EUROPÄISCHE
KOMMISSION

HOHER VERTRETER
DER UNION FÜR
AUSSEN- UND
SICHERHEITSPOLITIK

Brüssel, den 16.12.2020
JOIN(2020) 18 final

GEMEINSAME MITTEILUNG AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT GEMEINSAME MITTEILUNG AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

Die Cybersicherheitsstrategie der EU für die digitale Dekade

GEMEINSAME MITTEILUNG AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT GEMEINSAME MITTEILUNG AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

Die Cybersicherheitsstrategie der EU für die digitale Dekade

I. EINLEITUNG: EIN DIGITALER WANDEL UNTER WAHRUNG DER CYBERSICHERHEIT IN EINEM KOMPLEXEN BEDROHUNGSUMFELD

Cybersicherheit ist ein integraler Bestandteil der Sicherheit der Europäerinnen und Europäer. Unabhängig davon, ob es sich um vernetzte Geräte, Stromnetze oder Banken, Flugzeuge, öffentliche Verwaltungen oder Krankenhäuser handelt, die sie nutzen oder aufsuchen, verdienen die Menschen dabei die Gewissheit, dass sie vor Cyberbedrohungen geschützt werden. Wirtschaft, Demokratie und Gesellschaft in der EU hängen mehr denn je von sicheren und zuverlässigen digitalen Instrumenten und Verbindungen ab. Die Cybersicherheit ist daher von entscheidender Bedeutung, um ein resilientes, grünes und digitales Europa aufzubauen.

Verkehr, Energie und Gesundheit, Telekommunikation, Finanzen, Sicherheit, demokratische Prozesse, Raumfahrt und Verteidigung hängen stark von Netz- und Informationssystemen ab, die zunehmend miteinander verbunden sind. Sektorübergreifende wechselseitige Abhängigkeiten sind stark ausgeprägt, da Netze und Informationssysteme wiederum eine stetige Versorgung mit Strom benötigen. Die Zahl der vernetzten Geräte übersteigt bereits jetzt die Zahl der Menschen auf der Erde und dürfte Prognosen zufolge bis 2025 auf 25 Milliarden ansteigen[1]: ein Viertel dieser Geräte wird sich in Europa befinden. Die Digitalisierung der Arbeitsweisen wurde durch die COVID-19-Pandemie beschleunigt. 40 % der Arbeitnehmer in der EU sind in dieser Zeit zur Telearbeit übergegangen, was vermutlich dauerhafte Auswirkungen auf den Alltag haben wird.[2] Dies erhöht die Anfälligkeit für Cyberangriffe.[3] Vernetzte Objekte werden häufig mit bekannten Schwachstellen an den Verbraucher geliefert, wodurch sich die Angriffsfläche für böswillige Cyberaktivitäten weiter vergrößert.[4] Die Industrielandschaft in der EU ist zunehmend

[1] Schätzung der Telekommunikationsvereinigung GSMA; https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf. Die International Data Corporation prognostiziert 42,6 Milliarden vernetzte Maschinen, Sensoren und Kameras; https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[2] In einer im Juni 2020 durchgeführten Umfrage gaben 47 % der Führungskräfte aus der Wirtschaft an, dass sie es ihren Beschäftigten gestatten wollten, in Vollzeit von zu Hause aus zu arbeiten, auch wenn es möglich wird, wieder an den Arbeitsplatz zurückzukehren; 82 % wollten zumindest Telearbeit in Teilzeit ermöglichen; https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time.

[3] https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

[4] Eine der bisher schädlichsten Schadsoftwares mit dem Namen Mirai schuf Botnetze mit mehr als 600 000 Geräten, die Störungen auf mehreren großen Websites in Europa und den Vereinigten Staaten verursachten.

digitalisiert und vernetzt; dies bedeutet auch, dass Cyberangriffe weitaus größere Auswirkungen auf die Industrie und die Ökosysteme haben können als je zuvor.

Geopolitische Spannungen in Bezug auf das globale und offene Internet und die Kontrolle über die Technologien entlang der gesamten Lieferkette[5] verschärfen die Bedrohungslage noch. Diese Spannungen spiegeln sich in der zunehmenden Zahl von Nationalstaaten wider, die digitale Grenzen errichten. Beschränkungen des Internets und im Internet bedrohen den globalen und offenen Cyberraum ebenso wie die Rechtsstaatlichkeit, die Grundrechte, die Freiheit und die Demokratie – die Grundwerte der EU. Der Cyberraum wird vermehrt für politische und ideologische Zwecke genutzt. Er wird zum Schauplatz einer zunehmenden Polarisierung auf internationaler Ebene, die einen wirksamen Multilateralismus behindert. Hybride Bedrohungen verknüpfen Desinformationskampagnen mit Cyberangriffen auf Infrastrukturen, Wirtschaftsabläufe und demokratische Institutionen. Sie können physischen Schaden verursachen, unrechtmäßig Zugriff auf personenbezogenen Daten oder den Diebstahl von Industrie- oder Staatsgeheimnissen ermöglichen, Misstrauen säen und den sozialen Zusammenhalt schwächen. Solche Aktivitäten untergraben die internationale Sicherheit und Stabilität wie auch die Vorteile des Cyberraums für die wirtschaftliche, soziale und politische Entwicklung.

Böswillige Angriffe auf kritische Infrastrukturen sind weltweit eine große Gefahr.[6] Das Internet zeichnet sich durch eine dezentrale Architektur aus. Es hat keine zentrale Struktur und wird von vielen verschiedene Akteuren gemeinsam verwaltet. Es ist gelungen, den exponentiellen Anstieg des Datenverkehrs zu bewältigen, während das Internet gleichzeitig ein konstantes Ziel böswilliger Störungsversuche ist.[7] Zugleich steigen die Abhängigkeiten von den Kernfunktionen des globalen und offenen Internets, wie dem Domänennamensystem (DNS), und wesentlichen Internetdiensten für Kommunikation und Hosting, Anwendungen und Daten. Diese Dienste konzentrieren sich zunehmend in der Hand einiger weniger privater Unternehmen.[8] Dadurch ist die europäische Wirtschaft und Gesellschaft anfällig für geopolitische oder technische Störungen, die den Kern des Internets oder eines oder mehrere dieser Unternehmen betreffen können. Die zunehmende Internetnutzung und die sich infolge der Pandemie ändernden Nutzungsmuster haben die Störanfälligkeit der Lieferketten, die von dieser digitalen Infrastruktur abhängen, noch deutlicher gemacht.

---

5 Einschließlich elektronischer Komponenten, Datenanalysen, Cloud-Computing, schnellerer und intelligenterer Netze mit 5G und darüber hinaus, Verschlüsselung, künstlicher Intelligenz (KI) sowie neuer Rechenmodelle und vertrauenswürdiger Datenverarbeitungsparadigmen wie Blockchain, Cloud-to-edge und Quanteninformatik.

6 Siehe Weltwirtschaftsforum, Global Risks Report 2020.

7 Die Pandemie führte laut der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung zu einem Anstieg des Internetverkehrs um 60 %; https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/. Während der Ausgangsbeschränkungen im Rahmen der Coronavirus-Pandemie veröffentlichen das Gremium europäischer Regulierungsstellen für elektronische Kommunikation und die Kommission regelmäßig Berichte über den Stand der Internetkapazitäten. Einem Bericht der ENISA zufolge stieg die Gesamtzahl der DDoS-Angriffe (*Distributed Denial of Service*) im 3. Quartal 2019 um 241 % gegenüber dem 3. Quartal 2018. DDoS-Angriffe nehmen an Intensität zu, wobei der bisher größte Angriff im Februar 2020 stattfand und zu einem Spitzenverkehrsaufkommen von 2,3 Terabits pro Sekunde führte. Beim Ausfall von CenturyLink im August 2020 führte ein Routing-Problem bei dem US-Internetdiensteanbieter zu einem Rückgang des weltweiten Internetverkehrs um 3,5 %; https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service

8 Internet Society, The Global Internet Report: Consolidation in the Internet Economy; https://www.internetsociety.org/blog/2019/02/is-the-internet-shrinking-the-global-internet-report-consolidation-in-the-internet-economy-explores-this-question/

Sicherheitsbedenken sind einer der wichtigsten Faktoren, die von der Nutzung von Online-Diensten abschrecken[9]. Rund zwei Fünftel der Nutzerinnen und Nutzer in der EU hatten bereits Probleme mit der Sicherheit, und drei Fünftel fühlen sich nicht in der Lage, sich vor Cyberkriminalität zu schützen.[10] Ein Drittel hat in den letzten drei Jahren betrügerische E-Mails oder Telefonanrufe erhalten, in denen personenbezogene Daten erfragt wurden, aber 83 % haben noch nie einen Fall von Cyberkriminalität gemeldet. Jedes achte Unternehmen war schon von Cyberangriffen betroffen.[11] Mehr als die Hälfte der PCs von Unternehmen und Verbrauchern, die einmal mit Schadsoftware infiziert waren, sind es innerhalb desselben Jahres erneut.[12] Jedes Jahr gehen Hunderte Millionen Datensätze durch Verletzungen des Datenschutzes verloren; die durchschnittlichen Kosten solcher Verletzungen in einem einzigen Unternehmen stiegen im Jahr 2018 auf über 3,5 Mio. EUR.[13] Die Auswirkungen eines Cyberangriffs können häufig nicht isoliert werden. Vielmehr können sie in der gesamten Wirtschaft und Gesellschaft Kettenreaktionen auslösen, die Millionen von Einzelpersonen betreffen.[14]

Bei fast allen Arten von Straftaten haben die Ermittlungen eine digitale Komponente. Im Jahr 2019 hat sich Berichten zufolge die Zahl der Vorfälle gegenüber dem Vorjahr verdreifacht. Es gibt schätzungsweise 700 Mio. neue Beispiele von Schadsoftware – dem häufigsten Mittel zur Vorbereitung eines Cyberangriffs.[15] Die jährlichen Kosten der Cyberkriminalität für die Weltwirtschaft werden im Jahr 2020 auf 5,5 Billionen EUR geschätzt und liegen damit doppelt so hoch als im Jahr 2015.[16] Dies stellt den größten Transfer wirtschaftlichen Reichtums in der Geschichte dar, der noch weit über dem weltweiten Drogenhandel liegt. Bei einem großen Cybervorfall – dem Ransomware-Angriff mit WannaCry – im Jahr 2017 wurden die Kosten für die Weltwirtschaft auf über 6,5 Mrd. EUR geschätzt.[17]

Digitale Dienste und der Finanzsektor gehören neben dem öffentlichen Sektor und dem verarbeitenden Gewerbe zu den häufigsten Zielen von Cyberangriffen, doch die Bereitschaft und das Bewusstsein für Cyberangriffe bei Unternehmen und Einzelpersonen sind nach wie vor gering[18], und die Arbeitskräfte weisen einen

---

9 https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

10 Index für die digitale Wirtschaft und Gesellschaft 2020; https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020; https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

11 Eurostat-Pressemitteilung „Überwiegende Mehrheit der Unternehmen in der EU ergriff IKT-Sicherheitsmaßnahmen“, 6/2020 – 13. Januar 2020. „Cyberattacks on critical infrastructure have become the new normal across sectors such as energy, healthcare and transportation“; Weltwirtschaftsforum, Global Risks Report 2020.

12 Quelle: Comparitech.

13 Bericht „2020 Cost of a Data Breach“, Ponemon Institute, und auf der Grundlage einer quantitativen Analyse von 524 Verstößen aus letzter Zeit in 17 geografischen Gebieten und 17 Wirtschaftszweigen: https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

14 Bericht der Gemeinsamen Forschungsstelle (JRC), „Cybersecurity, our digital anchor“; https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/cybersecurity-our-digital-anchor

15 Quelle: AV-TEST, https://www.av-test.org/en/statistics/malware/.

16 JRC, „Cybersecurity, our digital anchor“.

17 Quelle: Cyence.

18 Auch in Bezug auf den Cyberdiebstahl von Geschäftsgeheimnissen, insbesondere bei KMU, ist das Bewusstsein der Unternehmen nach wie vor gering. PwC, Study on the scale and impact of industrial espionage and theft of

erheblichen Mangel an Cybersicherheitskompetenzen auf[19]. Im Jahr 2019 gab es fast 450 Cybersicherheitsvorfälle im Zusammenhang mit europäischen kritischen Infrastrukturen in Bereichen wie Finanzen und Energie[20]. Gesundheitsorganisationen und Angehörige der Gesundheits- und Pflegeberufe wurden während der Pandemie besonders hart getroffen. Da Technik und physische Welt untrennbar miteinander verwoben sind, bringen Cyberangriffe das Leben und das Wohlergehen der verletzlichsten Menschen in Gefahr.[21] Mehr als zwei Drittel der Unternehmen, insbesondere KMU, werden als „Neulinge" im Bereich der Cybersicherheit betrachtet, und europäische Unternehmen gelten als weniger gut vorbereitet als Unternehmen in Asien und Amerika.[22] Schätzungsweise 291 000 Stellen für Fachkräfte für Cybersicherheit sind in Europa unbesetzt. Die Einstellung und Schulung von Experten für Cybersicherheit ist ein langwieriger Prozess, der zu größeren Cybersicherheitsrisiken für Organisationen führt.[23]

Der EU mangelt es an einem kollektiven Lagebewusstsein für Cyberbedrohungen. Dies ist darauf zurückzuführen, dass die nationalen Behörden Informationen aus dem Privatsektor, die dazu beitragen könnten, den Stand der Cybersicherheit in der EU einzuschätzen, nicht systematisch sammeln und austauschen. Nur ein Bruchteil der Vorfälle wird von den Mitgliedstaaten gemeldet, und der Informationsaustausch ist weder systematisch noch umfassend[24]; Cyberangriffe sind möglicherweise nur ein Aspekt konzertierter böswilliger Angriffe auf europäische Gesellschaften. Derzeit besteht nur eine begrenzte gegenseitige operative Unterstützung zwischen den Mitgliedstaaten, und es gibt keinen operativen Mechanismus zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU im Falle groß angelegter grenzüberschreitender Cybervorfälle oder -krisen.[25]

Die Verbesserung der Cybersicherheit ist daher von entscheidender Bedeutung, damit die Menschen Vertrauen in die Innovation, Konnektivität und Automatisierung haben, diese nutzen und Vorteile daraus ziehen. Außerdem ist sie wesentlich für die Wahrung der Grundrechte und Grundfreiheiten, einschließlich des Rechts auf Privatsphäre und des Rechts auf Schutz personenbezogener Daten sowie der Meinungs- und Informationsfreiheit. Cybersicherheit ist unerlässlich für die Netzanbindung und das globale und offene Internet, das den Wandel in Wirtschaft und Gesellschaft in den 2020er Jahren unterstützen muss. Sie trägt zu mehr besseren Jobs, flexibleren Arbeitsplätzen, mehr Effizienz und Nachhaltigkeit in Verkehr und Landwirtschaft sowie zu einem leichteren und gerechteren Zugang zu Gesundheitsdiensten bei. Wegen grenzüberschreitender Netze und intelligenter Zähler sowie der Vermeidung einer unnötigen doppelten Datenspeicherung ist

---

trade secrets through cyber: Dissemination report on measures to tackle and prevent cyber-theft of trade secrets, 2018.

19 Siehe Threat Landscape 2020, ENISA. Außerdem: Data Breach Investigations Report 2020, Verizon; https://enterprise.verizon.com/resources/reports/dbir/

20 https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f

21 Mit Ransomware wurden Krankenhäuser und Patientenakten z. B. in Rumänien (Juni 2020), Düsseldorf (September 2020) und Vastaamo (Oktober 2020) angegriffen.

22 PwC, The Global State of Information Security 2018; ESI Thoughtlab, The Cybersecurity Imperative, 2019.

23 EU-Cybersicherheitsagentur, Cybersecurity Skills Development in the EU: The certification of cybersecurity degrees and ENISA's Higher Education Database, Dezember 2019.

