Rat der
Europäischen Union

Brüssel, den 27. Mai 2022
(OR. en)

9563/22

JAI 761	**DROIPEN 69**
COSI 149	**COPEN 210**
ENFOPOL 298	**FREMP 110**
ENFOCUSTOM 89	**JAIEX 61**
IXIM 145	**CFSP/PESC 705**
CT 99	**COPS 238**
CRIMORG 81	**HYBRID 49**
FRONT 218	**DISINFO 47**
ASIM 47	**TELECOM 248**
VISA 87	**DIGIT 108**
CYBER 191	**COMPET 408**
DATAPROTECT 175	**RECH 307**
CATS 30	

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	25. Mai 2022
Empfänger:	Generalsekretariat des Rates
Nr. Komm.dok.:	COM(2022) 252 final
Betr.:	MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT über den vierten Fortschrittsbericht zur EU-Strategie für die Sicherheitsunion

Die Delegationen erhalten in der Anlage das Dokument COM(2022) 252 final.

Anl.: COM(2022) 252 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 25.5.2022
COM(2022) 252 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

über den vierten Fortschrittsbericht zur EU-Strategie für die Sicherheitsunion

I. EINLEITUNG

Der russische Angriffskrieg gegen die Ukraine ist das beherrschende Thema auf der Sicherheitsagenda der EU. Der Krieg bedroht nicht nur die Ukraine, sondern schadet auch der globalen Stabilität und Sicherheit. Für die EU birgt er einige Risiken für die Sicherheit der Bürgerinnen und Bürger. Es sind neue Unsicherheiten im Hinblick auf die Energie- und Rohstoffversorgung aufgetreten. Kritische Infrastrukturen könnten Ziele von Cyberangriffen werden. Die innere Sicherheit der EU ist durch mögliche Angriffe oder Unfälle durch den Einsatz von chemischen, biologischen oder radiologischen Kampfmitteln im Kriegsgebiet bedroht. Die Schutzbedürftigkeit von Millionen Menschen, die vor dem Krieg geflohen sind, kann von der organisierten Kriminalität leicht ausgenutzt werden, und zwar in Form von Menschenhandel, wobei Frauen und Kindern besonders gefährdet sind.

Auf diese neuen und potentiellen Bedrohungen hat die EU entschlossen und geeint reagiert. Die Auswirkungen des Krieges beschränken sich zwar bislang hauptsächlich auf das Hoheitsgebiet der Ukraine. Dennoch hat die EU ihre *Wachsamkeit und Koordinierung* erhöht und beobachtet die Bedrohungslage genau. Außerdem arbeitet sie an der Stärkung ihrer Widerstandsfähigkeit, um somit die *Abwehrbereitschaft* zu erhöhen.

In ihrer Erklärung von Versailles vom 10. und 11. März 2022[1] haben die Staats- und Regierungschefs der EU hervorgehoben, wie wichtig es ist, sich auf rasch entstehende neue Herausforderungen vorzubereiten, unter anderem „indem wir uns vor der ständig zunehmenden hybriden Kriegsführung schützen, unsere Cyberabwehrfähigkeit stärken, unsere Infrastruktur – insbesondere unsere kritische Infrastruktur – schützen und Desinformation bekämpfen“.

Der Rahmen für die Sicherheitsunion ist von zentraler Bedeutung für die Gewährleistung der Sicherheit in der EU. Die vier strategischen Prioritäten der Strategie für eine Sicherheitsunion[2] sind für diese Aufgabe im aktuellen geopolitischen Umfeld nach wie vor relevant: i) ein zukunftsfähiges Sicherheitsumfeld, ii) Umgang mit sich wandelnden Bedrohungen, iii) Schutz der Europäerinnen und Europäer vor Terrorismus und organisierter Kriminalität und iv) eine starke europäische Sicherheitsgemeinschaft. Der Krieg hat gezeigt, dass die EU und ihre Mitgliedstaaten die ihnen im Rahmen der Strategie für eine Sicherheitsunion bereits zur Verfügung stehenden rechtlichen und politischen Instrumente umfassend nutzen müssen, die die Grundlage für eine koordinierte Unterstützung der Mitgliedstaaten durch die EU in Fragen der organisierten Kriminalität und des Terrorismus, der Cybersicherheit und der hybriden Bedrohungen bilden.

Die Europäischen Agenturen im Bereich Justiz und Inneres haben ihre Bemühungen in Reaktion auf den Krieg in der Ukraine verstärkt und spielen eine wichtige Rolle bei der Bewertung der Bedrohungen und der Unterstützung operativer Maßnahmen.[3] Ebenso wichtig ist die fortwährende Stärkung der operativen Praxis und der politischen Steuerung.

In diesem vierten Fortschrittsbericht zur EU-Strategie für eine Sicherheitsunion liegt der Schwerpunkt auf den Entwicklungen der letzten Monate seit Beginn des russischen Angriffskriegs gegen die Ukraine. Er enthält einen Überblick über die in den allen Bereichen

---

1 https://www.consilium.europa.eu/media/54802/20220311-versailles-declaration-de.pdf

2 COM(2020) 605.

3 Gemeinsame Erklärung der EU-Agenturen im Bereich Justiz und Inneres zur Ukraine | Asylagentur der Europäischen Union (europa.eu)

der Sicherheitsunion ergriffenen Maßnahmen. Außerdem werden die erforderlichen Schritte zur Abwehrbereitschaft gegen potentielle Sicherheitsbedrohungen im Zusammenhang mit dem Krieg in der Ukraine dargelegt. Der Fortschritt bei anderen Sicherheitsunionsdossiers kann dem Anhang entnommen werden.

II. CYBERSICHERHEIT UND KRITISCHE INFRASTRUKTUR

Seit Ausbruch des Krieges haben private Akteure und kriminelle Vereinigungen angekündigt, dass sie Cyberaktivitäten zur Unterstützung der einen oder anderen Seite durchführen. Hacktivismus[4] stellt aufgrund des Risikos von Auswirkungen auf kritische Dienste in der EU eine Bedrohung dar, wobei das Risiko von Angriffen aus offiziellen Netzwerken oder anderen unvorhergesehenen Ausstrahlungseffekten ausgeht. Der Krieg ist bislang zwar größtenteils mit konventionellen Mitteln mit nur begrenzten Ausstrahlungseffekten ausgetragen worden. Dennoch ist das Eskalationsrisiko real.

Die EU hat ihre Anstrengungen in Bezug auf Koordinierung und Abwehrbereitschaft intensiviert. Die vom Krieg ausgehenden Bedrohungen machen deutlich, dass eine Kultur des Austauschs von Informationen und Fachwissen zwischen der EU, den Mitgliedstaaten und den Cybersicherheitsgemeinschaften erforderlich ist. Dies umfasst auch den Aufbau einer integrierten und gemeinsamen Lageeinschätzung der Organe, Einrichtungen und sonstigen Stellen der EU und der Mitgliedstaaten insbesondere im Hinblick auf kritische Infrastrukturen, von denen das reibungslose Funktionieren des Binnenmarkts abhängt.

Einordnung der Cyberangriffe auf die Ukraine

Die Cyberangriffe auf die Ukraine begannen bereits vor dem russischen Angriff. In den ersten Kriegstagen richteten sie sich gegen Nutzerkonten der ukrainischen Streitkräfte und zielten darauf ab, wesentliche Dienste wie die Grenzkontrolle oder die Telekommunikation zu stören.[5]

Am 14. Januar 2022 gab der Hohe Vertreter eine Erklärung im Namen der Europäischen Union[6] ab, in der die Cyberangriffe gegen die Ukraine verurteilt und die uneingeschränkte Unterstützung der EU für die Ukraine unmissverständlich bekräftigt werden.

---

[4] Ein Beispiel aus der jüngsten Vergangenheit für Hacktivismus ist der Einsatz von „Protestware“ zur Verbreitung von Schadsoftware an russische IP-Adressen über ein beliebtes Open-Source-Paket, was zu Risiken für Lieferketten und einem Verlust von Vertrauen in die Open-Source-Bewegung führen könnte. Die Kommission hat klargestellt, dass (auch gutgemeinte) Cyberangriffe auf Russland illegal sind.

[5] Microsoft Special Report: An overview of Russia’s cyberattack activity in Ukraine (Microsoft-Sonderbericht: Ein Überblick über Russlands Cyberangriffe auf die Ukraine); The hybrid war in Ukraine - Microsoft On the Issues (Hybride Kriegsführung in der Ukraine - Microsoft-Analyse)

[6] https://www.consilium.europa.eu/de/press/press-releases/2022/01/14/ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union-on-the-cyberattack-against-ukraine/

Am 10. Mai verurteilten die Europäische Union und ihre Mitgliedstaaten gemeinsam mit ihren internationalen Partnern aufs Schärfste die böswilligen Cyberaktivitäten der Russischen Föderation gegen die Ukraine am 24. Februar, die auf das von Viasat betriebene Satellitennetzwerk KA-SAT abzielten und im direkten Zusammenhang mit dem Angriff der Russischen Föderation standen.[7] Dieser Cyberangriff hatte erhebliche Auswirkungen, die unterschiedslos zu Ausfällen und Störungen der Kommunikation bei mehreren staatlichen Behörden, Unternehmen und Nutzern in der Ukraine führten und von denen auch mehrere EU-Mitgliedstaaten betroffen waren.

Wachsamkeit und Koordinierung

Seit dem Angriffskrieg Russlands gegen die Ukraine wird die Cybersicherheitslage in den Mitgliedstaaten und den Einrichtungen der Union verstärkt überwacht. ENISA, die Agentur der Europäischen Union für Cybersicherheit, das bei Europol angesiedelte Europäische Zentrum zur Bekämpfung der Cyberkriminalität, das IT-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der EU (CERT-EU) und das EU-Zentrum für Informationsgewinnung und Lageerfassung (EU INTCEN) tragen alle zu einer gemeinsamen Lageerfassung innerhalb der Union bei, unter anderem durch eine regelmäßige Überwachung verdächtiger Cyberaktivitäten, insbesondere in bestimmten Sektoren wie Energie, Verkehr und Luftverkehr, und liefern Bewertungen, die als Richtschnur für Präventivmaßnahmen dienen.

