten für die Sicherheitsunion

Die EU kann in ihrer einzigartigen Rolle besonders gut auf diese neuen weltweiten Bedrohungen und Herausforderungen reagieren. Aus der obigen Bedrohungsanalyse lassen sich vier miteinander zusammenhängende strategische Prioritäten ableiten, an denen auf EU-Ebene unter uneingeschränkter Achtung der Grundrechte gearbeitet werden sollte: i) ein zukunftsfähiges Sicherheitsumfeld, ii) die Bewältigung sich wandelnder Bedrohungen, iii)

[31] Etwa die Integrierte EU-Regelung für die politische Reaktion auf Krisen (IPCR), das Zentrum für die Koordination von Notfallmaßnahmen, die Empfehlung der Kommission für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (C(2017) 6100 final) oder das Protokoll der EU für das operative Vorgehen bei der Abwehr hybrider Bedrohungen (SWD(2016) 227).

[32] Siehe Gemeinsame Mitteilung „Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen“, JOIN(2017) 450 final.

der Schutz der Europäer vor Terrorismus und organisiertem Verbrechen und iv) eine starke europäische Sicherheitsgemeinschaft.

1. Ein zukunftsfähiges Sicherheitsumfeld

Schutz und Widerstandsfähigkeit kritischer Infrastruktur

Die Menschen sind in ihrem Alltag auf wichtige Infrastruktur angewiesen, um reisen und arbeiten, grundlegende öffentliche Dienstleistungen wie Gesundheitsversorgung, Verkehr oder Energieversorgung nutzen oder ihre demokratischen Rechte ausüben zu können. Ist diese Infrastruktur nicht ausreichend geschützt und widerstandsfähig, so können Angriffe sowohl in einzelnen Mitgliedstaaten als auch potenziell in der gesamten EU massive Störungen, nicht nur digitaler Art, verursachen.

Der bestehende EU-Rahmen für den Schutz und die Widerstandsfähigkeit kritischer Infrastruktur[33] hat nicht mit den sich wandelnden Bedrohungen Schritt gehalten. Die zunehmenden wechselseitigen Abhängigkeiten führen dazu, dass Störungen in einem Sektor unmittelbare Auswirkungen auf den Betrieb in anderen Sektoren haben können: Ein Angriff auf die Stromerzeugung könnte die Telekommunikation, Krankenhäuser, Banken oder Flughäfen zum Stillstand bringen, ein Angriff auf die digitale Infrastruktur zu Störungen in den Stromnetzen oder im Finanzsektor führen. Mit der immer stärkeren Digitalisierung unserer Wirtschaft und Gesellschaft werden solche Bedrohungen immer akuter. Der Rechtsrahmen muss diesen zunehmenden Verflechtungen und Abhängigkeiten gerecht werden, indem er robuste Maßnahmen physischer und digitaler Natur für den Schutz und die Widerstandsfähigkeit kritischer Infrastruktur vorsieht. Grundlegende Dienste, auch solche, die sich auf Weltrauminfrastruktur stützen, müssen angemessen vor aktuellen und zu erwartenden Bedrohungen geschützt werden und auch widerstandsfähig sein. Dies bedeutet, dass ein System in der Lage sein muss, sich auf Zwischenfälle vorzubereiten und entsprechende Vorsorge zu treffen, diese Ereignisse abzumildern, sich davon zu erholen und sich besser daran anzupassen.

Gleichzeitig nutzen die Mitgliedstaaten bislang ihren Ermessensspielraum, indem sie bestehende Rechtsvorschriften auf unterschiedliche Art und Weise umsetzen. Die so entstehende Fragmentierung kann den Binnenmarkt untergraben und die grenzüberschreitende Koordinierung erschweren, insbesondere in Grenzregionen. Betreiber, die in verschiedenen Mitgliedstaaten wesentliche Dienste erbringen, müssen unterschiedliche Berichterstattungsregelungen einhalten. Die Kommission prüft derzeit, ob **neue Rahmen sowohl für physische als auch für digitale Infrastruktur** zu mehr Kohärenz und einem einheitlicheren Ansatz bei der Gewährleistung der zuverlässigen Bereitstellung wesentlicher Dienste führen könnten. Ein solcher Rahmen muss mit **sektorspezifischen Initiativen** einhergehen, um den spezifischen Risiken zu begegnen, denen kritische Infrastruktur etwa in den Bereichen Verkehr, Raumfahrt, Energie, Finanzwesen und Gesundheitsversorgung ausgesetzt ist.[34] Da der Finanzsektor stark von IT-Diensten abhängt und sehr anfällig für Cyberangriffe ist, wird ein erster Schritt in einer

[33] Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016), Richtlinie 2008/114/EG des Rates über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern.

[34] Da das Gesundheitswesen während der COVID-19-Krise unter besonderem Druck steht, wird die Kommission auch Initiativen zur Stärkung des EU-Rahmens für die Gesundheitssicherheit und der zuständigen EU-Agenturen in Erwägung ziehen, um auf schwerwiegende grenzübergreifende Gesundheitsbedrohungen zu reagieren.

Initiative für die Betriebsstabilität digitaler Systeme in diesem Bereich bestehen. Vor dem Hintergrund der besonderen Anfälligkeit und Tragweite des Energiesystems wird eine spezielle Initiative zur stärkeren Widerstandsfähigkeit der kritischen Energieinfrastruktur gegenüber physischen, digitalen und hybriden Bedrohungen beitragen und grenzübergreifend gleiche Wettbewerbsbedingungen für Energieunternehmen sicherstellen.

Auch sicherheitsrelevante Auswirkungen ausländischer Direktinvestitionen, die für kritische Infrastruktur oder Technologie Konsequenzen haben könnten, werden Gegenstand der Bewertung sein, die die EU-Mitgliedstaaten und die Kommission als Teil des neuen europäischen Rahmens für die Überprüfung ausländischer Direktinvestitionen durchführen werden.[35]

Die EU kann auch neue Instrumente zur Stärkung der Widerstandsfähigkeit kritischer Infrastruktur entwickeln. Das globale Internet hat sich bisher als sehr resilient erwiesen, insbesondere im Hinblick auf die Fähigkeit, erhöhten Datenverkehr zu verkraften. Wir müssen jedoch auf mögliche künftige Krisen vorbereitet sein, die eine Bedrohung für die Sicherheit, Stabilität und Widerstandsfähigkeit des Internets darstellen. Um sicherzustellen, dass das Internet stets funktionsfähig bleibt, müssen die Anfälligkeit für Cybervorfälle und böswillige Online-Aktivitäten und die Abhängigkeit von Infrastruktur und Diensten außerhalb der EU verringert werden. Dies erfordert eine Kombination aus Rechtsvorschriften, einschließlich der Überprüfung bestehender Vorschriften, um ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der EU zu gewährleisten, einer Erhöhung der Investitionen in Forschung und Innovation und einer Prüfung des Aufbaus bzw. der Festigung von grundlegender Internetinfrastruktur und wichtigen Ressourcen, insbesondere des Domänennamen-Systems[36].

Für den Schutz wichtiger digitaler Werte der EU und der Mitgliedstaaten ist die Bereitstellung eines Kanals für die sichere Kommunikation für kritische Infrastruktur ein zentrales Element. Die Kommission arbeitet mit den Mitgliedstaaten daran, in Verbindung mit dem in der Verordnung zur Aufstellung des Weltraumprogramms[37] enthaltenen System für staatliche Satellitenkommunikation eine zertifizierte, sichere, terrestrische und weltraumgestützte Ende-zu-Ende-Quantenkommunikationsinfrastruktur zu schaffen.

Cybersicherheit

Die Anzahl der Cyberangriffe nimmt weiterhin zu.[38] Diese Angriffe sind heute ausgefeilter als je zuvor, gehen von unterschiedlichsten Stellen innerhalb und außerhalb der EU aus und zielen auf besonders anfällige Bereiche ab. Häufig sind Staaten oder von Staaten unterstützte

---

[35] Nach dem vollständigen Inkrafttreten am 11. Oktober 2020 der Verordnung (EU) 2019/452 des Europäischen Parlaments und des Rates vom 19. März 2019 zur Schaffung eines Rahmens für die Überprüfung ausländischer Direktinvestitionen in der Union wird die EU über einen neuen Kooperationsmechanismus für Direktinvestitionen von außerhalb der EU verfügen, die die Sicherheit oder die öffentliche Ordnung beeinträchtigen könnten. Gemäß der Verordnung werden die Mitgliedstaaten und die Kommission mögliche Risiken im Zusammenhang mit solchen ausländischen Direktinvestitionen bewerten und, wo angezeigt und wo mehr als ein Mitgliedstaat betroffen ist, angemessene Vorschläge zur Risikominderung machen.

[36] Ein Domänennamen-System (DNS) ist ein hierarchisches und dezentrales Bezeichnungssystem für Computer, Dienste und andere Ressourcen, die mit dem Internet oder einem privaten Netzwerk verbunden sind. Es „übersetzt“ Domänennamen in die IP-Adressen, die erforderlich sind, um Computerdienste und -geräte zu lokalisieren und zu identifizieren.

[37] Vorschlag für eine Verordnung zur Aufstellung des Weltraumprogramms der Union und der Agentur der Europäischen Union für das Weltraumprogramm, COM(2018) 447.

[38] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

Akteure beteiligt und wichtige digitale Infrastruktur wie große Cloud-Anbieter das Ziel.[39] Cyberrisiken haben sich auch zu einer erheblichen Bedrohung für das Finanzsystem entwickelt. Schätzungen des Internationalen Währungsfonds zufolge liegen die von Cyberangriffen verursachten jährlichen Verluste weltweit mit etwa 100 Mrd. USD bei 9 % der Nettoeinnahmen der Banken.[40] Die Umstellung auf vernetzte Geräte bringt große Vorteile für die Nutzer mit sich. Da damit jedoch weniger Daten in Datenzentren gespeichert und mehr Daten bei den Nutzern „am Rand des Netzes“[41] verarbeitet werden, ist es in Cybersicherheitsfragen nicht mehr möglich, sich allein auf den Schutz zentraler Punkte zu konzentrieren[42].

Die EU hat 2017 einen Cybersicherheitsansatz vorgelegt, bei dem der Aufbau von Abwehrfähigkeit, eine rasche Reaktionsfähigkeit und die wirksame Abschreckung im Mittelpunkt stehen.[43] Die EU muss nun sicherstellen, dass ihre Cybersicherheitsfähigkeiten mit der Entwicklung der Lage mithalten, um sowohl die Abwehr- als auch die Reaktionsfähigkeit zu gewährleisten. Dies macht ein tatsächlich gesamtgesellschaftliches Konzept erforderlich, bei dem die Organe, Einrichtungen und sonstigen Stellen der EU, die Mitgliedstaaten, die Industrie, die Wissenschaft und auch die Einzelpersonen der Cybersicherheit die notwendige Priorität einräumen.[44] Dieses horizontale Konzept muss wiederum in Bereichen wie Energie, Finanzdienstleistungen, Verkehr oder Gesundheitsversorgung durch sektorspezifische Cybersicherheitskonzepte ergänzt werden. Die nächste Phase der Arbeit der EU sollte in einer überarbeiteten Cybersicherheitsstrategie der Europäischen Union zusammengefasst werden.

Neue und verstärkte Formen der Zusammenarbeit zwischen Nachrichtendiensten, dem EU-Zentrum INTCEN und anderen im Sicherheitsbereich tätigen Einrichtungen zu erschließen sollte Teil der Arbeit an der Verbesserung der Cybersicherheit sowie der Bekämpfung von Terrorismus, Extremismus, Radikalismus und hybriden Bedrohungen sein.

Vor dem Hintergrund des derzeitigen Aufbaus der **5G-Infrastruktur** in der EU und der möglichen Abhängigkeit vieler wesentlicher Dienste von 5G-Netzen wären die Folgen von systemischen und umfangreichen Störungen besonders gravierend. Im Rahmen des in der Empfehlung der Kommission zur Cybersicherheit der 5G-Netze[45] 2019 dargelegten Prozesses sind die Mitgliedstaaten nun gezielt in den Kernbereichen tätig geworden, die im EU-Instrumentarium für die 5G-Cybersicherheit[46] festgelegt sind.

Langfristig ist es insbesondere nötig, eine Kultur der **„eingebauten Cybersicherheit“** zu entwickeln, Produkte und Dienste also von vornherein sicher zu gestalten. Der neue europäische Rahmen für die Cybersicherheitszertifizierung gemäß dem Rechtsakt zur

---

[39] DDoS-Angriffe sind weiterhin eine ständige Bedrohung: Große Anbieter mussten massive DDoS-Angriffe abwehren, beispielsweise einen Angriff auf Amazon Web Services im Februar 2020.

[40] https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/

[41] Bei Edge-Computing „am Rand des Netzes“ handelt es sich um eine dezentrale, offene IT-Architektur mit dezentraler Verarbeitungsleistung, die mobiles Rechnen sowie Technologien für das Internet der Dinge ermöglicht. Beim Edge-Computing werden Daten vom Gerät selbst oder von einem Computer oder Server vor Ort verarbeitet und nicht an ein Rechenzentrum übermittelt.

[42] Mitteilung „Eine europäische Datenstrategie“, COM(2020) 66 final.

[43] Siehe Gemeinsame Mitteilung „Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen“, JOIN(2017) 450 final.

[44] Der Bericht „Cybersecurity – our digital Anchor“ der Gemeinsamen Forschungsstelle bietet vielseitige Einblicke in die Entwicklung der Cybersicherheit über die letzten 40 Jahre.

[45] Empfehlung der Kommission zur Cybersicherheit der 5G-Netze, COM(2019) 2335 final. In der Empfehlung ist vorgesehen, dass sie im letzten Quartal 2020 überprüft wird.

[46] Siehe Bericht der NIS-Kooperationsgruppe über die Umsetzung des Instrumentariums vom 24. Juli 2020.