24 Die Mitgliedstaaten müssen der Kooperationsgruppe jährlich einen zusammenfassenden Bericht über die gemäß Artikel 10 Absatz 3 der Richtlinie zur Netz- und Informationssicherheit (Richtlinie (EU) 2016/1148) eingegangenen Meldungen vorlegen.

25 Es bestehen Standardarbeitsanweisungen für die gegenseitige Unterstützung der Mitglieder des CSIRTs-Netzwerks.

sie auch für den Übergang zu sauberer Energie im Rahmen des europäischen Grünen Deals[26] von wesentlicher Bedeutung. Schließlich spielt sie eine entscheidende Rolle für die internationale Sicherheit und Stabilität und die Entwicklung der Volkswirtschaften, Demokratien und Gesellschaften weltweit. Behörden, Unternehmen und Einzelpersonen müssen daher digitale Instrumente verantwortungs- und sicherheitsbewusst einsetzen. Cybersicherheitsbewusstsein und -hygiene müssen den digitalen Wandel bei alltäglichen Aktivitäten unterstützen.

Die neue Cybersicherheitsstrategie der EU für die digitale Dekade ist ein Schlüsselelement für die Gestaltung der digitalen Zukunft Europas[27], den Aufbauplan der Kommission für Europa[28], die Strategie für eine Sicherheitsunion 2020–2025[29], die Globale Strategie für die Außen- und Sicherheitspolitik der EU[30] und die Strategische Agenda 2019–2024 des Europäischen Rates[31]. Darin wird dargelegt, wie die EU die Menschen, Unternehmen und Einrichtungen vor Cyberbedrohungen schützen, die internationale Zusammenarbeit voranbringen und bei der Sicherung eines globalen offenen Internets eine Führungsrolle übernehmen will.

II. GLOBAL DENKEN, EUROPÄISCH HANDELN

Mit dieser Strategie soll ein globales und offenes Internet mit starken Schutzvorkehrungen gewährleistet werden, um den Risiken für die Sicherheit, die Grundrechte und die Grundfreiheiten der Menschen in Europa zu begegnen. Ausgehend von den Fortschritten, die mit den vorherigen Strategien erzielt wurden, enthält sie konkrete Vorschläge für den Einsatz der **drei Hauptinstrumente – Regulierung, Investitionen und Politikvorgaben** –, mit denen **drei Handlungsbereiche der EU angegangen werden sollen: 1) Resilienz, technologische Souveränität und Führungsrolle, 2) Aufbau operativer Kapazitäten zur Prävention, Abschreckung und Reaktion und 3) Förderung eines globalen offenen Cyberraums**. Die EU setzt sich dafür ein, diese Strategie durch **Investitionen in den digitalen Wandel in der EU in nie da gewesener Höhe über die nächsten sieben Jahren** zu unterstützen, wodurch die bisherigen Investitionen möglicherweise vervierfacht werden, und zwar als Teil der neuen Technologie- und Industriepolitik und der Erholungsagenda[32].

Mithilfe von Anreizen, Verpflichtungen und Benchmarks muss die Cybersicherheit in all diese digitalen Investitionen einbezogen werden, insbesondere bei Schlüsseltechnologien wie künstliche Intelligenz (KI), Verschlüsselung und Quanteninformatik. Dies kann das Wachstum der europäischen Cybersicherheitsbranche stimulieren und die nötige Sicherheit schaffen, um den schrittweisen Ausstieg aus

---

26 Der europäische Grüne Deal, COM(2019) 640 final.

27 Gestaltung der digitalen Zukunft Europas, COM(2020) 67 final.

28 Die Stunde Europas: Schäden beheben und Perspektiven für die nächste Generation eröffnen, COM(2020) 456 final.

29 EU-Strategie für eine Sicherheitsunion 2020–2025, COM(2020) 605 final.

30 https://eeas.europa.eu/topics/eu-global-strategy_en

31 https://www.consilium.europa.eu/de/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/#

32 Die Investitionen in die gesamte Lieferkette für digitale Technik, die zum digitalen Wandel oder zur Bewältigung der sich daraus ergebenden Herausforderungen beitragen, dürften sich auf mindestens 20 % der 672,5 Mrd. EUR umfassenden Aufbau- und Resilienzfazilität belaufen; dies entspricht 134,5 Mrd. EUR in Form von Finanzhilfen und Darlehen. Die im mehrjährigen Finanzrahmen 2021–2027 vorgesehenen EU-Mittel, nämlich für die Cybersicherheit im Rahmen des Programms „Digitales Europa“ und für die Cybersicherheitsforschung im Rahmen von Horizont Europa (mit besonderem Schwerpunkt auf der Unterstützung von KMU) könnten sich insgesamt auf 2 Mrd. EUR belaufen, zuzüglich Investitionen der Mitgliedstaaten und der Industrie.

Altsystemen zu erleichtern. Der Europäische Verteidigungsfonds wird europäische Cyberabwehrlösungen als Teil der technologischen und industriellen Basis der europäischen Verteidigung unterstützen. Die Cybersicherheit wird in den externen Finanzierungsinstrumenten zur Unterstützung unserer Partner berücksichtigt, insbesondere dem Instrument für Nachbarschaft, Entwicklungszusammenarbeit und internationale Zusammenarbeit. Die Verhinderung des Missbrauchs von Technologien, der Schutz kritischer Infrastrukturen und die Gewährleistung der Integrität der Lieferketten ermöglichen es der EU ferner, die Normen, Regeln und Grundsätze der Vereinten Nationen für verantwortungsvolles staatliches Handeln[33] einzuhalten.

1. RESILIENZ, TECHNOLOGISCHE SOUVERÄNITÄT UND FÜHRUNGSROLLE

Die kritischen Infrastrukturen und die wesentlichen Dienste der EU sind zunehmend voneinander abhängig und digitalisiert. Alle mit dem Internet vernetzten Dinge in der EU, unabhängig davon, ob es sich um automatisierte Fahrzeuge, industrielle Steuerungssysteme oder Haushaltsgeräte handelt. Die gesamten Lieferketten, über die sie bereitgestellt werden, müssen sicher und widerstandsfähig gegen Cybervorfälle sein, und festgestellte Schwachstellen müssen rasch behoben werden können. Nur so hat der private und öffentliche Sektor in der EU die Möglichkeit, aus den sichersten Infrastrukturen und Diensten auszuwählen. Das kommende Jahrzehnt bietet der EU die Chance, bei der Entwicklung sicherer Technologien entlang der gesamten Lieferkette eine Führungsrolle zu übernehmen. Zur Gewährleistung der Resilienz und zur Stärkung der industriellen und technologischen Kapazitäten im Bereich der Cybersicherheit sollten alle erforderlichen Regulierungs-, Investitions- und Politikinstrumente mobilisiert werden. Die eingebaute Cybersicherheit für industrielle Prozesse, Operationen und Geräte kann Risiken mindern, potenziell die Kosten für Unternehmen und die Gesellschaft im weiteren Sinne senken und so die Resilienz erhöhen.

1.1 Resiliente Infrastrukturen und kritische Dienste

Die EU-**Vorschriften über die Sicherheit von Netz- und Informationssystemen (NIS)** stehen im Mittelpunkt des Binnenmarkts für Cybersicherheit. Die Kommission schlägt vor, diese Vorschriften im Rahmen einer überarbeiteten NIS-Richtlinie zu reformieren, um das Niveau der **Cyberabwehrfähigkeit aller einschlägigen öffentlichen und privaten Sektoren, die eine wichtige Funktion für Wirtschaft und Gesellschaft erfüllen, zu erhöhen**.[34] Die Überprüfung ist erforderlich, um Unstimmigkeiten im Binnenmarkt zu verringern, indem der Anwendungsbereich, die Anforderungen an die Sicherheit und die Meldung von Sicherheitsvorfällen, die nationale Beaufsichtigung und Durchsetzung sowie die Kapazitäten der zuständigen Behörden angeglichen werden.

Eine überarbeitete NIS-Richtlinie wird die Grundlage für spezifischere Vorschriften schaffen, die auch für strategisch wichtige Sektoren wie Energie, Verkehr und Gesundheitswesen erforderlich sind. Um einen kohärenten Ansatz zu gewährleisten, wie im Rahmen der Strategie für die Sicherheitsunion 2020–2025 angekündigt, wird die überarbeitete Richtlinie zusammen mit einer Überprüfung der Rechtsvorschriften für die Resilienz kritischer Infrastrukturen[35] vorgeschlagen. Energietechnologien, in die digitale Komponenten

[33] https://undocs.org/A/70/174
[34] [*Verweis auf NIS-Vorschlag einfügen*]
[35] [Verweis auf *Vorschlag* für eine Richtlinie über die Resilienz kritischer Einrichtungen einfügen].

eingebettet sind, und die Sicherheit der damit verbundenen Versorgungsketten sind wichtig für die Kontinuität wesentlicher Dienste und für die strategische Kontrolle kritischer Energieinfrastrukturen. Die Kommission wird daher Maßnahmen vorschlagen, darunter einen „Netzkodex“ mit Vorschriften für die Cybersicherheit bei grenzüberschreitenden Stromflüssen, der bis Ende 2022 angenommen werden sollen. Auch der Finanzsektor muss die Betriebsstabilität digitaler Systeme stärken und dafür sorgen, dass sie – wie von der Kommission vorgeschlagen[36] – allen Arten von IKT-bedingten Störungen und Bedrohungen standhalten können. Im Verkehrsbereich hat die Kommission die EU-Rechtsvorschriften für die Luftsicherheit um Bestimmungen zur Cybersicherheit[37] ergänzt und wird ihre Bemühungen fortsetzen, die Cyberabwehrfähigkeit bei allen Verkehrsträgern zu verbessern. Die Stärkung der Resilienz **demokratischer Prozesse und Institutionen** gegenüber Cyberangriffen ist ein Kernbestandteil des Europäischen Aktionsplans für Demokratie zur Sicherung und Förderung freier Wahlen, des demokratischen Diskurses und der Medienvielfalt.[38] Schließlich wird die Kommission im Hinblick auf die Sicherheit von Infrastrukturen und Diensten im Rahmen des künftigen Weltraumprogramms die Vertiefung der Galileo-Cybersicherheitsstrategie für die nächste Generation globaler Satellitennavigationsdienste und anderer neuer Komponenten des Weltraumprogramms fortsetzen.[39]

1.2 Aufbau eines europäischen Cyberschutzschilds

Mit der Ausweitung der Konnektivität und der zunehmenden Komplexität von Cyberangriffen erfüllen Informationsaustausch- und -analysezentren eine wertvolle Funktion, auch auf sektoraler Ebene, da sie den Informationsaustausch über Cyberbedrohungen zwischen verschiedenen Interessenträgern ermöglichen.[40] Darüber hinaus müssen Netze und Computersysteme ständig überwacht und analysiert werden, um Eindringlinge und Anomalien in Echtzeit zu erkennen. Zahlreiche private Unternehmen, öffentliche Einrichtungen und nationale Behörden haben daher Computer-Notfallteams (CSIRTs) und Sicherheitseinsatzzentren eingerichtet.

Sicherheitseinsatzzentren sind für die Sammlung von Protokollen[41] und die Isolierung verdächtiger Ereignisse in den von ihnen überwachten Kommunikationsnetzen von entscheidender Bedeutung. Dies geschieht durch die Erkennung von Signalen und Mustern und die Gewinnung von Bedrohungswissen aus den großen Datenmengen, die bewertet werden müssen. Die Zentren haben bereits zur Entdeckung böswilliger ausführbarer Dateien und damit zur Eindämmung von Cyberangriffen beigetragen. Die Arbeit in diesen Zentren ist

---

36 Vorschlag für eine Verordnung über die Betriebsstabilität digitaler Systeme im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014 und (EU) Nr. 909/2014, COM(2020) 595 final.

37 Durchführungsverordnung (EU) 2019/1583 der Kommission.

38 Mitteilung „Europäischer Aktionsplan für Demokratie“, COM(2020) 790. Im Rahmen des Plans werden die Wahlnetze der Mitgliedstaaten über das Europäische Kooperationsnetz für Wahlen die Entsendung gemeinsamer Expertenteams zur Abwehr von Bedrohungen – einschließlich Cyberbedrohungen – für Wahlprozesse unterstützen; https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en

39 Dazu gehören die neuen Initiativen für staatliche Satellitenkommunikation (GOVSATCOM) und für Weltraummüll (Beobachtung und Verfolgung von Objekten im Weltraum, SST).

40 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

41 Damit Strafverfolgung und Justiz sie als Beweismittel verwenden können.

sehr anspruchsvoll und hektisch, weshalb KI und insbesondere maschinelles Lernen den Praktikern wertvolle Unterstützung bieten können.[42]

Die Kommission schlägt vor, ein **Netz von Sicherheitseinsatzzentren in der gesamten EU**[43] aufzubauen und die Verbesserung bestehender und die Einrichtung neuer Zentren zu unterstützen. Darüber hinaus wird sie die Aus- und Weiterbildung der Beschäftigten in diesen Zentren unterstützen. Auf der Grundlage einer Bedarfsanalyse, die mit den einschlägigen Interessenträgern durchgeführt und von der EU-Cybersicherheitsagentur (ENISA) unterstützt wird, könnte sie mehr als 300 Mio. EUR zur Unterstützung der öffentlich-privaten und grenzüberschreitenden Zusammenarbeit bei der Schaffung nationaler und sektoraler Netze bereitstellen, an denen sich auch KMU beteiligen, wobei geeignete Bestimmungen für die Governance, den Datenaustausch und die Sicherheit zugrunde gelegt werden.

Den Mitgliedstaaten wird empfohlen, mit in dieses Projekt zu investieren. Die Zentren wären dann in der Lage, die entdeckten Signale effizienter zu übermitteln und in Beziehung zu setzen sowie hochwertige Erkenntnisse über Bedrohungen zu gewinnen, die an die Informationsaustausch- und -analysezentren und die nationalen Behörden weitergegeben werden, sodass eine umfassendere Lageerfassung möglich wird. Ziel wäre es, Schritt für Schritt so viele Zentren wie möglich in der gesamten EU miteinander zu vernetzen, um gemeinsames Wissen aufzubauen und bewährte Verfahren auszutauschen. Diese Zentren werden unterstützt, um die Erkennungs-, Analyse- und Reaktionsgeschwindigkeit bei Vorfällen mithilfe modernster KI-Fähigkeiten und maschinellen Lernens zu verbessern. Ergänzt werden sie durch die in der EU vom Gemeinsamen Unternehmen für europäisches Hochleistungsrechnen[44] entwickelte Hochleistungsrecheninfrastruktur.

Durch eine nachhaltige Zusammenarbeit und Kooperation wird dieses Netz die Behörden und alle Interessenträger, einschließlich der gemeinsamen Cyberstelle, rechtzeitig vor Cybersicherheitsvorfällen warnen können (siehe Abschnitt 2.1). **Es wird als echter Cybersicherheitsschutzschild für die EU dienen** und ein solides Geflecht aus Wachttürmen bieten, damit potenzielle Bedrohungen erkannt werden können, bevor sie schwere Schäden verursachen.

1.3 Eine extrem sichere Kommunikationsinfrastruktur

Die staatliche Satellitenkommunikation der Europäischen Union[45] ist eine Komponente des Weltraumprogramms und wird sichere und kosteneffiziente weltraumgestützte Kommunikationskapazitäten für die sicherheitskritischen Missionen und Operationen bereitstellen, die von der EU und ihren Mitgliedstaaten, einschließlich nationaler Sicherheitsakteure und der Organe und Einrichtungen der EU, verwaltet werden.

---

42 Quelle: Umfrage des Ponemon Institute Research, „Improving the Effectiveness of the SOC“, 2019; Studien zur Nutzung von KI in Sicherheitseinsatzzentren finden sich beispielsweise unter: Khraisat, A., Gondal, I., Vamplew, P. *et al.* Survey of intrusion detection systems: techniques, datasets and challenges, *Cybersecur* 2**,** 20 (2019).