Die Absprache und der Informationsaustausch mit Netzwerken im Bereich Cybersicherheit, wie dem Netzwerk der Verbindungsorganisationen für Cyberkrisen (CyCLONe), in dem einzelstaatliche Cybersicherheitsagenturen, die Kommission und ENISA vertreten sind, wurde ebenfalls intensiviert. Dieser Ansatz wird auch intern in den EU-Institutionen verfolgt. Dazu wurde ein Koordinierungsmechanismus eingerichtet, der Krisenstab für Cybersicherheit, der dafür sorgt, dass Informationen an alle relevanten Stellen, Organe und Agenturen weitergeleitet werden, darunter ENISA, das Europäische Zentrum zur Bekämpfung der Cyberkriminalität und CERT-EU. Es bedarf kontinuierlicher Bemühungen, um die Kommunikationskanäle zwischen den politischen, operativen und technischen Ebenen offenzuhalten und die Zusammenarbeit mit dem Netzwerk von Computer-Notfallteams (CSIRT) zu verbessern.

Europol hat das EU-Notfallprotokoll für die Strafverfolgung aktiviert, das eine verstärkte Überwachung von Cyberbedrohungen und den Informationsaustausch zwischen vielen Interessenträgern ermöglicht, um ein umfassendes Lagebild aus den Cyberinformationen zu erhalten.

Neben Cyberbedrohungen legen die Mitgliedstaaten, der EAD und die Dienststellen der Kommission ein erhöhtes Augenmerk auf die Gefährdung kritischer Infrastrukturen durch physische Bedrohungen. Kritische Infrastrukturen und die sie betreibenden Einrichtungen können physischen Risiken ausgesetzt sein, z. B. Sabotageakten durch Staaten oder staatlich unterstützte Akteure im Rahmen eventueller Vergeltungsmaßnahmen gegen die EU.

[7] Russische Cyberoperationen gegen die Ukraine: Erklärung des Hohen Vertreters im Namen der Europäischen Union – Consilium (europa.eu)

Abwehrbereitschaft

Die Abwehrbereitschaft im Bereich Cybersicherheit und Sicherheit kritischer Infrastrukturen ist angesichts des Risikos zunehmender Bedrohungen für Europa durch den Krieg wichtiger denn je. Zu den Bemühungen, die Abwehrbereitschaft zu erhöhen, gehören eine Reihe direkter Maßnahmen, von denen einige bereits vor Beginn des Angriffskriegs Russlands gegen die Ukraine geplant waren. Diese umfassen Übungen, Leitlinien, legislative Maßnahmen, die Stärkung der Widerstandsfähigkeit in kritischen Sektoren und die Zusammenarbeit mit Partnern.

Der französische Vorsitz im Rat der Europäischen Union organisierte zusammen mit dem Europäischen Auswärtigen Dienst (EAD) und der Agentur der Europäischen Union für Cybersicherheit (ENISA) Anfang 2022 eine Szenarioübung namens EU CyCLES (Cyber Crisis Linking Exercise on Solidarity) mit dem Ziel, auf politischer Ebene das Bewusstsein zu schärfen und die Zusammenarbeit zwischen den operativen und politischen Ebenen im Falle eines Cybergroßangriffs zu stärken.

ENISA und CERT-EU veröffentlichten im Februar **Leitlinien** zur Erhöhung der Widerstandsfähigkeit und der Abwehrbereitschaft in der EU[8]. Darin werden Organisationen des öffentlichen und privaten Sektors in der EU aufgefordert, ein Mindestmaß an bewährten Cybersicherheitsverfahren anzuwenden, um die Cybersicherheitskultur erheblich zu verbessern. Im März veröffentlichte CERT-EU mit Unterstützung von ENISA darauf aufbauend technische Leitlinien[9] sowie Sicherheitsleitlinien für eine bessere Konfiguration der App Signal[10] mit zahlreichen praktischen Tipps für Organisationen zur Verbesserung ihres Cybersicherheitsstands.

Legislative Initiativen

In der aktuellen Situation ist es dringend notwendig, **bestehende Rechtsvorschriften umzusetzen** und die **Annahme geplanter Initiativen** voranzutreiben.

Die Kommission unterstützt die Mitgliedstaaten bei der Umsetzung der NIS-Richtlinie[11], wonach die Mitgliedstaaten über angemessene Fähigkeiten verfügen sollten, z. B.in Form eines Computer-Notfallteams (CSIRT – Computer Security Incident Response Team), und zuständige Behörden benennen sollten. Die Richtlinie schafft eine Grundlage für eine wirksame Zusammenarbeit der Mitgliedstaaten. Die von den Mitgesetzgebern erzielte politische Einigung zur NIS-2-Richtlinie[12] ist ein weiterer Meilenstein auf dem Weg zur Schaffung einer robusten Abwehrbereitschaft der EU.

---

[8] Boosting your Organisation's Cyber Resilience (Stärkung der Cyberabwehrfähigkeit des eigenen Unternehmens), gemeinsame Veröffentlichung, 14.2.2022.

[9] Security Guidance 2022–01 - Cybersecurity mitigation measures against critical threats (Sicherheitsleitlinien 2022–01 – Cybersicherheit und Risikominderungsmaßnahmen gegen kritische Bedrohungen).

[10] CERT-EU Security Guidance 22-002 - Hardening Signal (CERT-EU Sicherheitsleitlinien 22-002 – Signal krisenfest machen.

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

[12] COM(2020) 823.

NIS 2 – eine weitere Stärkung der Abwehrbereitschaft

- In der neuen Richtlinie über Netz- und Informationssicherheit werden Mängel der vorangegangenen NIS-Richtlinie behoben, und die Richtlinie wird an die aktuellen Bedürfnisse angepasst und zukunftsfähig gemacht. Es werden die Mindestregeln für einen Rechtsrahmen aufgestellt und Mechanismen für eine wirksame Zusammenarbeit der zuständigen Behörden in allen Mitgliedstaaten festgelegt.
- Der Anwendungsbereich der Regeln wird auf neue Sektoren erweitert, die für Wirtschaft und Gesellschaft von entscheidender Bedeutung sind (zum Beispiel der Arzneimittel- und der Medizinproduktesektor oder die Nahrungs- und Genussmittelindustrie). Alle mittleren und großen Unternehmen, die in den Sektoren tätig sind oder die Art von Diensten erbringen, die unter die vorliegende Richtlinie fallen, fallen in den Anwendungsbereich der Richtlinie. Einrichtungen der öffentlichen Verwaltung von Zentralregierungen (mit Ausnahme der Justiz, der Parlamente und der Zentralbanken) und auf regionaler Ebene fallen ebenfalls unter die Richtlinie. Darüber hinaus können die Mitgliedstaaten beschließen, dass sie auch für solche Einrichtungen auf lokaler Ebene gilt.
- In der NIS-2-Richtlinie werden die Grundlagen für Risikomanagementmaßnahmen im Bereich der Cybersicherheit gelegt und das Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (CyCLONe), das die koordinierte Bewältigung großer Cybersicherheitsvorfälle unterstützen wird, offiziell eingerichtet.
- Des Weiteren enthält der Vorschlag genauerer Bestimmungen zum Vorgang der Meldung von Vorfällen, zum Inhalt der Meldungen und zum Zeitrahmen und sieht Abhilfemaßnahmen und Sanktionen zur Sicherstellung der Durchsetzung vor.
- Die Mitgliedstaaten haben ab dem Inkrafttreten der Richtlinie 21 Monate Zeit, die Bestimmungen in ihr nationales Recht umzusetzen.

Nach den Fortschritten bei der NIS-2-Richtlinie sollten die Verhandlungen über den Vorschlag für eine **Richtlinie über die Resilienz kritischer Einrichtungen**[13] so bald wie möglich abgeschlossen werden. Ist die Richtlinie erst einmal beschlossen und umgesetzt, dürfte dies die Resilienz kritischer Einrichtungen gegenüber einer Reihe von Bedrohungen, einschließlich Terroranschlägen, Insider-Bedrohungen und Sabotage, erhöhen. Von ebenso großer Bedeutung ist, dass die Richtlinie über die Resilienz kritischer Einrichtungen die gleichen ehrgeizigen Ziele verfolgt wie der Vorschlag der Kommission und dass der in der NIS-2-Richtlinie gefundene politische Kompromiss gewahrt bleibt. Zusammen werden diese Maßnahmen die Widerstandsfähigkeit und die Abwehrbereitschaft stärken, und zwar durch die Einrichtung eines kohärenteren und robusteren Systems, das auch nationale Pläne für die Reaktion auf Vorfälle und Krisen umfasst. Diese spielten auch in der Empfehlung der Kommission aus dem letzten Jahr zum Aufbau einer **Gemeinsamen Cyber-Einheit**[14] eine Rolle, in der dargelegt wird, wie die verschiedenen Akteure im Cybersicherheitsgefüge (Diplomaten, Polizei, Zivilpersonen und ggf. Verteidigungskräfte) auf operativer Ebene zusammenarbeiten sollten. Die aktuelle Bedrohungslage verdeutlicht, wie wichtig eine wirksame Zusammenarbeit wesentlicher Akteure ist.

[13] COM(2020) 829.

[14] Empfehlung zum Aufbau einer Gemeinsamen Cyber-Einheit|Shaping Europe's digital future | Gestaltung der digitalen Zukunft Europas – europa.eu)

Die Kommission überwacht weiterhin die Umsetzung des EU-Instrumentariums für die **5G-Cybersicherheit**[15]. In diesem Zusammenhang nahm die NIS-Kooperationsgruppe am 11. Mai einen Bericht zur Sicherheit von Open RAN[16] an. Außerdem arbeitet die Kommission weiterhin mit den Mitgliedstaaten daran, das Europäische Kompetenzzentrum für Cybersicherheit voll einsatzfähig zu machen.