Cybersicherheit[47] wird hier einen wichtigen Beitrag leisten. Dieser Rahmen befindet sich bereits im Aufbau. Zwei Schemata für die Zertifizierung sind in Vorbereitung und im Laufe dieses Jahres sollen die Prioritäten für weitere Schemata festgelegt werden. In diesem Bereich kommt der Zusammenarbeit der EU-Agentur für die Cybersicherheit (ENISA), der Datenschutzbehörden und des Europäischen Datenschutzausschusses[48] erhebliche Bedeutung zu.

Die Kommission hat bereits festgestellt, dass eine **gemeinsame Cyber-Stelle** für eine strukturierte und koordinierte operative Zusammenarbeit erforderlich ist. Diese könnte auch einen Amtshilfemechanismus auf EU-Ebene für Krisenzeiten umfassen. Ausgehend von dem Konzeptentwurf aus der entsprechenden Empfehlung[49] könnte mit der gemeinsamen Cyber-Stelle Vertrauen zwischen den verschiedenen Akteuren im europäischen Cybersicherheitsgefüge aufgebaut und den Mitgliedstaaten ein wichtiger Dienst angeboten werden. Die Kommission wird Gespräche mit den einschlägigen Interessenträgern aufnehmen (beginnend mit den Mitgliedstaaten) und bis Ende 2020 ein klares Verfahren, Etappenziele und eine Zeitplanung festlegen.

Wichtig sind auch gemeinsame Vorschriften zur Informations- und Cybersicherheit für alle Organe, Einrichtungen und sonstigen Stellen der EU. Das Ziel sollte darin bestehen, verbindliche und hohe gemeinsame Standards für den sicheren Informationsaustausch und die Sicherheit von digitaler Infrastruktur und digitalen Systemen in sämtlichen Organen, Einrichtungen und sonstigen Stellen der EU zu schaffen. Dieser neue Rahmen sollte eine enge und effiziente operative Zusammenarbeit im Bereich der Cybersicherheit zwischen den Organen, Einrichtungen und sonstigen Stellen der EU, bei der die Rolle des Computer-Notfallteams (CERT-EU) der Organe, Einrichtungen und sonstigen Stellen der EU im Mittelpunkt steht, unterstützen.

Da Cyberangriffe eine globale Bedrohung sind, kommt dem Aufbau und der Pflege **internationaler Partnerschaften** eine grundlegende Rolle bei der Vorbeugung, Abschreckung und Reaktion zu. Der Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten („Cyber Diplomacy Toolbox“)[50] enthält Maßnahmen im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik, einschließlich restriktiver Maßnahmen (Sanktionen), die eingesetzt werden können, um Tätigkeiten abzuwehren, die ihren politischen, sicherheitspolitischen oder wirtschaftlichen Interessen schaden. Die EU sollte zudem ihre Arbeit über Entwicklungs- und Zusammenarbeitsfonds vertiefen, um Partnerstaaten beim Kapazitätsaufbau zu unterstützen und damit ihr digitales Umfeld zu stärken und die Annahme nationaler Gesetzesreformen sowie die Übernahme internationaler Standards zu begünstigen. So wird die Abwehrfähigkeit der Gemeinschaft insgesamt gestärkt, einschließlich ihrer Fähigkeit, Cyberbedrohungen wirksam zu bekämpfen und darauf zu reagieren. Dazu gehört auch die Arbeit an der gezielten Förderung der EU-

[47] Verordnung (EU) 2019/881 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (Rechtsakt zur Cybersicherheit).

[48] Mitteilung „Datenschutz als Grundpfeiler der Teilhabe der Bürgerinnen und Bürger und des Ansatzes der EU für den digitalen Wandel – zwei Jahre Anwendung der Datenschutz-Grundverordnung“, COM(2020) 264 final.

[49] Empfehlung (EU) 2017/1584 der Kommission für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen.

[50] http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/de/pdf

Standards und der einschlägigen Gesetzgebung, um die Cybersicherheit von benachbarten Partnerländern[51] zu erhöhen.

Schutz des öffentlichen Raums

In der jüngeren Vergangenheit zielten terroristische Anschläge insbesondere auf den **öffentlichen Raum** ab, unter anderem auf Gebetsstätten oder Verkehrsknotenpunkte, deren unverbaute und leicht zugängliche Lage ausgenutzt wurde. Die Zunahme des Terrorismus, der auf politisch oder ideologisch motivierten Extremismus zurückgeht, hat diese Bedrohung noch verschärft. Deshalb sind sowohl schärfere Maßnahmen zum physischen Schutz solcher Orte als auch angemessene Überwachungssysteme erforderlich, die die Freiheit der Bürgerinnen und Bürger nicht untergraben.[52] Die Kommission wird die öffentlich-private Zusammenarbeit beim Schutz des öffentlichen Raums mit Finanzmitteln, dem Austausch von Erfahrungen und bewährten Verfahren sowie mit spezifischen Leitlinien[53] und Empfehlungen[54] fördern. Auch Sensibilisierung, die Formulierung von Leistungsanforderungen an Detektionsgeräte sowie deren Erprobung und die Intensivierung von Sicherheitsüberprüfungen, um gegen Insider-Bedrohungen vorzugehen, sollen Teil des Konzepts sein. Dem Umstand, dass Minderheiten und schutzbedürftige Personen unverhältnismäßig stark betroffen sein können – auch aufgrund ihrer Religion oder ihres Geschlechts – und deshalb besonderer Aufmerksamkeit bedürfen, ist Rechnung zu tragen. Regionalen und lokalen Behörden kommt bei der Verbesserung der Sicherheit des öffentlichen Raums eine wichtige Rolle zu. Die Kommission unterstützt auch Innovation im öffentlichen Raum in Städten[55]. Die Einrichtung der Partnerschaft für die „Sicherheit im öffentlichen Raum“ im Rahmen der neuen Städteagenda[56] im November 2018 steht für die feste Entschlossenheit der Mitgliedstaaten, der Kommission und der Städte, Sicherheitsbedrohungen im städtischen Raum besser zu bekämpfen.

Der Markt für **Drohnen**, für die es viele nützliche und gerechtfertigte Einsatzmöglichkeiten gibt, wächst immer weiter. Drohnen können jedoch auch von Straftätern und Terroristen missbräuchlich eingesetzt werden und so insbesondere im öffentlichen Raum zur Bedrohung werden. Ziele können unter anderem Einzelpersonen, Menschenansammlungen, kritische Infrastruktur, Strafverfolgungsbehörden, Grenzen und der öffentliche Raum sein. Kenntnisse für den Einsatz von Drohnen in Konflikten könnten entweder direkt (über aus dem Ausland zurückkehrende terroristische Kämpfer) oder über das Internet nach Europa gelangen. Ein erster Schritt sind hier Regeln, die die Europäische Agentur für Flugsicherheit bereits in

---

[51] Siehe Schlussfolgerungen des Rates zu den EU-Leitlinien für den Aufbau externer Cyberkapazitäten vom 26. Juni 2018.

[52] Biometrische Fernidentifikationssysteme müssen in dieser Hinsicht besonders genau geprüft werden. Die ersten Standpunkte der Kommission enthält das Weißbuch zur Künstlichen Intelligenz vom 19. Februar 2020, COM(2020) 65 final.

[53] Ein Beispiel ist der Leitfaden für die Auswahl geeigneter Sicherheitsbarrieren für den Schutz des öffentlichen Raums (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120307/hvm_v3.pdf).

[54] Die Arbeitsunterlage SWD(2019) 140 final enthält bewährte Verfahren und unter anderem einen Abschnitt zur öffentlich-privaten Zusammenarbeit. Die Finanzmittel aus dem Instrument für die finanzielle Unterstützung der polizeilichen Zusammenarbeit, der Kriminalprävention und Kriminalitätsbekämpfung und des Krisenmanagements fließen insbesondere in die Stärkung der öffentlich-privaten Zusammenarbeit.

[55] Im Rahmen der Initiative „Innovative Maßnahmen für eine nachhaltige Stadtentwicklung“, die über den Europäischen Fonds für regionale Entwicklung kofinanziert wird, werden drei Städte (Piräus in Griechenland, Tampere in Finnland und Turin in Italien) neue Lösungen erproben.

[56] Bei der EU-Städteagenda handelt sich um eine neue Methode der Zusammenarbeit auf mehreren Ebenen, die die Zusammenarbeit zwischen den Mitgliedstaaten, den Städten, der Kommission und anderen Interessenträgern fördert, um Wachstum, Lebensqualität und Innovation in den europäischen Städten zu fördern und soziale Herausforderungen zu ermitteln und zu bewältigen.

Bereichen wie der Registrierung der Betreiber von Drohnen und der Verpflichtung zur Fernidentifizierung von Drohnen entwickelt hat. Da Drohnen immer freier verfügbar, erschwinglicher und leistungsfähiger werden, besteht weiterer Handlungsbedarf. Mögliche Maßnahmen sind unter anderem Informationsaustausch, die Bereitstellung von Leitlinien und bewährten Verfahren für alle, einschließlich der Strafverfolgungsbehörden, und die Erprobung von Maßnahmen zur Drohnenabwehr.[57] Zudem sollten die Aspekte des Schutzes der Privatsphäre und des Datenschutzes beim Einsatz von Drohnen im öffentlichen Raum genauer geprüft und berücksichtigt werden.

Zentrale Maßnahmen
• Gesetzgebung im Bereich des Schutzes und der Widerstandsfähigkeit kritischer Infrastruktur • Die Überprüfung der Richtlinie zur Netz- und Informationssicherheit • Eine Initiative zur Verbesserung der Betriebsstabilität des Finanzsektors • Schutz und Cybersicherheit kritischer Energieinfrastruktur und Netzkodex zur Cybersicherheit für grenzüberschreitende Stromflüsse • Eine Cybersicherheitsstrategie der Europäischen Union • Weitere Schritte zur Schaffung einer gemeinsamen Cyber-Stelle • Gemeinsame Vorschriften zur Informations- und Cybersicherheit für alle Organe, Einrichtungen und sonstigen Stellen der EU • Verstärkte Zusammenarbeit zum Schutz des öffentlichen Raums, einschließlich Gebetsstätten • Austausch bewährter Verfahren zur Bekämpfung des missbräuchlichen Einsatzes von Drohnen

2. Umgang mit sich wandelnden Bedrohungen

Cyberkriminalität

Technologie eröffnet der Gesellschaft neue Möglichkeiten. Sie bietet unter anderem neue Instrumente für die Justiz und die Strafverfolgung. Gleichzeitig eröffnet sie aber auch ein neues Betätigungsfeld für Kriminelle. Es gibt immer mehr Schadsoftware und auch der Diebstahl persönlicher oder geschäftlicher Daten durch Hacking und das Sperren digitaler Aktivitäten nehmen zu, was zu finanziellen Schäden oder Rufschädigungen führt. Die beste Verteidigung bietet hier ein widerstandsfähiges Umfeld, das auf einer starken Cybersicherheit beruht. Die Strafverfolgungsbehörden müssen in der Lage sein, sich bei digitalen Ermittlungen auf klare Regeln für die Ermittlung und Verfolgung von Straftaten zu stützen und Opfern den erforderlichen Schutz zu gewähren. Die Arbeit in diesem Bereich sollte sich auf die Gemeinsame Task Force zur Bekämpfung der Cyberkriminalität bei Europol und das Notfallprotokoll für die Strafverfolgung stützen, das zur Koordinierung der Maßnahmen zur Bewältigung groß angelegter Cyberangriffe eingerichtet wurde. Von entscheidender Bedeutung sind hier auch wirksame Mechanismen, die öffentlich-private Partnerschaften und Zusammenarbeit ermöglichen.

Parallel dazu sollte die Bekämpfung der Cyberkriminalität in der gesamten EU zu einer strategischen Kommunikationspriorität werden, um die Europäer auf die Risiken

[57] Vor kurzem wurde ein mehrjähriges Testprogramm zur Unterstützung der Mitgliedstaaten bei der Entwicklung einer gemeinsamen Methodik und Testplattform in diesem Bereich geschaffen.

aufmerksam zu machen und über die möglichen Präventivmaßnahmen zu informieren. Dies sollte Teil eines proaktiven Ansatzes sein. Ein wichtiger Schritt ist ferner die vollständige Umsetzung des geltenden Rechtsrahmens[58]: Die Kommission wird erforderlichenfalls Vertragsverletzungsverfahren einleiten und ist bereit, diesen Rahmen laufend zu überprüfen, um sicherzustellen, dass er weiterhin seinen Zweck erfüllt. Die Kommission wird zudem gemeinsam mit Europol und der EU-Agentur für Cybersicherheit, ENISA, die Durchführbarkeit eines Schnellwarnsystems für Cyberkriminalität in der EU prüfen, das den Informationsfluss und rasche Reaktionen beim vermehrten Auftreten von Cyberkriminalität gewährleisten könnte.

Cyberkriminalität ist eine globale Herausforderung, die eine wirksame internationale Zusammenarbeit erfordert. Die EU unterstützt das Budapester Übereinkommen des Europarats über Computerkriminalität, das einen wirksamen und gut etablierten Rahmen bietet, mit dem alle Länder ermitteln können, welche Systeme und Kommunikationskanäle sie einrichten müssen, um wirksam zusammenarbeiten zu können.

Fast die Hälfte der EU-Bürgerinnen und Bürger ist besorgt über Datenmissbrauch[59] und insbesondere über **Identitätsdiebstahl**[60]. Bei der missbräuchlichen Nutzung der Identität kann es einerseits um die Erzielung eines finanziellen Gewinns gehen, sie kann aber auch erhebliche persönliche und psychologische Auswirkungen haben, da von einem Identitätsdieb veröffentlichte illegale Posts in manchen Fällen über Jahre im Internet bleiben. Die Kommission wird mögliche praktische Maßnahmen zum Schutz der potenziellen Opfer vor allen Formen des Identitätsdiebstahls prüfen und dabei die geplante europäische Initiative zur digitalen Identität berücksichtigen[61].

