Rat der
Europäischen Union

Brüssel, den 9. August 2021
(OR. en)

10137/1/21
REV 1

CYBER 181	**RECH 321**
JAI 773	**COMPET 510**
JAIEX 79	**IND 180**
EJUSTICE 67	**COTER 78**
COSI 128	**ENFOPOL 244**
DATAPROTECT 173	**COPS 249**
COPEN 289	**MI 501**
TELECOM 272	**IXIM 129**
PROCIV 78	**POLMIL 98**
CSC 255	**HYBRID 36**
CIS 82	**CSCI 95**
RELEX 590	**POLGEN 112**

ÜBERMITTLUNGSVERMERK

Nr. Komm.dok.:	JOIN(2021) 14 final/2
Betr.:	GEMEINSAME MITTEILUNG AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT Bericht über die Umsetzung der Cybersicherheitsstrategie der EU für die digitale Dekade

Die Delegationen erhalten in der Anlage das Dokument JOIN(2021) 14 final/2.

Anl.: JOIN(2021) 14 final/2

EUROPÄISCHE
KOMMISSION

HOHER VERTRETER
DER UNION FÜR
AUSSEN- UND
SICHERHEITSPOLITIK

Brüssel, den 6.8.2021
JOIN(2021) 14 final/2

CORRIGENDUM
This document corrects document JOIN(2021) 14 final of 23.6.2021
Concerns all language versions.
Removal of the institutional reference 2021/0166 (NLE).
The text shall read as follows:

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

Bericht über die Umsetzung der 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

Bericht über die Umsetzung der Cybersicherheitsstrategie der EU für die digitale Dekade

I. Abwehrfähigkeit gegen Cyberangriffe, operative Kapazitäten und Offenheit sind wichtiger denn je

Cybersicherheit ist für den Einsatz intelligenterer und umweltfreundlicherer Technik in der Welt nach der Pandemie unerlässlich. Sie ist für die Sicherheit der EU insgesamt unverzichtbar und bildet einen Pfeiler der Sicherheitsunion. Die soziale, politische und wirtschaftliche Entwicklung erfordert technologische Souveränität und einen globalen, offenen und sicheren Cyberraum, der auf Rechtsstaatlichkeit und auf der Achtung der Menschenrechte und Grundfreiheiten beruht. Dies war die zentrale Prämisse der Gemeinsamen Mitteilung der Kommission und des Hohen Vertreters für Außen- und Sicherheitspolitik über die Cybersicherheitsstrategie der EU für die digitale Dekade, die am 16. Dezember 2020 angenommen wurde[1]. Alle kritischen Einrichtungen können Opfer von Cyberangriffen werden. Die Entwicklungen in den vergangenen sechs Monaten haben verdeutlicht, dass der Schwerpunkt der Strategie auf der Beschleunigung rechtlicher Reformen, auf Investitionen und auf einer gemeinsamen operativen Reaktion liegen muss.

Die jüngsten Cyberangriffe haben insbesondere die zunehmende Verbreitung von Ransomware und Cyberspionage und die davon ausgehenden, wachsenden Gefahren für alle Wirtschaftszweige und die Gesellschaft insgesamt deutlich gemacht. Das Ausmaß der Sicherheitsvorfälle war außergewöhnlich hoch: so waren von den Angriffen auf Microsoft Exchange Hunderttausende Server betroffen; von der SolarWinds-Orion-Kampagne waren potenziell 18 000 Organisationen betroffen; beim Ransomware-Angriff auf den irischen Gesundheitsdienst wurden sensible Daten Hunderter Patienten erbeutet und medizinische Dienstleistungen gestört; der Cyberangriff auf das Abrechnungssystem von Colonial Pipeline führte zu einem Kraftstoffnotstand und massivem Datendiebstahl; und beim weltweit größten Rindfleischlieferanten wurde eine Betriebsunterbrechung verursacht[2]. Auch wenn das volle Ausmaß der entstandenen Schäden nach wie vor unklar ist, verdeutlicht jeder dieser Vorfälle, welche weitreichenden Folgen die böswillige Ausnutzung von Schwachstellen in Produkten, Diensten, Systemen und Netzen der Informations- und Kommunikationstechnik nach sich

[1] Gemeinsame Mitteilung an das Europäische Parlament und den Rat – Die Cybersicherheitsstrategie der EU für die digitale Dekade, JOIN(2020) 18.

