Rat der
Europäischen Union

Brüssel, den 4. August 2021
(OR. en)

11155/21

CYBER 218
JAI 904
TELECOM 307
CSC 300
CIS 99
RELEX 702
ENFOPOL 299
COPS 298
COSI 155
HYBRID 52
CSCI 115
POLGEN 151
DATAPROTECT 200

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	2. August 2021
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	C(2021) 4520 final
Betr.:	EMPFEHLUNG DER KOMMISSION vom 23.6.2021 zum Aufbau einer Gemeinsamen Cyber-Einheit

Die Delegationen erhalten in der Anlage das Dokument C(2021) 4520 final.

Anl.: C(2021) 4520 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 23.6.2021
C(2021) 4520 final

EMPFEHLUNG DER KOMMISSION

vom 23.6.2021

zum Aufbau einer Gemeinsamen Cyber-Einheit

EMPFEHLUNG DER KOMMISSION

vom 23.6.2021

zum Aufbau einer Gemeinsamen Cyber-Einheit

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 292,

in Erwägung nachstehender Gründe:

(1) Cybersicherheit ist von grundlegender Bedeutung für die erfolgreiche digitale Transformation von Wirtschaft und Gesellschaft. Die EU ist entschlossen, noch nie dagewesene Summen dafür bereitzustellen, dass sich Menschen, Unternehmen und Behörden auf digitale Instrumente verlassen können.

(2) Während der COVID-19-Pandemie haben die Bedeutung der Konnektivität und die Abhängigkeit Europas von stabilen Netz- und Informationssystemen noch zugenommen, und es hat sich gezeigt, dass die gesamte Lieferkette geschützt werden muss. Zuverlässige und sichere Netz- und Informationssysteme sind besonders wichtig für diejenigen, die an vorderster Front gegen die Pandemie kämpfen, wie z. B. Krankenhäuser, medizinische Einrichtungen und Impfstoffhersteller. Wenn die Bemühungen der EU um die Prävention, Aufdeckung, Abschreckung und Minderung der verheerendsten Cyberangriffe auf diese Einrichtungen sowie die Reaktion darauf koordiniert werden, könnten Menschenleben gerettet und Versuche verhindert werden, die die Fähigkeit der EU untergraben, die Pandemie so schnell wie möglich zu besiegen. Zudem trägt die Stärkung der Cyberabwehrfähigkeit der EU wirksam zur Förderung eines globalen, offenen, stabilen und sicheren Cyberraums bei.

(3) Da Cybersicherheitsbedrohungen nicht an Grenzen haltmachen und die Angriffe fortwährend zunehmen und immer komplexer, folgenschwerer und zielgerichteter werden[1], sollten die einschlägigen Cybersicherheitseinrichtungen und -akteure auch ihre Fähigkeit ausbauen, auf solche Bedrohungen und Angriffe zu reagieren, indem sie die vorhandenen Ressourcen nutzen und ihre Anstrengungen besser koordinieren. Alle einschlägigen Akteure in der EU müssen in der Lage sein, kollektiv zu reagieren und Informationen nicht nur dann auszutauschen, wenn es nicht anders geht.

(4) Trotz der erheblichen Fortschritte im Bereich Cybersicherheit, die dank der Zusammenarbeit zwischen den Mitgliedstaaten vor allem in der Kooperationsgruppe für Netz- und Informationssysteme (NIS-Kooperationsgruppe) und im gemäß der Richtlinie (EU) 2016/1148[2] errichteten Netzwerk nationaler Reaktionsteams für IT-Sicherheitsvorfälle (CSIRTs-Netz) erzielt werden konnten, gibt es immer noch keine

---

1 ENISA, 2020 Threat Landscape (ENISA-Bericht zur Bedrohungslage 2020); Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020 (Bewertung der Bedrohungslage im Bereich der organisierten Kriminalität im Internet 2020).

2 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

gemeinsame EU-Plattform, über die Informationen, die von verschiedenen Cybersicherheitsgemeinschaften zusammengetragen wurden, sicher und effizient ausgetauscht sowie operationelle Fähigkeiten koordiniert und von einschlägigen Akteuren mobilisiert werden können. Infolgedessen besteht die Gefahr, dass Cyberbedrohungen und Cybersicherheitsvorfälle isoliert voneinander angegangen werden, was die Effizienz verringert und zu mehr Schwachstellen führt. Außerdem fehlt es im Hinblick auf die Informationsweitergabe und auf die Unterstützung bei der Reaktion auf Sicherheitsvorfälle an einem Kanal auf EU-Ebene für die technische und operative Zusammenarbeit mit dem Privatsektor.

