Rat der
Europäischen Union

Brüssel, den 8. Oktober 2021
(OR. en)

12534/21

CYBER 253
JAI 1064
TELECOM 361
CSC 340
CIS 110
RELEX 827
ENFOPOL 343
COPS 341
COSI 179
HYBRID 59
CSCI 127
POLGEN 172
DATAPROTECT 230

I/A-PUNKT-VERMERK

Absender:	Generalsekretariat des Rates
Empfänger:	Ausschuss der Ständigen Vertreter (2. Teil)/Rat
Betr.:	Schlussfolgerungen des Rates zur Prüfung des Potenzials der Initiative für eine Gemeinsame Cyber-Einheit als Ergänzung zur koordinierten Reaktion der EU auf große Cybersicherheitsvorfälle und -krisen – Billigung

1. Am 23. Juni 2021 hat die Kommission ihre Empfehlung zum Aufbau einer Gemeinsamen Cyber-Einheit[1] veröffentlicht, um gegen die steigende Zahl schwerwiegender Cybersicherheitsvorfälle vorzugehen, die sich auf öffentliche Dienste sowie den Alltag von Unternehmen und Bürgern in der gesamten Europäischen Union auswirken.

2. Die Kommission hat die Empfehlung am 28. Juni 2021 in der Horizontalen Gruppe „Fragen des Cyberraums“ (HWPCI) vorgestellt. Im Anschluss daran fanden unter slowenischem Vorsitz in den Sitzungen der HWPCI vom 7. und 14. Juli 2021 Beratungen statt, um die Standpunkte der Mitgliedstaaten zur Empfehlung der Kommission einzuholen.

[1] C(2021) 4520 final (Dok. 11155/21 und 11155/21 ADD 1).

3. Bei der informellen Videokonferenz der Mitglieder der HWPCI vom 23. Juli 2021 hat der Vorsitz einen ersten Entwurf von Schlussfolgerungen des Rates zur Prüfung des Potenzials der Initiative für eine Gemeinsame Cyber-Einheit als Ergänzung zur koordinierten Reaktion der EU auf große Cybersicherheitsvorfälle und -krisen[2] vorgelegt. Dieser Entwurf von Schlussfolgerungen wurde in den Sitzungen der Mitglieder der HWPCI vom 8. und 29. September 2021 weiter erörtert.

4. In ihrer Sitzung vom 6. Oktober 2021 hat sich die HWPCI auf den in der Anlage wiedergegebenen Entwurf von Schlussfolgerungen des Rates verständigt.

5. Der Ausschuss der Ständigen Vertreter wird daher ersucht, dem Rat den in der Anlage wiedergegebenen Entwurf von Schlussfolgerungen des Rates zu unterbreiten und ihm zu empfehlen, den Entwurf von Schlussfolgerungen als A-Punkt seiner Tagesordnung anzunehmen.

---

[2] Dok. 10975/21.

ANLAGE

Entwurf von Schlussfolgerungen des Rates zur Prüfung des Potenzials der Initiative für eine Gemeinsame Cyber-Einheit als Ergänzung zur koordinierten Reaktion der EU auf große Cybersicherheitsvorfälle und - krisen

DER RAT DER EUROPÄISCHEN UNION —

UNTER HINWEIS auf

– seine Schlussfolgerungen zur Cybersicherheitsstrategie der EU für die digitale Dekade[3],

– seine Schlussfolgerungen zu einer koordinierten Reaktion der EU auf große Cybersicherheitsvorfälle und -krisen[4],

– seine Schlussfolgerungen zur Cyberdiplomatie[5],

– seine Schlussfolgerungen zu einem Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten („Cyber Diplomacy Toolbox“)[6],

– seine Schlussfolgerungen zu Sicherheit und Verteidigung[7],

– den EU-Politikrahmen für die Cyberabwehr[8],

– seine Schlussfolgerungen zur Gestaltung der digitalen Zukunft Europas[9],

– den Durchführungsbeschluss (EU) 2018/1993 des Rates vom 11. Dezember 2018 über die Integrierte EU-Regelung für die politische Reaktion auf Krisen,

---

3 Dok. 7290/21.
4 Dok. 10086/18.
5 Dok. 6122/15 + COR 1.
6 Dok. 10474/17.
7 Dok. 8396/21.
8 Dok. 15585/14.
9 Dok. 8711/20.