[2] Solarwinds, ein großes US-amerikanisches IT-Unternehmen, war 2020 Opfer eines Cyberangriffs, der sich über seine Kunden ausbreitete und monatelang unentdeckt blieb, wodurch die Hacker Zugang zu Tausenden von Unternehmen und Behörden erhielten, die die Orion-Plattform nutzten, darunter auch sechs Organe, Einrichtungen und sonstige Stellen der EU. Ab Januar 2021 wurde eine Reihe bislang unbekannter Schwachstellen (*Zero-Day-Exploits*) im Microsoft Exchange Server entdeckt, von denen E-Mail-Systeme in aller Welt betroffen sind. Im Mai war die Verwaltung des Gesundheitsdienstes (*Health Service Executive*) der Republik Irland einem Angriff ausgesetzt, der sich beträchtlich auf die Dienstkontinuität auswirkte. Colonial Pipeline, der größte US-amerikanische Kraftstoff-Fernleitungsnetzbetreiber, musste den Betrieb am 7. Mai einstellen, nachdem infolge eines Cyberangriffs seine wichtigsten IT-Systeme ausgefallen waren, und im Juni 2021 wurde JBS USA Holdings Inc., die US-amerikanische Zweigniederlassung des weltweit umsatzstärksten Fleischlieferanten erfolgreich mit Ransomware angegriffen, was schwere Betriebsstörungen verursachte.

ziehen kann. Es ist davon auszugehen, dass die Wirkung und Häufigkeit solcher Cyberangriffe weiter zunehmen wird und dass dadurch unsere Sicherheit gefährdet wird.

Deshalb ist es wichtig, dass die Europäische Union – wie in der Strategie dargelegt – nun schnell Fortschritte in allen Bereichen erzielt – legislativ, operativ, bei Investitionen und auf diplomatischem Parkett. Die Vorschläge für eine Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Cybersicherheitsniveaus in der Union („NIS2-Richtlinie“)[3], für eine Richtlinie über die Resilienz kritischer Einrichtungen[4] und für eine Verordnung und eine Richtlinie über die Betriebsstabilität digitaler Systeme[5] sollten daher so bald wie möglich verabschiedet werden. In diesem Zusammenhang kommt es darauf an, einen ehrgeizigen Ansatz insbesondere in Bezug auf Lieferketten zu verfolgen, denn die jüngsten Cyberangriffe waren auf Schwachstellen bei Software-Anbietern zurückzuführen, und Maßnahmen zu ergreifen, um die Behörden widerstandsfähiger zu machen und das rasche Melden von Sicherheitsvorfällen sicherzustellen. So ist es dringlicher denn je, ein Netz von Sicherheitseinsatzzentren („SOCs“) zur frühzeitigen Erkennung von Anzeichen für Cyberangriffe einzurichten und eine glaubwürdige, wirksame und kollektive Reaktionsfähigkeit der EU zur Abwehr großer Sicherheitsvorfälle – auch auf operativer Ebene – im Rahmen der Gemeinsamen Cyber-Einheit[6] aufzubauen. Angesichts der Zunahme von Cyberangriffen durch staatliche oder staatlich veranlasste Akteure muss weiterhin auf ein verantwortungsvolles staatliches Verhalten hingewirkt werden, und zwar sowohl innerhalb der Vereinten Nationen als auch durch Cyberdialoge und einen strukturierten Austausch mit regionalen Organisationen, einschließlich der Afrikanischen Union, des ASEAN-Regionalforums, der Organisation Amerikanischer Staaten (OAS) und der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE), sowie durch ein wirksames diplomatisches Einwirken, um böswilligen Handlungen im Cyberraum vorzubeugen, sie zu verhindern, davor abzuschrecken und darauf zu reagieren. Besondere Bedeutung kommt dabei der Zusammenarbeit mit gleich gesinnten Drittländern und den Prioritäten der transatlantischen Agenda zu. So sollten insbesondere Möglichkeiten der Zusammenarbeit zwischen der EU und den USA bei bestimmten Aspekten der Cybersicherheit weiter geprüft werden, auch im Hinblick auf den Informationsaustausch und die Bekämpfung von Ransomware.