(5) Die vorhandenen Rahmen und Strukturen sowie die Ressourcen und Fachkenntnis in den Mitgliedstaaten und den einschlägigen Organen, Einrichtungen und sonstigen Stellen der EU bilden eine solide Grundlage für eine kollektive Reaktion auf Cybersicherheitsbedrohungen, -vorfälle und -krisen[3]. Diese Architektur umfasst, auf der operativen Ebene, die Koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (Blueprint)[4], das CSIRTs-Netz und das Europäische Netz der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe)[5] sowie das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3) und die Gemeinsame Taskforce gegen die Cyberkriminalität (J-CAT) bei der Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und das EU-Notfallprotokoll für die Strafverfolgung (EU LE ERP). Die NIS-Kooperationsgruppe, das EU-Zentrum für Informationsgewinnung und -analyse (EU-INTCEN) und das Instrumentarium für die Cyberdiplomatie (Cyber Diplomacy Toolbox)[6] sowie Cyberabwehrprojekte im Rahmen der Ständigen Strukturierten Zusammenarbeit (SSZ)[7] tragen ebenfalls zur politischen und operativen Zusammenarbeit in verschiedenen Cybersicherheitsgemeinschaften bei. Die Agentur der Europäischen Union für Cybersicherheit (ENISA) ist laut ihrem gestärkten Mandat dafür zuständig, die operative Zusammenarbeit[8] im Bereich der Cybersicherheit von Netz- und Informationssystemen, der Nutzer dieser Systeme und anderer von

---

3 Das Europäische Netz der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) wurde von den Mitgliedstaaten auf die Blueprint-Empfehlung hin errichtet. Dabei handelt es sich um ein Netz nationaler Experten für operatives und Krisenmanagement, das laut Vorschlag der Kommission durch die Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 (COM(2020) 823 final) kodifiziert werden soll. 2020/0359 (COD) wurde im Dezember 2020 vorgeschlagen.

4 Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen.

5 Diese Empfehlung trägt dem Bericht über die Planübung Blueprint Operational Level Exercise (Blue OLEx) 2020 und insbesondere der vom Vorsitz verfassten Zusammenfassung der strategischen und politischen Beratungen über die gemeinsame Cyber-Einheit Rechnung.

6 Schlussfolgerungen des Rates zu einem Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten (Cyber Diplomacy Toolbox) vom 19. Juni 2017 (9906/17).

7 Vor allem das von Litauen koordinierte SSZ-Projekt „Teams für die rasche Reaktion auf Cybervorfälle und die gegenseitige Unterstützung im Bereich der Cybersicherheit“ und das von Deutschland koordinierte SSZ-Projekt „Koordinierungszentrum für den Cyber- und Informationsraum“.

8 Gemäß Artikel 7 der Verordnung (EU) 2019/881 muss die Agentur die operative Zusammenarbeit zwischen den Mitgliedstaaten, den Organen, Einrichtungen und sonstigen Stellen der Union und den Interessenträgern unterstützen. Dazu gehören die Unterstützung der Mitgliedstaaten bei der operativen Zusammenarbeit im CSIRTs-Netz, die Erstellung eines regelmäßigen ausführlichen technischen Lageberichts über Cybersicherheitsvorfälle und Cyberbedrohungen in der EU sowie Beiträge zur Entwicklung einer koordinierten Reaktion auf grenzüberschreitende Cybersicherheitsvorfälle und -krisen großen Ausmaßes. Außerdem trägt die ENISA mit dem Europäischen Sicherheits- und Verteidigungskolleg zu Fortbildungsmaßnahmen bei.

Cyberbedrohungen und Sicherheitsvorfällen betroffenen Personen zu unterstützen. Dank der Integrierten Regelung für die politische Reaktion auf Krisen (IPCR) ist die EU in der Lage, ihre politische Reaktion auf größere Krisen zu koordinieren, und dies gilt auch für Cyberangriffe großen Ausmaßes.

(6) Allerdings gibt es noch keinen Mechanismus, der die Nutzung der vorhandenen Ressourcen und gegenseitige Unterstützung der verschiedenen Cybergemeinschaften ermöglicht, die für die Sicherheit von Netz- und Informationssystemen, Cyberdiplomatie und im Krisenfall ggf. Cyberabwehr zuständig sind. Es gibt es auch keinen umfassenden Mechanismus auf EU-Ebene für die technische und operative Zusammenarbeit der verschiedenen Gemeinschaften in den Bereichen Lageerfassung, Abwehrbereitschaft und Reaktion. Abgesehen davon sollten durch Europol bzw. die INTCEN Synergien mit den Strafverfolgungs- und Nachrichtendiensten erzielt werden.

(7) Die Kommission, der Hohe Vertreter der Union für Außen- und Sicherheitspolitik (Hoher Vertreter), die Mitgliedstaaten und die einschlägigen Organe, Einrichtungen und sonstigen Stellen der EU erkennen an, wie wichtig es ist, die Stärken, Schwachstellen, Lücken und Überschneidungen der in den letzten Jahren geschaffenen Cybersicherheitsarchitektur der Union zu analysieren. In Absprache mit den Mitgliedstaaten hat die Kommission, unter Mitwirkung des Hohen Vertreters, in Reaktion auf diese Analyse und als wichtige Komponente der Strategie für eine Sicherheitsunion[9], der Digitalstrategie[10] und der Cybersicherheitsstrategie[11] ein Konzept für eine Gemeinsame Cyber-Einheit entwickelt.