Die Bekämpfung der Cyberkriminalität erfordert einen Blick in die Zukunft. Da die Gesellschaft neue technologische Entwicklungen nutzt, um Wirtschaft und Gesellschaft zu stärken, können Kriminelle ihrerseits versuchen, diese Instrumente zu missbräuchlichen Zwecken zu verwenden. So können Kriminelle beispielsweise künstliche Intelligenz einsetzen, um Passwörter zu erkennen und zu ermitteln oder die Erstellung von Schadsoftware zu vereinfachen, um Bilder und Tonaufnahmen zu nutzen, die dann für Identitätsdiebstahl oder -betrug verwendet werden können.

Moderne Strafverfolgung

Fachkräfte im Bereich Strafverfolgung und Angehörige von Rechtsberufen müssen sich an neue Technologien anpassen. Angesichts der technologischen Entwicklungen und neu auftretender Bedrohungen müssen die Strafverfolgungsbehörden Zugang zu neuen Instrumenten haben, neue Fähigkeiten erwerben und alternative Ermittlungstechniken entwickeln. Als Ergänzung zu den legislativen Maßnahmen, durch die der grenzübergreifende Zugang zu elektronischen Beweismitteln für strafrechtliche Ermittlungen verbessert werden soll, kann die EU die Strafverfolgungsbehörden dabei unterstützen, die erforderlichen Kapazitäten für Ermittlung, Sicherung und Auslesen der für Ermittlungen erforderlichen Daten und zur Verwendung dieser Daten als Beweismittel vor

[58] Richtlinie 2013/40/EU über Angriffe auf Informationssysteme.

[59] 46 % (Eurobarometer zur Einstellung der Europäer zur Cybersicherheit, Januar 2020).

[60] Die überwiegende Mehrheit der Befragten der Eurobarometer-Umfrage 2018 zu den Einstellungen der Europäer zur Internetsicherheit betrachtete Identitätsdiebstahl als schwere Straftat (95 %), 70 % betrachteten ihn sogar als eine sehr schwere Straftat. Die im Januar 2020 veröffentlichte Eurobarometer-Umfrage bestätigte, dass die Europäer angesichts von Cyberkriminalität, Online-Betrug und Identitätsdiebstahl besorgt sind: Zwei Drittel der Befragten äußerten sich besorgt über Bankbetrug (67 %) und Identitätsdiebstahl (66 %).

[61] Mitteilung vom 19. Februar 2020 „Gestaltung der digitalen Zukunft Europas“, COM (2020) 67.

Gericht aufzubauen. Die Kommission wird Maßnahmen zur **Verbesserung der Strafverfolgungskapazitäten bei digitalen Ermittlungen** prüfen und ermitteln, wie Forschung und Entwicklung optimal genutzt werden können, um neue Instrumente für die Strafverfolgung zu schaffen, und wie den Mitarbeitern der Strafverfolgungsbehörden und im Justizwesen die geeigneten Kompetenzen durch Schulungen vermittelt werden können. Dies wird auch die Bereitstellung strenger wissenschaftlicher Bewertungen und Testmethoden durch die Gemeinsame Forschungsstelle der Kommission beinhalten.

Gemeinsame Ansätze können auch gewährleisten, dass **künstliche Intelligenz, Weltraumfähigkeiten, Big Data** und **Hochleistungsrechnen** auf eine Art und Weise in die Sicherheitspolitik **integriert werden**, die sowohl bei der Verbrechensbekämpfung als auch im Hinblick auf die Wahrung der Grundrechte wirksam ist. Künstliche Intelligenz könnte ein wirksames Instrument zur Verbrechensbekämpfung sein, da durch die Analyse großer Mengen an Informationen, die Ermittlung von Mustern und das Erkennen von Anomalien riesige Ermittlungskapazitäten geschaffen werden können[62]. Sie kann auch konkrete Instrumente bieten, z. B. zur Erkennung terroristischer Online-Inhalte, zur Aufdeckung verdächtiger Transaktionen beim Verkauf gefährlicher Produkte oder zur Unterstützung von Bürgerinnen und Bürgern in Notsituationen. Um dieses Potenzial auszuschöpfen, gilt es, die Forschungs- und Innovationsgemeinschaft und Nutzer künstlicher Intelligenz im Rahmen einer geeigneten Governance und mit der richtigen technischen Infrastruktur unter aktiver Einbeziehung des Privatsektors und der Wissenschaft zusammenzubringen. Außerdem gilt es, dabei höchste Standards für die Achtung der Grundrechte zu gewährleisten und gleichzeitig für einen wirksamen Schutz der Bürgerinnen und Bürger zu sorgen. Insbesondere müssen Entscheidungen, die Einzelpersonen betreffen, einer Überprüfung durch den Menschen unterliegen und mit dem einschlägigen EU-Recht im Einklang stehen[63].

Bei rund 85 % der Ermittlungen zu schweren Straftaten werden elektronische Informationen und Beweismittel benötigt, und 65 % aller Anfragen sind an Anbieter gerichtet, die in einem Land ansässig sind, das einer anderen Gerichtsbarkeit unterliegt[64]. Die Tatsache, dass traditionelle materielle Spuren sich verlagert haben und stattdessen die Bedeutung digitaler Spuren zugenommen hat, vergrößert die Kluft zwischen den Möglichkeiten der Strafverfolgung und den Fähigkeiten von Kriminellen weiter. Es ist von wesentlicher Bedeutung, dass klare Regeln für den grenzübergreifenden Zugang zu elektronischen Beweismitteln für strafrechtliche Ermittlungen eingeführt werden. Um den Fachleuten ein effizientes Instrument an die Hand zu geben, ist es daher entscheidend, dass die Vorschläge zu den elektronischen Beweismitteln zeitnah vom Europäischen Parlament und dem Rat angenommen werden. Darüber hinaus ist es auch dringend nötig, den grenzübergreifenden Zugang zu elektronischen Beweismitteln im Wege multilateraler und bilateraler internationaler Verhandlungen zu regeln, um auf internationaler Ebene kompatible Regeln zu schaffen[65].

---

[62] Beispielsweise bei Finanzkriminalität.

[63] Dies bedeutet Einhaltung der geltenden Rechtsvorschriften, einschließlich der Datenschutz-Grundverordnung (EU) 2016/679 und der Richtlinie zum Datenschutz bei der Strafverfolgung (EU) 2016/680, die die Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung regelt.

[64] SWD(2018) 118 final der Kommission.

[65] Insbesondere das Zweite Zusatzprotokoll zum Budapester Übereinkommen des Europarats über Computerkriminalität und ein Abkommen zwischen der EU und den Vereinigten Staaten über den grenzübergreifenden Zugang zu elektronischen Beweismitteln.

Der **Zugang zu digitalen Beweismitteln** hängt auch von der Verfügbarkeit von Informationen ab. Werden Daten zu schnell gelöscht, können wichtige Beweise verschwinden, sodass es nicht mehr möglich ist, Verdächtige und kriminelle Netze (wie auch Opfer) zu identifizieren und ausfindig zu machen. Andererseits werfen Regelungen zur Vorratsdatenspeicherung Fragen im Bereich des Schutzes der Privatsphäre auf. Abhängig vom Ausgang der beim Europäischen Gerichtshof anhängigen Rechtssachen wird die Kommission das weitere Vorgehen bei der Vorratsdatenspeicherung prüfen.

Der Zugang zu Registrierungsinformationen für Internet-Domänennamen („WHOIS-Daten“)[66] ist wichtig für strafrechtliche Ermittlungen, die Cybersicherheit und den Verbraucherschutz. Allerdings wird es immer schwieriger, Zugang zu diesen Informationen zu erhalten, solange die Annahme einer neue WHOIS-Strategie durch die Zentralstelle für die Vergabe von Internet-Namen und -Adressen (ICANN) aussteht. Die Kommission wird weiterhin mit der ICANN und der Multi-Stakeholder-Gemeinschaft zusammenarbeiten, um sicherzustellen, dass berechtigte Zugangsnachfrager, einschließlich Strafverfolgungsbehörden, im Einklang mit den Datenschutzvorschriften der EU und internationalen Datenschutzvorschriften effizient Zugang zu WHOIS-Daten erhalten können. Dies umfasst auch die Prüfung möglicher Lösungen, einschließlich der Frage, ob die Regeln für den Zugang zu solchen Informationen möglicherweise durch Rechtsvorschriften präzisiert werden müssten.

Die Strafverfolgungs- und Justizbehörden müssen auch so ausgestattet sein, dass sie – unter Wahrung der Vertraulichkeit der Kommunikation – die erforderlichen Daten und Nachweise erhalten können, sobald die **5G-Architektur für den Mobilfunk** in der EU in vollem Umfang eingeführt ist. Im Hinblick auf die Ausarbeitung internationaler Normen, die Festlegung bewährter Verfahren, von Prozessen und der technischen Interoperabilität in wichtigen technologischen Bereichen wie KI, Internet der Dinge oder Blockchain-Technologien wird die Kommission einen verbesserten und koordinierten Ansatz unterstützen.

Heute betrifft ein erheblicher Teil der Ermittlungen gegen alle Formen von Kriminalität und Terrorismus **verschlüsselte Informationen**. Verschlüsselung ist für die digitale Welt ein wesentlicher Faktor, da dadurch digitale Systeme und Transaktionen gesichert und zudem eine Reihe von Grundrechten geschützt werden, darunter die Freiheit der Meinungsäußerung und der Schutz der Privatsphäre und personenbezogener Daten. Wird Verschlüsselung jedoch für kriminelle Zwecke eingesetzt, kann sie auch dazu dienen, die Identität von Straftätern zu verschleiern und den Inhalt ihrer Kommunikation zu verbergen. Die Kommission wird ausgewogene technische, operative und rechtliche Lösungen für die bestehenden Herausforderungen prüfen und unterstützen und einen Ansatz fördern, der sowohl die Wirksamkeit der Verschlüsselung beim Schutz der Privatsphäre und der Sicherheit bei der Kommunikation als auch eine wirksame Reaktion auf Kriminalität und Terrorismus gewährleistet.

Bekämpfung illegaler Online-Inhalte

Um die Sicherheit von Online-Umgebungen und physischen Umgebungen auf den gleichen Stand zu bringen, müssen weitere Schritte zur **Bekämpfung illegaler Online-Inhalte** unternommen werden. Bei den wichtigsten Bedrohungen für Bürgerinnen und Bürger wie Terrorismus, Extremismus oder sexuellem Missbrauch von Kindern kommt dem digitalen

[66] Gespeichert in Datenbanken, die von 2500 Register- und Registrierstellen-Betreibern in der ganzen Welt gepflegt werden.

Umfeld zunehmende Bedeutung zu: Daher sind konkrete Maßnahmen und die Schaffung eines Rahmens erforderlich, um die Achtung der Grundrechte zu gewährleisten. Ein wichtiger erster Schritt ist der rasche Abschluss der Verhandlungen über die vorgeschlagenen Rechtsvorschriften zu terroristischen Online-Inhalten[67] und die Umsetzung dieser Vorschriften. Die Stärkung der freiwilligen Zusammenarbeit zwischen Strafverfolgungsbehörden und Privatsektor im Rahmen des **EU-Internetforums** ist ebenfalls von entscheidender Bedeutung, um den Missbrauch des Internets durch Terroristen, gewalttätige Extremisten und Kriminelle zu bekämpfen. Die EU-Meldestelle für Internetinhalte bei Europol wird weiterhin eine entscheidende Rolle bei der Überwachung der Online-Aktivitäten terroristischer Gruppen und der von Plattformen ergriffenen Maßnahmen[68] sowie bei der Weiterentwicklung des **EU-Krisenprotokolls**[69] spielen. Um diese Herausforderungen auf globaler Ebene anzugehen, wird die Kommission darüber hinaus weiterhin mit internationalen Partnern zusammenarbeiten, unter anderem durch ihre Teilnahme am **Globalen Internetforum zur Bekämpfung des Terrorismus**. Im Rahmen des Programms zur Stärkung der Zivilgesellschaft wird weiter daran gearbeitet, die Entwicklung von Alternativ- und Gegennarrativen zu unterstützen[70].

Um die Verbreitung von Hetze im Internet zu verhindern und zu bekämpfen, hat die Kommission 2016 einen Verhaltenskodex für die Bekämpfung illegaler Hassreden im Internet eingeführt, in dem sich Online-Plattformen freiwillig dazu verpflichten, solche Inhalte zu entfernen. Aus der jüngsten Bewertung geht hervor, dass Unternehmen 90 % der gemeldeten Inhalte innerhalb von 24 Stunden prüfen und 71 % der als illegale Hassreden eingestuften Inhalte entfernen. Allerdings müssen die Plattformen die Transparenz und das Feedback an die Nutzer weiter verbessern und für eine kohärente Bewertung der gemeldeten Inhalte sorgen[71].

Das EU-Internetforum wird auch den Austausch über bestehende und in Entwicklung befindliche Technologien zur Bewältigung der Herausforderungen im Zusammenhang mit sexuellem Missbrauch von Kindern im Internet erleichtern. Die Bekämpfung des sexuellen Missbrauchs von Kindern im Internet steht im Mittelpunkt einer neuen Strategie zur verstärkten **Bekämpfung des sexuellen Missbrauchs von Kindern**[72], die darauf angelegt ist, die auf EU-Ebene verfügbaren Instrumente zur Bekämpfung dieser Straftaten optimal zu nutzen. Unternehmen müssen in der Lage sein, ihre Arbeit zur Erkennung und Entfernung von Darstellungen von sexuellem Missbrauch von Kindern im Internet fortzusetzen, und angesichts der durch diese Darstellungen verursachten Schäden muss es einen Rahmen geben, mit dem klare und dauerhafte Verpflichtungen zur Bewältigung des Problems festgelegt werden. In der Strategie soll auch angekündigt werden, dass die Kommission mit der Ausarbeitung sektorspezifischer Rechtsvorschriften zur wirksameren Bekämpfung des sexuellen Missbrauchs von Kindern im Internet – bei uneingeschränkter Achtung der Grundrechte – beginnen wird.

---

[67] Vorschlag zur Verhinderung der Verbreitung terroristischer Online-Inhalte, COM (2018) 640 vom 12. September 2018.

[68] Europol, November 2019.