II. Überblick über die ersten sechs Monate der Umsetzung

Eine Reihe strategischer Maßnahmen ist bereits weit fortgeschritten.

II.1 Resilienz, technologische Souveränität und Führungsrolle

In aller Welt sind Lieferketten und kritische Infrastrukturen heute ständig von Cyberangriffen bedroht, sogar Krankenhäuser im Kampf gegen die COVID-19-Pandemie. Die Kommission unterstützt die beiden Gesetzgeber bei der zügigen Verabschiedung der vorgeschlagenen Überarbeitung der NIS-Richtlinie, mit der ihr Anwendungsbereich insbesondere auf das Gesundheitswesen, einschließlich Forschungslabors und Herstellung wichtiger medizinischer

[3] Vorschlag für eine Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Cybersicherheitsniveaus in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148, COM(2020) 823.
[4] Vorschlag für eine Richtlinie über die Resilienz kritischer Einrichtungen, COM(2020) 829.
[5] Vorschlag für eine Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors 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; Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinien 2006/43/EG, 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 und (EU) 2016/2341, COM(2020) 596.
[6] [Empfehlung zur Gemeinsamen Cyber-Einheit].

Geräte und Arzneimittel, und auf neue Tätigkeiten im Energiesektor wie Wasserstofferzeugung, Fernwärme, Stromerzeugung und zentrale Erdölbevorratung ausgeweitet werden soll.

Die Verordnung zur Einrichtung des Kompetenzzentrums für Cybersicherheit und des Netzes nationaler Koordinierungszentren wurde am 20. Mai 2021 angenommen[7]. Sie wird Ressourcen der EU, der Mitgliedstaaten und der Industrie bündeln, um die technologischen und industriellen Cybersicherheitskapazitäten zu verbessern und auszubauen und die offene strategische Autonomie der EU zu stärken. Außerdem soll so eine Möglichkeit geschaffen werden, einen Teil der Tätigkeiten im Bereich der Cybersicherheit, die im Rahmen der Programme Horizont Europa und Digitales Europa und der Aufbau- und Resilienzfazilität finanziert werden, zu konsolidieren – dies betrifft Finanzmittel in Höhe von insgesamt bis zu 4,5 Mrd. EUR über die nächsten sechs Jahre[8]. Unterstützt werden soll dadurch auch bis 2023 die Entwicklung eines EU-Cyberschutzschilds zur Früherkennung von Cyberangriffen, das aus einem Netz von Sicherheitseinsatzzentren bestehen wird, die öffentlich oder privat sein können und auf künstlicher Intelligenz beruhende Instrumente einsetzen werden. Mehrere Mitgliedstaaten sehen den Aufbau solcher nationalen Zentren im Rahmen ihrer jeweiligen Aufbau- und Resilienzpläne vor. Die Kommission wird diese Bemühungen durch die Zuweisung von Mitteln aus dem Programm Digitales Europa ergänzen und deren schrittweise Einbindung unterstützen. Die Finanzierungsprogramme werden auch die EuroQCI-Initiative zum Aufbau einer sicheren Quantenkommunikationsinfrastruktur[9] unterstützen, die sich über die gesamte EU einschließlich ihrer überseeischen Gebiete erstrecken und die beste Kombination aus boden- und weltraumgestützter Technik einsetzen wird, ebenso wie eine besondere Haushaltslinie zur Steigerung der Widerstandsfähigkeit des Gesundheitswesens gegenüber Cyberangriffen.

Die Gewährleistung der Cybersicherheit der 5G-Netze ist ein kontinuierlicher Prozess, der die schrittweise 5G-Einführung und die Umsetzung des EU-Instrumentariums für die 5G-Cybersicherheit[10] begleiten wird. Die meisten Mitgliedstaaten verfügen bereits – oder demnächst – über einen Rahmen für die Auferlegung angemessener Beschränkungen für 5G-Anbieter. Die Anforderungen an Mobilfunknetzbetreiber werden mit der Umsetzung des europäischen Kodex für die elektronische Kommunikation in nationales Recht weiter verschärft. Gleichzeitig arbeitet die EU-Cybersicherheitsagentur (ENISA) derzeit an einem Vorschlag für ein EU-System für die Cybersicherheitszertifizierung von 5G-Netzen[11]. Im Hinblick auf neue Trends und Entwicklungen in der 5G-Lieferkette haben die Behörden der Mitgliedstaaten beschlossen, im Rahmen des EU-Instrumentariums eine gründliche Analyse

---

[7] Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren.