– seine Schlussfolgerungen zur Gemeinsamen Mitteilung an das Europäische Parlament und den Rat: „Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen“[10] sowie

– seine Schlussfolgerungen über Cybersicherheitskapazitäten und deren Aufbau in der EU[11] —

1. HEBT die Bedeutung der Cybersicherheit für den Aufbau eines widerstandsfähigen, digitalen und grünen Europas HERVOR; BETONT, dass Cybersicherheit für den Wohlstand und die Sicherheit der EU und ihrer Mitgliedstaaten, ihrer Bevölkerung, Unternehmen und Institutionen sowie für die Wahrung der Integrität unserer freien und demokratischen Gesellschaften unerlässlich ist;

2. IST SICH der grenz- und sektorübergreifenden Natur vieler Bedrohungen für die Cybersicherheit sowie der Risiken und potenziellen Auswirkungen der fortlaufenden Cyberkampagnen mit immer wirkungsvolleren, ausgeklügelteren, gezielteren, komplexeren, hartnäckigeren und/oder flächendeckenderen böswilligen Aktivitäten BEWUSST[12]. Die COVID-19-Pandemie hat die Schwachstellen unserer Gesellschaften und das Schadenspotenzial großer Cybersicherheitsvorfälle für Wirtschaft, Demokratie, grundlegende Dienste und kritische Infrastrukturen, insbesondere im Gesundheitssektor, noch deutlicher gemacht. Auch die Bedeutung der Konnektivität und die Abhängigkeit der Gesellschaft von zuverlässigen, vertrauenswürdigen und sicheren Netz- und Informationssystemen sind durch die Pandemie stärker zutage getreten. Letztlich hat sie die Notwendigkeit eines globalen, offenen, freien, stabilen und sicheren Internets sowie des Vertrauens in Produkte, Prozesse und Dienstleistungen der Informations- und Kommunikationstechnologie (IKT) und deren Sicherheit verdeutlicht, einschließlich der Notwendigkeit, eine widerstandsfähige Lieferkette zu gewährleisten;

---

10 Dok. 14435/17 + COR 1.
11 Dok. 7737/19.
12 ENISA-Bericht zur Bedrohungslage 2020.

3. BEKRÄFTIGT die Bedeutung der Cyberresilienz und der Weiterentwicklung des EU-Rahmens für das Krisenmanagement im Bereich der Cybersicherheit[13] mit dem Ziel einer effizienten und zeitnahen Reaktion auf EU-Ebene auf große Cybersicherheitsvorfälle und -krisen und der weiteren Integration in bestehende horizontale und sektorale Krisenreaktionsmechanismen der EU; UNTERSTREICHT die Rolle des Rates und der Integrierten Regelung für die politische Reaktion auf Krisen (IPCR) bei der Gewährleistung einer rechtzeitigen Koordinierung und Reaktion auf politischer Ebene der Union im Falle von Krisen mit weitreichenden Auswirkungen oder politischer Tragweite, unabhängig davon, ob sie ihren Ursprung innerhalb oder außerhalb der Union haben; HEBT HERVOR, wie wichtig es ist, solche Rahmen und Mechanismen regelmäßig zu erproben;

4. WEIST DARAUF HIN, dass Tätigkeiten auf EU-Ebene im Zusammenhang mit großen Cybersicherheitsvorfällen und -krisen im Einklang mit den Grundsätzen der Subsidiarität, der Verhältnismäßigkeit, der Komplementarität, der Vermeidung von Doppelungen und der Vertraulichkeit erfolgen; BEKRÄFTIGT, dass die Mitgliedstaaten die Hauptverantwortung für die Reaktion auf sie betreffende große Cybersicherheitsvorfälle und -krisen tragen; WEIST DARAUF HIN, wie wichtig es ist, die Zuständigkeiten der Mitgliedstaaten und ihre alleinige Verantwortung für die nationale Sicherheit gemäß Artikel 4 Absatz 2 des Vertrags über die Europäische Union zu achten, auch im Bereich der Cybersicherheit;

5. WEIST zugleich DARAUF HIN, wie wichtig es ist, die Zuständigkeiten und Mandate der Organe, Einrichtungen und sonstigen Stellen der EU zu achten. Dem Hohen Vertreter, der Kommission und anderen Organen, Einrichtungen und sonstigen Stellen der EU kommt laut Unionsrecht ebenfalls eine wichtige Rolle zu, unter anderem aufgrund der möglichen Auswirkungen großer Cybersicherheitsvorfälle und -krisen auf den Binnenmarkt sowie das Funktionieren der Organe, Einrichtungen und sonstigen Stellen der EU;

---

[13] Dok. 10086/18.