[69] Ein Europa, das schützt – EU-Krisenprotokoll: Reagieren auf terroristische Inhalte im Internet. (Oktober 2019).

[70] In Verbindung mit der Arbeit des Aufklärungsprogramms gegen Radikalisierung, siehe Abschnitt IV.3.

[71] https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf

[72] EU-Strategie für eine wirksamere Bekämpfung des sexuellen Missbrauchs von Kindern, COM(2020) 607 final.

Ganz allgemein werden durch das künftige Gesetz über digitale Dienste auch die Haftungs- und Sicherheitsvorschriften für digitale Dienste geklärt und verbessert werden und zudem Fehlanreize beseitigt, die Maßnahmen zur Bekämpfung illegaler Inhalte, Waren oder Dienstleistungen behindern.

Um zu erörtern, wie diese Herausforderungen auf globaler Ebene unter Wahrung der Werte und Grundrechte der EU angegangen werden können, wird die Kommission darüber hinaus weiterhin mit internationalen Partnern und dem **Globalen Internetforum zur Bekämpfung des Terrorismus** zusammenarbeiten, unter anderem über den unabhängigen beratenden Ausschuss. Dabei sollten auch neue Themen wie Algorithmen oder Online-Spiele berücksichtigt werden[73].

Hybride Bedrohungen

Ausmaß und Vielfalt hybrider Bedrohungen sind heute beispiellos. In der COVID-19-Krise hat sich dies deutlich gezeigt, als mehrere staatliche und nichtstaatliche Akteure versucht haben, die Pandemie zu instrumentalisieren – insbesondere durch Manipulation des Informationsumfelds und durch Bedrohungen für die zentrale Infrastruktur. Dies droht, den sozialen Zusammenhalt zu schwächen und das Vertrauen in die EU-Institutionen und die Regierungen der Mitgliedstaaten zu untergraben.

Das Konzept der EU zur Abwehr hybrider Bedrohungen ist im Gemeinsamen Rahmen von 2016[74] und in der Gemeinsamen Mitteilung von 2018 über die Stärkung der Resilienz zur Abwehr hybrider Bedrohungen[75] dargelegt. Die Maßnahmen auf EU-Ebene stützen sich auf ein umfangreiches Instrumentarium, das die Nahtstelle zwischen innerer und äußerer Sicherheit abdeckt und auf einem gesamtgesellschaftlichen Ansatz und einer engen Zusammenarbeit mit strategischen Partnern beruht, insbesondere mit der NATO und der G7. Zusammen mit dieser Strategie wird ein Bericht über die Umsetzung des Konzepts der EU für die Abwehr hybrider Bedrohungen veröffentlicht[76]. Auf der Grundlage der parallel zu dieser Strategie vorgelegten Bestandsaufnahme[77] werden die Kommissionsdienststellen und der Europäische Auswärtige Dienst eine **zugangsbeschränkte Online-Plattform** einrichten, auf der die Mitgliedstaaten auf Instrumente und Maßnahmen zur Abwehr hybrider Bedrohungen auf EU-Ebene verweisen können.

Die Verantwortung für die Abwehr hybrider Bedrohungen liegt zwar – aufgrund der inhärenten Verbindung mit der nationalen Sicherheits- und Verteidigungspolitik – in erster Linie bei den Mitgliedstaaten, es gibt jedoch auch einige Schwachstellen, die allen Mitgliedstaaten gemeinsam sind, und manche Bedrohungen erstrecken sich über Grenzen hinweg, wie etwa Bedrohungen, die sich gegen grenzüberschreitende Netze oder Infrastrukturen richten. Die Kommission und der Hohe Vertreter werden ein EU-Konzept für die Abwehr hybrider Bedrohungen ausarbeiten, in dem die externe und die interne Dimension nahtlos integriert werden und in das sowohl nationale als auch EU-weite

[73] Terroristen nutzen zunehmend die Messaging-Systeme von Gaming-Plattformen, um sich untereinander auszutauschen, und junge Terroristen spielen gewalttätige Angriffe in Videospielen nach.

[74] Gemeinsamer Rahmen für die Abwehr hybrider Bedrohungen – eine Antwort der Europäischen Union, JOIN(2016) 18.

[75] Stärkung der Resilienz und Ausbau der Kapazitäten zur Abwehr hybrider Bedrohungen, JOIN(2018) 16.

[76] SWD(2020) 153: Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats [Bericht über die Umsetzung des Gemeinsamen Rahmens für die Bekämpfung hybrider Bedrohungen (2016) und der Gemeinsamen Mitteilung „Stärkung der Resilienz und Ausbau der Kapazitäten zur Abwehr hybrider Bedrohungen“ (2018)].

[77] SWD(2020) 152: Mapping of the measures related to enhancing resilience and countering hybrid threats [Bestandsaufnahme der Maßnahmen zur Stärkung der Resilienz und zur Abwehr hybrider Bedrohungen].

Erwägungen einfließen werden. Es gilt, das gesamte Maßnahmenspektrum abzudecken – von der Früherkennung, Analyse, Sensibilisierung, Stärkung der Resilienz und Prävention bis hin zur Krisenreaktion und Folgenbewältigung.

Neben einer verstärkten Umsetzung wird angesichts der fortlaufenden Weiterentwicklung der hybriden Bedrohungen ein besonderer Schwerpunkt darauf liegen, **Erwägungen zu hybriden Bedrohungen durchgehend in die Politikgestaltung einzubeziehen**, um mit den dynamischen Entwicklungen Schritt zu halten und sicherzustellen, dass keine potenziell relevante Initiative übersehen wird. Zudem werden die Auswirkungen neuer Initiativen auch mithilfe von Kriterien bewertet, die sich speziell auf hybride Bedrohungen beziehen, und es werden auch Initiativen in Bereichen einbezogen werden, die bisher nicht in den Anwendungsbereich des Rahmens zur Abwehr hybrider Bedrohungen fallen, wie Bildung, Technologie und Forschung. Dieser Ansatz würde von den Arbeiten zur Konzeptualisierung hybrider Bedrohungen profitieren, die einen umfassenden Überblick über die verschiedenen Instrumente bieten, die von Angreifern genutzt werden können[78]. Ziel sollte es sein, sicherzustellen, dass der Entscheidungsprozess durch eine regelmäßige, umfassende, auf nachrichtendienstlichen Erkenntnissen beruhende Berichterstattung über die Entwicklung hybrider Bedrohungen untermauert wird. Dies wird sich weitgehend auf die Nachrichtendienste der Mitgliedstaaten und auf die weitere Verbesserung der nachrichtendienstlichen Zusammenarbeit mit den zuständigen Dienststellen der Mitgliedstaaten über das EU-INTCEN stützen.

Zum Ausbau der **Lageerfassung** werden die Kommissionsdienststellen und der Europäische Auswärtige Dienst Möglichkeiten zur Straffung des Informationsflusses aus verschiedenen Quellen, einschließlich der Mitgliedstaaten, sowie von EU-Agenturen wie ENISA, Europol und Frontex prüfen. Die EU-Analyseeinheit für hybride Bedrohungen bleibt auch künftig die Anlaufstelle der EU für die Bewertung hybrider Bedrohungen. Die **Stärkung der Resilienz** ist von zentraler Bedeutung für die Prävention von und den Schutz vor hybriden Bedrohungen. Es ist daher sehr wichtig, Fortschritte in diesem Bereich systematisch zu verfolgen und objektiv zu messen. Ein erster Schritt wird darin bestehen, sowohl für die Mitgliedstaaten als auch für die Organe und Einrichtungen der EU sektorspezifische Referenzwerte für die Resilienz gegenüber hybriden Bedrohungen festzulegen. Schließlich sollte zur Verbesserung der **Krisenvorsorge im Bereich hybrider Bedrohungen** das bestehende Protokoll, wie im EU-Playbook von 2016[79]vorgesehen, überarbeitet werden, um der derzeit erwogenen umfassenderen Überprüfung und Stärkung des Krisenreaktionssystems der EU Rechnung zu tragen[80]. Ziel ist es, die Wirkung des Handelns der EU zu maximieren, indem sektorspezifische Bewältigungsmaßnahmen rasch zusammengeführt und eine nahtlose Zusammenarbeit mit unseren Partnern, vor allem der NATO, sichergestellt wird.

Zentrale Maßnahmen

[78] The Landscape of Hybrid Threats: A conceptual Model [Die Landschaft hybrider Bedrohungen: ein konzeptionelles Modell], JRC117280, gemeinsam ausgearbeitet von der Gemeinsamen Forschungsstelle und dem Kompetenzzentrum für die Abwehr hybrider Bedrohungen.

[79] Gemeinsames Protokoll der EU für das operative Vorgehen bei der Abwehr hybrider Bedrohungen („EU Playbook"), SWD(2016) 227.

[80] Im Anschluss an ihre Videokonferenz vom 26. März 2020 nahmen die Mitglieder des Europäischen Rates eine Erklärung zu den EU-Maßnahmen als Reaktion auf den COVID-19-Ausbruch an, in der sie die Kommission ersuchten, Vorschläge für ein ehrgeizigeres und umfassenderes Krisenmanagementsystem in der EU zu unterbreiten.

- Sicherstellung der Umsetzung und der Zweckmäßigkeit der Rechtsvorschriften zur Cyberkriminalität
- Eine EU-Strategie für eine wirksamere Bekämpfung des sexuellen Missbrauchs von Kindern
- Vorschläge zur Erkennung und Entfernung von Darstellungen von sexuellem Kindesmissbrauch
- Ein EU-Konzept für die Abwehr hybrider Bedrohungen
- Überprüfung des Protokolls der EU für das operative Vorgehen bei der Abwehr hybrider Bedrohungen (EU-Playbook)
- Prüfung der Möglichkeiten zur Verbesserung der Strafverfolgungskapazität bei digitalen Ermittlungen

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

Terrorismus und Radikalisierung

Die Terrorgefahr in der EU ist nach wie vor hoch. Zwar gibt es insgesamt weniger Anschläge, doch kann ein Anschlag allein schon verheerende Auswirkungen haben. Radikalisierung kann zudem polarisieren und den sozialen Zusammenhalt allgemein destabilisieren. Die Mitgliedstaaten tragen die Hauptverantwortung für die Bekämpfung von Terrorismus und Radikalisierung. Die immer größer werdende grenz- und sektorübergreifende Dimension der Bedrohung macht jedoch weitere Schritte bei der Zusammenarbeit und Koordinierung auf EU-Ebene erforderlich. Die wirksame Umsetzung der EU-Rechtsvorschriften zur Terrorismusbekämpfung, unter anderem restriktiver Maßnahmen[81], hat Vorrang. Nach wie vor gilt es, das Mandat der Europäischen Staatsanwaltschaft auf terroristische Straftaten mit grenzüberschreitendem Bezug auszuweiten.

Die Bekämpfung des Terrorismus beginnt mit der Bekämpfung der eigentlichen Ursachen. Die Polarisierung der Gesellschaft, die tatsächliche oder wahrgenommene Diskriminierung und andere psychologische und soziologische Faktoren können die Menschen empfänglicher für radikale Diskurse machen. Die Bekämpfung der **Radikalisierung** geht daher Hand in Hand mit der Förderung des sozialen Zusammenhalts auf lokaler, nationaler und europäischer Ebene. In den letzten zehn Jahren sind mehrere wirkungsvolle Initiativen und Strategien entwickelt worden, insbesondere durch das EU-Aufklärungsnetzwerk gegen Radikalisierung und die EU-Initiative Städte gegen Radikalisierung.[82] Es ist jetzt an der Zeit zu prüfen, wie die Strategien, Initiativen und Fonds der EU zur Bekämpfung der Radikalisierung besser aufeinander abgestimmt werden können. Entsprechende Maßnahmen können unter Beteiligung aller Interessenträger, darunter der Fachkräfte vor Ort sowie der

[81] Mit Blick auf die Bekämpfung des Terrorismus hat der Rat allgemeine restriktive Maßnahmen gegen ISIL (Da'esh) und Al-Qaida sowie konkrete restriktive Maßnahmen gegen bestimmte Personen und Organisationen angenommen. Siehe Weltkarte der EU-Sanktionen (https://www.sanctionsmap.eu/#/main) mit einem Überblick über alle restriktiven Maßnahmen.

[82] Die Pilotinitiative „EU-Städte gegen Radikalisierung“ verfolgt zwei Ziele: Sie soll den Austausch von Fachwissen zwischen Städten in der EU fördern und Rückmeldungen dazu einholen, wie lokale Gemeinschaften auf EU-Ebene am besten unterstützt werden können.

politischen Entscheidungsträger und Hochschulen, zur Entwicklung von Fähigkeiten und Kompetenzen, zur Verbesserung der Zusammenarbeit, zur Stärkung der Faktengrundlage und zur Evaluierung der Fortschritte beitragen.[83] Weiche politische Maßnahmen wie Bildung, Kultur, Jugend und Sport können dazu beitragen, Radikalisierung zu verhindern, indem sie gefährdeten Jugendlichen Perspektiven eröffnen und den Zusammenhalt innerhalb der EU fördern.[84] Zu den prioritären Bereichen gehören Maßnahmen zur Früherkennung und zum Risikomanagement, zur Stärkung der Resilienz und zum Ausstieg, sowie zur Rehabilitation und Wiedereingliederung in die Gesellschaft.

Terroristen versuchen, **chemische, biologische, radiologische und nukleare** (CBRN)[85] Stoffe zu erwerben und als Waffe einzusetzen, sowie sich Wissen und Fähigkeiten zu deren Verwendung anzueignen.[86] Auf das Potenzial, das Anschläge mit CBRN-Stoffen haben, wird in terroristischer Propaganda ausführlich eingegangen. Aufgrund ihres potenziell hohen Schadens ist besondere Aufmerksamkeit erforderlich. Aufbauend auf dem Ansatz zur Regelung des Zugangs zu Ausgangsstoffen für Explosivstoffe wird die Kommission prüfen, den Zugang zu bestimmten gefährlichen Chemikalien, die zur Durchführung von Anschlägen verwendet werden könnten, zu beschränken. Der Ausbau der Kapazitäten der EU zur Katastrophenabwehr (rescEU) im Bereich der CBRN-Stoffe wird ebenfalls von entscheidender Bedeutung sein. Die Zusammenarbeit mit Drittländern ist wichtig, um eine gemeinsame CBRN-Sicherheitskultur zu schaffen und die CBRN-Exzellenzzentren der EU weltweit in vollem Umfang nutzen zu können. Zu dieser Zusammenarbeit gehören auch nationale Defizit- und Risikobewertungen, die Unterstützung nationaler und regionaler CBRN-Aktionspläne, der Austausch bewährter Verfahren und Maßnahmen zum Aufbau von CBRN-Kapazitäten.