43 Detailliertere Regelungen für die Governance, die Arbeitsweise und die Finanzierung dieser Zentren sowie die Art und Weise, wie sie bestehende Strukturen wie digitale Innovationszentren ergänzen sollen, werden entwickelt.

44 https://ec.europa.eu/digital-single-market/en/eurohpc-joint-undertaking

45 GOVSATCOM ist eine Komponente des Weltraumprogramms der Union.

Die Mitgliedstaaten haben zugesagt, gemeinsam mit der Kommission auf den Aufbau einer sicheren Quantenkommunikationsinfrastruktur (QCI) für Europa hinzuarbeiten[46]. Diese QCI wird den Behörden eine völlig neue, mit europäischer Technik geschaffene Möglichkeit eröffnen, um vertrauliche Informationen mit extrem sicherer Verschlüsselung zu übermitteln und sich so gegen Cyberangriffe zu schützen. Sie wird zwei Hauptkomponenten haben: bestehende terrestrische Glasfasernetze, die strategische Standorte auf nationaler und grenzüberschreitender Ebene miteinander verbinden, und eingebundene Weltraumsatelliten, die die gesamte EU, einschließlich ihrer überseeischen Gebiete, abdecken[47]. Diese Initiative zur Entwicklung und Einführung neuer und sichererer Verschlüsselungsformen und zur Erkundung neuer Wege zum Schutz kritischer Kommunikationsanlagen und Datenbestände kann dazu beitragen, sensible Informationen und somit auch kritische Infrastrukturen zu sichern.

In dieser Hinsicht und darüber hinaus wird die Kommission die mögliche Einführung eines sicheren multiorbitalen Konnektivitätssystems prüfen. Aufbauend auf GOVSATCOM und QCI würde dieses System Spitzentechnologien (Quanteninformatik, 5G, KI, Edge-Computing) miteinander integrieren, die den restriktivsten Cybersicherheitsrahmen einhalten, um für kritische staatliche Tätigkeiten konzeptionsbedingt sichere Dienste wie z. B. zuverlässige, sichere und kostengünstige Netzanbindungen und verschlüsselte Kommunikation zu ermöglichen.

1.4 Absicherung der Breitband-Mobilfunknetze der nächsten Generation

Die EU-Bürgerinnen und -Bürger und EU-Unternehmen, die fortgeschrittene und innovative Anwendungen nutzen, die durch **5G-Technik und künftige Netzgenerationen** ermöglicht werden, sollten sich auf höchste Sicherheitsstandards verlassen können. Die Mitgliedstaaten haben gemeinsam mit der Kommission und mit Unterstützung der ENISA im Januar 2020 mit dem 5G-Instrumentarium[48] der EU einen umfassenden und objektiven risikobasierten Ansatz für die 5G-Cybersicherheit eingeführt, der auf einer Bewertung möglicher Risikominderungspläne und der Ermittlung der wirksamsten Maßnahmen beruht. Darüber hinaus konsolidiert die EU ihre Fähigkeiten im 5G-Bereich und darüber hinaus, um Abhängigkeiten zu vermeiden und eine tragfähige und vielfältige Lieferkette zu fördern.

---

[46] Die Erklärung zur europäischen Quantenkommunikationsinfrastruktur (EuroQCI) ist von den meisten Mitgliedstaaten unterzeichnet worden. Die Entwicklung und der Aufbau der Infrastruktur sollen – vorbehaltlich eines geeigneten Governance-Rahmens – im Zeitraum 2021–2027 mit Mitteln des Programms Horizont Europa, des Programms Digitales Europa und der Europäischen Weltraumorganisation erfolgen, https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network

[47] Die Entwicklung einer Weltraumkomponente ist notwendig, um Punkt-zu-Punkt-Fernverbindungen (> 1000 km) zu realisieren, die mit bodengestützten Infrastrukturen nicht möglich sind. Dank der Ausnutzung bestimmter Eigenschaften der Quantenmechanik wird die QCI alle Beteiligten zunächst in die Lage versetzen, zufällige geheime Schlüssel zur Verschlüsselung und Entschlüsselung von Nachrichten auf sichere Weise auszutauschen. Dies umfasst auch den Aufbau einer Test- und Konformitätsinfrastruktur zur Bewertung der Konformität europäischer Quantenkommunikationsgeräte und -systeme mit der QCI sowie ihre Zertifizierung und Validierung vor ihrer Integration in die QCI. Sie wird so konzipiert sein, dass zusätzliche Anwendungen einbezogen werden können, sobald sie den erforderlichen technologischen Reifegrad erreichen. Das derzeitige Pilotprojekt OpenQKD (https://openqkd.eu/) ist ein Vorläufer dieser Test- und Konformitätsinfrastruktur.

[48] Mitteilung „Sichere 5G-Einführung in der EU – Umsetzung des EU-Instrumentariums“, COM(2020) 50.

Im Dezember 2020 veröffentlichte die Kommission einen Bericht über die Auswirkungen der Empfehlung vom 26. März 2019 zur Cybersicherheit der 5G-Netze[49]. Demnach wurden seit der Aufstellung des EU-Instrumentariums erhebliche Fortschritte erzielt. Die meisten Mitgliedstaaten sind nun auf dem richtigen Weg, um einen beträchtlichen Teil des Instrumentariums in naher Zukunft umzusetzen, wenn auch mit gewissen Abweichungen und verbleibenden Lücken, auf die in dem im Juli 2020 veröffentlichten Fortschrittsbericht[50] bereits hingewiesen wurde.

Im Oktober 2020 ersuchte der Europäische Rat die EU und ihre Mitgliedstaaten, das Instrumentarium für die 5G-Cybersicherheit in vollem Umfang zu nutzen und auf der Grundlage gemeinsamer objektiver Kriterien bei wichtigen Anlagen und Einrichtungen, die in den von der EU koordinierten Risikobewertungen als kritisch und sensibel eingestuft werden, die einschlägigen Beschränkungen für Hochrisikolieferanten anzuwenden[51].

Mit Blick auf die Zukunft sollten die EU und ihre Mitgliedstaaten sicherstellen, dass die schon ermittelten Risiken in angemessener und koordinierter Weise gemindert worden sind, insbesondere im Hinblick auf das Ziel, die Gefahren durch Hochrisikolieferanten so gering wie möglich zu halten und Abhängigkeiten von diesen Anbietern auf nationaler und Unionsebene zu vermeiden, und dass auch alle wichtigen neuen Entwicklungen oder Risiken berücksichtigt werden. Die Mitgliedstaaten werden aufgerufen, bei ihren Investitionen in digitale Kapazitäten und Konnektivität das Instrumentarium in vollem Umfang anzuwenden.

Auf der Grundlage des Berichts über die Auswirkungen der Empfehlung von 2019 ermuntert die Kommission die Mitgliedstaaten, die Arbeiten zur Umsetzung der wichtigsten Maßnahmen des Instrumentariums zu beschleunigen, damit sie bis zum zweiten Quartal 2021 abgeschlossen werden. Außerdem ruft sie die Mitgliedstaaten auf, die erzielten Fortschritte weiterhin gemeinsam zu beobachten und auf eine weitere Angleichung der Ansätze hinzuwirken. Zur Unterstützung dieses Prozesses werden auf EU-Ebene drei Hauptziele verfolgt: Gewährleistung der fortschreitenden EU-weiten Konvergenz der Risikominderungsansätze, Unterstützung des kontinuierlichen Wissensaustauschs und Kapazitätsaufbaus und Förderung der Resilienz der Lieferketten und anderer strategischer Sicherheitsziele der EU. Konkrete Maßnahmen in Bezug auf diese Hauptziele werden in der diesbezüglichen Anlage dieser Mitteilung aufgeführt.

Die Kommission wird weiterhin eng mit den Mitgliedstaaten zusammenarbeiten, um diese Ziele und Maßnahmen mit Unterstützung der ENISA zu verwirklichen (siehe Anhang).

Das 5G-Instrumentarium der EU hat auch in Drittländern Interesse gefunden, die derzeit ihre eigenen Konzepte zur Sicherung ihrer Kommunikationsnetze entwickeln. Die Dienststellen der Kommission sind gemeinsam mit dem Europäischen Auswärtigen Dienst und dem Netz der EU-Delegationen bereit, Behörden in der ganzen Welt auf Anfrage zusätzliche Informationen über den umfassenden, objektiven und risikogestützten EU-Ansatz zu geben.

[49] Bericht der Kommission über die Auswirkungen der Empfehlung der Kommission vom 26. März 2019 zur Cybersicherheit der 5G-Netze, 15. Dezember 2020.

[50] Bericht der NIS-Kooperationsgruppe über die Umsetzung des Instrumentariums, 24. Juli 2020.

[51] EUCO 13/20, Sondertagung des Europäischen Rates (1. und 2. Oktober 2020) – Schlussfolgerungen.

1.5 Ein Internet der sicheren Dinge

Jedes vernetzte Ding hat Schwachstellen, die ausgenutzt werden können und so potenziell weitverzweigte Auswirkungen nach sich ziehen könnten. Die Binnenmarktvorschriften enthalten bereits gewisse Schutzvorkehrungen gegen unsichere Produkte und Dienste. Die Kommission arbeitet zudem an **transparenten Sicherheitslösungen und Zertifizierungen im Rahmen des Rechtsakts zur Cybersicherheit** sowie an der Schaffung von Anreizen für Produkte und Dienste, die sicher sind, ohne an Leistung einzubüßen[52]. Sie wird im ersten Quartal 2021 ihr erstes fortlaufendes Arbeitsprogramm der Union annehmen (das mindestens alle drei Jahre aktualisiert werden soll), damit Unternehmen, nationale Behörden und Normungsgremien sich im Voraus auf künftige europäische Systeme für die Cybersicherheitszertifizierung[53] einstellen können. Mit der fortschreitenden Verbreitung des Internets der Dinge werden durchsetzbare Vorschriften immer wichtiger, um sowohl die allgemeine Resilienz als auch die Cybersicherheit zu stärken.

Die Kommission wird ein umfassendes Herangehen in Erwägung ziehen, möglicherweise auch **neue horizontale Vorschriften zur Verbesserung der Cybersicherheit aller vernetzten Produkte und zugehörigen Dienste im Binnenmarkt**[54]. Solche Vorschriften könnten eine **neue Sorgfaltspflicht für Hersteller vernetzter Geräte** umfassen, damit Software-Schwachstellen beseitigt, Software laufend gepflegt und Sicherheitsaktualisierungen durchgeführt werden, aber auch damit personenbezogene und sonstige sensible Daten am Ende der Lebensdauer solcher Geräte sicher gelöscht werden. Die Vorschriften würden das im Aktionsplan für die Kreislaufwirtschaft vorgesehene Recht auf Reparatur veralteter Software untermauern und laufende Maßnahmen ergänzen, die auf bestimmte Produktarten abzielen, z. B. die anstehenden Vorschläge für verbindliche Anforderungen an die Marktzulassung bestimmter Drahtlosprodukte (durch Erlass eines delegierten Rechtsaktes auf der Grundlage der Richtlinie über Funkanlagen[55]), und die der Einführung von Cybersicherheitsvorschriften für Kraftfahrzeuge dienen, damit diese ab Juli 2022 für alle neuen Fahrzeugtypen gelten[56]. Darüber hinaus würden sie auf der vorgeschlagenen Überarbeitung der allgemeinen Produktsicherheitsvorschriften aufbauen, die sich nicht direkt mit Aspekten der Cybersicherheit befassen[57].

---

52 Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit). Der Rechtsakt zur Cybersicherheit fördert die IKT-Zertifizierung auf EU-Ebene durch die Schaffung eines europäischen Rahmens für die Cybersicherheitszertifizierung, der eine freiwillige Aufstellung europäischer Programme für die Cybersicherheitszertifizierung erlaubt, mit dem Ziel, für IKT-Produkte, -Dienste und -Prozesse in der Union ein angemessenes Maß an Cybersicherheit zu gewährleisten und eine Fragmentierung des Binnenmarkts bei Zertifizierungsprogrammen in der Union zu verhindern. Parallel dazu sind Einstufungsunternehmen im Bereich der Cybersicherheit eher außerhalb der EU ansässig, bieten nur eine geringe Transparenz und werden kaum beaufsichtigt; https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings

53 Erforderlich nach Artikel 47 Absatz 5 des Rechtsakts zur Cybersicherheit.

54 In den Schlussfolgerungen des Rates werden horizontale Maßnahmen zur Cybersicherheit vernetzter Geräte gefordert, 13629/20, 2. Dezember 2020.

55 Richtlinie 2014/53/EU.

56 Nach den im Juni 2020 beschlossenen Vorgaben der Vereinten Nationen, http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf.

57 Überprüfung der derzeit geltenden allgemeinen Produktsicherheitsvorschriften (Richtlinie 2001/95/EG); weitere Vorschläge zur Anpassung der Haftungsvorschriften für Hersteller im digitalen Bereich sind innerhalb des EU-Rechtsrahmens für die Produkthaftung geplant.

1.6 Eine höhere globale Internetsicherheit

Die Funktionsfähigkeit und Integrität des Internets wird weltweit durch eine Reihe von Kernprotokollen und unterstützenden Infrastrukturen gewährleistet[58]. Dazu gehört das Domänennamensystem (DNS) mit seinem hierarchischen und delegierten Zonensystem, beginnend an der Hierarchiespitze mit der Root-Zone und den dreizehn DNS-Root-Servern[59], von denen das World Wide Web abhängt. Die Kommission beabsichtigt die Ausarbeitung **eines durch EU-Mittel unterstützten Notfallplans für die Bewältigung von Extremszenarien, die die Integrität und Verfügbarkeit des globalen DNS-Root-Systems beeinträchtigen**. Sie wird mit der ENISA, den Mitgliedstaaten, den beiden DNS-Root-Servern[60] in der EU sowie der Multi-Stakeholder-Gemeinschaft zusammenarbeiten, um zu bewerten, welche Rolle diesen Serverbetreibern bei der Gewährleistung eines unter allen Umständen weltweit funktionierenden Zugangs zum Internet zukommt.

Für den Zugriff auf eine Ressource, die sich unter einem bestimmten Domänennamen im Internet befindet, muss seine Anfrage (in der Regel ein *Uniform Resource Locator* oder eine URL-Adresse) in eine IP-Adresse übersetzt oder „aufgelöst“ werden, was unter Bezugnahme auf die DNS-Namenserver geschieht. Die Menschen und Organisationen in der EU sind jedoch zunehmend auf einige wenige öffentliche DNS-Auflösungsdienste angewiesen, die von Unternehmen betrieben werden, die nicht in der EU ansässig sind. Eine solche Konsolidierung der DNS-Adressauflösung in den Händen weniger Unternehmen[61] macht den Auflösungsprozess selbst anfällig für Störungen, wenn z. B. einer der großen Betreiber von einer schweren Störung betroffen ist. Außerdem erschwert sie den EU-Behörden das Vorgehen gegen mögliche böswillige Cyberangriffe und die Bewältigung großer geopolitischer und technischer Störfälle[62].

Um Sicherheitsprobleme im Zusammenhang mit der Marktkonzentration zu verringern, wird die Kommission die einschlägigen Beteiligten, darunter EU-Unternehmen, Internetdiensteanbieter und Browseranbieter, dazu aufrufen, eine Strategie zur Diversifizierung der DNS-Adressauflösung zu verfolgen. Außerdem hat die Kommission die Absicht, den Aufbau eines öffentlichen **europäischen DNS-Auflösungsdienstes** zu unterstützen, um so einen Betrag zu einer sicheren Internetkonnektivität zu leisten. Diese Initiative hat den Namen „DNS4EU“ und wird einen alternativen europäischen Dienst für den Zugang zum globalen Internet bieten. DNS4EU wird transparent sein, die neuesten

---

58 „Der öffentliche Kern des offenen Internets, d. h. seine wichtigsten Protokolle und Infrastrukturen, die ein globales öffentliches Gut sind, stellt die wesentlichen Funktionen des Internets als Ganzes bereit und bildet die Grundlage für dessen normalen Betrieb. Die ENISA sollte die Sicherheit und Stabilität dieses öffentlichen Kerns des offenen Internets unterstützen, unter anderem – aber nicht beschränkt auf – die wichtigsten Protokolle (insbesondere DNS, BGP und IPv6), den Betrieb des „Domain Name System“ (DNS) (wie den Betrieb aller Domänen der obersten Ebene) und den Betrieb der Root-Zone.“, Erwägungsgrund 23 des Rechtsakts zur Cybersicherheit.