Am 22. März 2022 hat die Kommission **neue Vorschriften** vorgeschlagen, **um einheitliche Maßnahmen für die Cyber- und Informationssicherheit aller Organe, Einrichtungen und sonstigen Stellen der EU festzulegen**. Diese Vorschriften werden die Widerstandsfähigkeit und die Reaktionsfähigkeit der EU-Verwaltung in Bezug auf Cyberbedrohungen und -sicherheitsvorfälle verbessern. Dadurch, dass diese Aktivitäten einen gemeinsamen Rahmen erhalten, werden die interinstitutionelle Zusammenarbeit gefestigt und die Risikoexposition verringert. Der Vorschlag für eine Cybersicherheits-Verordnung für die Organe, Einrichtungen und sonstigen Stellen der Union[17] sieht ein erweitertes Mandat von CERT-EU und die Schaffung eines neuen interinstitutionellen Cybersicherheitsbeirats vor. Außerdem werden die Cybersicherheitskapazitäten gefördert und regelmäßige Bewertungen des Reifegrads und eine bessere Cyberhygiene angeregt. Mit der vorgeschlagenen **Informationssicherheitsverordnung**[18] wird ein Mindestkatalog an Informationssicherheitsvorschriften und - standards für den sicheren Umgang mit Informationen und Informationsaustausch aller Organe, Einrichtungen und sonstigen Stellen der EU geschaffen, um einen verbesserten und kohärenten Schutz vor den zunehmenden Bedrohungen ihrer Informationssicherheit zu gewährleisten. Die Kommission fordert das Europäische Parlament und den Rat auf, diese Vorschläge zeitnah anzunehmen.

Die Kommission hat die öffentliche Konsultation zu Maßnahmen zur Stärkung der Cyberresilienz digitaler Produkte[19] abgeschlossen und bereitet einen Vorschlag vor, der im August veröffentlicht werden soll. Darin werden die Anfälligkeiten digitaler Produkte und ihrer Nebendienstleistungen in Angriff genommen, die nicht nur Chancen für die Volkswirtschaften und Gesellschaften der EU schaffen, sondern sie auch vor neue Herausforderungen stellen, denn je stärker alles miteinander vernetzt ist, umso eher beeinträchtigt ein Cybersicherheitsvorfall ein ganzes System und sorgt für Störungen bei gesellschaftlichen und wirtschaftlichen Tätigkeiten.

Am 9. März 2022 nahmen die für Telekommunikation zuständigen Minister des Rats einstimmig den Aufruf von Nevers[20] zur Stärkung der Cybersicherheitskapazitäten der EU an, der auch die Einrichtung eines neuen Notfallfonds für Cybersicherheit durch die Kommission vorsieht. Die Kommission erwägt die bestmögliche Nutzung bestehender Fonds zur Unterstützung von Präventions- und Reaktionsmaßnahmen.

Kritische Sektoren

---

15 https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

16 NIS Cooperation Group, Report on the cybersecurity of Open RAN, 11. Mai 2022.

17 COM(2022) 122.

18 COM(2022) 119.

19 Gesetz über Cyberresilienz – neue Cybersicherheitsvorschriften für digitale Produkte und Nebendienstleistungen (europa.eu)

20 08/03/2022 - Déclaration conjointe des ministres de l'Union européenne chargés du numérique et des communications électroniques adressée au secteur numérique - Presse - Ministère des Finances (economie.gouv.fr)

Die Sicherheit der **Energieversorgung** in der EU ist für das Wohlergehen der Bürgerinnen und Bürger und für ein reibungsloses Funktionieren unserer Volkswirtschaften von entscheidender Bedeutung. Die aktuelle Situation hat gezeigt, dass es in diesem Sektor klarer Regeln zur Cybersicherheit bedarf. Die Kommission arbeitet an einem Netzkodex zur Cybersicherheit für grenzüberschreitende Stromflüsse, wie er in der Elektrizitätsverordnung[21] vorgesehen ist, um Regeln für Risikobewertungen, gemeinsame Mindestanforderungen, Planung, Beobachtung, Berichterstattung und Krisenbewältigung festzulegen. Seit Russlands Angriffskrieg gegen die Ukraine sind die Zielsetzungen des geplanten Netzkodex zur Cybersicherheit noch relevanter geworden. Die Kommission hat außerdem eine strukturelle Zusammenarbeit zwischen ENISA, ENTSO-E[22], ENTSOG[23] und der Energiegemeinschaft bei der regelmäßigen Überwachung der Cybersicherheitslage im Energiesektor angestoßen.

Die EU arbeitet daran, die Sicherheit von Partnern zu schützen, ohne neue Risiken für sich selbst zu schaffen. Die Notsynchronisierung des ukrainischen und des moldauischen Stromnetzes mit dem kontinentaleuropäischen Netz erfolgte im März 2022 nach der Annahme von Risikominderungsmaßnahmen, insbesondere im Hinblick auf die Cybersicherheit.

Der Krieg und die Sanktionen haben auch den **Verkehrssektor** in der EU vor zahlreiche Herausforderungen gestellt. Diese reichen von Sicherheitsrisiken für die zivile Luftfahrt und Lkw-Fahrer in Konfliktgebieten bis hin zur Zerstörung der ukrainischen Verkehrsinfrastruktur, wodurch Lieferketten unterbrochen und die globale Ernährungssicherheit gefährdet werden. Die Agentur der Europäischen Union für Flugsicherheit rät in enger Absprache mit der Kommission und Eurocontrol, der Europäischen Organisation für Flugsicherung, den Luftverkehrsgesellschaften seit Beginn des Kriegs, nicht im Luftraum der Ukraine tätig zu sein und den Luftraum innerhalb von 100 Seemeilen zur belarussischen und zur russischen Grenze zur Ukraine zu meiden.

Die Kommission arbeitet darüber hinaus an der Stärkung der Abwehrbereitschaft und der Widerstandsfähigkeit des EU-Verkehrssektors. Am 23. Mai wurde ein neuer Notfallplan für den Verkehr[24] angenommen, in dem Schlussfolgerungen sowohl aus der COVID-19-Pandemie als auch aus dem militärischen Angriff Russlands auf die Ukraine gezogen werden. Darin wird ein Instrumentarium mit zehn Maßnahmen vorgeschlagen, die der EU und ihren Mitgliedstaaten eine Orientierung bei der Einführung von Krisenreaktionsmaßnahmen, einschließlich Gewährleistung eines Mindestmaßes an Konnektivität, Aufbau von Widerstandsfähigkeit gegen Cyberbedrohungen und hybride Bedrohungen sowie Ausbau der Zusammenarbeit mit internationalen Partnern im Hinblick auf die Krisenbereitschaft und -reaktion, bieten sollen. Außerdem wird die Bedeutung regelmäßiger auf bestehenden Verfahren aufbauender Notfallübungen für unterschiedliche Krisenszenarien zusammen mit den relevanten Agenturen oder anderen Akteuren hervorgehoben.

---

[21] Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates vom 5. Juni 2019 über den Elektrizitätsbinnenmarkt (ABl. L 158 vom 14.6.2019, S. 54). Ein Vorschlag wird derzeit von der Agentur für die Zusammenarbeit der Energieregulierungsbehörden geprüft.

[22] European Network of Transmission System Operators for Electricity (Europäisches Netz der Übertragungsnetzbetreiber (Strom)).

[23] European Network of Transmission System Operator for Gas (Europäisches Netz der Fernleitungsnetzbetreiber (Gas)).

[24] COM(2022) 21.

Innerhalb des **EU-Rahmens für die Gesundheitssicherheit** muss der Informationsaustausch auf der Grundlage des Frühwarn- und Reaktionssystems, einschließlich der Unterstützung medizinischer Evakuierungen aus der Ukraine, vor Cyberangriffen geschützt werden. Die Sicherheit des Systems wird daher verstärkt.

Zusammenarbeit mit Partnern

Die EU setzt ihre Zusammenarbeit mit ihren internationalen Partnern in der Verhinderung, Abschreckung, Abwehr böswilliger Handlungen im Cyberraum fort. Durch Russlands Angriffskrieg gegen die Ukraine ist die Zusammenarbeit in diesem Bereich wichtiger denn je. Der EAD tauscht sich in dieser Hinsicht zur Lageerfassung aus und arbeitet an koordinierten Reaktionen auf böswillige Cyberaktivitäten gegen die Ukraine sowie an der Unterstützung der Ukraine und anderer Akteure in der Region. Dazu arbeitet der EAD mit den USA und der NATO zusammen, um Komplementarität sicherzustellen und Überschneidungen zu vermeiden.

Die enge Zusammenarbeit mit den USA wurde auch im Rahmen des EU-US-Handels- und Technologierats (TTC) intensiviert. In der gemeinsamen Erklärung[25] nach dem Ministertreffen im Mai in Paris wird die wichtige Rolle des TCC für die erneuerte transatlantische Partnerschaft hervorgehoben, der die gemeinsamen Maßnahmen der EU und der USA in Anbetracht des russischen Angriffs auf die Ukraine koordiniert. Beide Parteien waren sich einig, dass eine enge Zusammenarbeit zur Stärkung der Widerstandsfähigkeit von Lieferketten wichtiger denn je ist. Des Weiteren wurde eine besondere Taskforce für die öffentliche Finanzierung sicherer und resilienter digitaler Infrastrukturen in Drittländern gebildet, die den Weg für eine gemeinsame öffentliche Finanzierung von Digitalprojekten in Drittländern durch die USA und die EU ebnen soll, und zwar auf der Grundlage einer Reihe gemeinsamer übergreifender Grundsätze.

Mit dem im März 2022 angenommenen Strategischen Kompass (siehe Abschnitt VII) wird das EU-Instrumentarium für die Cyberdiplomatie weiter gestärkt und die EU-Politik im Bereich Cyberabwehr ausgebaut, um besser auf Cyberangriffe vorbereitet zu sein und reagieren zu können. Dies ist Teil einer umfassenderen Strategie zur Stärkung der Fähigkeit der EU, in Krisen zu handeln und ihre Interessen zu verteidigen.

Unterstützung im Bereich Cybersicherheit für die Ukraine und Nachbarländer

Die EU hat die Ukraine bereits vor dem Krieg in der Cyberresilienz unterstützt. Schon im Juni 2021 fand ein erster Cyberdialog zwischen der EU und der Ukraine statt. Die EU leistete im Rahmen des mit 25 Mio. EUR ausgestatteten Programms „EU4Digital Ukraine“ Unterstützung für die Cybersicherheit und einen resilienten digitalen Wandel. Ein weiteres mit 1,5 Mio. EUR ausgestattetes Partnerschaftsprogramm soll den ukrainischen Cybersicherheitseinrichtungen bei der Angleichung an die EU-Standards helfen.

Mit Ausbruch des Kriegs fördert die EU die Zusammenarbeit zwischen Cyberexperten aus der EU und der Ukraine und koordiniert die Bereitstellung technischer Hilfe, Geräte, Software und relevanter Dienste zur Stärkung der Cyberresilienz und Cyberabwehr der Ukraine.