Die EU hat die fortschrittlichsten Rechtsvorschriften der Welt, um den Zugang zu **Ausgangsstoffen für Explosivstoffe**[87] zu beschränken und verdächtige Transaktionen aufzudecken, die auf den Bau improvisierter Sprengkörper abzielen. Nach wie vor ist die Gefahr, die von der Eigenherstellung von Explosivstoffen ausgeht, hoch, da diese EU-weit in zahlreichen Anschlägen verwendet werden.[88] Der erste Schritt muss darin bestehen, die Vorschriften umzusetzen sowie sicherzustellen, dass das Online-Umfeld keine Umgehung der Kontrollen ermöglicht.

Die effektive Verfolgung jener, die terroristische Straftaten begangen haben, unter anderem **ausländische terroristische Kämpfer**, die sich derzeit in Syrien und im Irak aufhalten, ist ebenfalls ein wichtiges Element der Terrorismusbekämpfung. Darum kümmern sich zwar in erster Linie die Mitgliedstaaten, doch kann die EU durch Koordinierung und Unterstützung den Mitgliedstaaten dabei helfen, gemeinsame Herausforderungen gemeinsam anzugehen.

---

[83] Beispielsweise Finanzierung im Rahmen des Europäischen Sicherheitsfonds und des Programms „Rechte, Gleichstellung und Unionsbürgerschaft".

[84] EU-Maßnahmen wie Virtueller Erasmus+-Austausch, eTwinning.

[85] In den vergangenen zwei Jahren gab es sowohl in Europa (Frankreich, Deutschland, Italien) als auch anderswo (Tunesien, Indonesien) mehrere Anschläge unter Verwendung biologischer Stoffe (in der Regel Toxine auf Pflanzenbasis).

[86] Der Rat hat restriktive Maßnahmen gegen die Verbreitung und den Einsatz chemischer Waffen angenommen.

[87] Chemikalien, die zur Eigenherstellung von Explosivstoffen missbraucht werden können. Diese sind in der Verordnung (EU) 2019/1148 über die Vermarktung und Verwendung von Ausgangsstoffen für Explosivstoffe geregelt.

[88] Beispiele für solche verheerenden Anschläge sind unter anderem die Anschläge in Oslo (2011), Paris (2015), Brüssel (2016) und Manchester (2017). Bei einem Anschlag mit einem selbst hergestellten Sprengkörper wurden 2019 in Lyon 13 Menschen verletzt.

Ein wichtiger Schritt sind daher die laufenden Maßnahmen zur vollständigen Umsetzung[89] der Vorschriften zur Grenzsicherheit und die umfassende Nutzung aller einschlägigen EU-Datenbanken zum Austausch von Informationen über bekannte Verdächtige. Neben der Identifizierung von Personen, von denen ein hohes Risiko ausgeht, bedarf es auch einer Strategie zur Wiedereingliederung und Rehabilitation. Eine berufsübergreifende Zusammenarbeit, darunter mit Strafvollzugspersonal und Bewährungshelfern, wird der Justiz dabei helfen, den Radikalisierungsprozess bis hin zum gewaltbereiten Extremismus besser zu verstehen und einen fundierteren Ansatz in Bezug auf Haftstrafen und Haftalternativen zu verfolgen.

Die Herausforderung, die ausländische terroristische Kämpfer darstellen, macht die Verknüpfung von innerer und **äußerer Sicherheit deutlich**. Die Zusammenarbeit bei der Terrorismusbekämpfung und der Prävention und Bekämpfung von Radikalisierung und gewaltbereitem Extremismus ist von zentraler Bedeutung für die innere Sicherheit der EU.[90] Gestützt auf das Fachwissen des Netzwerks der Experten für Terrorismusbekämpfung/Sicherheit müssen weitere Schritte zum Aufbau von Partnerschaften zur Terrorismusbekämpfung und zur Zusammenarbeit mit Ländern in der Nachbarschaft und darüber hinaus unternommen werden. Der gemeinsame Aktionsplan zur Terrorismusbekämpfung für den westlichen Balkan ist ein gutes Beispiel für eine solche Zusammenarbeit. Insbesondere gilt es, die Fähigkeit der Partnerländer zu unterstützen, ausländische terroristische Kämpfer zu identifizieren und ausfindig zu machen. Die EU wird auch weiterhin die multilaterale Zusammenarbeit fördern und dabei mit den führenden globalen Akteuren in diesem Bereich, wie den Vereinten Nationen, der NATO, dem Europarat, Interpol und der OSZE, zusammenarbeiten. Darüber hinaus wird sie mit dem Globalen Forum „Terrorismusbekämpfung“ und der internationalen Allianz gegen Da'esh sowie mit einschlägigen Akteuren der Zivilgesellschaft zusammenarbeiten. Die außenpolitischen Instrumente der Union, unter anderem im Bereich Entwicklung und Zusammenarbeit, spielen bei der Zusammenarbeit mit Drittstaaten ebenfalls eine wichtige Rolle, wenn es darum geht, Terrorismus und Piraterie zu verhindern. Die internationale Zusammenarbeit ist zudem von entscheidender Bedeutung, um alle Quellen der **Terrorismusfinanzierung** trockenzulegen, beispielsweise mithilfe der Arbeitsgruppe „Bekämpfung der Geldwäsche und der Terrorismusfinanzierung“.

Organisierte Kriminalität

Die organisierte Kriminalität verursacht enorme wirtschaftliche und personelle Kosten. Die wirtschaftlichen Verluste aufgrund von organisierter Kriminalität und Korruption belaufen sich auf 218 Milliarden € bis 282 Milliarden EUR jährlich.[91] 2017 liefen in Europa zu mehr als 5000 organisierten kriminellen Vereinigungen Ermittlungen – das ist ein Anstieg um 50 % gegenüber 2013.[92] Die organisierte Kriminalität operiert zunehmend grenzüberschreitend aus der unmittelbaren Nachbarschaft der EU. Es bedarf daher einer engeren operativen Zusammenarbeit und eines intensiveren Informationsaustauschs mit Partnern in der Nachbarschaft.

---

89 Einschließlich des neuen Mandats der Europäischen Agentur für die Grenz- und Küstenwache (Frontex).

90 In den Schlussfolgerungen des Rates vom 16. Juni 2020 wurde betont, dass es die Bürgerinnen und Bürger der EU vor Terrorismus und gewaltbereitem Extremismus in all ihren Formen und ungeachtet ihres Ursprungs zu schützen und das auswärtige Engagement und die Maßnahmen der EU im Bereich Terrorismusbekämpfung in bestimmten vorrangigen geografischen und thematischen Bereichen weiter zu verstärken gilt.

91 In Bezug auf das Bruttoinlandsprodukt (BIP); Europol-Bericht: „Does crime still pay? – Criminal asset recovery in the EU“ (2016).

92 Bewertungen der Bedrohungslage im Bereich der schweren und organisierten Kriminalität(SOCTA) (Europol, 2013 und 2017).

Die Kriminalität verlagert sich ins Internet und führt zu neuen Herausforderungen: Während der COVID-19-Pandemie nahmen Online-Betrügereien gegen risikoanfällige Gruppen sowie Diebstähle und Einbrüche zur Entwendung von Gesundheits- und Hygieneartikeln rasant zu.[93] Die EU muss ihre Arbeiten zur Bekämpfung der organisierten Kriminalität auch auf internationaler Ebene intensivieren und mehr Instrumente einsetzen, um den Geschäftsmodellen der organisierten Kriminalität die Grundlage zu entziehen. Die Bekämpfung der organisierten Kriminalität erfordert zudem eine enge Zusammenarbeit mit lokalen und regionalen Behörden sowie der Zivilgesellschaft, die wichtige Partner bei der Kriminalprävention sowie bei der Unterstützung von Opfern sind, wobei insbesondere die Behörden in den Grenzregionen gefordert sind. Diese Arbeiten werden in einer **Agenda zur Bekämpfung der organisierten Kriminalität** zusammengefasst.

Mehr als ein Drittel der in der EU aktiven organisierten kriminellen Vereinigungen sind an der Herstellung, dem illegalen Handel oder dem Vertrieb von Drogen beteiligt. Im Jahr 2019 starben mehr als achttausend Drogenabhängige an einer Überdosis. Der Großteil des **Drogenhandels** verläuft grenzüberschreitend, wobei viele Gewinne in die legale Wirtschaft einfließen.[94] Eine neue EU-Agenda zur Drogenbekämpfung[95] wird die Anstrengungen der EU und der Mitgliedstaaten zur Reduzierung des Drogenangebots und der Drogennachfrage unterstützen und hierzu gemeinsame Maßnahmen zur Lösung gemeinsamer Probleme sowie zur Intensivierung des Dialogs und der Zusammenarbeit zwischen der EU und externen Partnern in Drogenfragen formulieren. Im Anschluss an eine Evaluierung der Europäischen Beobachtungsstelle für Drogen und Drogensucht wird die Kommission prüfen, ob deren Mandat aktualisiert werden muss, um neuen Herausforderungen gerecht werden zu können.

Organisierte kriminelle Vereinigungen und Terroristen sind auch am Handel mit **illegalen Feuerwaffen maßgeblich beteiligt**. Zwischen 2009 und 2018 gab es in Europa 23 Massenschießereien, bei denen mehr als 340 Menschen ums Leben kamen.[96] Feuerwaffen gelangen häufig über die unmittelbare Nachbarschaft in die EU.[97] Dies macht deutlich, dass die Koordinierung und Zusammenarbeit sowohl innerhalb der EU als auch mit internationalen Partnern und insbesondere mit Interpol intensiviert werden muss, um die Erhebung von Informationen und die Berichterstattung über die Beschlagnahme von Feuerwaffen zu vereinheitlichen. Es ist ferner von entscheidender Bedeutung, die Rückverfolgbarkeit von Waffen auch über das Internet zu verbessern und den Informationsaustausch zwischen Genehmigungsbehörden und Strafverfolgungsbehörden sicherzustellen. Die Kommission hat einen neuen **EU-Aktionsplan gegen den unerlaubten Handel mit Feuerwaffen**[98] vorgelegt und wird auch prüfen, ob die Vorschriften über Ausfuhrgenehmigungen sowie Einfuhr- und Durchfuhrmaßnahmen für Feuerwaffen noch zweckmäßig sind.[99]

---

93 Europol, 2020.

94 EU-Drogenmarktbericht der EMCDDA und von Europol (November 2019).

95 EU-Agenda zur Drogenbekämpfung und Aktionsplan 2021-2025 (COM(2020) 606).

96 „Armed to kill"(Flemish Peace Institute, Oktober 2019).

97 Die EU finanziert seit 2002 die Bekämpfung der Verbreitung von Kleinwaffen und leichten Waffen in der Region sowie den illegalen Handel damit; insbesondere finanziert sie das südosteuropäische Netz der Feuerwaffenexperten (SEEFEN). Seit 2019 sind die Partner des Westbalkans vollumfänglich an der Priorität „Feuerwaffen" der Europäischen multidisziplinären Plattform gegen kriminelle Bedrohungen (EMPACT) beteiligt.

98 COM(2020) 608.

99 Verordnung (EU) Nr. 258/2012 zur Umsetzung des Artikels 10 des Protokolls der Vereinten Nationen gegen die unerlaubte Herstellung von Schusswaffen und gegen den unerlaubten Handel damit.

Für kriminelle Vereinigungen sind Migranten und Menschen, die internationalen Schutz benötigen, wie eine Ware. 90 % der irregulären Migranten, die in der EU ankommen, werden über kriminelle Netze eingeschleust.[100] Die Schleusung von Migranten ist häufig mit anderen Formen der organisierten Kriminalität verbunden, insbesondere dem Menschenhandel.[101]. Abgesehen von dem hohen menschlichen Preis, den der Menschenhandel fordert, schätzt Europol, dass sich die jährlichen Gewinne aller Formen der Ausbeutung durch Menschenhandel weltweit auf 29,4 Milliarden EUR belaufen. Diese Form der grenzüberschreitenden Kriminalität speist sich aus der illegalen Nachfrage von innerhalb und außerhalb der EU und wirkt sich auf alle EU-Mitgliedstaaten aus. Aufgrund der schlechten Erfolgsbilanz bei der Aufdeckung, Verfolgung und Verurteilung dieser Straftaten ist ein neues Konzept für ein energisches Vorgehen notwendig. Die einzelnen Maßnahmen sollen in einem neuen **umfassenden Konzept zur Bekämpfung des Menschenhandels** gebündelt werden. Darüber hinaus wird die Kommission einen **neuen EU-Aktionsplan gegen die Schleusung von Migranten** für den Zeitraum 2021-2025 vorlegen. Schwerpunkt ist beides Mal die Bekämpfung krimineller Netze durch eine intensivere Zusammenarbeit und verstärkte Unterstützung der Arbeit der Strafverfolgungsbehörden.