59 https://www.iana.org/domains/root/servers

60 Die von Netnod in Schweden betriebenen i.root-Server, und die von RIPE NCC in den Niederlanden betriebenen k.root-Server.

61 *Consolidation in the DNS resolver market – how much, how fast how dangerous?* (Konsolidierung auf dem Markt der DNS-Auflösung – wie viel, wie schnell, wie gefährlich?) (), *Evidence of decreasing Internet entropy – the lack of redundancy in DNS resolution by major websites and services* (Anzeichen für eine abnehmende Entropie des Internet – Redundanzmangel bei der DNS-Auflösung durch wichtige Websites und Dienste) ().

62 Es gibt auch Belege dafür, dass DNS-Daten für Profiling-Zwecke verwendet werden können, was Auswirkungen auf den Schutz der Privatsphäre und der Datenschutzrechte hat.

Sicherheits- und Datenschutznormen einhalten, den Grundsätzen des konzeptionsbedingten Datenschutzes und der datenschutzfreundlichen Voreinstellungen entsprechen und Teil der Europäischen Industrieallianz für Daten und Cloud[63] sein.

Darüber hinaus wird die Kommission in Abstimmung mit den Mitgliedstaaten und der Branche **die Verbreitung wichtiger Internetstandards, einschließlich IPv6[64], und etablierter Internetsicherheitsstandards und bewährter Verfahren für die DNS-, Routing- und E-Mail-Sicherheit beschleunigen[65]**. In Betracht kommen aber auch regulatorische Maßnahmen – zur Marktsteuerung – wie eine europäische Regelung zur schrittweisen IPv4-Abschaffung, falls hier keine ausreichenden Fortschritte erzielt werden. Die EU sollte (wie schon im Rahmen der EU-Afrika-Strategie[66]) die Umsetzung dieser Standards auch in Partnerländern fördern, um die Entwicklung des globalen und offenen Internets zu unterstützen und geschlossenen und kontrollierten Internetmodellen entgegenzutreten. Schließlich wird die Kommission prüfen, ob ein Mechanismus für eine systematischere Beobachtung und Erhebung aggregierter Daten über den Internetverkehr sowie für die Beratung in Bezug auf mögliche Störungen benötigt wird[67].

1.7 Eine verstärkte Präsenz in der technologischen Lieferkette

Mit ihrer geplanten finanziellen Unterstützung für den digitalen Wandel unter Wahrung der Cybersicherheit, die im mehrjährigen Finanzrahmen 2021–2027 vorgesehen ist, hat die EU die einzigartige Gelegenheit, ihre Ressourcen zu bündeln, um ihre Industriestrategie[68] und ihre Führungsrolle bei digitalen Technologien und Cybersicherheit entlang der gesamten digitalen Lieferkette (einschließlich Daten und Cloud, Prozessortechnik der nächsten Generation, extrem sichere Konnektivität und 6G-Netze) im Einklang mit ihren Werten und Prioritäten zu fördern. Das Eingreifen des öffentlichen Sektors sollte sich auf die Instrumente stützen, die vom EU-Rechtsrahmen für das öffentliche Auftragswesen und von wichtigen Vorhaben von gemeinsamem europäischem Interesse bereitgestellt werden. Darüber hinaus können private Investitionen mithilfe öffentlich-privater Partnerschaften (auch ausgehend von den Erfahrungen mit der vertraglichen öffentlich-privaten Partnerschaft für Cybersicherheit und deren Umsetzung durch die Europäische Cybersicherheitsorganisation), aber auch mit Risikokapital zur Unterstützung von KMU oder Industrieallianzen und Strategien zum Aufbau von technologischen Fähigkeiten mobilisiert werden.

Einen besonderen Schwerpunkt werden dabei das Instrument für technische Unterstützung[69] und der optimale Einsatz der neuesten Cybersicherheitswerkzeuge durch KMU bilden – insbesondere jene, die nicht in den Anwendungsbereich der überarbeiteten NIS-Richtlinie

---

63 Gemeinsame Erklärung: „Aufbau der Cloud der nächsten Generation für Unternehmen und den öffentlichen Sektor in der EU“, https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe.

64 Die IPv6-Einführung ist infolge der erheblichen Angebotsverknappung und des Kostenanstiegs bei IPv4-Adressen inzwischen weiter vorangekommen. Allerdings verläuft die IPv6-Einführung in der EU uneinheitlich.

65 Zu diesen Standards zählen DNSSEC, HTTPS, DNS über HTTPS (DoH), DNS über TLS (DoT), SPF, DKIM, DMARC, STARTTLS und DANE sowie Normen und bewährte Verfahren für das Routing, z. B. die Routing-Sicherheitsnormen MANRS (*Mutually Agreed Norms for Routing Security*).

66 Gemeinsame Mitteilung „Auf dem Weg zu einer umfassenden Strategie mit Afrika“, 9.3.2020, JOIN(2020) 4 final.

67 Eine solche „Internet-Beobachtungsstelle“ könnte in den Tätigkeitsbereich des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung fallen; Vorschlag für eine Verordnung zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren, COM(2018) 630 final.

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

69 https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=COM:2020:0409:FIN

fallen. Dazu gehören unter anderem auch besondere Tätigkeiten der digitalen Innovationszentren im Rahmen des Programms „Digitales Europa“. Ziel ist es, ein Investitionsvolumen seitens der Mitgliedstaaten zu erreichen, das mit den Investitionen vergleichbar ist, die von der Industrie im Zuge einer Partnerschaft getätigt werden, die im Rahmen des vorgeschlagenen des **Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren (CCCN)** gemeinsam mit den Mitgliedstaaten verwaltet wird. Das CCCN sollte mit Zuarbeiten aus Industrie und Wissenschaft eine Schlüsselrolle beim Aufbau der technologischen Souveränität der EU im Bereich der Cybersicherheit, beim Aufbau von Kapazitäten zur Sicherung sensibler Infrastrukturen wie 5G und bei der Verringerung der bei den wichtigsten Technologien bestehenden Abhängigkeit von anderen Teilen der Welt übernehmen.

Die Kommission hat die Absicht, gegebenenfalls mithilfe des CCCN, die Entwicklung eines besonderen Master-Programms für Cybersicherheit zu unterstützen und an der Ausarbeitung eines gemeinsamen europäischen Fahrplans für Forschung und Innovation im Bereich der Cybersicherheit in der Zeit nach 2020 mitzuwirken. Investitionen im Rahmen des CCCN würden auch auf der von den Netzen der Exzellenzzentren für Cybersicherheit durchgeführten Forschungs- und Entwicklungszusammenarbeit aufbauen, da hier die besten europäischen Forschungsteams mit der Wirtschaft zusammentreffen, um – im Einklang mit dem Fahrplan der Europäischen Cybersicherheitsorganisation[70] – gemeinsame Forschungspläne aufzustellen und umzusetzen. Die Kommission wird sich weiterhin auf die Forschungsarbeiten der ENISA und von Europol stützen und im Rahmen des Programms Horizont Europa einzelne Internet-Innovatoren unterstützen, die datenschutzfreundliche und sichere Kommunikationstechnik auf der Grundlage von Open-Source-Software und -Hardware entwickeln, wie gegenwärtig im Rahmen der Forschungsinitiative zum Internet der nächsten Generation.

1.8 Qualifizierte Cyberfachkräfte in der EU

Ein wichtiger Teil des allgemeinen Schutzes vor Cyberbedrohungen besteht darin, dass die EU ihre Fachkräfte ausbildet und schult, die besten Talente auf dem Gebiet der Cybersicherheit fördert, anzieht und bindet und in eine Forschung und Innovation von Weltrang investiert. In diesem Bereich besteht ein großes Potenzial. Gerade die Entwicklung, Anziehung und Bindung vielfältigerer Talente bedarf hier der besonderen Aufmerksamkeit. Der überarbeitete Aktionsplan für digitale Bildung[71] wird dazu beitragen, Fragen der Cybersicherheit stärker ins Bewusstsein der Menschen, vor allem der Kinder und Jugendlichen, wie auch der Organisationen, allen voran der KMU, zu rücken. Außerdem dient er der Förderung von Frauen in der Ausbildung in den Bereichen Mathematik, Informatik, Naturwissenschaften und Technik (MINT-Fächer), der beruflichen Weiterbildung im IKT-Bereich und der Umschulung auf digitale Kompetenzen. Überdies wird die Kommission gemeinsam mit dem bei Europol angesiedelten Amt der EU für geistiges Eigentum, der ENISA, den Mitgliedstaaten und dem Privatsektor Aufklärungsinstrumente schaffen und Leitlinien entwickeln, um die EU-Unternehmen **widerstandfähiger gegen Cyberdiebstahl geistigen Eigentums** zu machen[72].

Die Cybersicherheits- und Cyberabwehrfähigkeiten auf EU-Ebene sollten ferner durch Bildung – auch berufliche Aus- und Weiterbildung, Sensibilisierung und Übungen – weiter

[70] https://ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies
[71] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_de
[72] https://ec.europa.eu/commission/presscorner/detail/de/IP_20_2187

verbessert werden. Zu diesem Zweck sollten alle einschlägigen EU-Akteure wie die ENISA, die Europäische Verteidigungsagentur (EDA) und das Europäische Sicherheits- und Verteidigungskolleg (ESVK)[73] Synergien zwischen ihren jeweiligen Tätigkeiten anstreben.

Strategische Initiativen

Die EU sollte für Folgendes sorgen:

- Verabschiedung der überarbeiteten NIS-Richtlinie;
- Regulierungsmaßnahmen für ein Internet der sicheren Dinge;
- öffentliche und private Investitionen von bis zu 4,5 Mrd. EUR im Zeitraum 2021–2027 mithilfe der CCCN-Investitionen in die Cybersicherheit (insbesondere im Rahmen der Programme Digitales Europa und Horizont Europa und der Aufbau- und Resilienzfazilität);
- Aufbau eines EU-Netzes KI-gestützter Sicherheitseinsatzzentren und einer extrem sicheren Kommunikationsinfrastruktur, die Quantentechnik nutzt;
- breite Einführung von Cybersicherheitstechnik durch eine gezielte Unterstützung von KMU im Rahmen der digitalen Innovationszentren;
- Entwicklung eines DNS-Auflösungsdienstes als sichere und offene Alternative für den Internetzugang der Bürger, Unternehmen und öffentlichen Verwaltungen in der EU;
- Abschluss der Umsetzung des 5G-Instrumentariums bis zum zweiten Quartal 2021 (siehe Anhang).

2. AUFBAU OPERATIVER KAPAZITÄTEN ZUR PRÄVENTION, ABSCHRECKUNG UND REAKTION

Cybervorfälle, seien es Unfälle oder vorsätzliche Handlungen von Kriminellen, staatlichen und anderen nichtstaatlichen Akteuren, können enorme Schäden verursachen. Ihr Maßstab und ihre Komplexität, mit denen – häufig unter Nutzung von Diensten, Hardware und Software Dritter – das Endziel angegriffen wird, machen es für die EU schwierig, ihr kollektives Bedrohungsumfeld zu beherrschen, wenn es keinen systematischen und umfassenden Informationsaustausch und keine Zusammenarbeit mit dem Ziel einer gemeinsamen Reaktion gibt. Die EU ist bestrebt, den Mitgliedstaaten **durch die vollständige Umsetzung der Regulierungsinstrumente, die Mobilisierung und die Zusammenarbeit** dabei zu helfen, ihre Bürgerinnen und Bürger sowie ihre wirtschaftlichen Interessen und ihre nationalen Sicherheitsinteressen unter uneingeschränkter Achtung der Grundrechte und Grundfreiheiten und der Rechtsstaatlichkeit zu verteidigen. Die Vorbeugung, Abschreckung und Reaktion im Hinblick auf Cyberbedrohungen ist Aufgabe mehrerer Gemeinschaften bzw. Kreise, zu denen verschiedene Netze, die Organe, Einrichtungen und Stellen der EU sowie Behörden der Mitgliedstaaten gehören und die sich dazu ihrer jeweiligen Instrumente und Initiativen[74] bedienen. Zu diesen Kreisen zählen: i) NIS-Behörden wie CSIRTs und

[73] Über die Plattform für Aus- und Weiterbildung, Evaluierung und Übung im Cyberbereich (ETEE).

[74] Beispielsweise die Unterstützung der operativen Zusammenarbeit und des Krisenmanagements durch die Agentur der Europäischen Union für Cybersicherheit (ENISA), das CSIRTs-Netzwerk, das *Cyber Crises Liaison Organisation Network* (Netz der Verbindungsorganisationen für Cyberkrisen oder CyCLONe-Netz –

Katastrophenschutzkräfte; ii) Strafverfolgungs- und Justizbehörden; iii) Cyberdiplomatie; iv) Cyberabwehr.

2.1 Eine gemeinsame Cyberstelle

Eine gemeinsame Cyberstelle würde als virtuelle und physische Plattform für die Zusammenarbeit der verschiedenen Cybersicherheitskreise in der EU dienen, wobei der Schwerpunkt auf der operativen und technischen Koordinierung bei schwerwiegenden grenzüberschreitenden Cybervorfällen und -bedrohungen liegen würde.

Die gemeinsame Cyberstelle wäre ein wichtiger Schritt hin zur Vervollständigung des **europäischen Rahmens für das Krisenmanagement im Bereich der Cybersicherheit**. Wie in den politischen Leitlinien der Kommissionspräsidentin[75] umrissen, sollte die Cyberstelle den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU dabei helfen, die vorhandenen Strukturen, Ressourcen und Fähigkeiten in vollem Umfang zu nutzen, und einen **Need-to-share-Ansatz** fördern. Mit der Cyberstelle könnten die bisherigen Fortschritte bei der Umsetzung der Empfehlung von 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (Blueprint)[76] konsolidiert werden. Außerdem könnte die Zusammenarbeit im Bereich der Blueprint-Architektur weiter ausgebaut und der Fortschritt genutzt werden, der insbesondere in der NIS-Kooperationsgruppe und im CyCLONe-Netz erzielt wurde.

Damit könnten **zwei Hauptlücken** geschlossen werden, aufgrund deren derzeit eine erhöhte Anfälligkeit besteht und sich Ineffizienzen bei der Reaktion auf grenzüberschreitende Vorfälle und Bedrohungen, die die Union betreffen, ergeben. Erstens verfügen die **Kreise**, die sich mit zivilen Cyberfragen und Cyberfragen in den Bereichen Diplomatie, Strafverfolgung und Verteidigung befassen, noch nicht über einen gemeinsamen Raum, der eine strukturierte Zusammenarbeit fördern und die operative und technische Zusammenarbeit erleichtern würde. Zweitens können die einschlägigen Akteure im Bereich der Cybersicherheit das **Potenzial** der operativen Zusammenarbeit und der gegenseitigen Unterstützung innerhalb der bestehenden Netze und Kreise noch nicht voll ausschöpfen. Ein Problem ist das Fehlen einer Plattform, die die operative Zusammenarbeit mit dem privaten Sektor ermöglichen würde. Die Cyberstelle sollte für eine bessere und schnellere Koordinierung sorgen und gewährleisten, dass die EU für massive Cybervorfälle und -krisen gewappnet ist und auf diese reagieren kann.