Darüber hinaus arbeitet die EU an der Bewertung einer mittelfristigen Unterstützung Moldaus, Georgiens und der Länder des Westbalkans. Am 3. und 4. März 2022 fand eine

[25] https://ec.europa.eu/commission/presscorner/detail/de/STATEMENT_22_3108

gemeinsame Bewertungsmission in Moldau zur Cybersicherheit statt und führte zur Annahme einer speziellen Krisenreaktionsmaßnahme zur raschen Erhöhung der Cybersicherheit im Land. Eine ähnliche Unterstützung in der Krisenreaktion wird derzeit für eine Reihe von Ländern im Westbalkan vorbereitet, die aufgrund ihres Anschlusses an EU-Sanktionen als besonders gefährdet einzustufen sind. Außerdem wird eine zusätzliche Unterstützung Moldaus im Rahmen der Europäischen Friedensfazilität evaluiert.

III. ORGANISIERTE KRIMINALITTÄT UND TERRORISMUS

Russlands Angriffskrieg gegen die Ukraine hat Millionen Menschen zur Flucht gezwungen. Die Bewegungen über die Außengrenzen der EU haben dadurch enorm zugenommen. Bis 18. Mai sind nahezu 6 Millionen Menschen aus der Ukraine und Moldau in die EU eingereist, 2,8 Millionen sind zwecks vorübergehenden Schutzes in der EU registriert. Die EU hat sich bemüht, die vor dem Krieg fliehenden Menschen so zügig und flexibel wie möglich aufzunehmen, ohne die Sicherheit an der Außengrenze der EU zu gefährden. Die EU hat neue Maßnahmen ergriffen, um den vor dem Krieg Flüchtenden vorübergehenden Schutz zu gewähren, und ist entschlossen, alle neu Ankommenden gleich zu behandeln. Gleichzeitig dürfen die möglichen Risiken nicht außer Acht gelassen werden, die mit so großen Menschenbewegungen einhergehen. Die EU bleibt daher, unterstützt von den zuständigen EU-Agenturen, wachsam im Hinblick auf neue Entwicklungen in der organisierten Kriminalität und im Terrorismus.

Ein starker Schengen-Raum in Zeiten wachsender Bedrohungen

Die Gewährleistung eines hohen Maßes an Sicherheit im Schengen-Raum und in der EU war noch nie so wichtig wie heute in einem Umfeld gestiegener Bedrohungen durch den Krieg kurz hinter der EU-Außengrenze.

In Erfüllung der ehrgeizigen Agenda für den Schengen-Raum, die in der Strategie vom Juni 2021 festgelegt wurde, legte die Kommission im Mai den ersten Schengen-Statusbericht[26] vor. Der jährliche Schengen-Zyklus schafft ein neues Management-Modell für den Schengen-Raum und sieht einen regelmäßigen „Gesundheits-Check“ des Schengen-Raums vor. So können Probleme frühzeitig erkannt und wirksame Folgemaßnahmen ergriffen werden, um den Schengen-Raum stärker und widerstandsfähiger zu machen.

Im ersten Bericht wird festgestellt, dass die Bemühungen zur Umsetzung wichtiger Initiativen auf EU-Ebene, darunter systematische Kontrollen aller Reisenden an den Außengrenzen, volle Ausschöpfung der Mandate von Frontex und Europol sowie geplante und bestehende Instrumente zur grenzüberschreitenden polizeilichen Zusammenarbeit, verstärkt werden müssen.

Eine wichtige Rolle für die Verbesserung der internen Sicherheit und des Grenzschutzes kommt dabei insbesondere der neuen Architektur der EU-Informationssysteme für Grenzen, Migration und Sicherheit zu. Die wirksame Umsetzung aller Elemente des Interoperabilitätsrahmens innerhalb der vereinbarten Zeiträume ist von entscheidender

[26] COM(2022) 301.

Bedeutung.

Wachsamkeit und Koordinierung

Um neu auftauchende kriminelle und terroristische Bedrohungen wahrnehmen und gegen kriminelle Netzwerke und Einzelpersonen vorgehen zu können, die den Krieg gegen die Ukraine für sich zu nutzen versuchen, ist eine enge Zusammenarbeit auf dem Gebiet der Strafverfolgung sowohl zwischen den Mitgliedstaaten als auch mit Drittländern erforderlich. Die Mitgliedstaaten und operativen Partner geben verfügbare relevante Informationen und kriminalpolizeiliche Erkenntnisse an Europol weiter, das die Informationen abgleicht und analysiert und daraus operative Erkenntnismitteilungen wie zum Beispiel Frühwarnmeldungen und Bedrohungsanalysen erstellt, die wiederum an die Partner weitergegeben werden.

Organisierte Kriminalität

Die organisierte Kriminalität hat bereits Wege gefunden, die aktuelle Situation auszunutzen. In einer ersten kriminalpolizeilichen Analyse wurden in einigen Bereichen Kriminalitätsmuster ermittelt. Dazu gehören Menschenhandel, falsche Einfuhr- und Ausfuhranmeldungen für Waren, Online-Betrug, Cyberkriminalität und unerlaubter Handel mit Feuerwaffen. Außerdem gibt es Belege dafür, dass Cyberkriminelle sich als Spendensammler für die Ukraine ausgeben, um Geld und Kryptowährungen zu stehlen.[27] Es ist möglich, dass kriminelle Vereinigungen aus der Ukraine aufgrund der aktuellen Lage versuchen, ihre Tätigkeiten in die EU zu verlagern.

Die Kommission und der französische EU-Ratsvorsitz haben zusammen mit den JI-Agenturen der EU und insbesondere Europol die Europäische multidisziplinäre Plattform gegen kriminelle Bedrohungen (**EMPACT**) mobilisiert, um bestehende und neue Bedrohungen durch die organisierte Kriminalität zu analysieren, zu antizipieren, zu verhindern und zu bekämpfen. Am 7. April 2022 organisierte Europol ein EMPACT-Treffen, bei dem Vertreter und Sachverständige aus den EU-Mitgliedstaaten und der EU-Sicherheitsgemeinschaft zusammenkamen, um sich gemeinsam mit den Bedrohungen durch schwere und organisierte Kriminalität zu beschäftigen, die im Zuge des Kriegs in der Ukraine entstanden sind. Zu den besprochenen konkreten Schritten gehörten das Sammeln von mehr Informationen, die Umsetzung operativer Sofortmaßnahmen und die Neuausrichtung bestehender Maßnahmen sowie gemeinsame Ad-hoc-Aktionstage.

CELBET (Sachverständigenteam für die östlichen und südöstlichen Zollaußengrenzen (Landgrenzen)) – ein von der Europäischen Kommission finanziertes Projekt der Zusammenarbeit – verfolgt im Rahmen seines Auftrags, Zollbedienstete operativ zu unterstützen und zu beraten, die Entwicklungen an der Grenze und überwacht Beschlagnahmen durch den Zoll an den Grenzübergängen an der EU-Außengrenze (Polen, Slowakei, Ungarn und Rumänien) zur Ukraine.

[27] Die Threat Analysis Group von Google hat eine wachsende Zahl von Betrügern beobachtet, die den Krieg in der Ukraine als Lockmittel für Phishing- und Schadsoftware-Angriffe nutzen. Mitarbeiter des im Bereich Internetsicherheit tätigen Unternehmens Cyren melden einen Anstieg von Betrugsversuchen im Bereich Kryptowährungen. Die Betrüger nutzen den Konflikt für falsche Spendenseiten im Internet.

Kriminelle und terroristische Aktivitäten

In der EU ist zwar im Zusammenhang mit dem russischen Einmarsch in die Ukraine bislang keine unmittelbare terroristische Bedrohung entstanden. Dennoch ist Wachsamkeit gefragt.

Aufgrund des erhöhten Risikos für kriminelle und terroristische Aktivitäten ist es wichtig, dass die Mitgliedstaaten die einschlägigen EU-Datenbanken wie das Schengener Informationssystem nutzen, um gegebenenfalls Daten einzutragen, und diese Datenbanken bei Kontrollen von in die EU einreisenden Personen konsultieren. Auf diese Weise können Personen, die eine Bedrohung für die innere Sicherheit der EU darstellen, leichter an den Außengrenzen erkannt werden. Die Agentur der Europäischen Union für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA) sorgt nach wie vor für die uneingeschränkte Verfügbarkeit und Effizienz der Grenzmanagementsysteme der EU. In Leitlinien[28] für die Mitgliedstaaten wird dargelegt, wie zwischen dem erforderlichen reibungslosen Ablauf der Einreisen an der Außengrenze und den notwendigen Sicherheitskontrollen ein Gleichgewicht gefunden werden kann.

Abwehrbereitschaft

Neben Leitlinien und Koordinierung ist die Abwehrbereitschaft der EU durch die Bereitstellung von Personal der EU-Agenturen gestärkt worden.

Europol setzt operative Teams in den EU-Mitgliedstaaten ein, die an die Ukraine grenzen. Die Teams bestehen aus Europol-Gastbeamten aus den Mitgliedstaaten und Europol-Experten in Ungarn, Litauen, Polen, Rumänien und der Slowakei sowie Moldau.[29] Die Europol-Gastbeamten unterstützen die nationalen Behörden bei Überprüfungen in der zweiten Kontrolllinie an den EU-Außengrenzen. Die Europol-Experten unterstützen die Erhebung und Analyse von Informationen zur Aufdeckung terroristischer und krimineller Bedrohungen, zur Unterstützung von Ermittlungen und zur Identifizierung von Personen, die ein Risiko darstellen, wenn sie die EU betreten. Die operativen Teams sammeln Informationen, die in die Bewertungen zur Bedrohungslage durch kriminelle Aktivitäten einfließen, die den Mitgliedstaaten zur Verfügung stehen. Dank dieser Informationsgewinnung kann Europol Entwicklungen vorwegnehmen und operative Tätigkeiten mit den Mitgliedstaaten abstimmen, um auf die Aktivitäten krimineller Vereinigungen zu reagieren, die den Krieg gegen die Ukraine für sich zu nutzen versuchen, sowie über den ukrainischen Verbindungsbeamten im Hauptquartier von Europol in den Niederlanden die Strafverfolgung in der Ukraine aktiv unterstützen.