6. UNTERSTREICHT, dass bei der Weiterentwicklung des EU-Rahmens für das Krisenmanagement im Bereich der Cybersicherheit unnötige Doppelungen vermieden sowie Komplementarität und Mehrwert angestrebt werden müssen und dass die Kohärenz mit bestehenden Mechanismen, Initiativen, Netzen, Prozessen und Verfahren auf nationaler und europäischer Ebene gewährleistet werden muss; HEBT HERVOR, wie wichtig es ist, bestehende Verfahren und Strukturen zu straffen, um die Komplexität zu verringern und die Zugänglichkeit und Reaktionsfähigkeit gegenüber denjenigen, die um Hilfe und Solidarität ersuchen, im Interesse des Zusammenhalts in der Union zu verbessern;

7. ERKENNT die Anwendbarkeit des Völkerrechts, einschließlich der Charta der Vereinten Nationen in ihrer Gesamtheit, des humanitären Völkerrechts und der Menschenrechtsnormen im Cyberraum, AN und FÖRDERT die Einhaltung der freiwilligen, nicht bindenden Normen, Regeln und Grundsätze für verantwortungsvolles Verhalten von Staaten im Cyberraum, die von allen VN-Mitgliedstaaten gebilligt wurden;

8. BEGRÜßT die Fortschritte, die in den vergangenen Jahren im Rat, insbesondere in der Horizontalen Gruppe „Fragen des Cyberraums“ (HWPCI) und anderen einschlägigen Ratsgruppen, sowie durch die Einrichtung weiterer Initiativen, Netze und Mechanismen für die Zusammenarbeit und den Informationsaustausch zwischen Mitgliedstaaten erzielt wurden, insbesondere der NIS-Kooperationsgruppe und des mit der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 geschaffenen CSIRTs-Netzwerks, des Netzwerks der Verbindungsorganisationen für Cyberkrisen (CyCLONe) sowie einschlägiger Projekte im Bereich der Cyberabwehr, die im Rahmen der Ständigen Strukturierten Zusammenarbeit (SSZ)[14], der Gemeinsamen Taskforce gegen die Cyberkriminalität (J-CAT), des Europäischen Justiziellen Netzes gegen Cyberkriminalität (EJCN), der freiwilligen Beiträge der Mitgliedstaaten zum EU INTCEN und der Koordinierung und Zusammenarbeit im Rahmen des Instrumentariums für die Cyberdiplomatie eingeleitet wurden;

---

14 Insbesondere das von Litauen koordinierte Projekt „Teams für die rasche Reaktion auf Cybervorfälle und die gegenseitige Unterstützung im Bereich der Cybersicherheit“, das von Deutschland koordinierte Projekt „Koordinierungszentrum für den Cyber- und Informationsraum“ und das von Griechenland koordinierte Projekt „Plattform für den Austausch von Informationen über die Reaktion auf Cyberbedrohungen und -vorfälle“.

9. VERWEIST auf die bestehenden Rahmen für die Zusammenarbeit zwischen den Organen, Einrichtungen und sonstigen Stellen der EU, wie etwa die strukturierte Zusammenarbeit zwischen ENISA und CERT-EU und die Vereinbarung zwischen ENISA, der Europäischen Verteidigungsagentur (EDA), dem bei Europol eingerichteten Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3) und CERT-EU; UNTERSTREICHT, wie wichtig ein kontinuierlicher regelmäßiger Informationsaustausch mit dem Rat über die weiteren Entwicklungen in diesen Rahmen für die Zusammenarbeit ist;

10. HEBT HERVOR, wie wichtig es ist, die Zusammenarbeit und den Informationsaustausch zwischen den verschiedenen Cybergemeinschaften innerhalb der EU und ihrer Mitgliedstaaten auf allen erforderlichen Ebenen – technisch, operativ und strategisch/politisch – zu verstärken und bestehende Krisenbewältigungsmechanismen, Netze, Strukturen, Prozesse und Verfahren miteinander zu verknüpfen, wenn dies die Bewältigung großer Cybersicherheitsvorfälle und -krisen unterstützt und verbessert;

11. WÜRDIGT die Fortschritte, die eine Gruppe von Mitgliedstaaten im Rahmen der SSZ bei der Schaffung gemeinsamer operativer Cyberfähigkeiten mit der Bezeichnung „Teams für die rasche Reaktion auf Cybervorfälle“ erzielt hat, die die freiwillige Zusammenarbeit im Cyberbereich durch gegenseitige Unterstützung vertiefen sollen, auch in Reaktion auf große Cybersicherheitsvorfälle und -krisen;