Die gemeinsame Cyberstelle wäre keine zusätzliche eigenständige Einrichtung und würde auch die Zuständigkeiten und Befugnisse der nationalen Cybersicherheitsbehörden und der EU-Beteiligten nicht berühren. Vielmehr würde die Cyberstelle als Ort dienen, an dem die Beteiligten einander helfen und Fachwissen austauschen können, insbesondere wenn

---

das nach dem Vorschlag für die überarbeitete NIS-Richtlinie zum EU-CyCLONe-Netz werden soll), die NIS-Kooperationsgruppe, „rescEU“, das Europäische Zentrum zur Bekämpfung der Cyberkriminalität und die Gemeinsame Task Force zur Bekämpfung der Cyberkriminalität bei Europol sowie das Notfallprotokoll für die Strafverfolgung, das EU-Zentrum für Informationsgewinnung und -analyse (EU INTCEN) und das EU-Instrumentarium für die Cyberdiplomatie, das Einheitliche Analyseverfahren (SIAC), die Cyberprojekte im Rahmen der Ständigen Strukturierten Zusammenarbeit (SSZ), insbesondere die Teams für die rasche Reaktion auf Cybervorfälle und die gegenseitige Unterstützung im Bereich der Cybersicherheit (CRRT).

75 „Eine Union, die mehr erreichen will: Meine Agenda für Europa“, Politische Leitlinien für die künftige Europäische Kommission 2019-2024 von Ursula von der Leyen.

76 Blueprint-Empfehlung (C(2017) 6100 final) vom 13.9.2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen.

verschiedene Cyberkreise Hand in Hand arbeiten müssen. Zugleich haben die jüngsten Ereignisse gezeigt, dass die EU der Cyberbedrohungslandschaft und deren Realitäten mit mehr Ehrgeiz und erhöhter Bereitschaft begegnen muss. Im Rahmen ihrer Beiträge zur gemeinsamen Cyberstelle sind die EU-Akteure (die Kommission und die Einrichtungen und sonstigen Stellen der EU) daher bereit, ihre Ressourcen und Fähigkeiten erheblich zu steigern, um besser vorbereitet und widerstandsfähiger zu sein.

Die gemeinsame Cyberstelle würde drei Hauptziele erfüllen. Erstens würde sie sicherstellen, dass alle Cyberkreise **vorbereitet** sind; zweitens würde der Informationsaustausch für eine stetige gemeinsame **Lageerfassung** sorgen; drittens würde die Cyberstelle die koordinierte **Reaktion** und Wiederherstellung stärken. Um diese Ziele zu erreichen, sollte sich die Stelle auf genau definierte **Blöcke und Ziele** stützen, etwa die Gewährleistung eines **sicheren und raschen Informationsaustauschs**, die Verbesserung der **Zusammenarbeit** zwischen den Beteiligten, einschließlich der Interaktion zwischen den Mitgliedstaaten und den einschlägigen EU-Einrichtungen, den Aufbau strukturierter **Partnerschaften mit vertrauenswürdigen Unternehmen** und die Erleichterung eines koordinierten Ansatzes für die **Zusammenarbeit mit externen Partnern**. So könnte die Cyberstelle ausgehend von einer Bestandsaufnahme der auf nationaler und EU-Ebene vorhandenen Fähigkeiten die Entwicklung eines Rahmens für die Zusammenarbeit erleichtern.

Um die gemeinsame Cyberstelle zum Scharnier der operativen Zusammenarbeit der EU im Bereich der Cybersicherheit zu machen, wird die Kommission in Zusammenarbeit mit den Mitgliedstaaten und den einschlägigen Organen, Einrichtungen und sonstigen Stellen der EU, einschließlich ENISA, CERT-EU und Europol, einen **schrittweisen und inklusiven Ansatz** anstreben, wobei die Zuständigkeiten und Mandate aller Beteiligten uneingeschränkt berücksichtigt werden. Im Einklang mit diesem Ansatz könnte die Cyberstelle dazu beitragen, die Zusammenarbeit innerhalb einzelner Cyberkreise voranzubringen, sofern die Beteiligten dies für erforderlich halten.

Für den Aufbau der gemeinsamen Cyberstelle werden vier Etappen vorgeschlagen:

- *Definieren*, Bestandsaufnahme der Fähigkeiten auf nationaler und EU-Ebene;
- *Vorbereiten,* Ausarbeitung eines Rahmens für strukturierte Zusammenarbeit und Unterstützung;
- *Einführen*, Umsetzung dieses Rahmens mithilfe der von den Beteiligten bereitgestellten Ressourcen, sodass die gemeinsame Cyberstelle einsatzbereit ist;
- *Expandieren,* Stärkung der koordinierten Reaktionsfähigkeit unter Einbeziehung von Industrie und Partnern.

Aufbauend auf den Ergebnissen der Konsultation mit den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU[77] wird die Kommission unter Beteiligung des Hohen Vertreters im Einklang mit dessen Zuständigkeiten bis Februar 2021 das Verfahren, die Etappenziele und den Zeitplan für die **Definition, Vorbereitung, Einführung und Expansion der gemeinsamen Cyberstelle** vorstellen.

[77] Die Konsultation der Mitgliedstaaten (auch während der Übung Blue OLEx20, bei der die Leiterinnen und Leiter der nationalen Cybersicherheitsbehörden zusammenkamen) und der Organe, Einrichtungen und sonstigen Stellen der EU erfolgte im Zeitraum Juli-November 2020.

2.2 Bekämpfung der Cyberkriminalität

Unsere Abhängigkeit von Online-Tools hat die Angriffsfläche für Cyberkriminelle exponentiell erhöht und dazu geführt, dass Ermittlungen bei fast allen Arten von Kriminalität eine digitale Komponente aufweisen. Zudem sind zentrale Gesellschaftsbereiche von Cyberakteuren bzw. Personen bedroht, die Cyberinstrumente zur Planung und Durchführung illegaler Handlungen einsetzen. Somit gibt es enge Verbindungen zur allgemeinen Sicherheitspolitik der EU, wie sich dies in den Cyberaspekten der EU-Strategie für eine Sicherheitsunion von 2020 und in der EU-Agenda für die Terrorismusbekämpfung widerspiegelt[78].

Die wirksame Bekämpfung der Cyberkriminalität ist ein Schlüsselfaktor für die Gewährleistung der Cybersicherheit: Abschreckung kann nicht allein durch Widerstandsfähigkeit erreicht werden, sondern erfordert auch, dass Straftäter erkannt und verfolgt werden. Daher ist es wesentlich, die Zusammenarbeit und den Austausch zwischen den Akteuren im Bereich der Cybersicherheit und jenen im Bereich der Strafverfolgung zu fördern. Auf EU-Ebene haben Europol und ENISA daher bereits eine enge Zusammenarbeit aufgebaut, gemeinsame Konferenzen und Workshops organisiert und der Kommission, den Mitgliedstaaten und anderen Interessenträgern gemeinsame Berichte über Cybersicherheitsbedrohungen und technologische Herausforderungen vorgelegt. Die Kommission wird diesen integrierten Ansatz weiter unterstützen, um eine kohärente und wirksame Reaktion auf der Grundlage eines umfassenden Informationsbildes zu gewährleisten.

Ein wichtiges Element dieser Reaktion ist, dass die EU und die nationalen Behörden die Kapazitäten der Strafverfolgungsbehörden zur Ermittlung im Bereich der Cyberkriminalität erweitern und erhöhen, wobei die Grundrechte uneingeschränkt zu achten sind und das erforderliche Gleichgewicht zwischen den verschiedenen Rechten und Interessen sichergestellt sein muss. Damit die EU der Cyberkriminalität begegnen kann, müssen die Rechtsvorschriften vollständig umgesetzt und zweckmäßig sein; dabei sollte Nachdruck auf die Bekämpfung des sexuellen Missbrauchs von Kindern im Internet und auf digitale Ermittlungen gelegt werden, auch bei Kriminalität im „Darknet“. Die Strafverfolgungsbehörden müssen umfassend für digitale Ermittlungen gerüstet sein. Die Kommission wird daher einen Aktionsplan vorlegen, um die digitalen Kapazitäten der Strafverfolgungsbehörden zu stärken, indem diese mit den erforderlichen Fähigkeiten und Instrumenten ausgestattet werden. Zudem wird Europol seine Rolle als Kompetenzzentrum weiter ausbauen, um die nationalen Strafverfolgungsbehörden bei der Bekämpfung der durch den Cyberraum ermöglichten und der von diesem abhängigen Kriminalität zu unterstützen und zur Festlegung gemeinsamer forensischer Standards (über das Innovationslabor und die Plattform von Europol) beizutragen. Alle diese Tätigkeiten erfordern eine angemessene Beteiligung der Mitgliedstaaten, die dazu angehalten werden, die nationalen Programme des Fonds für die innere Sicherheit in Anspruch zu nehmen und bei Aufforderungen zur Einreichung von Vorschlägen im Rahmen der thematischen Fazilität entsprechende Projekte vorzuschlagen.

[78] Mitteilung über die EU-Agenda für Terrorismusbekämpfung: Antizipieren, verhindern, schützen, reagieren, 9.12.2020 (COM(2020) 795 final).

Die Kommission wird mit allen geeigneten Mitteln, auch Vertragsverletzungsverfahren, dafür sorgen, dass die Richtlinie über Angriffe auf Informationssysteme[79] von 2013 vollständig umgesetzt und angewendet wird, auch im Hinblick auf die Bereitstellung statistischer Daten durch die Mitgliedstaaten. Sie wird dem Missbrauch von Domain-Namen – unter anderem zur Verbreitung illegaler Inhalte – wirksamer vorbeugen und darauf hinarbeiten, dass genaue Registrierungsdaten verfügbar sind; dafür wird sie weiter mit der Zentralstelle für die Vergabe von Internet-Namen und -Adressen (Internet Corporation for Assigned Names and Numbers – ICANN) und anderen Akteuren des Internet-Governance-Systems zusammenarbeiten, insbesondere über die Arbeitsgruppe für öffentliche Sicherheit des ICANN-Ausschusses für die Beratung von Regierungen. Der Vorschlag in der überarbeiteten NIS-Richtlinie sieht daher vor, vollständige Datenbanken mit Domain-Namen und genauen Registrierungsdaten (WHOIS-Daten) zu führen und den legalen Zugriff auf diese Daten zu ermöglichen, da dies für die Gewährleistung der Sicherheit, Stabilität und Widerstandsfähigkeit des DNS wesentlich ist.

Die Kommission wird sich zudem weiter dafür einsetzen, dass geeignete Kanäle für den grenzüberschreitenden Zugriff auf elektronische Beweismittel bei strafrechtlichen Ermittlungen – die bei 85 % der Ermittlungen benötigt werden, wobei 65 % aller Anfragen an Diensteanbieter mit Sitz in einem anderen Hoheitsgebiet gerichtet sind – bereitgestellt und die entsprechenden Vorschriften präzisiert werden. Zu diesem Zweck wird die Kommission darauf hinarbeiten, dass das „Paket zu elektronischen Beweismitteln“ sowie konkrete Maßnahmen angenommen und anschließend umgesetzt werden[80]. Um den Fachleuten ein effizientes Instrument an die Hand zu geben, ist es entscheidend, dass die Vorschläge zu den elektronischen Beweismitteln zeitnah vom Europäischen Parlament und dem Rat angenommen werden. Elektronische Beweismittel müssen lesbar sein. Daher wird die Kommission weiter darauf hinarbeiten, dass die Fähigkeiten der Rechtsdurchsetzung im Bereich der digitalen Ermittlungen gefördert werden, auch im Hinblick auf die Verschlüsselung bei strafrechtlichen Ermittlungen, wobei deren Funktion zum Schutz der Grundrechte und der Cybersicherheit uneingeschränkt gewahrt bleibt.

2.3 EU-Instrumentarium für die Cyberdiplomatie

Die EU hat ihr **Instrumentarium für die Cyberdiplomatie**[81] zur Vorbeugung, Abschreckung und Reaktion im Hinblick auf böswillige Cyberaktivitäten eingesetzt. Nach der Einführung des Rechtsrahmens für gezielte restriktive Maßnahmen gegen Cyberangriffe im Mai 2019[82] hat die EU im Juli 2020 sechs Personen und drei Einrichtungen, die für

---

79 Richtlinie 2013/40/EU über Angriffe auf Informationssysteme.

80 COM(2018) 225 und 226; C(2020) 2779 final. Unlängst ist insbesondere das SIRIUS-Projekt im Rahmen des Partnerschaftsinstruments mit zusätzlichen Mitteln ausgestattet worden, um die Kanäle für den legalen grenzüberschreitenden Zugriff auf elektronische Beweismittel bei strafrechtlichen Ermittlungen zu verbessern – die bei 85 % der Ermittlungen im Zusammenhang mit schweren Straftaten erforderlich sind, wobei 65 % aller Anfragen an Anbieter mit Sitz in einem anderen Hoheitsgebiet gerichtet sind – und auf internationaler Ebene kompatible Vorschriften festzulegen.

81 https://www.consilium.europa.eu/de/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

82 Beschluss (GASP) 2019/797 des Rates vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen (ABl. L 129I vom 17.5.2019, S. 13) und Verordnung (EU) 2019/796 des Rates vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen (ABl. L 129I vom 17.5.2019, S. 1)

Cyberangriffe auf die EU und ihre Mitgliedstaaten verantwortlich oder daran beteiligt waren, auf die entsprechende Liste gesetzt[83]. Im Oktober 2020 wurde zwei weitere Personen und eine weitere Einrichtung auf die Liste gesetzt[84]. Böswilligen Cyberaktivitäten, auch solchen, die in geringer Intensität über einen längeren Zeitraum anhalten, sollte mit einer wirksamen und umfassenden gemeinsamen diplomatischen Reaktion der EU begegnet werden, wobei das gesamte Spektrum der auf EU-Ebene verfügbaren Maßnahmen ausgeschöpft werden sollte.

Eine rasche und wirksame gemeinsame diplomatische Reaktion der EU erfordert eine robuste gemeinsame Lageerfassung und die Fähigkeit, schnell einen gemeinsamen EU-Standpunkt festzulegen. Der Hohe Vertreter der Union für Außen- und Sicherheitspolitik wird die Einrichtung einer **Arbeitsgruppe der Mitgliedstaaten für EU-Cybernachrichtendienste** innerhalb des Zentrums der EU für Informationsgewinnung und -erfassung (Intelligence and Situation Centre – INTCEN) fördern, um die strategische nachrichtendienstliche Zusammenarbeit gegen Cyberbedrohungen und -aktivitäten voranzubringen. Durch diese Arbeiten wird die Lageerfassung in der EU und die Beschlussfassung im Hinblick auf eine gemeinsame diplomatische Reaktion weiter gefördert werden. Die Arbeitsgruppe soll mit den vorhandenen Strukturen[85], erforderlichenfalls auch mit jenen, die sich mit der allgemeineren Bedrohung der hybriden und ausländischen Einmischung befassen, in Kontakt treten, um Informationen über die Lageerfassung einzuholen und diese zu bewerten.