Organisierte kriminelle Vereinigungen sowie Terroristen suchen auch nach Gewinnmöglichkeiten in anderen Bereichen, insbesondere solchen, die hohe Gewinne mit geringem Entdeckungsrisiko bieten, wie **Umweltkriminalität**. Die illegale Jagd und der illegale Artenhandel, der illegale Bergbau, der illegale Holzeinschlag sowie die illegale Abfallentsorgung und -verbringung stehen weltweit an vierter Stelle krimineller Geschäftstätigkeit.[102] Auch die Emissionshandelssysteme und die europäischen Energiezertifizierungssysteme werden kriminell ausgebeutet ebenso wie Finanzmittel, die für die ökologische Widerstandsfähigkeit und die nachhaltige Entwicklung bereitgestellt werden. Die Kommission fördert Maßnahmen der EU, der Mitgliedstaaten und der internationalen Gemeinschaft zur verstärkten Bekämpfung der Umweltkriminalität[103] und prüft darüber hinaus, ob die Richtlinie über den strafrechtlichen Schutz der Umwelt[104] noch ihren Zweck erfüllt. Der **illegale Handel mit Kulturgütern** gehört inzwischen ebenfalls zu den lukrativsten kriminellen Aktivitäten. Er ist eine Finanzierungsquelle für Terroristen und die organisierte Kriminalität und weitet sich aus. Es sollten Schritte erwogen werden, um die Online- und Offline-Rückverfolgbarkeit von Kulturgütern im Binnenmarkt und bei der Zusammenarbeit mit Drittländern, wo Kulturgüter geraubt werden, zu verbessern, sowie um Strafverfolgung und Wissenschaft aktiv zu unterstützen.

Wirtschafts- und Finanzstraftaten sind sehr komplex und betreffen jährlich Millionen von Bürgerinnen und Bürgern und tausende Unternehmen in der EU. Betrugsbekämpfung ist wichtig und erfordert Maßnahmen auf EU-Ebene. Europol unterstützt gemeinsam mit Eurojust, der Europäischen Staatsanwaltschaft und dem Europäischen Amt für Betrugsbekämpfung die Mitgliedstaaten und die EU dabei, die Wirtschafts- und Finanzmärkte und das Geld der europäischen Steuerzahler vor Betrug zu schützen. Die Europäische Staatsanwaltschaft wird Ende 2020 voll arbeitsfähig sein und Straftaten gegen den EU-Haushalt, wie Betrug, Korruption und Geldwäsche, untersuchen, verfolgen und vor

[100] Quelle: Europol.
[101] Europol, EMSC, 4. Jahresbericht.
[102] UNEP-INTERPOL Rapid Response Assessment: The Rise of Environmental Crime, Juni 2016.
[103] Siehe „Der europäische Grüne Deal“ (COM(2019) 640 final).
[104] Richtlinie 2008/99/EG über den strafrechtlichen Schutz der Umwelt.

Gericht bringen. Sie wird auch gegen den grenzüberschreitenden Mehrwertsteuerbetrug vorgehen, der den Steuerzahler jährlich mindestens 50 Milliarden EUR kostet.

Die Kommission wird darüber hinaus den weiteren Erwerb von Fachwissen und die Ausarbeitung eines Rechtsrahmens für neu auftretende Risiken, wie Kryptoanlagen und neue Zahlungssysteme, unterstützen. Sie wird insbesondere eine Strategie für den Umgang mit dem neuen Phänomen von Kryptoanlagen wie Bitcoin und den Auswirkungen dieser neuen Technologien auf die Art und Weise, wie finanzielle Vermögenswerte begeben, ausgetauscht, übertragen und erworben werden, erarbeiten.

In der Europäischen Union sollte es keine Toleranz für illegale Geldströme geben. Die EU hat in über dreißig Jahren einen soliden Rechtsrahmen für die Verhütung und Bekämpfung von **Geldwäsche** und Terrorismusfinanzierung entwickelt, der den Anforderungen an den Schutz personenbezogener Daten in vollem Umfang Rechnung trägt. Nichtsdestotrotz besteht zunehmend Einvernehmen darüber, dass die Umsetzung des aktuellen Rechtsrahmens wesentlich verbessert werden muss. Erhebliche Unterschiede bei dessen Anwendung und gravierende Mängel bei der Durchsetzung der Vorschriften müssen angegangen werden. Wie im Aktionsplan vom Mai 2020[105] dargelegt, werden derzeit Optionen zur Verbesserung des EU-Rahmens zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung ausgelotet. Dabei werden Bereiche wie die Vernetzung nationaler zentraler Bankkontenregister einbezogen, die den Zugang der zentralen Meldestellen und zuständigen Behörden zu Finanzdaten entscheidend beschleunigen könnte.

Die **Gewinne organisierter krimineller Vereinigungen** in der EU werden auf jährlich 110 Milliarden EUR geschätzt. Zu den derzeitigen Maßnahmen gehören harmonisierte Rechtsvorschriften über die Abschöpfung und Einziehung von Vermögenswerten[106], um die Sicherstellung und Einziehung von Erträgen aus Straftaten in der EU zu verbessern und das gegenseitige Vertrauen und die wirksame grenzüberschreitende Zusammenarbeit zwischen den Mitgliedstaaten zu erleichtern. Nur etwa 1 % dieser Gewinne wird eingezogen[107], sodass organisierte kriminelle Vereinigungen in die Expansion ihrer kriminellen Aktivitäten investieren und die legale Wirtschaft infiltrieren können. Insbesondere kleine und mittlere Unternehmen, die nur schwer Zugang zu Krediten haben, sind ein zentrales Ziel der Geldwäsche. Die Kommission wird die Umsetzung der Rechtsvorschriften[108] und den möglichen Bedarf an weiteren gemeinsamen Vorschriften, darunter die Einziehung ohne vorhergehende Verurteilung, prüfen. Die Vermögensabschöpfungsstellen[109] könnten als wichtige Akteure bei der Rückführung von Vermögenswerten auch mit besseren Instrumenten ausgestattet werden, um Vermögen EU-weit schneller zu ermitteln und aufzuspüren und damit die Einziehungsquoten zu erhöhen.

Es besteht ein enger Zusammenhang zwischen organisierter Kriminalität und **Korruption**. Grob geschätzt kostet allein die Korruption die EU-Wirtschaft jährlich

[105] Aktionsplan zur Verhinderung von Geldwäsche und Terrorismusfinanzierung (C(2020) 2800).

[106] Nach EU-Recht müssen in allen Mitgliedstaaten Vermögensabschöpfungsstellen eingerichtet werden.

[107] Bericht über die Abschöpfung und Einziehung von Vermögenswerten: Straftaten dürfen sich nicht auszahlen (COM(2020) 217 final).

[108] Richtlinie 2014/42/EU des Europäischen Parlaments und des Rates über die Sicherstellung und Einziehung von Tatwerkzeugen und Erträgen aus Straftaten.

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

120 Milliarden EUR.[110] Die Prävention und Bekämpfung von Korruption werden weiterhin regelmäßig im Rahmen des Rechtsstaatlichkeitsmechanismus sowie des Europäischen Semesters überwacht. Im Rahmen des Europäischen Semesters werden Herausforderungen bei der Bekämpfung von Korruption etwa im Bereich der Vergabe öffentlicher Aufträge, der öffentlichen Verwaltung, des Unternehmensumfelds oder Gesundheitswesens bewertet. Der neue Jahresbericht der Kommission über die Rechtsstaatlichkeit wird sich auch mit der Korruptionsbekämpfung auseinandersetzen und einen präventiven Dialog mit nationalen Behörden und Interessenträgern auf EU- und nationaler Ebene ermöglichen. Von Organisationen der Zivilgesellschaft können ebenfalls entscheidende Impulse für Maßnahmen der Behörden zur Prävention und Bekämpfung von organisierter Kriminalität und Korruption ausgehen. Diese Gruppen könnten in einem gemeinsamen Forum sinnvoll zusammengeführt werden. Aufgrund ihres grenzübergreifenden Charakters ist die Zusammenarbeit mit den Nachbarregionen der EU und deren Unterstützung bei der Bekämpfung der organisierten Kriminalität und Korruption eine weitere wichtige Dimension.

Zentrale Maßnahmen
• EU-Agenda für Terrorismusbekämpfung mit verbesserten Maßnahmen zur Bekämpfung der Radikalisierung in der EU • Neue Kooperation mit wichtigen Drittstaaten und internationalen Organisationen bei der Terrorismusbekämpfung • Agenda zur Bekämpfung der organisierten Kriminalität, einschließlich des Menschenhandels • EU-Agenda zur Drogenbekämpfung und Aktionsplan 2021-2025 • Evaluierung der Europäischen Beobachtungsstelle für Drogen und Drogensucht • EU-Aktionsplan gegen den unerlaubten Handel mit Feuerwaffen (2020-2025) • Überarbeitung der Rechtsvorschriften über die Sicherstellung und Einziehung von Vermögenswerten sowie über Vermögensabschöpfungsstellen • Bewertung der Richtlinie über den strafrechtlichen Schutz der Umwelt • EU-Aktionsplan gegen die Schleusung von Migranten (2021-2025)

4. Eine starke europäische Sicherheitsgemeinschaft

Eine echte, effektive Sicherheitsunion muss das gemeinsame Anliegen aller Bereiche unserer Gesellschaft sein. Um Vorsorge und Resilienz auf allen Ebenen zu gewährleisten, vor allem mit Blick auf jene, die besonders gefährdet sind wie Opfer und Zeugen, müssen alle Beteiligten – die Exekutive einschließlich der Strafverfolgung ebenso wie der Privatsektor, das Bildungswesen und die Bürger selbst – eingebunden, entsprechend ausgestattet und gut miteinander vernetzt werden.

Alle Politikbereiche brauchen eine Sicherheitsdimension. Die EU kann auf allen Ebenen einen Beitrag dazu leisten. Häusliche Gewalt gehört in der EU zu den größten Sicherheitsrisiken. 22 % aller Frauen in der EU haben bereits Gewalt durch einen Intimpartner erfahren.[111] Der Beitritt der EU zum Übereinkommen von Istanbul zur

[110] Wie hoch die durch Korruption verursachten Kosten für die Wirtschaft insgesamt sind, lässt sich nur schwer feststellen. Entsprechende Schätzungen der Internationalen Handelskammer, von Transparency International, der Initiative „Global Compact“ der Vereinten Nationen und dem Weltwirtschaftsforum legen nahe, dass Korruption 5 % des weltweiten BIP ausmacht.

[111] Eine Union der Gleichheit: Strategie für die Gleichstellung der Geschlechter 2020-2025 (COM(2020) 152).

Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt bleibt eine der wichtigsten Prioritäten. Sollten die Verhandlungen auch weiterhin nicht vorankommen, wird die Kommission andere Maßnahmen ergreifen und unter anderem vorschlagen, Gewalt gegen Frauen in die im Vertrag festgelegten, EU-weit geltenden Straftatbestände aufzunehmen, um die Ziele des Übereinkommens zu erreichen.

Zusammenarbeit und Informationsaustausch

Einer der wichtigsten Beiträge, die die EU zum Schutz der Bürger leisten kann, ist es, diejenigen, die für die Sicherheit verantwortlich sind, so zu unterstützen, dass sie gut zusammenarbeiten. Zusammenarbeit und Informationsaustausch sind die wirksamsten Instrumente zur Bekämpfung von Kriminalität und Terrorismus und zur Durchsetzung von Recht und Gesetz. Sie müssen zielgerichtet und zeitnah erfolgen, wenn sie wirksam sein sollen. Sie müssen in gemeinsame Garantien und Kontrollen eingebettet sein, um Vertrauen zu schaffen.

Zur Weiterentwicklung der **operativen Zusammenarbeit zwischen den Mitgliedstaaten bei der Strafverfolgung wurden** diverse EU-Instrumente und sektorspezifische Strategien[112] eingeführt. Eines der wichtigsten Instrumente der EU zur Unterstützung der Zusammenarbeit zwischen den Mitgliedstaaten bei der Strafverfolgung ist das Schengener Informationssystem, mit dem Daten über gesuchte und vermisste Personen und Gegenstände in Echtzeit ausgetauscht werden können. Sein Erfolg zeigt sich an der Festnahme von Straftätern, der Beschlagnahme von Drogen und der Rettung potenzieller Opfer.[113] Durch eine einheitlichere Anwendung und Modernisierung der verfügbaren Instrumente ließe sich die Zusammenarbeit noch verbessern. Der Großteil des EU-Rechtsrahmens, der der operativen Zusammenarbeit im Bereich der Strafverfolgung zugrunde liegt, wurde vor 30 Jahren entworfen. Ein komplexes Netz bilateraler Abkommen, von denen viele inzwischen überholt sind oder unzureichend genutzt werden, birgt die Gefahr einer uneinheitlichen Rechtsanwendung auf Ebene der Mitgliedstaaten. In kleineren Ländern oder Binnenstaaten müssen grenzüberschreitend tätige Strafverfolgungsbeamte bei ihrem Einsatz in manchen Fällen bis zu sieben verschiedene Regelwerke beachten: Dies hat zur Folge, dass einige Einsätze wie die Nacheile von Verdächtigen über Binnengrenzen schlicht und einfach nicht stattfinden. Auch die operative Zusammenarbeit bei neuen Technologien wie Drohnen fällt nicht unter den derzeitigen EU-Rahmen.

Die operative Wirksamkeit kann durch eine gezielte Zusammenarbeit bei der Strafverfolgung unterstützt werden, die auch dazu beitragen kann, wichtige Unterstützung für andere politische Ziele zu leisten, etwa durch die Bereitstellung von Sicherheitserkenntnissen für die Überprüfung ausländischer Direktinvestitionen. Die Kommission wird prüfen, welchen Beitrag ein Kodex für die polizeiliche Zusammenarbeit leisten könnte. Die Strafverfolgungsbehörden der Mitgliedstaaten greifen zunehmend auf Unterstützung und Fachwissen auf EU-Ebene zurück. So kommt dem EU-INTCEN inzwischen eine Schlüsselrolle bei der Förderung des Austauschs strategischer nachrichtendienstlicher Erkenntnisse zwischen den Nachrichten- und Sicherheitsdiensten der Mitgliedstaaten zu, die eine nachrichtendienstliche Lageerfassung für die EU-Organe ermöglichen.[114] Auch **Europol** kann durch eine erweiterte Zusammenarbeit mit Drittländern

[112] Z. B. der Aktionsplan für die EU-Strategie für maritime Sicherheit, der erhebliche Verbesserungen bei der Zusammenarbeit zwischen den zuständigen EU-Agenturen im Bereich der Küstenwache gebracht hat.