Die **Europäische Agentur für die Grenz- und Küstenwache (Frontex)** ist ebenfalls in den Mitgliedstaaten sowie in Nachbarländern der EU zur Unterstützung von Grenzkontrolltätigkeiten anwesend. In der EU, im Westbalkan und in Moldau sind derzeit mehr als 2100 Grenzschutzbeamte im Einsatz. Das **Europäische Unterstützungsbüro für Asylfragen (EASO)** setzt knapp 750 Bedienstete in den südlichen Mitgliedstaaten und in

[28] Mitteilung der Kommission über operative Leitlinien für das Außengrenzenmanagement zur Erleichterung des Grenzübertritts an den Grenzen zwischen der Ukraine und der EU (2022/C 104 I/01).

[29] Stand 3. Mai hat Europol einen Europol-Bediensteten und drei Gastbeamte in der Slowakei, einen Europol-Bediensteten in Polen, einen Europol-Bediensteten und vier Gastbeamte in Rumänien und zwei Gastbeamte in Ungarn im Einsatz. In Moldau sind ein Europol-Bediensteter und zwei Gastbeamte eingesetzt.

Litauen zur Unterstützung der operativen Tätigkeiten, Stärkung der Aufnahmekapazitäten und Hilfe bei Asylverfahren ein.

Gestützt auf den Prümer Beschluss[30], der den Mitgliedstaaten einen Rahmen für den Einsatz von Strafverfolgungsbeamten für gemeinsame Operationen (z. B. gemeinsame Streifen) bietet, haben die Kommission und der französische Vorsitz im Rat der Europäischen Union ein gemeinsames Schreiben an alle Mitgliedstaaten gerichtet, um den Bedarf zu ermitteln und um die Entsendung von Polizeibeamten zu bitten, damit gemeinsame Streifen in den EU-Grenzstaaten durchgeführt werden können, die von den massenhaften Grenzübertritten aufgrund des Krieges am stärksten betroffen sind. Die Kommission wird diese Einsätze aus dem Fonds für die innere Sicherheit (Polizei) finanzieren.

Bekämpfung des Menschenhandels

Die EU hat seit den ersten Kriegstagen die Risiken eines bestimmten Bereichs krimineller Aktivitäten im Blick, die durch die großen Bewegungen von in der EU Schutz suchenden Menschen begünstigt werden. Es ist dringend erforderlich, Menschenhandel zu verhindern, der für gefährdete Personen auf der Flucht, hauptsächlich **Frauen und Kinder**, eine Gefahr darstellt, z. B. in Form falscher Transport- oder Unterkunftsangebote.

Im März verschickten Europol und Eurojust Frühwarnmeldungen zum Risiko des Menschenhandels und der Ausbeutung von Opfern aus der Ukraine an die zuständigen nationalen Behörden. Eurojust unterstützt den Informationsaustausch und treibt die justizielle Zusammenarbeit, auch mit der Ukraine, voran. Ermittlungen zu Menschenhandel wurden zur Koordinierung an die Agentur weitergeleitet.

Der EU-Koordinator für die Bekämpfung des Menschenhandels hat Treffen mit dem EU-Netz nationaler Berichterstatter oder gleichwertiger Mechanismen, den Agenturen im Bereich Justiz und Inneres und der EU-Plattform der Zivilgesellschaft zur Bekämpfung des Menschenhandels organisiert, um sich über die Maßnahmen auszutauschen, die zur Verhinderung und Bekämpfung von Missbrauch und zum Schutz von Opfern erforderlich sind. In mehreren Mitgliedstaaten wurden Untersuchungen zu mutmaßlichen Fällen eingeleitet.

Die EU hat auf diese reale Bedrohung für Menschen, die die Hilfe der EU benötigen, rasch und energisch sowie in koordinierter Weise reagiert. Den Mitgliedstaaten, die die Richtlinie über vorübergehenden Schutz zur Unterstützung von aus der Ukraine flüchtenden Menschen umsetzen, wurden umgehend operative Leitlinien[31] an die Hand gegeben, die sich auch mit dem Problem des Menschenhandels befassen. Als Teil des 10-Punkte-Plans für eine stärkere europäische Koordinierung der Aufnahme von Menschen, die vor dem Krieg gegen die Ukraine fliehen[32], der auf der Tagung des Rates „Justiz und Inneres“ am 28. März 2022 vorgelegt wurde, erarbeitete der EU-Koordinator für die Bekämpfung des Menschenhandels in Absprache mit den EU-Agenturen und den Mitgliedstaaten einen gemeinsamen Plan zur

[30] 2008/615/JI, 2008/616/JI.
[31] C/2022/1806, EUR-Lex - 52022XC0321(03) - DE - EUR-Lex (europa.eu).
[32] https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1647940863274&uri=CELEX%3A52022XC0321%2803%29

Bekämpfung von Menschenhandel[33] zur Verhinderung von Menschenhandel und zur Unterstützung von Opfern. Ein besonderer Schwerpunkt liegt auf der Registrierung von Einrichtungen und Personen (einschließlich Freiwilligen), die Unterkunft, Transport und andere Arten der Hilfe anbieten möchten, sowie auf der Durchführung von Zuverlässigkeitsüberprüfungen. Die Kommission hat sich außerdem mit dem EASO in Verbindung gesetzt, um die Identifizierung von Opfern von Menschenhandel im Rahmen der Gesundheitsuntersuchungen in Aufnahmezentren zu unterstützen. Unbegleitete und von ihren Angehörigen getrennte Kinder sind besonders gefährdet, Opfer von Missbrauch, sexueller Ausbeutung oder Zwangskriminalität zu werden. Die erwähnten operativen Leitlinien enthalten auch Ratschläge für die Mitgliedstaaten, wie Kinder und insbesondere unbegleitete Minderjährige bei der Einreise aufgenommen und unterstützt werden können. Um diejenigen zu sensibilisieren, die dem Risiko ausgesetzt sind, hat die Kommission eine eigene Webseite eingerichtet, die praktische Ratschläge enthält, wie man Menschenhändler vermeidet.

Während einige Maßnahmen zur Erhöhung der Abwehrbereitschaft in Reaktion auf die neuen Umstände durch den Krieg ergriffen wurden, gehen andere wichtige Maßnahmen auf **Gesetzgebungsinitiativen** zurück, die bereits vor dem Angriffskrieg Russlands gegen die Ukraine geplant waren.

Die Kommission begrüßt die im Februar 2022 erzielte Einigung über das überarbeitete Mandat von **Europol**[34], das es Europol ermöglichen wird, die Mitgliedstaaten in ihrem Kampf gegen die organisierte Kriminalität und Terrorismus besser zu unterstützen. Die Agentur wird damit über die richtigen Instrumente und Garantien verfügen, um die Polizeikräfte bei der Analyse von Massendaten zur Aufklärung von Straftaten und bei der Entwicklung bahnbrechender Methoden zur Bekämpfung der Cyberkriminalität zu unterstützen. Diese Änderungen gehen einher mit einem verstärkten Datenschutzrahmen sowie einer stärkeren parlamentarischen Kontrolle und Rechenschaftspflicht.

Das von der Kommission am 8. Dezember 2021 vorgestellte Maßnahmenpaket für die polizeiliche Zusammenarbeit[35], über das derzeit verhandelt wird, wird die Zusammenarbeit zwischen Strafverfolgungsbeamten unterschiedlicher Mitgliedstaaten stärken, da der Austausch von Daten schneller, einfacher und sicherer möglich sein wird und die operative polizeiliche Zusammenarbeit vor Ort gestärkt und effizienter wird. Die Kommission fordert das Europäische Parlament und den Rat auf, dieses Paket rasch anzunehmen.

Sind diese Legislativvorschläge erst einmal beschlossen und umgesetzt, werden sie die Strafverfolgung im Kampf gegen die grenzüberschreitende organisierte Kriminalität unterstützen. Dies ist insbesondere vor dem Hintergrund wichtig, dass kriminelle Vereinigungen aus der Ukraine aufgrund der aktuellen Lage versuchen könnten, ihre Tätigkeiten in die EU zu verlagern.

Die **Beratende Mission der EU in der Ukraine** unterstützt seit 2014 die Reform der Strafverfolgung und rechtsstaatlicher Institutionen im Land. Im März 2022 wurde das Mandat der Mission überarbeitet, um die Unterstützung an den ukrainischen Grenzübergängen zu

[33] https://ec.europa.eu/home-affairs/news/new-anti-trafficking-plan-protect-people-fleeing-war-ukraine-2022-05-11_en
[34] COM/2020/796.
[35] COM/2021/780, COM/2021/782, COM/2021/784.

Polen, Rumänien und der Slowakei zu ermöglichen und zur Lageeinschätzung im Hinblick auf grenzüberschreitende kriminelle Aktivitäten, einschließlich Menschenhandel, und den Strom von Hilfsgütern in die Ukraine beizutragen.

IV. WAFFEN, GEFÄHRLICHE GÜTER UND KRITISCHE VORFÄLLE

Der Krieg hat zu einem enormen Anstieg der Verbreitung von Feuerwaffen und anderen Waffen in der Ukraine geführt. Dies stellt neue Risiken für die EU und andere Nachbarstaaten der Ukraine dar.

Wachsamkeit und Koordinierung

Die im März vorgelegten operativen Leitlinien[36] enthalten Ratschläge für die Mitgliedstaaten, wie sie die Herausforderung der erhöhten Verbreitung von Feuerwaffen angesichts der Massenzuströme an der EU-Außengrenze bewältigen können. In den Leitlinien wird hervorgehoben, dass stets kontrolliert werden sollte, ob Feuerwaffen vorhanden sind, und dass niemand ohne eine entsprechende Genehmigung mit einer Feuerwaffe in die EU einreisen darf. Sind vorgefundene Feuerwaffen von den ukrainischen Behörden als fehlend gemeldet worden, sollten die Mitgliedstaaten sie im Schengener Informationssystem melden.

Alle Feuerwaffenlieferungen in die Ukraine müssen unbedingt ordnungsgemäß mit allen sachdienlichen Informationen (einschließlich Typ, Land und Jahr der Herstellung, Marke, Fabrikat, Kaliber, Seriennummer) protokolliert werden, um die Rückverfolgbarkeit dieser Feuerwaffen sowohl in der Ukraine als auch in der EU zu erleichtern.