12. WÜRDIGT die Erfahrung und die permanente Reaktionsfähigkeit der Strafverfolgungsbehörden im Bereich der operativen Zusammenarbeit und des sicheren Informationsaustauschs gegen große grenzüberschreitende Cyberangriffe im Rahmen des EU-Notfallprotokolls für die Strafverfolgung;

13. WÜRDIGT die anhaltende Umsetzung des Rahmens für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten („Instrumentarium für die Cyberdiplomatie“); WEIST DARAUF HIN, dass es jedem Mitgliedstaat freisteht, von Fall zu Fall seine eigene souveräne Entscheidung über die Zuordnung böswilliger Cyberaktivitäten zu treffen; WEIST DARAUF HIN, dass die Maßnahmen, die im Rahmen einer gemeinsamen diplomatischen Reaktion der EU auf böswillige Cyberaktivitäten ergriffen werden, auf einer zwischen den Mitgliedstaaten abgestimmten gemeinsamen Lageerfassung beruhen sollten. Das EU INTCEN spielt eine zentrale Rolle als Knotenpunkt für die Bereitstellung von Lageerfassung und Bedrohungsanalysen in Cyberfragen für die EU, auf der Grundlage freiwilliger nachrichtendienstlicher Beiträge der Mitgliedstaaten und unbeschadet ihrer Zuständigkeiten;

14. BEKRÄFTIGT die Bedeutung der gegenseitigen Unterstützung und Solidarität im Einklang mit Artikel 42 Absatz 7 des Vertrags über die Europäische Union und Artikel 222 des Vertrags über die Arbeitsweise der Europäischen Union und RUFT zu weiteren Übungen mit einer Cyberdimension AUF; WEIST DARAUF HIN, dass für den Fall eines großen Cybersicherheitsvorfalls oder einer großen Cybersicherheitskrise Überlegungen über die Verknüpfung zwischen dem EU-Rahmen für das Krisenmanagement im Bereich der Cybersicherheit, dem Instrumentarium für die Cyberdiplomatie und den Bestimmungen der oben genannten Artikel angestellt werden müssen; WEIST ferner DARAUF HIN, dass die Verpflichtungen der Mitgliedstaaten, die sich aus Artikel 42 Absatz 7 des Vertrags über die Europäische Union ergeben, den besonderen Charakter der Sicherheits- und Verteidigungspolitik bestimmter Mitgliedstaaten unberührt lassen; WEIST zudem DARAUF HIN, dass die NATO für die ihr angehörenden Staaten das Fundament der kollektiven Verteidigung bleibt;

15. WÜRDIGT die Zusammenarbeit zwischen der EU und der NATO im Bereich der Cybersicherheit und -abwehr, einschließlich des Informationsaustauschs zwischen CERT-EU und der „NATO Computer Incident Response Capability“ (NCIRC), unter uneingeschränkter Achtung der Grundsätze der Transparenz, der Gegenseitigkeit und der Inklusivität sowie der Beschlussfassungsautonomie beider Organisationen;

16. IST SICH BEWUSST, wie wichtig es ist, im Hinblick auf den Informationsaustausch und die Bereitstellung einschlägigen Fachwissens sowie vertrauenswürdiger Lösungen und Dienste gegebenenfalls mit dem Privatsektor zusammenzuarbeiten, beispielsweise auch bei der Unterstützung der Reaktion auf Vorfälle und der Stärkung der Lageerfassung zwischen verschiedenen Cybergemeinschaften;

17. BETONT, wie wichtig sichere Kommunikationskanäle für den Austausch von Verschlusssachen und sensiblen Informationen sind; HEBT HERVOR, dass weitere Fortschritte erforderlich sind.

