Rat der
Europäischen Union

Brüssel, den 23. Juni 2021
(OR. en)

10137/21
ADD 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

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	23. Juni 2021
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	JOIN(2021) 14 final - ANNEX
Betr.:	ANHANG der Gemeinsamen 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 - ANNEX.

Anl.: JOIN(2021) 14 final - ANNEX

EUROPÄISCHE
KOMMISSION

HOHER VERTRETER
DER UNION FÜR
AUSSEN- UND
SICHERHEITSPOLITIK

Brüssel, den 23.6.2021
JOIN(2021) 14 final

ANNEX

ANHANG

der

Gemeinsamen Mitteilung an das Europäische Parlament und den Rat

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

Fortschritte bei der Umsetzung der strategischen Initiativen

Nr.	Initiative	Kommission/ Hoher Vertreter	Stand
1) Resilienz, technologische Souveränität und Führungsrolle			
1.1	Verabschiedung der **überarbeiteten NIS-Richtlinie**	KOM	Das Europäische Parlament wird seinen Standpunkt voraussichtlich Ende 2021 endgültig festlegen. Der Rat legt seinen Bericht über den Stand der Verhandlungen im Juni 2021 vor. Ergänzend dazu und unter Beachtung der besonderen Vorschriften für den Energiesektor wird derzeit im Rahmen der Elektrizitätsverordnung (EU) 2019/943 ein Netzkodex zur Cybersicherheit ausgearbeitet, um die Widerstandsfähigkeit und den Schutz des Energiesektors zu erhöhen. Das Europäische Parlament wird seinen Standpunkt zur Verordnung und zur Richtlinie über die Betriebsstabilität digitaler Systeme (DORA) voraussichtlich in der zweiten Jahreshälfte 2021 endgültig festlegen. Der Rat wird voraussichtlich im Juni 2021 eine allgemeine Ausrichtung zu dem Vorschlag festlegen.
1.2	Regulierungsmaßnahmen für ein **Internet der sicheren Dinge**	KOM	Derzeit laufen Untersuchungen und Konsultationen in Bezug auf umfassende Vorschriften. Es gibt Fortschritte auf dem Weg zu einem delegierten Rechtsakt im Rahmen der Richtlinie 2014/53/EU über Funkanlagen, der möglicherweise im Jahr 2021 angenommen werden könnte; Kraftfahrzeugvorschriften für alle neuen Fahrzeugtypen müssen ab Juli 2022 umgesetzt werden. Die Kommission arbeitet mit Interessenträgern an der Rolle, die der Cybersicherheitszertifizierung von Produkten, Prozessen und Diensten in verschiedenen Sektoren zukommt.
1.3	**Investitionen in die Cybersicherheit** (vor allem mit Mitteln aus den Programmen Digitales Europa und Horizont Europa und der Aufbau- und Resilienzfazilität), insbesondere über das Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung und gegebenenfalls das	KOM	In Kürze werden neue Arbeitsprogramme für die Finanzierungsmechanismen der Programme Horizont Europa und Digitales Europa angenommen, die dann vom neuen Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung und dem Netz der Kompetenzzentren verwaltet werden sollen.

Nr.	Initiative	Kommission/ Hoher Vertreter	Stand
	Netz der Kompetenzzentren, um im Zeitraum 2021–2027 bis zu 4,5 Mrd. EUR an öffentlichen und privaten Investitionen zu erreichen		
1.4	Ein EU-Netz von KI-gestützten **Sicherheitseinsatzzentren** [das **Cyberschutzschild** der EU] und eine ultrasichere Quantenkommunikationsinfrastruktur [EuroQCI]	KOM	Die Mitgliedstaaten werden dazu angehalten, über Sicherheitseinsatzzentren (SOCs) eigene nationale Einsatzkapazitäten aufzubauen. Mehrere Mitgliedstaaten haben die Absicht, die Aufbau- und Resilienzfazilität zur Förderung der SOCs heranzuziehen; derzeit laufen Gespräche zwischen der Kommission und anderen Organen, Einrichtungen und sonstigen Stellen der EU und den Mitgliedstaaten über Möglichkeiten der Einbindung der SOCs und der Unterbringung der Rechen- und Analysekapazitäten[1]. Die Mitgliedstaaten setzen sich weiter gemeinsam mit der Kommission und der Europäischen Weltraumorganisation dafür ein, die EuroQCI-Initiative voranzubringen. Der EuroQCI-Aktionsplan muss noch von den Mitgliedstaaten gebilligt werden. Die ersten Aufforderungen im Rahmen des Programms Digitales Europa zur Unterstützung nationaler QCI-Netze und zur Entwicklung der für EuroQCI benötigten Schlüsseltechnologien werden in Kürze veröffentlicht. Im Februar 2020 nahm die Kommission 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. Mehrere Mitgliedstaaten haben Initiativen zur sicheren Konnektivität in ihre im Rahmen der RFF geförderten Aufbau- und Resilienzpläne aufgenommen. Der Aufbau grenzüberschreitender Verbindungen zwischen nationalen Netzen wird durch Maßnahmen im Rahmen des Digitalteils der Fazilität „Connecting Europe“ (CEF2) unterstützt. Mehrere Mitgliedstaaten haben EuroQCI in ihre Aufbau- und Resilienzpläne aufgenommen.