Die EU hat die rücksichtslosen militärischen Angriffe Russlands auf und in der Nähe von zivilen nuklearen, biologischen und chemischen Anlagen in der Ukraine sowie alle Handlungen, die die Sicherheit dieser Anlagen gefährden, öffentlich verurteilt. Die Kommission beobachtet die Lage in der Ukraine und legt dabei ein besonderes Augenmerk auf radiologische Bedrohungen, die für die innere Sicherheit der EU am meisten Anlass zur Sorge geben.[37] Des Weiteren hat die Kommission ein Auge auf potentielle chemische Bedrohungen und hat einen internen Koordinierungsmechanismus für den Fall eingerichtet, dass eine schnelle Risikobewertung notwendig ist.

Abwehrbereitschaft

Die Ukraine gehört bereits zu den Ländern, die im EU-Aktionsplan gegen den unerlaubten Handel mit Feuerwaffen (2020–2025) für bestimmte Maßnahmen auf externer Ebene als besonders wichtig eingestuft wurden. Außerdem gibt es im Rahmen der EMPACT-Projektgruppe „Feuerwaffen“ eine spezifische operative Maßnahme in der Region, die die Ukraine einschließt. Angesichts des Risikos, dass Feuerwaffen umgelenkt werden, braucht es jedoch spezielle, von der EU finanzierte Projekte sowie eine operative Zusammenarbeit mit Europol, Frontex und der EMPACT-Projektgruppe „Feuerwaffen“. Die Kommission wird demnächst einen Vorschlag zur Überarbeitung der Verordnung über Schusswaffen[38] zur Aus-

[36] Mitteilung der Kommission über operative Leitlinien für das Außengrenzenmanagement zur Erleichterung des Grenzübertritts an den Grenzen zwischen der Ukraine und der EU (2022/C 104 I/01).

[37] Die Kommission wird zusammen mit US-Partnern einen Workshop zu den Risiken im Zusammenhang mit radiologischen Materialien in Krankenhäusern, die der behördlichen Kontrolle entgleiten, durchführen.

[38] Verordnung (EU) Nr. 258/2012 des Europäischen Parlaments und des Rates vom 14. März 2012

, Ein- und Durchfuhr ziviler Schusswaffen vorlegen, der sich in den rechtlichen und operativen Gesamtrahmen zur Verhinderung, Aufdeckung, Untersuchung und Verfolgung des unerlaubten Handels mit Feuerwaffen einfügt.

Zur Verbesserung der Abwehr- und Reaktionsbereitschaft der EU in Bezug auf Risiken für die öffentliche Gesundheit, einschließlich chemischer, biologischer, radiologischer und nuklearer Risiken (CBRN), baut die Kommission, finanziert durch die Einrichtung der Europäischen Behörde für die Krisenvorsorge und - reaktion bei gesundheitlichen Notlagen (HERA)[39], über das Katastrophenschutzverfahren der Union strategische Reserven an Bewältigungskapazitäten auf. Die Dienststellen der Kommission arbeiten gemeinsam am Aufbau einer strategischen rescEU-Reserve im Umfang von 540,5 Mio. EUR. Der Vorrat umfasst Ausrüstung und Arzneimittel, Impfstoffe und andere Therapeutika zur Behandlung von Patienten, die im Zusammenhang mit CBRN-Vorfällen gesundheitsgefährdenden Stoffen ausgesetzt sind, sowie eine rescEU-Dekontaminierungsreserve zur Bereitstellung von Dekontaminierungsausrüstung und von Expertenteams. Als raschen ersten Schritt hat die EU ihre medizinische rescEU-Reserve für die Beschaffung von Kaliumiodidtabletten, die zum Schutz der Menschen vor den schädlichen Auswirkungen von Strahlung verwendet werden können, sowie anderer dringend in der Ukraine benötigter Mittel mobilisiert. Mit Unterstützung Frankreichs und Spaniens wurden so über das EU-Katastrophenschutzverfahren bereits fast 3 Millionen Jodtabletten für die Ukraine bereitgestellt.

V. KOORDINIERTES VORGEHEN, UM RUSSISCHE ANGREIFER ZUR RECHENSCHAFT ZU ZIEHEN

Die EU spielt eine entscheidende Rolle bei den Maßnahmen der internationalen Gemeinschaft, um Druck auf Russland auszuüben, damit es seinen nicht hinnehmbaren und gegen das Völkerrecht verstoßenden Angriff auf den ukrainischen Staat und die in dem Konflikt gefangenen Zivilisten beendet. Dazu gehören Maßnahmen, die den Tätern die Folgen aufzeigen, einschließlich schwerwiegender Sanktionen, sowie Maßnahmen zur Untersuchung von Kriegsverbrechen und zur Erleichterung der Strafverfolgung.

Restriktive Maßnahmen und Einziehung von Vermögenswerten

Seit der Anerkennung der nicht von der Regierung kontrollierten Gebiete in den ukrainischen Oblasten Donezk und Luhansk durch Russland am 21. Februar 2022 und dem Einmarsch in die Ukraine am 24. Februar 2022 hat die EU restriktive Maßnahmen in einem bis dahin nicht gekanntem Ausmaß gegen Russland ergriffen. Bislang wurden fünf Sanktionspakete beschlossen. Die Maßnahmen konzentrieren sich auf wichtige Sektoren, darunter Finanzen, Handel, Verkehr, Verteidigung und Medien, und richten sich gegen die politische und militärische Elite sowie gegen prominente russische und belarussische Oligarchen. Die Liste

---

zur Umsetzung des Artikels 10 des Protokolls der Vereinten Nationen gegen die unerlaubte Herstellung von Schusswaffen,

dazugehörigen Teilen und Komponenten und Munition und gegen den unerlaubten Handel damit, in Ergänzung des Übereinkommens der Vereinten Nationen

gegen die grenzüberschreitende organisierte Kriminalität (VN-Feuerwaffenprotokoll) und zur Einführung von Ausfuhrgenehmigungen

für Feuerwaffen, deren Teile, Komponenten und Munition sowie von Maßnahmen betreffend deren Einfuhr und Durchfuhr.

[39] HERA-Arbeitsplan 2022 (europa.eu)

umfasst bereits mehr als 1000 Personen und 80 Unternehmen. Der Rat berät derzeit über ein sechstes Sanktionspaket.

Die Auswirkungen dieser und vorangegangener restriktiver Maßnahmen gegen russische und belarussische Personen und Unternehmen hängen von ihrer Umsetzung ab. Eine Koordinierung durch die EU kann erheblich dazu beitragen, mögliche Schlupflöcher zu schließen. Die Kommission hat Interessenträgern in Form schriftlicher Leitlinien, gemeinsamer Treffen und einer Expertengruppe umfassend unterstützt und eine Palette an Ressourcen zur Erleichterung der Einhaltung zur Verfügung gestellt.

Außerdem hat die Kommission die Task Force „Freeze and Seize" eingerichtet, an der die Dienststellen der Kommission, die Mitgliedstaaten, Eurojust und Europol beteiligt sind. Die Mitgliedstaaten haben mitgeteilt, dass sie bis jetzt Vermögenswerte in Höhe von 9,89 Mrd. EUR eingefroren haben.[40] Am 11. April startete Europol gemeinsam mit den Mitgliedstaaten, Eurojust und Frontex die Operation Oscar zur Unterstützung von Finanzermittlungen und strafrechtlichen Ermittlungen in Bezug auf illegal erworbene Vermögenswerte von natürlichen und juristischen Personen, die unter die EU-Sanktionen im Zusammenhang mit Russlands Krieg gegen die Ukraine fallen. Die Task Force „Freeze and Seize" arbeitet eng mit der Task Force „Russian Elites, Proxies, and Oligarchs (REPO)", die von den G7-Ländern (Kanada, Frankreich, Deutschland, Italien, Japan, Vereinigtes Königreich, Vereinigte Staaten) eingerichtet wurde, sowie gleichgesinnten Partnern wie Australien, der US-Task Force „KleptoCapture" und der ukrainischen Task Force zusammen.

Die Task Force „Freeze and Seize" dient als Plattform für die Koordinierung und Erleichterung des Informations- und Erfahrungsaustauschs zwischen den Mitgliedstaaten, die Bereitstellung von Leitlinien für die Umsetzung von Sanktionen und den erleichterten Austausch bewährter Verfahren in strafrechtlichen Ermittlungen und der Einziehung von Vermögenswerten. Besonders wichtig ist, dass die Strafverfolgungsbehörden im Hinblick auf potentielle Straftaten durch mit Sanktionen belegte Personen und Unternehmen wachsam sind und proaktiv vorgehen. Die Task Force möchte außerdem Diskussionen über die mögliche Verwendung eingezogener Gelder, zum Beispiel für den Wiederaufbau der Ukraine, voranbringen.

Die Kommission nimmt heute ein Paket zur **Abschöpfung und Einziehung von Vermögenswerten**[41] an, in das die Erfahrungen mit der Umsetzung der restriktiven Maßnahmen der Union gegen russische und belarussische Personen und Unternehmen eingeflossen sind. Es wird die effektive Umsetzung der restriktiven Maßnahmen der Union innerhalb der gesamten EU erleichtern, indem es ein rasches Aufspüren und Ermitteln von Vermögen ermöglicht, das im Eigentum oder unter der Kontrolle von Personen oder Unternehmen steht, die diesen Maßnahmen unterliegen. Der verbesserte Rahmen für die Abschöpfung und Einziehung von Vermögenswerten gilt auch bei Verstößen gegen restriktive Maßnahmen und stellt somit ein wirksames Aufspüren, Einfrieren, Verwalten und Einziehen von Erlösen sicher, die aus Verstößen gegen restriktive Maßnahmen stammen. Damit die Vermögenswerte von Personen und Unternehmen, die gegen die restriktiven Maßnahmen verstoßen, auch wirklich eingezogen werden können, legt die Kommission heute außerdem einen Vorschlag für einen Beschluss des Rates über die Aufnahme des Verstoßes

[40] Zusätzlich wurde ein Guthaben der russischen Zentralbank in Höhe von etwa 23 Mrd. EUR blockiert.
[41] COM(2022) 245.

gegen Sanktionen in die Liste der EU-Straftaten in Artikel 83 Absatz 1 AEUV[42] sowie eine begleitende Mitteilung[43] zu einer Richtlinie zur Angleichung der Begriffsbestimmung von Straftaten und Strafen für den Verstoß gegen restriktive Maßnahmen vor.