Diesbezüglich und unter Berücksichtigung der vorstehenden Ausführungen verfährt der Rat wie folgt: Er

18. WÜRDIGT die Empfehlung der Kommission zum Aufbau einer Gemeinsamen Cyber-Einheit als eine Initiative, die bei der Weiterentwicklung des EU-Rahmens für das Krisenmanagement im Bereich der Cybersicherheit in Betracht gezogen werden sollte[15];

19. RUFT die EU und ihre Mitgliedstaaten AUF, ihre Bemühungen um einen umfassenderen und wirksameren EU-Rahmen für das Krisenmanagement im Bereich der Cybersicherheit fortzusetzen und dabei auf bestehenden Mechanismen und den bereits erzielten Fortschritten aufzubauen und das Potenzial der Initiative für eine Gemeinsame Cyber-Einheit zur Ergänzung dieser Mechanismen durch einen schrittweisen Ansatz zu berücksichtigen; BETONT, dass ein schrittweiser, transparenter und inklusiver Prozess für die Stärkung des Vertrauens und damit für die Weiterentwicklung eines EU-Rahmens für das Krisenmanagement im Bereich der Cybersicherheit von entscheidender Bedeutung ist; bei diesem Prozess sollten die bestehenden Rollen, Zuständigkeiten und Mandate der Mitgliedstaaten und der Organe, Einrichtungen und sonstigen Stellen der EU sowie die in diesen Schlussfolgerungen dargelegten Grundsätze, einschließlich Verhältnismäßigkeit, Subsidiarität, Inklusivität, Komplementarität, Vermeidung von Doppelungen und Vertraulichkeit von Informationen, geachtet werden; BETONT zugleich, dass eine etwaige Beteiligung an oder Beiträge von Mitgliedstaaten zu einer Gemeinsamen Cyber-Einheit freiwillig sind;

---

15 C(2021) 4520 final (Dok. 11155/21 und 11155/21 ADD 1).

20. BETONT, dass angemessene Arbeitsmethoden und eine angemessene Governance festgelegt werden müssen, um zu ermöglichen, dass alle Mitgliedstaaten in die Beratungen, die Entwicklung und wirksame Entscheidungsprozesse über den EU-Rahmen für das Krisenmanagement im Bereich der Cybersicherheit, einschließlich der Initiative für eine Gemeinsame Cyber-Einheit, einbezogen und daran beteiligt werden; FORDERT, dass die in den Verträgen verankerten Vorrechte des Rates und der Grundsatz der loyalen Zusammenarbeit geachtet werden;

21. UNTERSTREICHT, wie wichtig es ist, alle einschlägigen Cybergemeinschaften innerhalb der EU und ihrer Mitgliedstaaten zu ermitteln und einzubeziehen und dabei ihre unterschiedlichen Rollen und Zuständigkeiten bei verschiedenen Arten großer Cybersicherheitsvorfälle und -krisen zu berücksichtigen; UNTERSTREICHT die maßgebliche Rolle des Rates, insbesondere im Rahmen der HWPCI, bei der Politikgestaltung und Koordinierung im Hinblick auf die Weiterentwicklung des EU-Rahmens für das Krisenmanagement im Bereich der Cybersicherheit; ERSUCHT daher die Mitgliedstaaten, die Kommission, den Europäischen Auswärtigen Dienst (EAD), das EU INTCEN, CERT-EU, ENISA, Europol (EC3), Eurojust (EJCN), das Europäische Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (ECCC) sowie Vertreter des CSIRT-Netzwerks, des CyCLONe, der NIS-Kooperationsgruppe, der EDA und einschlägiger SSZ-Projekte ebenso wie andere potenzielle Interessenträger, sich in diesem Prozess einzubringen. Eine potenzielle Arbeitsgruppe, wie sie in der Empfehlung der Kommission vorgeschlagen wird, könnte als vorübergehendes Forum, in dem Vertreter aller einschlägigen Cyber-gemeinschaften innerhalb der Mitgliedstaaten und der EU zusammenkommen, weiter geprüft werden, wobei eine angemessene Vertretung aller Mitgliedstaaten zu gewährleisten und unter der politischen Leitung des Rates zu handeln ist. Eine solche Arbeitsgruppe sollte regelmäßig über ihre Tätigkeiten berichten und dem Rat gegebenenfalls Vorschläge zur Erörterung, Billigung und weiteren Lenkung unterbreiten. Darüber hinaus könnten weitere Formen des Dialogs innerhalb und zwischen Gemeinschaften eingerichtet werden, unter anderem durch Workshops, Seminare, gemeinsame Schulungen und Übungen;

22. UNTERSTREICHT die Rolle des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (ECCC) und des Netzwerks nationaler Koordinierungszentren im Zusammenhang mit der potenziellen Gemeinsamen Cyber-Einheit, insbesondere angesichts ihrer Aufgabe, die technologischen Kapazitäten, technologischen Lösungen, Fähigkeiten und Kompetenzen der Union im Bereich der Cybersicherheit erheblich zu verbessern;