[113] Die Bekämpfung der organisierten Kriminalität durch die EU im Jahr 2019 (Rat, 2020).

[114] Das EU-INTCEN dient als einziges Zugangstor für die Nachrichten- und Sicherheitsdienste der Mitgliedstaaten und soll der EU eine erkenntnisgestützte Lageerfassung ermöglichen.

im Einklang mit anderen außenpolitischen Maßnahmen und Instrumenten der EU eine Schlüsselrolle bei der Bekämpfung von Kriminalität und Terrorismus spielen. Europol steht jedoch heute vor einer Reihe schwerwiegender Sachzwänge, insbesondere in Bezug auf den direkten Austausch personenbezogener Daten mit privaten Parteien, die es daran hindern, die Mitgliedstaaten bei der Bekämpfung von Terrorismus und Kriminalität wirksam zu unterstützen. Das Mandat von Europol wird derzeit daraufhin geprüft, wie es so verbessert werden kann, dass die Agentur ihre Aufgaben in vollem Umfang erfüllen kann. Die zuständigen Behörden auf EU-Ebene (wie OLAF, Europol, Eurojust und die Europäische Staatsanwaltschaft) sollten dementsprechend ebenfalls enger zusammenarbeiten und ihren Informationsaustausch verbessern.

Ein weiteres wichtiges Bindeglied ist **Eurojust**, mit dessen Weiterentwicklung die Synergien zwischen der justiziellen Zusammenarbeit in Zivil- und Strafsachen maximiert werden könnten. Die EU würde auch in strategischer Hinsicht von einer größeren Kohärenz profitieren: **EMPACT**[115], der EU-Politikzyklus zur Bekämpfung der schweren und internationalen organisierten Kriminalität, bietet Behörden eine kriminalpolizeiliche erkenntnisgestützte Methodik, um gemeinsam gegen die größten kriminellen Bedrohungen vorzugehen, die die EU betreffen. Er hat in den letzten zehn Jahren im operativen Bereich wichtige Ergebnisse gebracht.[116] Der bestehende Mechanismus sollte auf der Grundlage der Erfahrungen der Fachleute gestrafft und vereinfacht werden, um den dringendsten, sich abzeichnenden kriminellen Bedrohungen im neuen Politikzyklus 2022-2025 besser begegnen zu können.

Rechtzeitige, relevante **Informationen** sind für die tägliche Arbeit bei der Verfolgung von Straftaten von entscheidender Bedeutung. Trotz der Entwicklung neuer Datenbanken auf EU-Ebene für Sicherheit und Grenzmanagement befinden sich nach wie vor viele Informationen in nationalen Datenbanken oder werden außerhalb dieser Instrumente ausgetauscht. Dies führt zu einer erheblichen zusätzlichen Arbeitsbelastung, zu Verzögerungen und einem erhöhten Risiko, dass wichtige Informationen übersehen werden. Bessere, schnellere und einfachere Verfahren, die alle Sicherheitsakteure einbeziehen, würden zu besseren Ergebnissen führen. Die richtigen Instrumente sind unerlässlich, wenn sich das Potenzial des Informationsaustauschs bei der wirksamen Verfolgung von Straftaten entfalten soll, wobei die erforderlichen Garantien zu wahren sind, damit der Datenaustausch im Einklang mit den Datenschutzgesetzen und den Grundrechten erfolgen kann. Angesichts technologischer, kriminaltechnischer und datenschutzrechtlicher Entwicklungen und geänderter operativer Erfordernisse könnte die EU prüfen, ob Instrumente wie die **Prümer Beschlüsse von 2008**, mit denen ein automatisierter Austausch von DNA-, Fingerabdruck- und Fahrzeugregisterdaten eingeführt wurde, modernisiert werden müssen, um den automatisierten Austausch zusätzlicher Datenkategorien zu ermöglichen, die bereits in den strafrechtlichen oder anderen Datenbanken der Mitgliedstaaten für strafrechtliche Ermittlungen verfügbar sind. Darüber hinaus wird die Kommission prüfen, inwieweit ein Austausch von Polizeiakten möglich ist, der bei der Feststellung helfen kann, ob eine bestimmte Person in anderen Mitgliedstaaten polizeilich bekannt ist, und wie der Zugang zu diesen Akten unter Wahrung aller erforderlichen Garantien erleichtert werden kann.

Die **Informationen über Reisende** haben dazu beigetragen, die Grenzkontrollen zu verbessern, die irreguläre Migration zu verringern und Personen zu identifizieren, die ein

[115] EMPACT steht für European Multidisciplinary Platform Against Criminal Threats (Europäische multidisziplinäre Plattform gegen kriminelle Bedrohungen).

[116] https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf

Sicherheitsrisiko darstellen. Bei den erweiterten Fluggastdaten handelt es sich um die biografischen Daten der Fluggäste, die von den Fluggesellschaften bei der Abfertigung erhoben und den Grenzkontrollbehörden am Bestimmungsort vorab übermittelt werden. Eine Überarbeitung des Rechtsrahmens[117] könnte eine effektivere Nutzung der Informationen ermöglichen und den Passagierverkehr erleichtern, ohne Abstriche bei den Datenschutzvorschriften zu machen. Fluggastdatensätze (Passenger Name Records – PNR) sind die von den Fluggästen bei der Buchung von Flügen bereitgestellten Daten. Die korrekte Anwendung der PNR-Richtlinie[118] ist von entscheidender Bedeutung. Die Kommission wird diese weiterhin unterstützen und durchsetzen. Darüber hinaus wird die Kommission mittelfristig eine Überprüfung des derzeitigen Konzepts für die **Übermittlung von PNR-Daten an Drittländer** in die Wege leiten.

Die **justizielle Zusammenarbeit** ist eine notwendige Ergänzung der Polizeiarbeit bei der Bekämpfung der grenzüberschreitenden Kriminalität. Bei der justiziellen Zusammenarbeit hat sich in den letzten 20 Jahren ein grundlegender Wandel vollzogen. Einrichtungen wie die **Europäische Staatsanwaltschaft** und **Eurojust** müssen über die nötigen Mittel verfügen, um voll funktionsfähig zu sein, oder sie müssen weiter ausgebaut werden. Die Zusammenarbeit zwischen Angehörigen der Rechtsberufe könnte auch durch weitere Schritte im Hinblick auf die gegenseitige Anerkennung gerichtlicher Entscheidungen, die justizielle Aus- und Fortbildung und den Informationsaustausch verbessert werden. Ziel sollte es sein, das Vertrauen unter den Richtern und Staatsanwälten, das für reibungslose grenzübergreifende Verfahren von zentraler Bedeutung ist, zu stärken. Auch durch den Einsatz **digitaler Technologien** ließe sich die Leistungsfähigkeit unserer Justizsysteme verbessern. Derzeit wird ein neues System für den digitalen Austausch eingerichtet, mit dem Europäische Ermittlungsanordnungen, Rechtshilfeersuchen und damit zusammenhängende Mitteilungen mit Unterstützung von Eurojust zwischen den Mitgliedstaaten übermittelt werden können. Die Kommission wird mit den Mitgliedstaaten zusammenarbeiten, um die Einführung der erforderlichen IT-Systeme auf nationaler Ebene zu beschleunigen.

Die internationale Zusammenarbeit ist auch für eine erfolgreiche Zusammenarbeit der Strafverfolgungsbehörden und der Justizbehörden von entscheidender Bedeutung. Bilaterale Abkommen mit wichtigen Partnern spielen eine Schlüsselrolle bei der Sicherung von Informationen und Beweisen aus Ländern außerhalb der EU. **Interpol** kommt als einer der größten zwischenstaatlichen kriminalpolizeilichen Organisationen dabei eine wichtige Aufgabe zu. Die Kommission wird prüfen, wie die Zusammenarbeit mit Interpol auf operativer und strategischer Ebene intensiviert werden kann und ob ein Zugang zu Interpol-Datenbanken möglich ist. Die Strafverfolgungsbehörden in der EU stützen sich bei der Erkennung und Ermittlung von Straftätern und Terroristen auch auf wichtige Partnerländer. **Sicherheitspartnerschaften zwischen der EU und Drittländern** könnten intensiviert werden, um die Zusammenarbeit bei der Bekämpfung gemeinsamer Bedrohungen wie Terrorismus, organisierter Kriminalität, Cyberkriminalität, sexuellem Missbrauch von Kindern und Menschenhandel zu erweitern. Ein solcher Ansatz würde auf gemeinsamen Sicherheitsinteressen beruhen und auf etablierten Kooperations- und Sicherheitsdialogen aufbauen.

Neben Informationen kann der Austausch von Fachwissen von besonderem Nutzen sein, wenn es darum geht, die Strafverfolgungsbehörden besser auf **nicht herkömmliche**

[117] Richtlinie 2004/82/EG des Rates über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln.

[118] Richtlinie (EU) 2016/681 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität.

Bedrohungen vorzubereiten. Die Kommission wird nicht nur den Austausch bewährter Verfahren fördern, sondern auch die Einführung eines **Koordinierungsmechanismus auf EU-Ebene für Polizeikräfte** im Falle höherer Gewalt wie Pandemien prüfen. Die Pandemie hat auch gezeigt, dass eine Präsenz der Polizei in der digitalen Gemeinschaft (Digital Community Policing), flankiert von Regelungen zur Erleichterung der Online-Polizeiarbeit, von grundlegender Bedeutung für die Bekämpfung von Kriminalität und Terrorismus sein wird. Partnerschaften zwischen der Polizei und sozialen Gruppen – sowohl im Internet als auch außerhalb – können Kriminalität entgegenwirken und den Einfluss von organisierter Kriminalität, Radikalisierung und terroristischen Aktivitäten abmildern. Verbindungen zwischen der Polizeiarbeit auf lokaler, regionaler, nationaler und europäischer Ebene sind ein Schlüsselfaktor für den Erfolg der EU-Sicherheitsunion insgesamt.

Der Beitrag starker Außengrenzen

Ein modernes und effizientes Management der Außengrenzen hat den doppelten Nutzen, dass zum einen die Integrität des Schengen-Raums und zum anderen die Sicherheit unserer Bürgerinnen und Bürger gewahrt wird. Die Einbindung aller relevanten Akteure im Interesse einer größtmöglichen Sicherheit an den Grenzen kann die Prävention von grenzüberschreitender Kriminalität und Terrorismus konkret beeinflussen. Gemeinsame operative Einsätze der kürzlich gestärkten Europäischen Grenz- und Küstenwache[119] tragen zur Prävention und Aufdeckung grenzüberschreitender Kriminalität an den **Außengrenzen** der EU und darüber hinaus bei. Der Beitrag der Zollbehörden zur Aufdeckung von Sicherheitsrisiken bei allen Waren vor ihrer Ankunft in der EU und zur Kontrolle von Waren nach ihrer Ankunft ist für die Bekämpfung der grenzüberschreitenden Kriminalität und des Terrorismus von entscheidender Bedeutung. Im anstehenden Aktionsplan zur Zollunion werden Maßnahmen zur Stärkung des Risikomanagements und zur Verbesserung der inneren Sicherheit angekündigt, unter anderem durch die Prüfung einer möglichen Verknüpfung zwischen den einschlägigen Informationssystemen für die Sicherheitsrisikoanalyse.

Der Rahmen für die **Interoperabilität zwischen EU-Informationssystemen** im Bereich Justiz und Inneres wurde im Mai 2019 angenommen. Mit dieser neuen Architektur sollen Effizienz und Wirksamkeit der neuen oder modernisierten Informationssysteme verbessert werden.[120] Strafverfolgungsbeamte, Grenzschutzbeamte und Migrationsbeamte werden so auf schnellere und systematischere Informationen zugreifen können. Dies wird eine korrekte Identifizierung und die Bekämpfung von Identitätsbetrug erleichtern. Der Interoperabilität der Systeme sollte daher sowohl auf politischer als auch auf technischer Ebene Vorrang eingeräumt werden. Eine enge Zusammenarbeit zwischen den EU-Agenturen und allen Mitgliedstaaten ist unverzichtbar, wenn bis 2023 vollständige Interoperabilität erreicht werden soll.

Reisedokumentenbetrug gilt als eine der am häufigsten begangenen Straftaten. Er erleichtert Kriminellen und Terroristen das Reisen im Verborgenen und spielt eine

[119] Bestehend aus der Europäischen Agentur für die Grenz- und Küstenwache (Frontex) und dem Grenzschutz und der Küstenwache der Mitgliedstaaten.

[120] Hierzu zählen das Einreise-/Ausreisesystem (EES), das Europäische Reiseinformations- und -genehmigungssystem (ETIAS), das erweiterte Europäische Strafregisterinformationssystem (ECRIS-TCN), das Schengener Informationssystem, das Visa-Informationssystem und Eurodac (dessen Aktualisierung ansteht).

Schlüsselrolle sowohl beim Menschenhandel als auch beim Drogenhandel.[121] Die Kommission wird prüfen, wie die bestehenden Arbeiten zu den Sicherheitsstandards für EU-Aufenthalts- und Reisedokumente – auch durch Digitalisierung – ausgeweitet werden können. Ab August 2021 werden die Mitgliedstaaten mit der Ausstellung von Personalausweisen und Aufenthaltsdokumenten nach harmonisierten Sicherheitsstandards beginnen, zu denen ein Chip mit biometrischen Identifikatoren gehört, der von allen EU-Grenzbehörden überprüft werden kann. Die Kommission wird die Anwendung der neuen Vorschriften, einschließlich der schrittweisen Ersetzung der derzeit im Umlauf befindlichen Dokumente, überwachen.

Intensivierung von Sicherheitsforschung und Innovation

Die Maßnahmen zur Gewährleistung der Cybersicherheit und zur Bekämpfung der organisierten Kriminalität, der Cyberkriminalität und des Terrorismus stützen sich in hohem Maße auf die Entwicklung zukunftsgerichteter Instrumente zur Schaffung sichererer neuer Technologien, zur Bewältigung der technologischen Herausforderungen und zur Unterstützung der Arbeit der Strafverfolgungsbehörden. Hier sind auch der Privatsektor und die Industrie gefordert.