Das Paket ist ein wichtiger Schritt in der Bekämpfung der organisierten Kriminalität. Es steht im Einklang mit den von der Kommission in der Strategie für eine Sicherheitsunion und der Strategie zur Bekämpfung der organisierten Kriminalität in den Jahren 2020–2025[44] gemachten Zusagen. Mit dem Paket werden die Richtlinie über die Einziehung von Erträgen aus Straftaten von 2014, der Beschluss des Rates von 2007 über Vermögensabschöpfungsstellen und der Rahmenbeschluss des Rates von 2005 über die Einziehung von Erträgen, Tatwerkzeugen und Vermögensgegenständen aus Straftaten überarbeitet, um die Kapazitäten zum Aufspüren und Ermitteln und letztlich zum Einziehen illegaler Gewinne auszubauen und somit die sehr niedrigen Einziehungsraten in der EU[45] zu erhöhen. Mit dem Paket werden der Umfang der erfassten Straftaten sowie die Vorschriften zur Einziehung auf die Fälle erweitert, in denen eine strafrechtliche Verurteilung für eine bestimmte Straftat nicht möglich ist, die Vermögenswerte aber eindeutig aus kriminellen Aktivitäten stammen. Mit der Überarbeitung wird auch die wirksame Verwaltung eingefrorener und eingezogener Vermögenswerte gestärkt und die Kapazitäten der Vermögensabschöpfungsstellen zum Aufspüren und Ermitteln illegaler Vermögenswerte ausgeweitet. Der neue EU-Rahmen zur Abschöpfung von Vermögenswerten wird den komplexen modus operandi krimineller Vereinigungen gerecht, die häufig grenzüberschreitend tätig sind und unterschiedliche Methoden zur Verschleierung ihrer Vermögenswerte nutzen, u. a. durch Rückgriff auf Kryptowerte.

Koordiniertes justizielles Vorgehen

Auf EU-Ebene werden Anstrengungen unternommen, ein koordiniertes justizielles Vorgehen gegen mutmaßliche völkerrechtliche Verbrechen in der Ukraine sicherzustellen, so dass Täter zur Rechenschaft gezogen werden können.

Zwei Mitgliedstaaten und die Ukraine haben eine gemeinsame Ermittlungsgruppe (GEG) zur Untersuchung von Kriegsverbrechen, Verbrechen gegen die Menschlichkeit und anderer völkerrechtlicher Verbrechen eingerichtet, die mutmaßlich auf dem Hoheitsgebiet der Ukraine verübt wurden. Eurojust unterstützt die GEG rechtlich, analytisch, finanziell und logistisch. Seit 25. April 2022 beteiligt sich die Anklagebehörde des Internationalen Strafgerichtshofs an der GEG[46], mit weiteren Teilnehmern wird in naher Zukunft gerechnet.

Am 25. April 2022 legte die Kommission einen Vorschlag für eine Verordnung zur Änderung der Eurojust-Verordnung[47] vor, damit Eurojust Beweismittel für völkerrechtliche Kernverbrechen sichern, analysieren und aufbewahren kann. Eurojust und Europol werden in diesem Prozess eng zusammenarbeiten. Eine wichtige Rolle bei der Koordinierung des justiziellen Vorgehens kommt auch dem Genozid-Netz zu, dessen bei Eurojust angesiedeltes

[42] COM(2022) 247.
[43] COM(2022) 249.
[44] COM(2021) 170.
[45] Laut Schätzungen von Europol werden nur 2 % der Erträge aus Straftaten eingefroren (2,4 Mrd. EUR) und 1 % eingezogen (1,2 Mrd. EUR), während sich die Einnahmen aus der organisierten Kriminalität in den neun bedeutendsten Kriminalitätsbereichen der EU im Jahr 2019 auf 139 Mrd. EUR (1 % des BIP der EU) beliefen.
[46] https://www.eurojust.europa.eu/eurojust-and-the-war-in-ukraine
[47] COM(2022) 187 final.

Sekretariat einen Atlas der aktuell in der Ukraine tätigen NRO erstellt hat und Angehörige der Rechtsberufe aus den Mitgliedstaaten und der Ukraine beim Umgang mit akuten Fällen im Zusammenhang mit dem Krieg unterstützt.

Im April 2022 überarbeitete der Rat erneut das Mandat der **Beratenden Mission der EU in der Ukraine** und machte somit den Weg für die Mission frei, die ukrainischen Behörden bei der Untersuchung und Verfolgung völkerrechtlicher Verbrechen im Zusammenhang mit dem militärischen Angriff Russlands zu unterstützen. Die Mission berät die ukrainischen Behörden bei der Untersuchung und Verfolgung völkerrechtlicher Verbrechen, erforderlichen Änderungen an ukrainischen Gesetzen, der Kommunikationsstrategie sowie der Schulung zu entsprechenden Themen. Die Mission reiht sich in eine Vielzahl an Koordinierungsinitiativen in diesem Kontext ein und ist zusammen mit der EU-Delegation Teil der gemeinsamen Beratergruppe von EU und USA zu Verbrechen gegen die Menschlichkeit in der Ukraine.

VI. MANIPULATION VON INFORMATIONEN UND EINMISCHUNG AUS DEM AUSLAND

Die aktuellen geopolitischen Entwicklungen haben die Risiken einer Einmischung aus dem Ausland deutlich gemacht. Der militärische Angriff Russlands auf die Ukraine ging mit **Manipulation von Informationen und Einmischung** einher. Haltlose Behauptungen von Nazismus und Völkermord der ukrainischen Regierung, Operationen unter falscher Flagge und unbegründete Anschuldigungen gegen die NATO und den Westen wurden zur Begründung der brutalen Angriffe auf die Ukraine herangezogen, während freie Meinungsäußerung und unabhängige Berichterstattung in Russland unterdrückt wurden. Es geht weiterhin eine Gefahr von manipulierten audio-visuellen Materialien und Desinformation aus, die Russland als Vorwand nutzen könnte, um weitere militärische Angriffe zu starten, um den ukrainischen Widerstand zu brechen, um die internationale Gemeinschaft in ihrer Ablehnung des Krieges zu spalten oder um Zweifel an den Verstößen Russlands gegen das Völkerrecht zu säen. Die EU hat sich im Strategischen Kompass dazu verpflichtet, entschlossen auf ausländische Informationsmanipulation und Einmischung zu reagieren und ihre Resilienz und die Fähigkeit zur Bekämpfung zu stärken.[48] Im Europäischen Aktionsplan für Demokratie[49], dem koordinierten Plan der Kommission zur Bekämpfung von Desinformation und Stärkung der demokratischen Resilienz, wird die Manipulation demokratischer Debatten innerhalb der EU thematisiert.

Wachsamkeit und Koordinierung

Die Europäische Union reagierte mit entschiedenen und koordinierten Maßnahmen auf die russische Desinformationskampagne im Rahmen des militärischen Angriffs auf die Ukraine. Die EU arbeitet über das Schnellwarnsystem eng mit den Mitgliedstaaten sowie mit internationalen Partnern wie der NATO, den USA und Kanada sowie im Rahmen des G7-Schnellreaktionsmechanismus zusammen, um Erkenntnisse über Manipulationstrends und -taktiken des Kremls zu teilen. Die Bemühungen, die Manipulationen des Kreml zu dekonstruieren, wurden intensiviert, insbesondere über die Webseite EUvsDisinfo, die faktenbasierte Informationen zur EU, Ukraine und der Region sowie zu Russland auf Englisch, Russisch, Ukrainisch und in anderen Sprachen bereitstellt. Am 2. März wurde die Ausstrahlung der Kanäle der russischen Staatsmedien RT und Sputnik in der EU und in die

[48] https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/de/pdf
[49] COM(2020) 790.

EU infolge der von der EU verabschiedeten restriktiven Maßnahmen ausgesetzt. Online-Plattformen, führende soziale Netzwerke, Werbetreibende und Unterzeichner aus der Werbebranche des Verhaltenskodexes für den Bereich der Desinformation[50] handeln umgehend, um die Desinformation im Zusammenhang mit der russischen Aggression gegen die Ukraine einzudämmen. Die Kommission und der EAD überwachen diese Anstrengungen. Die zur Verfügung stehenden Informationen zeigen, dass die Plattformen ihre Überwachungs- und Interventionsinstrumente in Bezug auf den Krieg verstärkt haben.

Darüber hinaus finden zeitnah Maßnahmen zur Unterstützung von Ländern in Zentralasien und dem Westbalkan statt zur Stärkung der Widerstandsfähigkeit gegen Desinformation und zur Bekämpfung der ausländischen Manipulation von Informationen und der Einmischung aus dem Ausland.

Abwehrbereitschaft

Der unverhohlene Einsatz von Manipulation von Informationen und Einmischung aus dem Ausland, einschließlich Desinformation als ein Instrument der hybriden Bedrohung, hat die Folgemaßnahmen zum Aktionsplan für Demokratie in Europa noch dringlicher werden lassen. In den letzten Monaten haben die EU-Einrichtungen die Mitgliedstaaten bei der Bekämpfung von Manipulation und Einmischung aus dem Ausland unterstützt. Dies erfolgte insbesondere im Rahmen des Schnellwarnsystems, über das Erkenntnisse zu den angewandten Taktiken der Manipulatoren und zu Reaktionsstrategien geteilt werden. Es laufen Diskussionen zur Stärkung der Gesamtantwort der EU auf Manipulation und Einmischung aus dem Ausland. Grundlage hierfür bildet ein Konzeptpapier des EAD zur Entwicklung eines **Instrumentariums** zur Abwendung dieser Bedrohung. Bestehende interne Maßnahmen und neue EU-Instrumente der Gemeinsamen Außen- und Sicherheitspolitik werden so zusammengeführt. Außerdem kommen die energischen Maßnahmen des Europäischen Auswärtigen Dienstes Stratcom[51] und der Kommission zum Tragen.