23. ERSUCHT die EU und ihre Mitgliedstaaten, sich bei der Weiterentwicklung des EU-Rahmens für das Krisenmanagement im Bereich der Cybersicherheit einzubringen, unter anderem durch die Prüfung des Potenzials einer Initiative für eine Gemeinsame Cyber-Einheit, durch die Festlegung und Formulierung des Prozesses, einschließlich Etappenzielen und eines Zeitplans, sowie durch die Klärung der Ziele und möglichen Aufgaben und Zuständigkeiten; HEBT HERVOR, dass vorrangig bestehende Netze und Interaktionen innerhalb der einzelnen Gemeinschaften konsolidiert werden müssen und dass eine gründliche Bestandsaufnahme etwaiger Lücken und Erfordernisse beim Informationsaustausch innerhalb und zwischen Cybergemeinschaften sowie innerhalb und zwischen europäischen Organen, Einrichtungen und sonstigen Stellen vorgenommen und anschließend mögliche vorrangige Ziele und Prioritäten einer potenziellen Gemeinsamen Cyber-Einheit vereinbart werden müssen; BETONT – ohne dem Ergebnis vorzugreifen –, dass der Schwerpunkt auf die Ermittlung des Bedarfs an Informationsaustausch gelegt werden muss, um eine gemeinsame Lageerfassung aller einschlägigen Gemeinschaften aufzubauen; bei der Ermittlung von Lücken und Erfordernissen beim Informationsaustausch, einschließlich der möglichen Nutzung virtueller Plattformen, sollte sicheren Kommunikationskanälen für den Austausch von Verschlusssachen und sensiblen Informationen weiterhin gebührende Aufmerksamkeit gewidmet werden, wobei BETONT wird, wie wichtig es ist, bereits bestehende Infrastrukturen zu nutzen; mit der Einführung eines mehrstufigen Ansatzes soll Vertrauen aufgebaut und eine Grundlage für mögliche weitere Schritte zur Verbesserung der Abwehrbereitschaft und der operativen Zusammenarbeit geschaffen werden; IST SICH BEWUSST, dass unterschiedliche Ziele unterschiedliche Lösungen und das Engagement unterschiedlicher Vertreter einschlägiger Cybergemeinschaften innerhalb der EU und ihrer Mitgliedstaaten rechtfertigen könnten;

24. RUFT dazu AUF, während des gesamten Prozesses weitere Überlegungen zu einer Rechtsgrundlage für die potenzielle Gemeinsame Cyber-Einheit anzustellen, einschließlich einer Bewertung der Aufgaben und Funktionen im Vergleich zu denen, die der ENISA in der Empfehlung vor dem Hintergrund des Artikels 7 der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 zugewiesen werden; RUFT zu weiteren Überlegungen zu einzelnen Elementen der Empfehlung zur Gemeinsamen Cyber-Einheit AUF, auch im Hinblick auf die Idee der Schnellen EU-Einsatzteams für Cybersicherheit und den EU-Plan für die Reaktion auf Cybersicherheitsvorfälle und -krisen; HEBT HERVOR, dass eine potenzielle Gemeinsame Cyber-Einheit die Zuständigkeiten, Mandate und rechtlichen Befugnisse ihrer möglichen künftigen Teilnehmer achten muss;

25. RUFT die EU und ihre Mitgliedstaaten AUF, das Potenzial einer Initiative für eine Gemeinsame Cyber-Einheit zu prüfen, auch aus der Perspektive der Organe, Einrichtungen und sonstigen Stellen der EU, um die laufenden Bemühungen auf Ebene der Mitgliedstaaten zu ergänzen; BEGRÜßT die Absicht der Kommission, die Widerstandsfähigkeit der einschlägigen Organe, Einrichtungen und sonstigen Stellen der EU durch ihren anstehenden Vorschlag für eine Verordnung über gemeinsame verbindliche Cybersicherheitsvorschriften für die Organe, Einrichtungen und sonstigen Stellen der EU zu stärken;

26. BEKRÄFTIGT abschließend sein Engagement für die Verbesserung der Cyberresilienz und die Weiterentwicklung des EU-Rahmens für das Krisenmanagement im Bereich der Cybersicherheit und WIRD die Fortschritte REGELMÄßIG ÜBERPRÜFEN und weitere Leitlinien für die Ergänzung des EU-Rahmens für das Krisenmanagement im Bereich der Cybersicherheit bereitstellen.