Um die Fähigkeit der EU zur Vorbeugung, Abschreckung und Reaktion im Hinblick auf böswillige Cyberaktivitäten zu stärken, wird der Hohe Vertreter unter Beteiligung der Kommission im Einklang mit deren Zuständigkeiten einen Vorschlag zur näheren Definition der EU-**Cyberabschreckung** vorlegen. Aufbauend auf den bisherigen Arbeiten im Rahmen des Instrumentariums für die Cyberdiplomatie sollte die Cyberabschreckung zum verantwortungsvollen Verhalten und zur Zusammenarbeit der Staaten im Cyberraum beitragen und besondere Vorgaben zur Bekämpfung jener Cyberangriffe enthalten, die die massivsten Auswirkungen haben, insbesondere solche, die unsere kritische Infrastrukturen und demokratischen Institutionen und Verfahren betreffen[86], sowie Angriffe auf Lieferketten und den durch den Cyberraum ermöglichten Diebstahl geistigen Eigentums. Im Rahmen der Cyberabschreckung sollte dargelegt werden, wie die EU und die Mitgliedstaaten ihre politischen, wirtschaftlichen, diplomatischen, rechtlichen und strategischen Kommunikationsmittel gegen böswillige Cyberaktivitäten wirksamer einsetzen und ihre Fähigkeiten zur Zuordnung böswilliger Cyberaktivitäten ausbauen können. Darüber hinaus

[83] Beschluss (GASP) 2020/1127 des Rates vom 30. Juli 2020 zur Änderung des Beschlusses (GASP) 2019/797 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen (ST/9564/2020/INIT) (ABl. L 246 vom 30.7.2020, S. 12) und Durchführungsverordnung (EU) 2020/1125 des Rates vom 30. Juli 2020 zur Durchführung der Verordnung (EU) 2019/796 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen (ST/9568/2020/INIT) (ABl. L 246 vom 30.7.2020, S. 4).

[84] Beschluss (GASP) 2020/1537 des Rates vom 22. Oktober 2020 zur Änderung des Beschlusses (GASP) 2019/797 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen (ABl. L 351I vom 22.10.2020, S. 5) und Durchführungsverordnung (EU) 2020/1536 des Rates vom 22. Oktober 2020 zur Durchführung der Verordnung (EU) 2019/796 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen (ABl. L 351I vom 22.10.2020, S. 1).

[85] Etwa das Einheitliche Analyseverfahren (Single Intelligence Analysis Capacity – SIAC) der EU und erforderlichenfalls die einschlägigen Projekte im Rahmen der SSZ sowie das Schnellwarnsystem (Rapid Alert System – RAS) von 2018, das eingerichtet wurde, um das EU-Gesamtkonzept zur Bekämpfung der Desinformation zu unterstützen.

[86] Insbesondere indem Synergien mit den Initiativen im Rahmen des Europäischen Aktionsplans für Demokratie angestrebt werden.

wird der Hohe Vertreter gemeinsam mit dem Rat und der Kommission **zusätzliche Maßnahmen im Rahmen des Instrumentariums für die Cyberdiplomatie** in Betracht ziehen, einschließlich der Möglichkeit weiterer Optionen für restriktive Maßnahmen sowie der Prüfung der **Abstimmung mit qualifizierter Mehrheit über die Listenaufnahme im Rahmen der horizontalen Sanktionsregelung gegen Cyberangriffe**. Außerdem sollte die EU weitere Anstrengungen unternehmen, um die **Zusammenarbeit mit internationalen Partnern**, einschließlich der NATO, zu **stärken**, das gemeinsame Verständnis der Bedrohungslandschaft voranzubringen, Kooperationsmechanismen zu entwickeln und kooperative diplomatische Reaktionen zu identifizieren.

Zudem wird der Hohe Vertreter unter Beteiligung der Kommission eine Aktualisierung der **Leitlinien zur Umsetzung des Instrumentariums für die Cyberdiplomatie**[87], auch im Hinblick auf eine effizientere Beschlussfassung, vorschlagen und weiter regelmäßig Übungen und Bewertungen im Zusammenhang mit dem Instrumentarium für die Cyberdiplomatie organisieren. Darüber hinaus sollte die EU das **Instrumentarium für die Cyberdiplomatie stärker in die Krisenmechanismen der EU integrieren** und Synergien mit den Anstrengungen gegen hybride Bedrohungen, Desinformation und ausländische Einmischung im Rahmen des Gemeinsamen Rahmens für die Abwehr hybrider Bedrohungen[88] und des Europäischen Aktionsplans für Demokratie anstreben. In diesem Zusammenhang sollte die EU Überlegungen über die Wechselwirkungen zwischen dem Instrumentarium für die Cyberdiplomatie und der möglichen Anwendung des Artikels 42 Absatz 7 EUV und des Artikels 222 AEUV[89] anstellen.

2.4 Ausbau der Fähigkeiten im Bereich der Cyberabwehr

Die EU und die Mitgliedstaaten müssen ihre Fähigkeiten der Vorbeugung und Reaktion im Hinblick auf Cyberbedrohungen gemäß den Zielvorgaben der EU, die sich aus der Globalen Strategie der EU[90] von 2016 ergeben, ausbauen. Der Hohe Vertreter wird daher in Zusammenarbeit mit der Kommission eine **Überprüfung des Rahmens für die Cyberabwehr** (Cyber Defence Policy Framework – CDPF) vorlegen, um die Koordinierung und Zusammenarbeit zwischen den EU-Akteuren[91] sowie mit und zwischen den Mitgliedstaaten, auch in Bezug auf Missionen und Operationen im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP), weiter zu verbessern. Der CDPF sollte in den bevorstehenden Strategischen Kompass einfließen[92], sodass sichergestellt ist, dass Cybersicherheit und Cyberabwehr stärker in die umfassendere Sicherheits- und Verteidigungsagenda eingebunden sind.

Im Jahr 2018 benannte die EU den Cyberraum als einen Einsatzbereich[93]. In einer künftigen **„militärischen Vision und Strategie für den Cyberraum als Einsatzbereich“** sollte der EU-Militärausschuss genauer definieren, wie der Cyberraum als Einsatzbereich militärische Missionen und Operationen der EU im Rahmen der GSVP ermöglicht. Das von der

87 13007/17.
88 https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52016JC0018&from=EN
89 Klausel über gegenseitige Verteidigung bzw. Solidaritätsklausel.
90 Schlussfolgerungen des Rates (14149/16) zur Umsetzung der Globalen Strategie der Europäischen Union im Bereich der Sicherheit und Verteidigung.
91 Insbesondere der EAD, einschließlich des EU-Militärstabs (EUMS) und des Europäischen Sicherheits- und Verteidigungskollegs (ESVK), die Kommission und EU-Agenturen, insbesondere die Europäische Verteidigungsagentur (European Defence Agency – EDA).
92 Schlussfolgerungen des Rates vom 17. Juni 2020 zu Sicherheit und Verteidigung (8910/20).
93 https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/de/pdf

Europäischen Verteidigungsagentur (European Defence Agency – EDA) eingerichtete **militärische CERT-Netz**[94] wird weiter zu einer erheblichen Stärkung der Zusammenarbeit zwischen den Mitgliedstaaten beitragen. Um die Cybersicherheit kritischer Weltrauminfrastrukturen, die in die Zuständigkeit des Weltraumprogramms fallen, zu gewährleisten, wird zudem die Europäische Agentur für das Weltraumprogramm und insbesondere die Galileo-Sicherheitszentrale gestärkt und ihr Mandat auf andere kritische Ressourcen des Weltraumprogramms ausgeweitet.

Die EU und die Mitgliedstaaten sollten über verschiedene Strategien und Instrumente der EU, insbesondere den CDPF, weitere Impulse für die **Entwicklung modernster Fähigkeiten der Cyberabwehr** geben sowie gegebenenfalls auf den Arbeiten der EDA aufbauen. Nachdruck muss dabei insbesondere auf die Entwicklung und Nutzung von Schlüsseltechnologien wie KI, Verschlüsselung und Quanteninformatik gelegt werden. Im Einklang mit den EU-Prioritäten für die Fähigkeitenentwicklung 2018[95] sollte die EU auf der Grundlage der Ergebnisse des ersten umfassenden Berichts über die Koordinierte Jährliche Überprüfung der Verteidigung (Coordinated Annual Review on Defence – CARD)[96] die Zusammenarbeit zwischen den Mitgliedstaaten bei **Forschung, Innovation und Fähigkeitenentwicklung im Bereich der Cyberabwehr** weiter fördern und die Mitgliedstaaten dazu anhalten, das Potenzial der **Ständigen Strukturierten Zusammenarbeit (SSZ)**[97] und des **EDF**[98] voll auszuschöpfen.

Im **Aktionsplan der Kommission für Synergien zwischen der zivilen, der Verteidigungs- und der Raumfahrtindustrie**, der im ersten Quartal 2021 vorgelegt werden soll, werden Maßnahmen enthalten sein, mit denen Synergien auf der Ebene der Programme, Technologien, Innovation und Start-ups im Einklang mit der Governance der jeweiligen Programme gefördert werden sollen[99].

Zur Förderung des Informationsaustauschs und der gegenseitigen Unterstützung sollten zudem relevante Synergien und Schnittstellen mit Initiativen im Bereich der Cyberabwehr, die in anderen Kontexten, einschließlich der kollaborativen Cyberprojekte[100] der Mitgliedstaaten im Rahmen der SSZ, vorangetrieben werden, sowie mit den EU-Cybersicherheitsstrukturen entwickelt werden.

Strategische Initiativen

---

94 Mit der Einrichtung eines militärischen CERT-Netzes der EU wird einem im CDPF von 2018 festgelegten Ziel entsprochen; gefördert werden soll die aktive Interaktion und der aktive Informationsaustausch zwischen den militärischen CERT der EU-Mitgliedstaaten.

95 Im Juni 2018 vereinbarten die Mitgliedstaaten im EDA-Lenkungsausschuss, die Zusammenarbeit im Verteidigungsbereich auf EU-Ebene zu leiten.

96 Im November 2020 von den Verteidigungsministern im EDA-Lenkungsausschuss gebilligt. https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card)

97 Derzeit gibt es mehrere Cyberprojekte des SSZ, insbesondere die Plattform für den Austausch von Informationen über Cyberbedrohungen und -vorfälle, Teams für die rasche Reaktion auf Cybervorfälle und die gegenseitige Unterstützung im Bereich der Cybersicherheit, EU-Cyberakademie und -innovationszentrum sowie das Koordinierungszentrum für den Cyber- und Informationsraum (Cyber and Information Domain Coordination Centre – CIDCC).

98 Im Rahmen des EDF hat die Kommission bereits Möglichkeiten für gemeinsame Forschungs- und Entwicklungsmaßnahmen im Bereich der Cyberabwehr benannt, deren Ziel die Stärkung der Zusammenarbeit, der Innovationsfähigkeit und der Wettbewerbsfähigkeit der Verteidigungsindustrie ist.

99 Etwa Horizont Europa, Digitales Europa und EDF.

100 https://pesco.europa.eu/

Die EU sollte

- den europäischen Rahmen für das Krisenmanagement im Bereich der Cybersicherheit vervollständigen und die Verfahren, die Etappenziele und den Zeitplan für die Einrichtung der gemeinsamen Cyberstelle festlegen;
- die Umsetzung der Agenda zur Bekämpfung der Cyberkriminalität im Rahmen der Strategie für die Sicherheitsunion fortsetzen;
- die Mitgliedstaaten zur Einsetzung einer Arbeitsgruppe „Cyberintelligenz“ im Rahmen des EU-INTCEN anhalten und dazu beitragen;
- die EU-Cyberabschreckung voranbringen, um für Vorbeugung, Abschreckung und Reaktion im Hinblick auf böswillige Cyberaktivitäten zu sorgen;
- den Rahmen für die Cyberabwehr überprüfen;
- die Entwicklung einer „militärischen Vision und Strategie der EU für den Cyberraum als Einsatzbereich“ für militärische GSVP-Missionen und -Operationen fördern;
- Synergien zwischen der zivilen, der Verteidigungs- und der Weltraumindustrie unterstützen und
- die Cybersicherheit kritischer Weltrauminfrastrukturen im Rahmen des Weltraumprogramms stärken.

3 FÖRDERUNG EINES GLOBALEN OFFENEN CYBERRAUMS

Die EU sollte sich in Zusammenarbeit mit internationalen Partnern weiter für ein politisches Modell des Cyberraums einsetzen, das auf Rechtsstaatlichkeit gegründet ist, die Menschenrechte, Grundfreiheiten und demokratischen Werte achtet und weltweit den sozialen, wirtschaftlichen und politischen Fortschritt fördert, und zu einer Sicherheitsunion beitragen. Die internationale Zusammenarbeit ist von entscheidender Bedeutung, damit der Cyberraum global, offen, stabil und sicher bleibt. Die EU sollte daher weiter mit Drittländern, internationalen Organisationen und der Multi-Stakeholder-Gemeinschaft zur Entwicklung und Umsetzung einer kohärenten, ganzheitlichen internationalen Cyberpolitik zusammenarbeiten, wobei der zunehmenden Verknüpfung zwischen den wirtschaftlichen Aspekten neuer Technologien, der inneren Sicherheit sowie der Außen-, Sicherheits- und Verteidigungspolitik Rechnung zu tragen ist. Die EU kann als starker Wirtschafts- und Handelsblock, der auf die zentralen Werte der Demokratie, Rechtsstaatlichkeit und die Achtung der Grundrechte gegründet ist, bei der Festlegung und Förderung internationaler Normen und Standards eine einzigartige führende Rolle spielen.

3.1. Führungsrolle der EU bei Standards, Normen und Rahmenbedingungen für den Cyberraum

Mehr Einsatz für internationale Normung

Um ihre Vision des Cyberraums auf internationaler Ebene voranzubringen, muss die EU **ihr Engagement und ihre Führungsrolle im Rahmen internationaler Normungsverfahren verstärken und ihre Vertretung in internationalen und europäischen Normungsgremien**

sowie in anderen Normungsorganisationen ausbauen[101]. Da sich digitale Technologien rasch entwickeln, gewinnen internationale Standards, die traditionelle Regulierungsanstrengungen ergänzen, in Bereichen wie KI, Cloud, Quanteninformatik und Quantenkommunikation zunehmend an Bedeutung. Drittländer setzen zunehmend auf internationale Normung, um ihre politische und ideologische Agenda voranzubringen, die häufig nicht den Werten der EU entspricht. Darüber hinaus wächst die Gefahr, dass konkurrierende internationale Normensysteme entstehen, was zu einer Fragmentierung führen würde.

Die Festlegung internationaler Standards für neu entstehende Technologien und die Kernarchitektur des Internets im Einklang mit den Werten der EU ist von entscheidender Bedeutung, um sicherzustellen, dass das Internet global und offen bleibt und die Technologien auf den Menschen und den Schutz der Privatsphäre ausgerichtet sind und in rechtmäßiger, sicherer und ethischer Weise genutzt werden. Im Rahmen ihrer künftigen Normungsstrategie sollte die EU ihre **Ziele für internationale Normen** definieren und proaktiv koordinierte Maßnahmen ergreifen, um diese auf internationaler Ebene zu fördern. Dabei sollte eine engere Zusammenarbeit und Lastenteilung mit gleich gesinnten Partnern und europäischen Interessenträgern angestrebt werden.

Förderung eines verantwortungsvollen staatlichen Handelns im Cyberraum

Die EU setzt ihre Zusammenarbeit mit internationalen Partnern fort, um einen globalen, offenen, stabilen und sicheren Cyberraum zu fördern, in dem **das Völkerrecht – insbesondere die Charta der Vereinten Nationen**[102] – geachtet wird und die **freiwilligen, nicht bindenden Normen, Regeln und Grundsätze der Vereinten Nationen für verantwortungsvolles staatliches Handeln**[103] eingehalten werden. Angesichts der Verschlechterung wirksamer multilateraler Gespräche über die internationale Sicherheit im Cyberraum ist es umso wichtiger, dass die EU und die Mitgliedstaaten bei den Beratungen in den VN und anderen einschlägigen internationalen Foren eine proaktivere Haltung einnehmen. Die EU ist am besten in der Lage, die **Standpunkte der Mitgliedstaaten in internationalen Foren geltend zu machen, zu koordinieren und zu konsolidieren**, und sollte einen **Standpunkt der EU in Bezug auf die Anwendung des Völkerrechts im Cyberraum ausarbeiten**. Auch der Hohe Vertreter ist bestrebt, gemeinsam mit den Mitgliedstaaten ihren umfassenden und einvernehmlichen Vorschlag eines politisches Engagements für ein **Aktionsprogramm der Vereinten Nationen zur Förderung von verantwortungsvollem staatlichen Handeln im Cyberraum**[104] voranzubringen. Aufbauend

[101] Genannt seien etwa die Internationale Normungsorganisation (International Organization for Standardization – ISO), die Internationale Elektrotechnische Kommission (International Electrotechnical Commission – IEC), die Internationale Fernmeldeunion (International Telecommunication Union – ITU), das Europäisches Komitee für Normung (European Committee for Standardisation – CEN), das Europäische Komitee für elektrotechnische Normung (European Committee for Electrotechnical Standardization – CENELEC), das Europäische Institut für Telekommunikationsnormen (European Telecommunications Standards Institute – ETSI), die Internettechnik-Arbeitsgruppe (Internet Engineering Task Force – IETF), das Partnerschaftsprojekt zur 3. Generation (3rd Generation Partnership Project – 3GPP) und der Berufsverband der Ingenieure in Elektrotechnik und Informationstechnik (Institute of Electrical and Electronics Engineers – IEEE).