Die europäische Beobachtungsstelle für digitale Medien (EDMO) hat im Zuge des Kriegsausbruchs in der Ukraine eine Task Force zur Desinformation eingerichtet und koordiniert die Arbeit von Faktenprüfern und Forschern ihres Netzwerks. Sie hat untersucht, wie Anhänger von COVID-19-Verschwörungstheorien rasch auf prorussische Falschmeldungen umgestiegen sind und diese verbreitet haben, eine Verschiebung, die in mehreren Mitgliedstaaten beobachtet wurde.[52]

Ziel des Vorschlags für ein Gesetz über digitale Dienste ist die Anpassung an sich schnell weiterentwickelnde digitale Technologien und die damit einhergehenden technologischen und demokratischen Herausforderungen wie Hassreden, Desinformation im Internet und Destabilisierungsstrategien. Die Verhandlungen des Europäischen Parlaments und des Rates

---

[50] https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

[51] Die Abteilung Strategic Communication, Task Forces and Information Analysis des Europäischen Auswärtigen Dienstes bietet Unterstützung in der strategischen Kommunikation bei der Umsetzung der Außen- und Sicherheitspolitik der EU in Bezug auf prioritäre Regionen (südliche und östliche Nachbarschaft, Westbalkan) und entwickelt dazu spezielle Maßnahmen der strategischen Kommunikation mit dem Schwerpunkt auf der Förderung der Politik, der Werte, Ziele und Interessen der EU und setzt diese Maßnahmen um.

[52] https://edmo.eu/2022/03/30/how-covid-19-conspiracy-theorists-pivoted-to-pro-russian-hoaxes/

haben erhebliche Fortschritte gemacht, so dass eine rasche Annahme des Pakets möglich sein sollte.

VII. ALLGEMEINE ABWEHRBEREITSCHAFT

In einer Zeit, in der der Krieg nach Europa zurückgekehrt ist und umfassende geopolitische Änderungen stattfinden, hat die Koordinierung der Sicherheit in der EU einen Gang zugelegt und knüpft an Initiativen an, die bereits vor Beginn des russischen Angriffskriegs gegen die Ukraine geplant waren. Initiativen, bei denen es hauptsächlich um die externe Sicherheit der EU geht, wirken sich massiv auf die internationale Agenda der Sicherheitsunion aus.

Am 15. Februar 2022 legte die Kommission das Verteidigungspaket mit einer Reihe von Initiativen in Bereichen vor, die für die Verteidigung und die Sicherheit der EU von entscheidender Bedeutung sind.[53] Dieser Beitrag der Kommission zur europäischen Verteidigung und Sicherheit deckt eine ganze Bandbreite an Herausforderungen ab. Es werden konkrete Schritte für einen besser integrierten und wettbewerbsfähigeren europäischen Verteidigungsmarkt vorgeschlagen. Dazu sollen insbesondere die Zusammenarbeit innerhalb der EU verbessert und Skaleneffekte geschaffen werden. Der Vorschlag enthält außerdem einen Fahrplan für kritische Sicherheits- und Verteidigungstechnologien zur Förderung der Forschung, technologischen Entwicklung und Innovation in diesen Sektoren und Verringerung von Abhängigkeiten bei kritischen Technologien und Wertschöpfungsketten. Ein weiteres Ziel des Pakets ist die Stärkung der verteidigungsorientierten Bereiche der Raumfahrt auf EU-Ebene. Des Weiteren wird der Frage nachgegangen, wie die Kommission ihre Maßnahmen zur Abwendung hybrider Bedrohungen, auch im Cyberbereich, ausbauen, die militärische Mobilität inner- und außerhalb Europas verbessern und die Herausforderungen des Klimawandels im Zusammenhang mit der Verteidigung weiter bewältigen kann. In Ergänzung zu dieser Arbeit enthält die Gemeinsame Mitteilung vom 18. Mai zur **Analyse von Investitionslücken in der Verteidigung und zum künftigen Vorgehen**[54] Überlegungen zu den Kapazitätsdefiziten und industriellen Rückständen, die es zu bewältigen gilt, wobei die am meisten gefährdeten EU-Mitgliedstaaten unterstützt werden sollten und Maßnahmen zur Minderung der festgestellten Mängel zu bestimmen sind.

Die Widerstandsfähigkeit der EU gegenüber diesen Bedrohungen erfordert auch auf Fähigkeiten ausgerichtete Ansätze in allen Sicherheitssektoren, wie sie im Aktionsplan der Kommission für Synergien zwischen der zivilen, der Verteidigungs- und der Weltraumindustrie[55] angestrebt werden. An der Förderung von auf Fähigkeiten ausgerichteten Ansätzen im Bereich der internen Sicherheit und der Strafverfolgung wird derzeit gearbeitet.

---

53 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/contributing-european-defence_en

54 JOIN(2022) 24.

55 COM(2021) 70.

Am 21. März 2022 nahm der Rat den **Strategischen Kompass für Sicherheit und Verteidigung**[56] an, der kurz darauf vom Europäischen Rat gebilligt wurde. Darin wird ein ehrgeiziger Aktionsplan für die Stärkung der Sicherheits- und Verteidigungspolitik der EU bis 2030 dargelegt. Das Ziel ist es, die EU zu einem stärkeren und fähigeren Bereitsteller von Sicherheit zu machen, der seine Bürgerinnen und Bürger schützt und zu Weltfrieden und Sicherheit beiträgt. Der Kompass enthält konkrete Vorschläge und einen sehr genauen Zeitplan für die Umsetzung, damit die EU in Krisen entschlossener handeln kann.

Ein Ziel im Strategischen Kompass ist die Entwicklung eines EU-Instrumentariums gegen hybride Bedrohungen, das einen Rahmen für eine koordinierte Reaktion, einschließlich interner und externer Maßnahmen, auf gegen die EU und ihre Mitgliedstaaten gerichtete hybride Kampagnen bieten sollte. Nach der Festlegung sektorspezifischer Referenzwerte für die Resilienz[57] im Januar 2022 wird eine Analyse der Lücken und des Bedarfs durchgeführt. Innerhalb dieses Rahmens wird die EU ihre Abwehrbereitschaft, Widerstandsfähigkeit und Reaktionsfähigkeit auf Bedrohungen durch die russische Aggression und sonstige Versuche zur Destabilisierung von Demokratien und der auf Regeln beruhenden multilateralen Ordnung weiter ausbauen.

VIII. AUSBLICK

Die EU wird sehr wachsam gegenüber sich entwickelnden Bedrohungen bleiben und **Abwehrbereitschaft und Widerstandsfähigkeit gegen alle Eventualitäten** aufbauen müssen. Die Auswirkungen des Krieges können sehr unterschiedliche Formen annehmen, von denen noch nicht alle vorherzusehen sind.

Das Ausmaß der Verlagerung ukrainischer krimineller Netzwerke ist noch nicht bekannt. Die bisherige Fallarbeit von Eurojust deutet an, dass Heroin aus Afghanistan neuerdings verstärkt über die Ukraine in die EU eingeführt wird, was durch Erkenntnisse der Europäischen Beobachtungsstelle für Drogen und Drogensucht (EMCDDA) untermauert wird[58]. Die instabile Lage kann ein Vorgehen gegen den Heroinhandel auf dieser Route erschweren und birgt das Risiko einer möglichen Zunahme des Drogenflusses in die EU.

Einige Risiken für die EU dürften zum Ende der Kämpfe oder während eventueller Kampfpausen eher zunehmen. Besondere Aufmerksamkeit gilt der Verbreitung von Feuerwaffen. Dieses Risiko wird zunehmen, wenn die Kämpfe in der Ukraine nachlassen. Erfahrungen aus der Vergangenheit zeigen, dass ein Risiko besteht, dass zurückkehrende ausländische Kämpfer, die Kampferfahrungen gesammelt haben und möglicherweise mit extremistischen Gruppen in Kontakt gekommen sind, zu einem späteren Zeitpunkt terroristische Aktionen in der EU verüben. Dieses mögliche Szenarium sollte aufmerksam

---

[56] Ein Strategischer Kompass für Sicherheit und Verteidigung – Für eine Europäische Union, die ihre Bürgerinnen und Bürger, Werte und Interessen schützt und zu Weltfrieden und internationaler Sicherheit beiträgt: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/de/pdf

[57] SWD(2022) 21 final.

[58] Report on the drug and alcoholic situation in Ukraine for 2020 (according to 2019 data) (Bericht zur Lage von Drogen und Alkohol in der Ukraine 2020 (anhand von Daten von 2019)), EMCDDA, Stopping the trafficking of a heroin substitute in France, Poland and Ukraine, including the planning and execution of a controlled delivery (Dem illegalen Handel mit einem Heroin-Ersatzstoff im Frankreich, Polen und der Ukraine Einhalt gebieten, einschließlich Planung und Umsetzung einer kontrollierten Lieferung) 2021/00446, Eurojust, Mai 2020.

beobachtet werden. Die Kommission unterstützt bereits Beratungen zwischen den Mitgliedstaaten zu den Herausforderungen, die ausländische Freiwillige mit extremistischem Hintergrund mit sich bringen.

Angesichts dieser potentiellen Bedrohungen ist es wichtig, die Umsetzung der Strategie für eine Sicherheitsunion weiter voranzutreiben. Das gleiche gilt für die Umsetzung wichtiger Strategien wie der Cybersicherheitsstrategie der EU, der Strategie zur Bekämpfung der organisierten Kriminalität (2020–2025), der EU-Agenda für Terrorismusbekämpfung (2020–2025), dem EU-Aktionsplan gegen den unerlaubten Handel mit Feuerwaffen (2020–2025), der EU-Strategie zur Bekämpfung des Menschenhandels (2021–2025) und der EU-Drogenstrategie (2021–2025).

Die Bemühungen, die EU mit dem dafür notwendigen Rechtsrahmen auszustatten, werden fortgesetzt. So erstellt die Kommission zum Beispiel gerade die Folgenabschätzung für einen Vorschlag zur Regulierung des Inverkehrbringens und der Verwendung hochgefährlicher Chemikalien.

IX. FAZIT

Die Sicherheitsunion spielt weiterhin eine wichtige Rolle dabei, die EU und ihre Mitgliedstaaten für die Abwendung bestehender und möglicher Bedrohungen gut aufzustellen. Der russische Angriffskrieg gegen die Ukraine hat gezeigt, wie schnell theoretische Bedrohungen real werden können und wie wichtig Wachsamkeit, Koordinierung und Abwehrbereitschaft sind.

Der vorliegende vierte Fortschrittsbericht zur EU-Strategie für eine Sicherheitsunion zeigt, dass die EU in der Lage ist, selbst auf außergewöhnliche und unerwartete Bedrohungen, wie die im Zusammenhang mit dem russischen Angriffskrieg gegen die Ukraine, angemessen zu reagieren. Eine entschlossene Umsetzung der Strategie für eine Sicherheitsunion ist wichtiger denn je.