[1] Die Gespräche finden im Rahmen des CSIRT-Netzes, des Netzwerks der Verbindungsorganisationen für Cyberkrisen (CyCLoNe) und der NIS-Kooperationsgruppe statt.

Nr.	Initiative	Kommission/ Hoher Vertreter	Stand
1.5	Breite Einführung von Cybersicherheitstechnik durch eine **gezielte Unterstützung von KMU** im Rahmen der digitalen Innovationszentren	KOM	Die Kommission bemüht sich darum, dass Inhalte und Fachwissen im Bereich der Cybersicherheit über die Initiative „Europäische digitale Innovationszentren“ (Programm Digitales Europa) und in Verbindung mit den nationalen Koordinierungszentren für Cybersicherheit bereitgestellt werden. Cybersicherheitsakteure wie die Europäische Cybersicherheitsorganisation (ECSO) entwickeln derzeit einen „Dienstleistungskatalog“ für die auf Cybersicherheit ausgerichteten Innovationszentren.
1.6	Entwicklung eines **DNS-Auflösungsdienstes der EU** als sichere und offene Alternative für den Internetzugang der Bürger, Unternehmen und öffentlichen Verwaltungen in der EU [**DNS4EU**]	KOM	Das Arbeitsprogramm 2021–2023 für den Digitalteil der Fazilität „Connecting Europe“ (CEF2)[2] sieht Mittel für die Entwicklung von DNS4EU vor, und eine diesbezügliche Aufforderung zur Einreichung von Vorschlägen für das Projekt ist für 2021 geplant. Neben den Aspekten der Internetsicherheit führt die Kommission derzeit Gespräche mit Internet-Akteuren und beabsichtigt die Einleitung einer Studie im Hinblick auf die Ausarbeitung eines durch EU-Mittel unterstützten Notfallplans für die **Bewältigung von Extremszenarios**, die die Integrität und Verfügbarkeit des globalen DNS-Root-Systems beeinträchtigen. Eine Studie, die sich mit der Beobachtung der Entwicklung und Einführung wichtiger Internetstandards, die der EU-Politik dienen, und mit der beschleunigten **Verbreitung wichtiger Internetstandards** wie Internet-Protokoll Version 6 (IPv6) und wohl etablierter Internetsicherheitsstandards und bewährter Verfahren für DNS, Routing und E-Mail-Sicherheit befasst, wird gerade vorbereitet (geplanter Start im Herbst 2021). Im Rahmen des Programms Digitales Europa wird die Einrichtung einer **Internetbeobachtungsstelle** als eine der Tätigkeiten des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung erwogen.

[2] Am 12. März 2021 erzielten das Europäische Parlament und der Rat eine Einigung über die vorgeschlagene Fazilität „Connecting Europe“ (CEF2).