[102] https://www.un.org/en/sections/un-charter/un-charter-full-text/

[103] Dies geht aus den einschlägigen, von der VN-Generalversammlung gebilligten Berichten der Gruppen von Regierungssachverständigen (UN-GGE) für Entwicklungen auf dem Gebiet der Information und Telekommunikation im Kontext der internationalen Sicherheit hervor, insbesondere den Berichten von 2015, 2013 und 2010.

[104] https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf

auf dem Besitzstand, wie er von der VN-Generalversammlung gebilligt wurde[105], bietet das Aktionsprogramm eine Grundlage für die Zusammenarbeit und den Austausch bewährter Verfahren innerhalb der VN und sieht einen Mechanismus vor, um die Normen für verantwortungsvolles staatliches Handeln praktisch umzusetzen und den Kapazitätsaufbau zu fördern. Darüber hinaus strebt der Hohe Vertreter die Stärkung und Förderung **vertrauensbildender Maßnahmen** zwischen den Staaten an, die auch den Austausch bewährter Verfahren auf regionaler und multilateraler Ebene sowie Beiträge zur überregionalen Zusammenarbeit beinhalten.

Die zunehmende globale Vernetzung darf nicht zu Zensur, Massenüberwachung, Verletzungen des Datenschutzes und Unterdrückung der Zivilgesellschaft, der Wissenschaft und der Bürgerinnen und Bürger führen. Die EU sollte beim Schutz und der Förderung der **Menschenrechte und Grundfreiheiten** im Internet weiter eine führende Rolle spielen. Sie sollte dazu auf eine umfassendere Einhaltung der internationalen Rechtsvorschriften und Normen im Bereich der Menschenrechte[106] hinwirken, ihren Aktionsplan für Menschenrechte und Demokratie 2020–2024[107] umsetzen und ihre Menschenrechtsleitlinien für die Meinungsfreiheit online und offline[108] vorantreiben und damit **der praktischen Anwendung der EU-Instrumente neue Impulse geben**. Die EU sollte nachhaltige Anstrengungen zum **Schutz von Menschenrechtsverteidigern, der Zivilgesellschaft und von Wissenschaftskreisen unternehmen, die sich mit Fragen wie Cybersicherheit, Datenschutz, Überwachung und Zensur im Internet befassen**. Zu diesem Zweck sollte sie weitere praktische Leitlinien erstellen, bewährte Verfahren fördern und ihre Bemühungen gegen den Missbrauch neu entstehender Technologien verstärken, insbesondere indem bei Bedarf diplomatische Maßnahmen ergriffen und die Ausfuhr solcher Technologien kontrolliert wird. Die EU sollte sich auch weiterhin für den Schutz der gefährdetsten Mitglieder der Gesellschaft im Internet einsetzen, indem sie Rechtsvorschriften zum besseren Schutz von Kindern vor sexuellem Missbrauch und sexueller Ausbeutung sowie eine Strategie für die Rechte des Kindes vorlegt.

Das Budapester Übereinkommen über Computerkriminalität

Die EU bietet weiterhin Unterstützung für Drittländer, die dem **Budapester Europaratsübereinkommen über Computerkriminalität** beitreten möchten. Außerdem unterstützt sie die Abschlussarbeiten zum **zweiten Zusatzprotokoll** zu dem Übereinkommen, das Maßnahmen und Garantien zur Verbesserung der internationalen Zusammenarbeit zwischen Strafverfolgungs- und Justizbehörden sowie zwischen Behörden und Diensteanbietern in anderen Ländern beinhaltet und an dessen Aushandlung die Kommission im Namen der EU teilnimmt[109]. Die aktuelle Initiative für ein neues Rechtsinstrument zur Cyberkriminalität auf VN-Ebene birgt das Risiko, dass Spaltungen verstärkt und dringend benötigte nationale Reformen und die damit verbundenen Bemühungen um den Kapazitätsaufbau gebremst werden, was die wirksame internationale Zusammenarbeit bei der

[105] Dies geht aus den einschlägigen, von der VN-Generalversammlung gebilligten Berichten der Gruppen von Regierungssachverständigen (UN-GGE) für Entwicklungen auf dem Gebiet der Information und Telekommunikation im Kontext der internationalen Sicherheit hervor, insbesondere den Berichten von 2015, 2013 und 2010.

[106] Insbesondere die Charta der Vereinten Nationen und die Allgemeine Erklärung der Menschenrechte.

[107] https://www.consilium.europa.eu/en/press/press-releases/2020/11/19/council-approves-conclusions-on-the-eu-action-plan-on-human-rights-and-democracy-2020-2024/

[108] https://www.consilium.europa.eu/media/28348/142549.pdf

[109] Beschluss des Rates vom Juni 2019 (Ref. 9116/19).

Bekämpfung der Cyberkriminalität behindern könnte. Die EU sieht deshalb keinen Bedarf für ein neues Rechtsinstrument zur Cyberkriminalität auf VN-Ebene. Die EU beteiligt sich weiterhin am **multilateralen Austausch über Cyberkriminalität**, um durch Inklusion, Transparenz und Berücksichtigung des verfügbaren Fachwissens die Achtung der Menschenrechte und Grundfreiheiten sicherzustellen und so einen Mehrwert für alle zu schaffen.

3.2 Zusammenarbeit mit Partnern und der Multi-Stakeholder-Gemeinschaft

Die EU sollte **ihre Cyber-Dialoge mit Drittländern intensivieren und ausweiten**, um ihre Werte und ihre Vision für den Cyberraum zu fördern, bewährte Verfahren auszutauschen und eine wirksamere Zusammenarbeit zu erreichen. Darüber hinaus sollte die EU einen **strukturierten Austausch mit regionalen Organisationen** wie der Afrikanischen Union, dem ASEAN-Regionalforum, der Organisation Amerikanischer Staaten und der Organisation für Sicherheit und Zusammenarbeit in Europa einrichten. Gleichzeitig sollte sich die EU bemühen, mit anderen Partnern auf der Grundlage von Fragen von gemeinsamem Interesse einen Konsens zu finden, wo dies möglich und sinnvoll ist. Die EU sollte in Zusammenarbeit mit ihren Delegationen und gegebenenfalls den Botschaften der Mitgliedstaaten in der Welt ein informelles **EU-Netz für Cyberdiplomatie** errichten, um für ihre Vision für den Cyberraum zu werben, Informationen auszutauschen und sich regelmäßig über die Entwicklungen im Cyberraum abzustimmen[110].

Aufbauend auf den Gemeinsamen Erklärungen vom 8. Juli 2016[111] und 10. Juli 2018[112] sollte die EU die **Zusammenarbeit zwischen der EU und der NATO** weiter vorantreiben, insbesondere in Bezug auf Interoperabilitätsanforderungen für die Cyberabwehr. Die EU sollte in dieser Hinsicht die Anbindung der einschlägigen GSVP-Strukturen an das *Federated Mission Networking* (FMN) der NATO weiterverfolgen, um die Interoperabilität mit den Netzen der NATO und den Partnern zu ermöglichen, wo dies erforderlich ist. Zudem sollte die Zusammenarbeit zwischen EU und NATO in Bezug auf Ausbildung, Schulung und Übungen näher erörtert werden, und es sollten Synergien zwischen dem Europäischen Sicherheits- und Verteidigungskolleg und dem Kompetenzzentrum für kooperativen Schutz vor Computerangriffen der NATO angestrebt werden.

Ihren Wertvorstellungen entsprechend unterstützt und fördert die EU mit Nachdruck das **Multi-Stakeholder-Modell für die Internet-Governance**. Keine einzelne Stelle, Regierung oder internationale Organisation sollte die Kontrolle über das Internet anstreben. Die EU sollte weiterhin in Foren[113] mitwirken, um die Zusammenarbeit zu verbessern und den Schutz der Grundrechte und Grundfreiheiten zu gewährleisten, insbesondere in Bezug auf die Menschenwürde, die Privatsphäre sowie die freie Meinungsäußerung und Informationsfreiheit. Um die Zusammenarbeit der verschiedenen Interessenträger in Fragen der Cybersicherheit voranzubringen, streben die Kommission und der Hohe Vertreter im Rahmen ihrer jeweiligen Zuständigkeiten an, den **regelmäßigen und strukturierten Austausch mit den Akteuren** – einschließlich Privatsektor, Wissenschaft und Zivilgesellschaft – zu intensivieren, wobei betont wird, dass die Vernetzung des Cyberraums

[110] Auch die Tätigkeiten des informellen EU-Netzwerks für digitale Diplomatie, in das die Außenministerien der Mitgliedstaaten eingebunden sind, könnten hierdurch unterstützt werden.

[111] http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/

[112] https://www.consilium.europa.eu/de/press/press-releases/2018/07/10/eu-nato-joint-declaration/

[113] Beispielsweise die Zentralstelle für die Vergabe von Internet-Namen und -Adressen (ICANN) und das Internet-Governance-Forum (IGF).

alle Interessenträger dazu verpflichtet, im Hinblick auf einen globalen, offenen, stabilen und sicheren Cyberraum miteinander zu kooperieren und ihrer spezifischen Verantwortung für dessen Aufrechterhaltung gerecht zu werden. Diese Anstrengungen werden wertvolle Beiträge zu potenziellen zentralen Maßnahmen auf EU-Ebene leisten.

3.3 Stärkung der globalen Kapazitäten zur Erhöhung der globalen Widerstandsfähigkeit

Die EU unterstützt ihre Partner weiterhin bei der Verbesserung ihrer Fähigkeiten, Cyberangriffe abzuwehren, Cyberdelikte aufzuklären und zu ahnden sowie gegen Cyberbedrohungen vorzugehen, damit alle Länder von den sozialen, wirtschaftlichen und politischen Vorteilen, die das Internet und der Einsatz von Technologien bieten, profitieren können. Zur Gewährleistung der Gesamtkohärenz sollte die EU eine **EU-Agenda für den Aufbau externer Cyberkapazitäten** entwickeln, mit der diese Bemühungen im Einklang mit ihren Leitlinien für den Aufbau externer Cyberkapazitäten[114] sowie der Agenda 2030 für nachhaltige Entwicklung[115] kanalisiert werden. Im Rahmen der Agenda sollte das Fachwissen der Mitgliedstaaten sowie der einschlägigen Organe, Einrichtungen und sonstigen Stellen und Initiativen der EU – einschließlich des EU-Netzes für den Cyberkapazitätsaufbau[116] – nach Maßgabe ihrer jeweiligen Mandate genutzt werden. Es soll ein **EU-Gremium für den Cyberkapazitätsaufbau** eingerichtet werden, an dem einschlägige institutionelle Interessenträger der EU teilnehmen und das die Fortschritte überwacht, zusätzliche Synergien ermittelt und etwaige Lücken erkennt. Das Gremium könnte außerdem die verstärkte Zusammenarbeit mit den Mitgliedstaaten, Partnern aus dem öffentlichen und dem privaten Sektor sowie mit anderen relevanten internationalen Gremien unterstützen, um die Anstrengungen zu koordinieren und Doppelarbeit zu vermeiden.

Die **EU-Maßnahmen für den Aufbau von Cyberkapazitäten** sollten sich weiter auf den westlichen Balkan, die Nachbarschaft der EU sowie auf die Partnerländer konzentrieren, in denen die digitale Entwicklung rasch voranschreitet. Die Entwicklung von Rechtsvorschriften und politischen Maßnahmen in den Partnerländern sollte von der EU im Einklang mit ihren einschlägigen Strategien und Standards der Cyberdiplomatie unterstützt werden. Der Aspekt der Cybersicherheit sollte in dieser Hinsicht in die EU-Bemühungen zum Aufbau digitaler Kapazitäten grundsätzlich mit einbezogen werden. Die EU sollte zu diesem Zweck ein Schulungsprogramm für ihre Bediensteten entwickeln, deren Aufgabe es ist, die Bemühungen der EU um den Aufbau digitaler Kapazitäten sowie externer Cyberkapazitäten umzusetzen. Im Einklang mit den Anstrengungen im Rahmen des Europäischen Aktionsplans für Demokratie sollte die EU diesen Ländern auch dabei helfen, den wachsenden Herausforderungen durch böswillige Cyberaktivitäten, die der Entwicklung ihrer Gesellschaften und der **Integrität und Sicherheit demokratischer Systeme** schaden, Herr zu werden. Das Peer-Learning zwischen EU-Mitgliedstaaten, beteiligten EU-Agenturen und Drittländern könnte in dieser Hinsicht besonders nützlich sein.

Schließlich können auch zivile GSVP-Missionen, die im Rahmen des Paktes für die zivile GSVP von 2018[117] durchgeführt werden, zum umfassenderen Vorgehen der EU zur Bewältigung der Herausforderungen im Bereich der Cybersicherheit gehören, insbesondere durch Förderung der Rechtsstaatlichkeit in Partnerländern und Stärkung ihrer Kapazitäten im Bereich der Strafverfolgung und Zivilverwaltung.

---

[114] https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf
[115] https://ec.europa.eu/environment/sustainable-development/SDGs/index_en.htm
[116] https://www.eucybernet.eu/
[117] https://data.consilium.europa.eu/doc/document/ST-14611-2019-INIT/de/pdf

Strategische Initiativen

Die EU sollte

- eine Reihe von Zielen für internationale Normungsverfahren festlegen und diese Ziele auf internationaler Ebene fördern;
- die internationale Sicherheit und Stabilität im Cyberraum stärken, insbesondere durch einen Vorschlag der EU und ihrer Mitgliedstaaten für ein Aktionsprogramm der Vereinten Nationen zur Förderung von verantwortungsvollem staatlichen Handeln im Cyberraum;
- praktische Orientierungshilfe zur Einhaltung der Menschenrechte und Beachtung der Grundfreiheiten im Cyberraum bieten;
- Kinder besser vor sexuellem Missbrauch und sexueller Ausbeutung schützen und eine Strategie für die Rechte des Kindes verabschieden;
- das Budapester Übereinkommen über Computerkriminalität stärken und fördern, u. a. durch die Arbeiten am zweiten Zusatzprotokoll zu dem Übereinkommen;
- den Cyber-Dialog der EU mit Drittländern, regionalen und internationalen Organisationen ausweiten, u. a. durch ein informelles EU-Netz für Cyberdiplomatie;
- den Austausch mit der Multi-Stakeholder-Gemeinschaft verstärken, insbesondere durch einen regelmäßigen und strukturierten Austausch mit dem Privatsektor, der Wissenschaft und der Zivilgesellschaft;
- eine EU-Agenda für den Aufbau externer Cyberkapazitäten und die Einrichtung eines EU-Gremiums für den Cyberkapazitätsaufbau vorschlagen.

III. CYBERSICHERHEIT IN DEN ORGANEN, EINRICHTUNGEN UND SONSTIGEN STELLEN DER EU

Angesichts ihres ausgeprägten politischen Profils, ihrer wichtigen Aufgaben bei der Koordinierung hochsensibler Themen und ihrer Rolle bei der Verwaltung großer Summen öffentlicher Gelder sind die **Organe, Einrichtungen und sonstigen Stellen der EU regelmäßig das Ziel von Cyberangriffen** und insbesondere von Cyberspionage. Allerdings sind die Fähigkeiten der einzelnen Einrichtungen, Cyberangriffe abzuwehren und böswillige Cyberaktivitäten zu erkennen und darauf zu reagieren, sehr unterschiedlich entwickelt. Deshalb muss das generelle Cybersicherheitsniveau durch kohärente und einheitliche Regeln verbessert werden.