[8] Das Kompetenzzentrum für Cybersicherheit wird dabei vor allem über die Verwendung der für Cybersicherheit vorgesehenen Mittel der Programme Digitales Europa und Horizont Europa sowie der Mitgliedstaaten entscheiden und deren Verwaltung übernehmen.

[9] https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network

[10] Bericht über die Auswirkungen der Empfehlung der Kommission vom 26. März 2019 zur Cybersicherheit der 5G-Netze, SWD(2020) 357 final, 16. Dezember 2020.

[11] Die Ausarbeitung des Systems erfolgt mit Unterstützung der NIS-Kooperationsgruppe gemäß Artikel 48 des Rechtsakts zur Cybersicherheit; Verordnung (EU) 2019/881 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. https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-commission-requests-eu-cybersecurity-agency-develop-certification.

der Auswirkungen offener, disaggregierter und interoperabler Netztechnik (Open RAN) auf die Sicherheit einzuleiten. Die Ergebnisse dieser Arbeiten werden ein weiterer Beitrag zum abgestimmten Vorgehen bei der Sicherheit von 5G-Netzen sein.

Es bedarf noch größerer Anstrengungen, insbesondere im Rahmen des Aktionsplans der EU für digitale Bildung, um den massiven Fachkräftemangel zu beheben, der Prognosen zufolge bis 2022 weltweit auf fast zwei Millionen unbesetzte Stellen im Bereich der Cybersicherheit ansteigen wird, davon 350 000 unbesetzte Stellen allein in Europa, und um die gravierende Unterrepräsentation von Frauen in der IKT-Branche zu beheben die weltweit nur 11 % und in Europa noch weniger (7 %) der Arbeitskräfte im Bereich der Cybersicherheit ausmachen[12]. Bei anderen laufenden Politikinitiativen geht es um Vorarbeiten für künftige Initiativen zur Sicherheit des Internets der Dinge, um Normen für das Internet und um den Aufbau eines gemeinnützigen Dienstes zur Auflösung von Domänennamen (DNS4EU).

II.2 Aufbau operativer Kapazitäten zur Prävention, Abschreckung und Reaktion

Angesichts der Zunahme staatlicher und staatlich veranlasster Angriffe, aber auch krimineller Angriffe auf Netze und Informationssysteme und zunehmender Abhängigkeit von Datenbanken, die sensible Informationen enthalten, muss die EU ihre Cybergemeinschaften engmaschiger miteinander vernetzen. Diese müssen in abgestimmter Weise auf die zivilen, kriminellen, diplomatischen und verteidigungspolitischen Aspekte groß angelegter Cyberangriffe reagieren, wie sie in jüngster Zeit in vielen sensiblen Wirtschaftszweigen zu beobachten sind. Es sind daher Anstrengungen aller Gemeinschaften nötig, um die vier Schritte zu vollziehen, die in der zusammen mit diesem Bericht abgegebenen Empfehlung der Kommission für die Einrichtung der Gemeinsamen Cyber-Einheit als Mechanismus für die weitere Koordinierung und die Schließung von Lücken bei der Reaktion der EU auf Cyberbedrohungen dargelegt worden sind[13]. Im Zuge der Bekämpfung der Cyberkriminalität wurde eine politische Einigung über die befristete Verordnung zur Bekämpfung des sexuellen Missbrauchs von Kindern im Internet erzielt, die in Kürze zu Annahme ansteht[14], und die Notwendigkeit, die Strafverfolgungsbehörden mit den digitalen Instrumenten auszustatten, die sie benötigen, in den Mittelpunkt der neuen Strategie der Kommission zur Bekämpfung der organisierten Kriminalität[15] gestellt. Außerdem nahm die Kommission im Februar 2020 einen Aktionsplan für Synergien zwischen der zivilen, der Verteidigungs- und der Weltraumindustrie an, der ein neues Vorzeigeprojekt für den Aufbau eines sicheren weltraumgestützten globalen Konnektivitätssystems der EU vorsieht. Es soll „Hochgeschwindigkeitsanbindungen für jedermann in Europa zugänglich machen und für ein widerstandsfähiges Konnektivitätssystem sorgen, das es Europa ermöglicht, unter allen Umständen die Anbindung nicht zu verlieren“[16].