Nr.	Initiative	Kommission/ Hoher Vertreter	Stand
1.7	Abschluss der **Umsetzung des 5G-Instrumentariums**	KOM	Mit Unterstützung der Kommission und der ENISA haben die Mitgliedstaaten weitere Fortschritte bei der Umsetzung des 5G-Instrumentariums gemacht, insbesondere im Hinblick auf die Beschränkungen für Hochrisikoanbieter. Weitere Maßnahmen auf EU-Ebene sind die Ausarbeitung eines EU-Zertifizierungssystems für 5G-Netze und die Einleitung einer Analyse der Sicherheitsauswirkungen von Open RAN-Technik durch die NIS-Kooperationsgruppe.
2) Aufbau operativer Kapazitäten zur Prävention, Abschreckung und Reaktion			
2.1	Vervollständigung des europäischen Rahmens für das Krisenmanagement im Bereich der Cybersicherheit und Festlegung der Verfahren, der Etappenziele und des Zeitplans für die Einrichtung der **Gemeinsamen Cyber-Einheit**	KOM mit HV	Am 23. Juni 2021 gab die Kommission eine Empfehlung zum Aufbau der gemeinsamen Cyber-Einheit ab, in der sie auf Etappenziele, den Prozess und den Zeitplan eingeht, wobei auch die Gespräche mit den Mitgliedstaaten berücksichtigt werden.
2.2	Fortführung der Umsetzung der **Agenda zur Bekämpfung der Cyberkriminalität im Rahmen der Strategie für die Sicherheitsunion**	KOM	Die Mitgliedstaaten ermitteln mit Unterstützung der Kommission bewährte Verfahren für die Erhebung, Erstellung und Veröffentlichung statistischer Daten über Berichte, Strafverfolgungen und Verurteilungen wegen Cyberangriffsdelikten im Sinne der Richtlinie 2013/40/EU über Angriffe auf Informationssysteme. Die Kommission überwacht die Fortschritte, die von sieben Mitgliedstaaten infolge der anhängigen Vertragsverletzungsverfahren wegen unzureichender Umsetzung der Richtlinie 2013/40/EU erzielt werden. Weitere Vertragsverletzungsverfahren können noch im Jahresverlauf 2021 eingeleitet werden. Die Kommission hat eine Untersuchung zum Identitätsdiebstahl in Auftrag gegeben, deren Ergebnisse bis Dezember 2021 erwartet werden. Die Datenerhebung zur Kriminalstatistik wird im Jahr 2021 im Einklang mit Artikel 14 der Richtlinie 2013/40/EU ausgeweitet.

Nr.	Initiative	Kommission/ Hoher Vertreter	Stand
2.3	Förderung und Erleichterung der Einsetzung einer **Arbeitsgruppe der Mitgliedstaaten zur Cyberaufklärung im Rahmen des EU-Zentrums für Informationsgewinnung und -analyse (EUINTCEN)**	HV	Der Hohe Vertreter fördert und erleichtert weiterhin die Einsetzung einer Arbeitsgruppe der Mitgliedstaaten zur Cyberaufklärung, um die spezifischen Kapazitäten des INTCEN in diesem Bereich auf der Grundlage freiwilliger nachrichtendienstlicher Beiträge aus den Mitgliedstaaten – unbeschadet ihrer Zuständigkeiten – zu stärken. Es sind weitere Gespräche zwischen dem EAD und den Mitgliedstaaten geplant.
2.4	Voranbringen der **EU-Cyberabschreckung**, um für Vorbeugung, Verhinderung, Abschreckung und Reaktion im Hinblick auf böswillige Cyberaktivitäten zu sorgen	HV mit KOM	Als Beitrag zur Entwicklung des EU-Instrumentariums für die Cyberdiplomatie[3] überprüft der EAD gegenwärtig die Leitlinien zur Umsetzung des Rahmens für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten. Ein Vorschlag für die EU-Cyberabschreckung wird derzeit unter Mitwirkung der Kommission im Einklang mit ihren Zuständigkeiten ausgearbeitet und soll vom Hohen Vertreter Anfang 2022 dem Rat vorgelegt werden. Am 16. April 2021 wurde im Namen der EU eine Erklärung abgegeben, in der die Solidarität mit den Vereinigten Staaten in Bezug auf die Folgen böswilliger Cyberaktivitäten, insbesondere des Cyberangriffs auf SolarWinds, zum Ausdruck gebracht wurde[4]. Zur weiteren Förderung der internationalen Zusammenarbeit veranstaltete der EAD am 17. Mai 2021 gemeinsam mit dem Ratsvorsitz und dem Institut der Europäischen Union für Sicherheitsstudien eine Diskussion, um das gegenseitige Verständnis der jeweiligen diplomatischen Ansätze für die Vorbeugung, Abschreckung und Reaktion auf böswillige Cyberaktivitäten zu verbessern.
2.5	Überprüfung des **Politikrahmens für die Cyberabwehr**	HV mit KOM	Die Überprüfung des Politikrahmens für die Cyberabwehr in Verbindung mit den Mitgliedstaaten und Interessenträgern begann im Mai 2021.