Fortschritte gab es **im Bereich der Informationssicherheit**, wo die **Vorschriften für den Schutz von EU-Verschlusssachen und von nicht als Verschlusssache eingestuften vertraulichen Informationen** kohärenter gestaltet wurden. Gleichwohl sind die Systeme für die Behandlung von Verschlusssachen noch immer nur zum Teil interoperabel, was die reibungslose Informationsübermittlung zwischen den verschiedenen Einrichtungen erschwert. Weitere Fortschritte sind notwendig, um zu einem interinstitutionellen Ansatz für den Umgang mit EU-Verschlusssachen und nicht als Verschlusssache eingestuften vertraulichen Informationen zu gelangen, der dann auch als Modell für die Interoperabilität zwischen den Mitgliedstaaten dienen könnte. Außerdem sollte eine gemeinsame Grundlage geschaffen werden, um die Verfahren mit den Mitgliedstaaten zu vereinfachen. Die EU sollte auch ihre

Fähigkeit, mit den einschlägigen Partnern sicher zu kommunizieren, weiterentwickeln und dabei so weit wie möglich auf bestehenden Regelungen und Verfahren aufbauen.

Die Kommission wird deshalb **2021,** wie in der Strategie für die Sicherheitsunion angekündigt, **gemeinsame verbindliche Vorschriften zur Informationssicherheit sowie zur Cybersicherheit für alle Organe, Einrichtungen und sonstigen Stellen der EU** vorschlagen und sich dabei auf die laufenden interinstitutionellen EU-Beratungen über Cybersicherheit[118] stützen.

Die aktuellen und künftigen Entwicklungen im Bereich der Telearbeit werden auch zusätzliche Investitionen in sichere Ausrüstungen, Infrastrukturen und Instrumente erforderlich machen, damit vertrauliche und als Verschlusssache eingestufte Dossiers auch in Telearbeit bearbeitet werden können.

Höhere Investitionen sind auch deshalb notwendig, weil die Cyberbedrohungen zunehmend feindseliger werden und die Organe, Einrichtungen und sonstigen Stellen der EU immer häufiger komplexen Cyberangriffen ausgesetzt sind und deshalb einen hohen Grad an „Cyberreife“ erreichen müssen. Derzeit wird für alle Organe, Einrichtungen und sonstigen Stellen der EU ein Programm zur Sensibilisierung für Cyberfragen eingerichtet, um das Bewusstsein des Personals zu schärfen, die Cyberhygiene zu verbessern und eine gemeinsame Kultur der Cybersicherheit zu fördern.

Das CERT-EU muss durch einen verbesserten Finanzierungsmechanismus gestärkt werden, damit es den Organen, Einrichtungen und sonstigen Stellen der EU besser dabei helfen kann, die neuen Cybersicherheitsvorschriften anzuwenden und ihre Abwehrfähigkeit gegenüber Cyberangriffen zu verbessern. Das Mandat des CERT-EU muss ebenfalls gestärkt werden, um es mit stabilen Mitteln für die Erreichung dieser Ziele auszustatten.

Strategische Initiativen

1. Verordnung über die Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der EU,
2. Verordnung über gemeinsame Cybersicherheitsvorschriften für die Organe, Einrichtungen und sonstigen Stellen der EU,
3. neue Rechtsgrundlage für das CERT-EU zur Stärkung seines Mandats und seiner Finanzausstattung.

IV. SCHLUSSFOLGERUNGEN

Die konzertierte Umsetzung dieser Strategie wird zu einer digitalen Dekade der Cybersicherheit in der EU, zur Verwirklichung einer Sicherheitsunion sowie zur Stärkung der Position der EU in der Welt beitragen.

Die EU sollte Standards und Normen für erstklassige Cybersicherheitslösungen und Cybersicherheitsstandards für wesentliche Dienste und kritische Infrastrukturen sowie für die Entwicklung und Anwendung neuer Technologien vorantreiben. Jede Organisation und jede

[118] Regelmäßige interinstitutionelle Gespräche der EU über Cybersicherheit sind Teil eines umfassenderen Austauschs über die Chancen und Herausforderungen, die der digitale Wandel für die EU-Organe mit sich bringt.

Person, die das Internet nutzt, ist Teil der Lösung für einen digitalen Wandel, bei dem die Cybersicherheit gewahrt bleibt.

Die Kommission und der Hohe Vertreter werden im Rahmen ihrer jeweiligen Zuständigkeiten die Fortschritte bei der Umsetzung dieser Strategie überwachen und Evaluierungskriterien entwickeln. Bei dieser Überwachung sollten auch die Berichte der ENISA sowie die regelmäßigen Berichte der Kommission über die Sicherheitsunion berücksichtigt werden. Die Ergebnisse werden zur Verwirklichung der Ziele der anstehenden Digitalen Dekade beitragen[119]. Im Rahmen ihrer jeweiligen Zuständigkeiten werden die Kommission und der Hohe Vertreter weiter mit den Mitgliedstaaten zusammenarbeiten, um gegebenenfalls praktische Maßnahmen zu ermitteln, mit denen die vier Cybersicherheitskreise in der EU – kritische Infrastrukturen und Resilienz des Binnenmarkts, Justiz und Strafverfolgung, Cyberdiplomatie und Cyberabwehr – einander nähergebracht werden können. Darüber hinaus werden die Kommission und der Hohe Vertreter ihre Zusammenarbeit mit der Multi-Stakeholder-Gemeinschaft fortsetzen und betonen, dass auch alle, die das Internet nutzen, ihren Beitrag zur Aufrechterhaltung eines globalen, offenen, stabilen und sicheren Cyberraums leisten müssen, in dem alle ihr digitales Leben in Sicherheit führen können.

[119] Wie im Arbeitsprogramm 2021 der Kommission angekündigt.

Anlage: Nächste Schritte zur Gewährleistung der Cybersicherheit von 5G-Netzen

Gestützt auf die Ergebnisse der Überarbeitung der Kommissionsempfehlung zur Cybersicherheit von 5G-Netzen[120] sollten sich die nächsten Schritte der auf EU-Ebene koordinierten Arbeiten auf drei Hauptziele sowie auf zentrale kurz- und mittelfristige Maßnahmen konzentrieren, die in der nachstehenden Tabelle aufgeführt sind und von den Behörden der Mitgliedstaaten, der Kommission und der ENISA umgesetzt werden sollten.

In der nächsten Phase geht es zunächst darum, **das Instrumentarium auf nationaler Ebene vollständig umzusetzen und die im Fortschrittsbericht vom Juli 2020 aufgezeigten Probleme in Angriff zu nehmen**. In dieser Hinsicht käme einigen der strategischen Maßnahmen des Instrumentariums eine **verstärkte Koordinierungsarbeit oder ein besserer Informationsaustausch** im Rahmen der NIS-Kooperationsgruppe – wie im Fortschrittsbericht bereits angesprochen – zugute, woraus unter Umständen **bewährte Verfahren oder Leitfäden** hervorgehen könnten. Bei den technischen Maßnahmen könnte die ENISA weitere Unterstützung leisten, indem sie – aufbauend auf der bereits geleisteten Arbeit – bestimmte Aspekte eingehender untersucht und **einen umfassenden Überblick über alle einschlägigen Leitlinien zu den für Mobilfunknetzbetreiber geltenden Anforderungen an die Cybersicherheit von 5G-Netzen erstellt**.

Zweitens betonten die Mitgliedstaaten, wie wichtig es ist, stets auf der Höhe der Zeit zu sein und die **Entwicklungen in den Bereichen Technologie, 5G-Architektur, Bedrohungen, Anwendungs- und Einsatzmöglichkeiten im 5G-Bereich sowie externe Faktoren kontinuierlich zu verfolgen**, damit **neue oder entstehende Risiken erkannt und bewältigt** werden können. Darüber hinaus sollten in der ersten Risikoanalyse mehrere Aspekte näher untersucht werden, insbesondere um sicherzustellen, dass sich die Analyse auf das gesamte 5G-Ökosystem mit allen relevanten Teilen der Netzinfrastruktur und der 5G-Lieferkette erstreckt. Obwohl das Instrumentarium flexibel und anpassungsfähig ausgelegt ist, könnte es bei Bedarf mittelfristig erweitert oder geändert werden, damit es stets umfassend und aktuell bleibt.

Drittens sollten **weitere Maßnahmen auf EU-Ebene** ergriffen werden, um die Ziele des Instrumentariums zu verwirklichen und zu ergänzen und sie vollständig in die einschlägigen Strategien der Union und der Kommission zu integrieren. Dabei geht es vor allem um die Maßnahmen, die von der Kommission in ihrer Mitteilung über das Instrumentarium vom 29. Januar 2020[121] für eine Vielzahl von Bereichen angekündigt wurden (EU-Mittel für sichere 5G-Netze, Investitionen in die 5G-Technik und deren Folgetechnik, handelspolitische Schutzinstrumente und Wettbewerb zur Vermeidung von Verzerrungen auf dem 5G-Zuliefermarkt u. a.).

Die federführenden Akteure sollten gegebenenfalls Anfang 2021 die genauen Regelungen und Etappenziele für die nachstehend genannten zentralen Maßnahmen vereinbaren.

[120] Bericht der Kommission über die Auswirkungen ihrer Empfehlung 2019/534 vom 26. März 2019 zur Cybersicherheit von 5G-Netzen.

[121] Mitteilung der Kommission „Sichere 5G-Einführung in der EU – Umsetzung des EU-Instrumentariums“ vom 29. Januar 2020, COM(2020) 50 final.

Hauptziel 1: Einheitliche nationale Ansätze für eine wirksame Risikominderung in der gesamten EU		
Bereiche	**Zentrale kurz- und mittelfristige Maßnahmen**	**Federführende Akteure**
Umsetzung des Instrumentariums durch die Mitgliedstaaten	Vollständige Umsetzung der in den Schlussfolgerungen zum Instrumentarium empfohlenen Maßnahmen bis zum zweiten Quartal 2021 mit regelmäßiger Bestandsaufnahme im Rahmen der NIS-Kooperationsgruppe.	Behörden der Mitgliedstaaten
Austausch von Informationen und bewährten Verfahren zu strategischen Maßnahmen in Bezug auf Anbieter	Verstärkter Informationsaustausch und Prüfung möglicher bewährter Verfahren, insbesondere in Bezug auf: - Beschränkungen für Hochrisikoanbieter (SM03) und Maßnahmen im Zusammenhang mit der Erbringung verwalteter Dienste (SM04); - Sicherheit und Widerstandsfähigkeit der Lieferkette, insbesondere im Nachgang zur GEREK-Erhebung über SM05-SM06.	Behörden der Mitgliedstaaten, Kommission
Kapazitätsaufbau und Leitlinien für technische Maßnahmen	Durchführung gezielter technischer Analysen und Entwicklung gemeinsamer Leitlinien und Instrumente, darunter: - eine umfassende dynamische Matrix von Sicherheitskontrollen und bewährten Verfahren für 5G-Sicherheit; Leitlinien im Hinblick auf die Umsetzung ausgewählter technischer Maßnahmen des Instrumentariums.	ENISA, Behörden der Mitgliedstaaten
Hauptziel 2: Unterstützung von kontinuierlichem Wissensaustausch und Kapazitätsaufbau		
Bereiche	**Zentrale kurz- und mittelfristige Maßnahmen**	**Federführende Akteure**
Kontinuierlicher Wissensaufbau	Organisation von Tätigkeiten zum Wissensaufbau über die Technik und damit verbundene Herausforderungen (offene Architekturen, 5G-Merkmale wie Virtualisierung, Containerisierung, Slicing), Entwicklung der Bedrohungslage, reale Vorfälle usw.	ENISA, Behörden der Mitgliedstaaten, sonstige Interessenträger
Risikobewertungen	Aktualisierung und Austausch von Informationen über aktuelle nationale Risikobewertungen	Behörden der Mitgliedstaaten, Kommission, ENISA
Gemeinsame EU-finanzierte Projekte zur Unterstützung der Umsetzung des Instrumentariums	Finanzielle Unterstützung von Projekten, mit denen die Umsetzung des Instrumentariums mit EU-Mitteln gefördert wird, insbesondere im Rahmen des Programms „Digitales Europa“ (z. B. Kapazitätsaufbauprojekte für nationale Behörden, Versuchsfelder oder andere weit entwickelte Kapazitäten)	Behörden der Mitgliedstaaten, Kommission
Zusammenarbeit der Interessenträger	Förderung der Zusammenarbeit der mit 5G-Cybersicherheit befassten nationalen Behörden (z. B. NIS-Kooperationsgruppe, für Cybersicherheit zuständige Behörden, Regulierungsbehörden im Bereich der Telekommunikation) und mit privaten Interessenträgern	Behörden der Mitgliedstaaten, Kommission, ENISA
Hauptziel 3: Förderung einer widerstandsfähigen Lieferkette und anderer strategischer Sicherheitsziele der EU		

Bereiche	**Zentrale kurz- und mittelfristige Maßnahmen**	**Federführende Akteure**
Normung	Festlegung und Umsetzung eines konkreten Aktionsplans für eine stärkere Vertretung der EU in Normungsgremien im Rahmen der anstehenden Arbeiten der NIS-Untergruppe für Normung. Ziel ist die Erreichung spezifischer Sicherheitsziele, u. a. die Förderung interoperabler Schnittstellen, um eine Diversifizierung der Anbieter zu fördern.	Behörden der Mitgliedstaaten
Widerstandsfähigkeit der Lieferkette	- Gründliche Analyse des 5G-Ökosystems und der zugehörigen Lieferkette, um wichtige Anlagen und potenzielle kritischen Abhängigkeiten besser ermitteln und überwachen zu können; - Gewährleistung eines funktionierenden 5G-Markts und der zugehörigen Lieferkette im Einklang mit den Handels- und Wettbewerbsvorschriften und -zielen der EU gemäß der Mitteilung der Kommission vom 29. Januar; Anwendung des FDI-Mechanismus (Überprüfung ausländischer Direktinvestitionen) bei geplanten Investitionen, die die 5G-Wertschöpfungskette betreffen könnten, wobei den Zielen des Instrumentariums Rechnung zu tragen ist; - Beobachtung bestehender und sich abzeichnender Marktrends sowie Bewertung der Risiken und Chancen bei OpenRAN, u. a. in einer unabhängigen Studie.	Behörden der Mitgliedstaaten, Kommission
Zertifizierung	Beginn der Vorbereitungen in Bezug auf (ein) geeignete(s) Zertifizierungssystem(e) für wichtige 5G-Komponenten und auf Verfahren der Anbieter, um bestimmte Risiken im Zusammenhang mit technischen Schwachstellen, wie sie in den Risikominderungsplänen des Instrumentariums aufgeführt sind, besser zu bewältigen.	Kommission, ENISA, nationale Behörden, sonstige Interessenträger
EU-Kapazitäten und sicherer Netzausbau	- Investitionen in FuI und Kapazitäten, insbesondere durch Schaffung der Partnerschaft „Intelligente Netze und Dienste“; - Anwendung der einschlägigen Sicherheitsbedingungen in den Finanzierungsprogrammen und -instrumenten der EU (intern und extern) gemäß der Mitteilung der Kommission vom 29. Januar.	Mitgliedstaaten, Kommission, Akteure der 5G-Wirtschaft
Externe Aspekte	Positive Beantwortung von Anfragen aus Drittländern, die das Toolbox-Konzept der EU nachvollziehen und gegebenenfalls anwenden wollen.	Mitgliedstaaten, Kommission EAD, EU-Delegationen