---

[12] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_de

[13] [Die Gemeinsame Cyber-Einheit würde eine koordinierte Reaktion auf große Cybervorfälle und -krisen und anschließende Folgenbewältigung ermöglichen und dazu beitragen, dass Ressourcen für die Unterstützung mobilisiert werden. Sie würde sich auf Experten aus allen Cybersicherheitsbereichen stützen, um eine gemeinsame Lageerfassung und die erforderliche Vorsorge und Abwehrbereitschaft zu gewährleisten. Außerdem würde sie auf Anfrage eines oder mehrerer Mitgliedstaaten die Unterstützungsmechanismen koordinieren.]

[14] https://www.europarl.europa.eu/news/de/press-room/20210430IPR03213/provisional-agreement-on-temporary-rules-to-detect-and-remove-online-child-abuse

[15] EU-Strategie zur Bekämpfung der organisierten Kriminalität 2021–2025, COM(2021) 170, 14.4.2021.

[16] COM(2021) 70 vom 22.2.2021.

Aus internationaler Sicht bereitet der Hohe Vertreter im Einklang mit den im strategischen Kompass[17] gesteckten Zielen derzeit die Überprüfung des Politikrahmens für die Cyberabwehr vor, deren Ergebnisse den Mitgliedstaaten im zweiten Halbjahr 2021 vorgelegt werden sollen. Der Hohe Vertreter arbeitet an der Verbesserung der Fähigkeit der EU, böswilligen Cyberaktivitäten vorzubeugen, sie zu verhindern, davor abzuschrecken und darauf zu reagieren, auch durch eine verstärkte internationale Zusammenarbeit. Am 17. Mai 2021 veranstaltete der Europäische Auswärtige Dienst (EAD) in Zusammenarbeit mit dem portugiesischen Ratsvorsitz und dem Institut der Europäischen Union für Sicherheitsstudien (EUISS) eine szenariobasierte Diskussion mit EU-Mitgliedstaaten und internationalen Partnern, um das gegenseitige Verständnis der jeweiligen diplomatischen Ansätze für die Vorbeugung, Verhinderung, Abschreckung und Reaktion auf böswillige Cyberaktivitäten zu verbessern und diesbezüglich Möglichkeiten für eine weitere Verstärkung der internationalen Zusammenarbeit zu ermitteln[18]. Um das Instrumentarium der EU für die Cyberdiplomatie weiter zu verbessern, sammelt der EAD Erkenntnisse und Erfahrungen und kann dementsprechend die Leitlinien zur Umsetzung des Rahmens für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten überprüfen.

Wie in der Cybersicherheitsstrategie der EU für das digitale Jahrzehnt angekündigt, veranlasst die Kommission eine Untersuchung zur Entwicklung von Aufklärungsinstrumenten, mit denen, die Abwehrbereitschaft und Widerstandsfähigkeit von EU-Unternehmen gegen Cyberdiebstahl geistigen Eigentums gestärkt werden soll[19]. Darüber hinaus intensivierte die Kommission die Durchsetzungsmaßnahmen im Zusammenhang mit der Richtlinie 2013/40/EU über Angriffe auf Informationssysteme und leitete im Juni 2021 weitere Vertragsverletzungsverfahren gegen mehrere Mitgliedstaaten ein[20]. Gegebenenfalls wird die Kommission weitere Maßnahmen in Erwägung ziehen. Ebenfalls von großer Bedeutung wird die Verbesserung der verfügbaren Cybersicherheitskompetenzen unter den Arbeitskräften in der EU sein. Daher wird das Kompetenzzentrum für Cybersicherheit diesbezüglich wichtige Maßnahmen ergreifen, um das Wissen und die Kapazitäten zu verbessern und die Entwicklung fachübergreifender Kompetenzen im Bereich der Cybersicherheit zu fördern.