[3] Beschlüsse (GASP) 2020/1127, 2020/1537 und 2020/651 des Rates als Teil des Dok. 9916/17.

[4] https://www.consilium.europa.eu/de/press/press-releases/2021/04/15/declaration-by-the-high-representative-on-behalf-of-the-european-union-expressing-solidarity-with-the-united-states-on-the-impact-of-the-solarwinds-cyber-operation/

Nr.	Initiative	Kommission/ Hoher Vertreter	Stand
2.6	Förderung der Entwicklung einer „**militärischen Vision und Strategie der EU für den Cyberraum** als Einsatzbereich“ für militärische GSVP-Missionen und -Operationen	HV	Die militärische Vision und Strategie für den Cyberraum als Einsatzbereich soll in nationale Strategien einfließen und damit die Harmonisierung der EU-Tätigkeiten im Bereich der Cyberabwehr unterstützen. Der zweite Workshop zur konzeptionellen Entwicklung im Bereich der Cyberabwehr fand am 28. und 29. April 2021 statt und die Ergebnisse sollen dem EU-Militärausschuss im Juni 2021 vorgestellt werden.
2.7	Unterstützung von **Synergien zwischen der zivilen, der Verteidigungs- und der Weltraumindustrie**	KOM	Im Februar 2021 wurde ein Aktionsplan zur Förderung von Synergien zwischen den Sektoren angenommen.
2.8	Stärkung der **Cybersicherheit kritischer Weltrauminfrastrukturen** im Rahmen des Weltraumprogramms	KOM	Ein Arbeitsprogramm ist in Vorbereitung.
3) Förderung eines globalen offenen Cyberraums			
3.1	Festlegung einer Reihe von **Zielen für internationale Normungsverfahren** und Förderung dieser Ziele auf internationaler Ebene	KOM	An diesen Zielen wird derzeit gearbeitet.
3.2	Stärkung der internationalen Sicherheit und Stabilität im Cyberraum, insbesondere durch einen Vorschlag der EU und ihrer Mitgliedstaaten für ein **Aktionsprogramm der Vereinten Nationen zur Förderung von verantwortungsvollem staatlichen Handeln im Cyberraum**	HV	Die EU setzt die Ausarbeitung des Aktionsprogramms fort und stützt sich dabei auf den Konsensbericht vom 12. März 2021 der offenen Arbeitsgruppe der Vereinten Nationen für Entwicklungen auf dem Gebiet der Information und Telekommunikation im Kontext der internationalen Sicherheit.
3.3	Bereitstellung **praktischer Orientierungshilfe zur Einhaltung der Menschenrechte und Beachtung der Grundfreiheiten** im Cyberraum	HV mit KOM	Aufbauend auf dem Aktionsplan für Menschenrechte und Demokratie (2020–2024) und ihren Menschenrechtsleitlinien für die Meinungsfreiheit online und offline wird sich die EU weiterhin für eine umfassendere Einhaltung der internationalen Rechtsvorschriften und Normen im Bereich der Menschenrechte einsetzen. Für das zweite Halbjahr 2021 sind Koordinierungstreffen mit einschlägigen Interessenträgern geplant.