Innovation sollte als strategisches Instrument zur Abwehr aktueller Bedrohungen und zur Antizipation künftiger Risiken und Chancen betrachtet werden. Innovative Technologien können neue Instrumente zur Unterstützung von Strafverfolgungsbehörden und anderen Sicherheitsakteuren hervorbringen. Künstliche Intelligenz und Massendatenanalyse könnten sich Hochleistungsrechentechnik zunutze machen, um eine bessere Aufklärung und eine schnelle, umfassende Analyse zu ermöglichen.[122] Eine wesentliche Voraussetzung für die Entwicklung zuverlässiger Technologien sind hochwertige Datensätze, die die zuständigen Behörden für das Trainieren, Testen und Validieren von Algorithmen nutzen können.[123] Generell besteht heutzutage ein hohes Risiko technologischer Abhängigkeit. So ist die EU beispielsweise Nettoimporteur von Cybersicherheitsprodukten und -diensten – mit allem, was dies für die Wirtschaft und für kritische Infrastrukturen mit sich bringt. Um die Technologie zu beherrschen und die Kontinuität der Versorgung auch im Falle von Zwischenfällen und Krisen zu gewährleisten, braucht Europa Präsenz und Kapazitäten in den kritischen Teilen der jeweiligen Wertschöpfungsketten.

Forschung, Innovation und technologische Entwicklung in der EU bieten die Möglichkeit, die Sicherheitsdimension bei der Entwicklung dieser Technologien und ihrer Anwendung zu berücksichtigen. Von der nächsten Generation von EU-Finanzierungsvorschlägen könnten wichtige Impulse ausgehen.[124] Bei Initiativen zu europäischen Datenräumen und Cloud-Infrastrukturen wird die Sicherheit von Anfang an berücksichtigt. Das Europäische Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung und das Netz nationaler Koordinierungszentren[125] sollen eine

[121] Der Zusammenhang zwischen Dokumentenbetrug und Menschenhandel wird im Zweiten Bericht über die Fortschritte bei der Bekämpfung des Menschenhandels (COM(2018) 777), im Begleitdokument SWD(2018) 473 und im Europol-Lagebericht von 2016 über Menschenhandel in der EU erläutert.

[122] Hierzu sei auf die Strategie der Kommission zur Künstlichen Intelligenz verwiesen.

[123] Eine europäische Datenstrategie (COM(2020) 66 final).

[124] Die Vorschläge der Kommission für Horizont Europa, den Fonds für die innere Sicherheit, den Fonds für integriertes Grenzmanagement, das Programm EUInvest, den Europäischen Fonds für regionale Entwicklung und das Programm „Digitales Europa“ werden die Entwicklung und den Einsatz innovativer Sicherheitstechnologien und -lösungen entlang der Sicherheitswertschöpfungskette unterstützen.

[125] Vorschlag vom 12. September 2018 zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren, (COM(2018) 630).

leistungsfähige, effiziente Struktur schaffen, um Forschungskapazitäten und -ergebnisse im Bereich der Cybersicherheit zu bündeln und auszutauschen. Das Weltraumprogramm der EU bietet Dienste, die die Sicherheit der EU, ihrer Mitgliedstaaten und der Bürgerinnen und Bürger unterstützen.[126]

Mit über 600 Projekten im Gesamtwert von fast 3 Mrd. EUR seit 2007 ist die von der EU finanzierte Sicherheitsforschung ein Schlüsselinstrument für die Förderung von Technologie und Wissen zur Unterstützung von Sicherheitslösungen. Im Rahmen der Überprüfung des Mandats von Europol wird die Kommission die Gründung eines **europäischen Innovationszentrums für die innere Sicherheit**[127] prüfen, das gemeinsame Lösungen für gemeinsame sicherheitspolitische Herausforderungen und Chancen erarbeiten könnte, was die Mitgliedstaaten allein möglicherweise nicht leisten können. Die Zusammenarbeit ist von grundlegender Bedeutung, um Investitionen so zu bündeln, dass sie die bestmögliche Wirkung erzielen, und um innovative Technologien zu entwickeln, die sowohl sicherheitspolitisch als auch wirtschaftlich von Nutzen sind.

Sicherheitskompetenzen und Sicherheitsbewusstsein

Für eine krisenfestere Gesellschaft mit besser gerüsteten Unternehmen, Verwaltungen und besser vorbereiteten Bürgern kommt es entscheidend darauf an, dass ein Bewusstsein für Sicherheitsfragen und Kompetenzen im Umgang mit potenziellen Bedrohungen vorhanden sind. Probleme mit der IT-Infrastruktur und elektronischen Systemen haben offenbart, dass unsere personellen Kapazitäten für die Abwehrbereitschaft und Reaktionsfähigkeit im Bereich der Cybersicherheit verbessert werden müssen. Die Pandemie hat auch die Bedeutung der Digitalisierung in allen Bereichen der Wirtschaft und Gesellschaft der EU deutlich gemacht.

Schon ein **Grundwissen über Sicherheitsbedrohungen** und wie man sich davor schützen kann, kann sich konkret auf die Resilienz einer Gesellschaft auswirken. Das Bewusstsein für die Risiken der Cyberkriminalität und die Notwendigkeit, sich davor zu schützen, können Hand in Hand gehen mit Schutzmaßnahmen, die Diensteanbieter zur Abwehr von Cyberangriffen vorsehen. Informationen über die Gefahren und Risiken des Drogenhandels können Kriminellen den Erfolg erschweren. Die EU kann die Verbreitung bewährter Verfahren fördern, beispielsweise durch das Netz der Safer-Internet-Zentren[128], und sicherstellen, dass diese Ziele in ihren eigenen Programmen berücksichtigt werden.

In den künftigen Aktionsplan für digitale Bildung sollten gezielte Maßnahmen zum Aufbau von IT-Sicherheitskompetenzen für die gesamte Bevölkerung aufgenommen werden. Die kürzlich angenommene Kompetenzagenda[129] unterstützt den Kompetenzerwerb im Laufe des gesamten Lebens. Sie umfasst gezielte Maßnahmen zur Erhöhung der Zahl der Hochschulabsolventen in Naturwissenschaften, Technologie, Ingenieurwesen, Kunst und Mathematik, die in Spitzenforschungsgebieten wie Cybersicherheit benötigt werden.

---

[126] So bietet Copernicus beispielsweise Dienste an, die die Überwachung der EU-Außengrenzen und die Meeresüberwachung ermöglichen, was zur Bekämpfung von Piraterie und Schmuggel sowie zur Unterstützung kritischer Infrastrukturen beiträgt. Sobald diese Dienste voll einsatzfähig sind, werden sie ein wichtiger Faktor für zivile und militärische Missionen und Operationen sein.

[127] Das Zentrum würde auch mit der Europäischen Grenz- und Küstenwache/Frontex, CEPOL, eu-LISA und der Gemeinsamen Forschungsstelle zusammenarbeiten.

[128] Siehe www.betterinternetforkids.eu: Das zentrale Portal und die nationalen Safer-Internet-Zentren werden derzeit im Rahmen der Fazilität „Connecting Europe“ im Bereich Telekommunikation (CEF/Telecom) finanziert. Weitere Mittel wurden im Rahmen des Programms „Digitales Europa“ vorgeschlagen.

[129] Europäische Kompetenzagenda für nachhaltige Wettbewerbsfähigkeit, soziale Gerechtigkeit und Resilienz (COM(2020) 274 final).

Zusätzliche Maßnahmen, die aus dem Programm „Digitales Europa“ finanziert werden, werden es Fachkräften ermöglichen, mit den Entwicklungen der Sicherheitslage Schritt zu halten, und gleichzeitig dem EU-weiten Mangel an Arbeitskräften in diesem Bereich entgegenwirken. Insgesamt sollen die Maßnahmen den Erwerb von Kompetenzen im Umgang mit Sicherheitsbedrohungen ermöglichen, sodass Unternehmen die Fachkräfte finden können, die sie in diesem Bereich benötigen. Der künftige Europäische Forschungsraum und der Europäische Bildungsraum werden Berufe in den Bereichen Naturwissenschaften, Technologie, Ingenieurwesen, Kunst und Mathematik fördern.

Wichtig ist auch der Zugang der **Opfer** zu ihren Rechten. Sie müssen die notwendige Hilfe und Unterstützung erhalten, die sie aufgrund ihrer besonderen Situation benötigen. Besondere Anstrengungen sind erforderlich, wenn es um Minderheiten und besonders schutzbedürftige Opfer geht wie Kinder oder Frauen, die Opfer häuslicher Gewalt oder zum Zwecke der sexuellen Ausbeutung Opfer von Menschenhandel geworden sind.[130]

Eine besondere Bedeutung kommt der Verbesserung der **Kompetenzen im Bereich der Strafverfolgung** zu. Die gegenwärtigen wie die neuen technologischen Bedrohungen erfordern mehr Investitionen in die Höherqualifizierung der Strafverfolgungsbediensteten schon zu Beginn ihrer Laufbahn und während ihres gesamten aktiven Dienstes. Die CEPOL ist ein wichtiger Partner, der die Mitgliedstaaten bei dieser Aufgabe unterstützen kann. Schulungen im Bereich der Strafverfolgung zum Thema Rassismus und Fremdenfeindlichkeit und allgemein zu den Bürgerrechten müssen wesentlicher Bestandteil einer EU-Sicherheitskultur sein. Die nationalen Justizsysteme und die Angehörigen der Rechtsberufe müssen ebenfalls in der Lage sein, sich auf neue Herausforderungen einzustellen und darauf zu reagieren. Schulungen sind von entscheidender Bedeutung, damit die Behörden vor Ort die bestehenden Instrumente für ihre Arbeit nutzen können. Darüber hinaus sollten alle Anstrengungen unternommen werden, um eine durchgängige Berücksichtigung der Geschlechtergleichstellung zu erreichen und den Anteil von Frauen im Bereich der Strafverfolgung zu erhöhen.

Zentrale Maßnahmen
• Stärkung des Mandats von Europol • Prüfung eines „EU-Kodex für die polizeiliche Zusammenarbeit“ und einer polizeilichen Koordinierung in Krisenzeiten • Stärkung von Eurojust zur Herstellung einer Verbindung zwischen Justiz- und Strafverfolgungsbehörden • Überarbeitung der Richtlinie über vorab übermittelte Fluggastdaten • Mitteilung über die externe Dimension von Fluggastdatensätzen • Intensivierung der Zusammenarbeit zwischen der EU und Interpol • Eckpunkte für Verhandlungen mit wichtigen Drittländern über den Informationsaustausch • Bessere Sicherheitsstandards für Reisedokumente • Überlegungen im Hinblick auf ein europäisches Innovationszentrum für innere Sicherheit

[130] Siehe die Strategie für die Gleichstellung der Geschlechter (COM(2020) 152), die EU-Strategie für die Rechte von Opfern (COM(2020) 258) und die Europäische Strategie für ein besseres Internet für Kinder (COM(2012) 196).

V. Schlussfolgerung

In zunehmend unruhigen Zeiten gilt die Europäische Union nach wie vor weithin als einer der sichersten Orte der Welt. Das sollten wir jedoch nicht als selbstverständlich ansehen.

Mit der neuen Strategie für die Sicherheitsunion wird das Fundament für eine Sicherheitsgemeinschaft gelegt, die die gesamte europäische Gesellschaft umfasst. Sie beruht auf dem Wissen, dass Sicherheit eine gemeinsame Verantwortung ist. Sicherheit geht jeden an. Alle staatlichen Stellen, Unternehmen, sozialen Organisationen, Institutionen, Bürgerinnen und Bürger müssen ihrer Verantwortung gerecht werden, damit unsere Gesellschaft sicherer wird.

Sicherheitsfragen müssen jetzt aus einem viel breiteren Blickwinkel betrachtet werden als in der Vergangenheit. Unangebrachte Differenzierungen zwischen physisch und virtuell müssen überwunden werden. Die EU-Strategie für die Sicherheitsunion vereint das gesamte Spektrum der Sicherheitsbedürfnisse und konzentriert sich auf die Bereiche, die für die Sicherheit der EU in den kommenden Jahren am wichtigsten sein werden. Sie trägt auch dem Umstand Rechnung, dass Sicherheitsbedrohungen nicht an Landesgrenzen haltmachen und innere und äußere Sicherheit zunehmend ineinandergreifen.[131] Für die EU wird es hier darauf ankommen, zum Schutz ihrer Bürgerinnen und Bürger mit internationalen Partnern zusammenzuarbeiten und diese Strategie in enger Abstimmung mit dem auswärtigen Handeln der EU umzusetzen.

Unsere Sicherheit und unsere Grundwerte gehen Hand in Hand. Bei allen im Rahmen dieser Strategie vorgeschlagenen Maßnahmen und Initiativen werden wir die Grundrechte und unsere europäischen Werte uneingeschränkt achten. Sie sind das Fundament unserer europäischen Lebensweise und müssen im Mittelpunkt unserer gesamten Arbeit stehen.

Die Kommission ist sich völlig darüber im Klaren, dass jede Politik oder Maßnahme nur so gut ist wie ihre Umsetzung. Daher muss unermüdlich auf eine korrekte Umsetzung und Durchsetzung bestehender und künftiger Rechtsvorschriften gedrungen werden. Dies werden wir anhand einer regelmäßigen Berichterstattung über die Sicherheitsunion überprüfen. Die Kommission wird das Europäische Parlament, den Rat und die Interessenträger umfassend informieren und in alle einschlägigen Maßnahmen einbeziehen. Darüber hinaus ist die Kommission bereit, zusammen mit den Organen über die Strategie für die Sicherheitsunion zu diskutieren und gemeinsame Debatten zu veranstalten, bei denen wir uns sowohl mit dem Sachstand als auch mit den künftigen Herausforderungen befassen.

Die Kommission ersucht das Europäische Parlament und den Rat, die Strategie für die Sicherheitsunion als Grundlage für Zusammenarbeit und gemeinsames Handeln im Sicherheitsbereich in den nächsten fünf Jahren zu billigen.

[131] Siehe die EU Global Strategy.