II.3 Förderung eines globalen offenen Cyberraums

Die Bedrohungslage wird durch geopolitische Spannungen in Bezug auf das globale und offene Internet und die Technologien entlang der gesamten Lieferkette noch verschärft. Beschränkungen im und in Bezug auf das Internet, die Zunahme von böswilligen Cyberaktivitäten und von Vorgängen, die die Sicherheit und Integrität von Produkten und Diensten der Informations- und Kommunikationstechnik beeinträchtigen, stellen eine Bedrohung für einen globalen und offenen Cyberraum sowie für die Rechtsstaatlichkeit, die Menschenrechte, die Grundfreiheiten und die demokratischen Werte dar. Daher arbeitet der Hohe Vertreter gemeinsam mit den Mitgliedstaaten darauf hin, das verantwortungsvolle staatliche Handeln im Cyberraum voranzubringen, insbesondere durch die Einrichtung eines Aktionsprogramms zur Förderung verantwortungsvollen staatlichen Handelns auf Ebene der Vereinten Nationen, zusammen mit den 53 weiteren Geldgebern, aufbauend auf der

[17] Schlussfolgerungen des Rates vom 17. Juni 2020 zu Sicherheit und Verteidigung (8910/20).
[18] https://eeas.europa.eu/headquarters/headquarters-homepage/98588/cyberspace-strengthening-cooperation-promoting-security-and-stability_de
[19] COM(2020) 760 vom 25.11.2020.
[20] Die betreffenden Mitgliedstaaten sind Belgien, Österreich, die Tschechische Republik, Estland, Luxemburg, Polen und Schweden.

Empfehlung des Konsensberichts vom 12. März 2021 der offenen Arbeitsgruppe der Vereinten Nationen für Entwicklungen auf dem Gebiet der Information und Telekommunikation im Kontext der internationalen Sicherheit[21]. Die EU arbeitet an der Stärkung und Ausweitung der Beziehungen zu Drittländern, internationalen und regionalen Organisationen sowie der Multi-Stakeholder-Gemeinschaft durch Cyberdialoge – wie in der Strategie dargelegt – und durch die Einrichtung eines EU-Netzes für Cyberdiplomatie. Darüber hinaus wird das EU-Gremium für den Cyberkapazitätsaufbau[22] eingerichtet, das es den Organen, Einrichtungen und sonstigen Stellen der EU ermöglichen wird, die externen Bemühungen der EU zum Aufbau von Cyberkapazitäten besser zu koordinieren und besser zusammenzuarbeiten.

Im Rahmen der Vereinten Nationen billigte die Generalversammlung der VN am 26. Mai 2021 die Modalitäten für die Arbeit des mit der Resolution 74/247 eingesetzten Ad-hoc-Ausschusses zur Bekämpfung des Einsatzes von Informations- und Kommunikationstechnik für kriminelle Zwecke[23]. Die schließlich angenommenen Modalitäten enthalten wichtige Elemente zur Gewährleistung inklusiver Entscheidungsverfahren und einer stärkeren Beteiligung der Zivilgesellschaft an den Arbeiten des Ad-hoc-Ausschusses. Die erste Verhandlungsrunde des Prozesses, der zu einem neuen VN-Übereinkommen führen soll, wird im Januar 2022 in New York stattfinden.

Auf der Plenartagung des Ausschusses der Vertragsstaaten des Budapester Übereinkommens des Europarats über Computerkriminalität am 28. Mai 2021 schlossen die Vertragsstaaten die Beratungen ab und nahmen einen Textentwurf für das Zweite Zusatzprotokoll zu dem Übereinkommen[24] an, mit dem die Zusammenarbeit in Sachen Cyberkriminalität und elektronische Beweismittel bei strafrechtlichen Ermittlungen verbessert werden soll. Die Kommission nahm im Namen der EU an den Gesprächen teil[25]. Dies dürfte die Grundlage für den förmlichen Abschluss der Verhandlungen im zweiten Halbjahr 2021 und die anschließende Eröffnung des zweiten Zusatzprotokolls zur Unterzeichnung Anfang 2022 bilden.

Die EU und ihre Partner bekräftigten im Juni 2021 ihre Entschlossenheit, gemeinsam gegen die akute und eskalierende Bedrohung durch kriminelle Ransomware-Netze vorzugehen, die eine Gefahr für unsere Bürger und Unternehmen darstellen, sowie ein gemeinsames Verständnis darüber zu fördern, wie das geltende Völkerrecht im Cyberraum angewendet werden soll, und für diesen Ansatz in den Vereinten Nationen und anderen internationalen Foren zu werben. Außerdem forderte sie alle Staaten auf, kriminelle Ransomware-Netze, die von ihren Hoheitsgebieten aus operieren, umgehend zu ermitteln und zu zerschlagen und sie für ihr Handeln zur Rechenschaft zu ziehen[26].