Nr.	Initiative	Kommission/ Hoher Vertreter	Stand
3.4	Besserer **Schutz der Kinder vor sexuellem Missbrauch und sexueller Ausbeutung** und Verabschiedung einer Strategie für die Rechte des Kindes	KOM	Im Mai 2021 erzielten das Europäische Parlament und der Rat eine Einigung über eine befristete Verordnung, mit der sichergestellt werden soll, dass Anbieter von Online-Kommunikationsdiensten ihre freiwillige Praxis der Aufdeckung und Meldung von im Internet verbreiteten Material über sexuellen Missbrauch von Kindern und dessen Entfernung fortsetzen können. Die Kommission arbeitet derzeit an einem Vorschlag für einen dauerhaften Rahmen.
3.5	Stärkung und Förderung des **Budapester Übereinkommens über Computerkriminalität**, u. a. durch die Arbeiten am zweiten Zusatzprotokoll zu dem Übereinkommen	KOM mit HV	Die Kommission nimmt im Namen der EU an den Verhandlungen über das Zweite Zusatzprotokoll teil, das möglicherweise Anfang 2022 zur Unterzeichnung aufgelegt werden könnte.
3.6	Ausweitung des **Cyberdialogs der EU mit Drittländern**, regionalen und internationalen Organisationen, u. a. durch ein informelles EU-**Netz für Cyberdiplomatie**	HV mit KOM	Die EU überlegt derzeit, wie die derzeitigen Cyberdialoge gestärkt und ausgeweitet werden können. Gegenwärtig gibt es solche Cyberdialoge mit Brasilien, China, Indien, Japan, der Republik Südkorea und den USA. Ein erster Cyberdialog zwischen der EU und der Ukraine fand am 3. Juni 2021 statt. Darüber hinaus sieht das mit dem Vereinigten Königreich geschlossene Handels- und Kooperationsabkommen Bemühungen um die Einrichtung eines Cyberdialogs zwischen der EU und dem Vereinigten Königreich vor. Mit den EU-Delegationen und gegebenenfalls den Botschaften der Mitgliedstaaten in aller Welt laufen derzeit Vorbereitungen zur Errichtung eines informellen EU-Netzes für Cyberdiplomatie, um für die Vision der EU für den Cyberraum zu werben, Informationen auszutauschen und sich regelmäßig über die Entwicklungen im Cyberraum abzustimmen. Das Netz für Cyberdiplomatie wird seine Arbeit voraussichtlich in der zweiten Jahreshälfte 2021 aufnehmen.
3.7	Verstärkung des **Austauschs mit der Multi-Stakeholder-Gemeinschaft**, insbesondere durch einen regelmäßigen und strukturierten Austausch mit dem Privatsektor, der Wissenschaft und der Zivilgesellschaft	KOM mit HV	Der regelmäßige und strukturierte Austausch mit Interessenträgern, auch aus Privatsektor, Wissenschaft und Zivilgesellschaft, sollte intensiviert werden, auch im Rahmen der Überlegungen zur Infrastruktur für den Dialog über Cyberfragen (siehe Abschnitt 3.6).

Nr.	Initiative	Kommission/ Hoher Vertreter	Stand
3.8	Vorschlag für eine EU-Agenda für den Aufbau externer Cyberkapazitäten und die Einrichtung eines **EU-Gremium für den Cyberkapazitätsaufbau**	KOM mit HV	Die Beratungen über die Einrichtung des EU-Gremiums für den Cyberkapazitätsaufbau sind im Gange. Eine erste Auftaktsitzung fand im April 2021 statt. Sobald das Gremium eingerichtet ist, wird es die EU-Agenda ausarbeiten.
Cybersicherheit in den Organen, Einrichtungen und sonstigen Stellen der EU			
A.1	Verordnung über gemeinsame Vorschriften für die **Informationssicherheit** in den Organen, Einrichtungen und sonstigen Stellen der EU	KOM	Die Kommission berät mit den anderen Organen, Einrichtungen und sonstigen Stellen sowie den nationalen Sicherheitsexperten der Mitgliedstaaten über die Annahme eines Vorschlags im 4. Quartal 2021.
A.2	Verordnung über **gemeinsame Cybersicherheitsvorschriften** für die Organe, Einrichtungen und sonstigen Stellen der EU	KOM	Die Kommission führt gemeinsam mit anderen Organen, Einrichtungen und sonstigen Stellen eine vergleichende Bewertung der Cybersicherheitspolitik durch und prüft die Bedrohungslage im Hinblick auf die Annahme eines Vorschlags im 4. Quartal 2021.
A.3	Neue **Rechtsgrundlage für das CERT-EU** zur Stärkung seiner Stabilität und seiner Finanzausstattung	KOM	Die Kommission erwägt gemeinsam mit anderen Organen, Einrichtungen und sonstigen Stellen die Festlegung der neuen gemeinsamen Cybersicherheitsvorschriften als Rechtsgrundlage für die Stärkung des CERT-EU, um der steigenden Zahl erheblicher Sicherheitsvorfälle zu begegnen. Ein entsprechender Vorschlag soll unter Punkt A.2 vorgelegt werden.