---

[21] https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf
[22] https://www.eucybernet.eu/
[23] https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html
[24] https://rm.coe.int/0900001680a2aa42
[25] Das zweite Zusatzprotokoll zum Budapester Übereinkommen des Europarats über Computerkriminalität enthält Maßnahmen und Garantien zur Verbesserung der internationalen Zusammenarbeit zwischen Strafverfolgungs- und Justizbehörden sowie zwischen Behörden und Diensteanbietern in anderen Ländern; an seiner Aushandlung nimmt die Kommission im Namen der EU teil; Beschluss des Rates vom Juni 2019, Dok. 9116/19.
[26] Erklärung zum Gipfeltreffen EU-USA, 15. Juni 2021, https://www.consilium.europa.eu/media/50443/eu-us-summit-joint-statement-15-june-final-final.pdf. Kommuniqué des G7-Gipfels von Carbis Bay: Unsere gemeinsame Agenda für globale Maßnahmen für einen besseren Wiederaufbau, 13. Juni 2021, https://www.consilium.europa.eu/media/50361/carbis-bay-g7-summit-communique.pdf.

II.4 Cybersicherheit in den Organen, Einrichtungen und sonstigen Stellen der EU

Die EU hat die Anhebung der Standards für Cybersicherheit und Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der EU in Angriff genommen. Dazu führt die Kommission Konsultationen der Interessenträger und ein Benchmarking der derzeitigen Politik durch, damit bis Ende 2021 neue Vorschläge angenommen werden können.

III. Hintergrund dieses Berichts

Am 16. Dezember 2020 nahmen die Kommission und der Hohe Vertreter die Cybersicherheitsstrategie der EU an. Angesichts zunehmender und komplexer Bedrohungen für die europäischen Netze und Informationssysteme werden darin Prioritäten und Leitaktionen zur Verbesserung der Abwehrfähigkeit, Autonomie, Führungsstärke und operativen Kapazitäten Europas sowie zur Förderung eines globalen und offenen Cyberraums und diesbezüglicher internationaler Partnerschaften festgelegt. Die Kommission und der Hohe Vertreter sagten zu, die Fortschritte bei der Umsetzung der Strategie zu überwachen.

In seiner Erklärung vom 26. Februar 2021 forderte der Europäische Rat die Kommission und den Hohen Vertreter auf, bis Juni 2021 über die Umsetzung der Strategie Bericht zu erstatten[27]. In seinen Schlussfolgerungen vom 9. März 2021 begrüßte der Rat die Strategie und betonte, dass die Cybersicherheit für den Aufbau eines resilienten, grünen und digitalen Europas von entscheidender Bedeutung ist. Ferner rief er die Kommission und den Hohen Vertreter auf, einen detaillierten Umsetzungsplan mit den Prioritäten und dem Zeitplan für die geplanten Maßnahmen aufzustellen[28]. Die Strategie wird derzeit von den zuständigen Ausschüssen des Europäischen Parlaments geprüft, wobei die Gefahr einer fragmentierten Regulierung aber auch die Gelegenheit, die europäische Industrie im Zuge der Digitalisierung zu stärken, hervorzuheben sind[29]. Der Europäische Wirtschafts- und Sozialausschuss verabschiedete am 27. April 2021 eine Stellungnahme, in der er die Strategie als positiven Schritt zum Schutz vor globalen Cyberbedrohungen und zur Sicherung des Wirtschaftswachstums begrüßte[30].

Im vorliegenden Bericht wird auf diese Entwicklungen eingegangen und insbesondere der Aufforderung des Europäischen Rates Folge geleistet.

[27] https://www.consilium.europa.eu/media/48625/2526-02-21-euco-statement-en.pdf
[28] https://www.consilium.europa.eu/de/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/
[29] (2021/2568(RSP)).
[30] https://www.eesc.europa.eu/de/our-work/opinions-information-reports/opinions/communication-cybersecurity-strategy