(8) In Krisenfällen sollten sich die Mitgliedstaaten auf die EU-Solidarität in Form koordinierter Hilfe auch von allen vier Cybersicherheitsgemeinschaften, d. h. der zivilen, der Strafverfolgungs-[12], der Diplomatie- und gegebenenfalls der Verteidigungsgemeinschaft, verlassen können. Inwieweit sich Teilnehmer aus einer oder mehreren Gemeinschaften einbringen, hängt von der Art des Sicherheitsvorfalls bzw. der Sicherheitskrise großen Ausmaßes und folglich auch von der Art der erforderlichen Gegenmaßnahmen ab. Bei Cyberbedrohungen sowie Cybersicherheitsvorfällen und -krisen sind gut ausgebildete Sachverständige und technische Ausrüstung entscheidend für die Vermeidung schwerer Schäden und eine wirksame Folgenbewältigung. Daher wird die Gemeinsame Cyber-Einheit in erster Linie klar benannte technische und operative Fähigkeiten (vor allem Sachverständige und Ausrüstung) Mitgliedstaaten im Bedarfsfall zur Verfügung stellen. Dank dieser Plattform werden die Teilnehmer in der einzigartigen Position sein, diese Fähigkeiten durch Schnelle EU-Einsatzteams für Cybersicherheit auszubauen und zu koordinieren und gleichzeitig für angemessene Synergien mit den bereits bestehenden SSZ-Cyberprojekten zu sorgen.

---

9 Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – EU-Strategie für eine Sicherheitsunion, COM(2020) 605 final.

10 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Gestaltung der digitalen Zukunft Europas, COM(2020) 67 final.

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

12 Auch für die justizielle Zusammenarbeit relevant.

(9) Die Gemeinsame Cyber-Einheit ist zugleich eine virtuelle und eine physische Plattform und erfordert nicht die Schaffung eines zusätzlichen, eigenständigen Gremiums. Ihre Errichtung sollte die Zuständigkeiten und Befugnisse der nationalen Cybersicherheitsbehörden und der einschlägigen Einrichtungen der Union unberührt lassen. Die Gemeinsame Cyber-Einheit sollte auf Absichtserklärungen zwischen ihren Teilnehmern beruhen. Als Plattform für eine sichere und schnelle operative und technische Zusammenarbeit zwischen den EU-Einrichtungen und den Behörden der Mitgliedstaaten sollte sie auf bestehenden Strukturen, Ressourcen und Fähigkeiten aufbauen und deren Leistungsfähigkeit steigern. Sie sollte auch alle Cybersicherheitsgemeinschaften zusammenbringen, d. h. die zivile, die Strafverfolgungs-, die Diplomatie- und die Verteidigungsgemeinschaft. Die Plattformteilnehmer sollten entweder eine operative Rolle spielen oder eine unterstützende Funktion haben. Zu den operativen Teilnehmern sollten die ENISA, Europol, das Computer-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der EU (CERT-EU), die Kommission, der Europäische Auswärtige Dienst (einschließlich INTCEN), das CSIRTs-Netz und EU-CyCLONe gehören. Zu den unterstützenden Teilnehmern sollten die Europäische Verteidigungsagentur (EDA), der Vorsitz der NIS-Kooperationsgruppe, die Horizontale Gruppe „Cyberfragen“ des Rates und ein Vertreter der einschlägigen SSZ-Projekte[13] gehören. Da die Mitgliedstaaten über die operativen Fähigkeiten und Kompetenzen verfügen, um auf Cyberbedrohungen, Cybersicherheitsvorfälle und -krisen großen Ausmaßes zu reagieren, sollten sich die Plattformteilnehmer bei der Verfolgung ihrer Ziele in erster Linie auf ihre eigenen Kapazitäten stützen, wobei die einschlägigen Einrichtungen der Union Hilfe leisten können.

(10) Die Gemeinsame Cyber-Einheit sollte dem 2017 mit dem Konzeptentwurf „Blueprint“ eingeleiteten Prozess neue Impulse geben. Sie sollte die Blueprint-Architektur weiter operationalisieren und ein entscheidender Schritt hin zu einem europäischen Rahmen für das Cybersicherheitskrisenmanagement sein, der der koordinierten und rechtzeitigen Ermittlung und Minderung von sowie Reaktion auf Bedrohungen und Risiken dient. Durch diesen Schritt sollte die Gemeinsame Cyber-Einheit die EU dabei unterstützen, auf aktuelle und sich abzeichnende Bedrohungen zu reagieren.

(11) Durch Ihre Beteiligung an der Gemeinsamen Cyber-Einheit sollte operative und unterstützende Teilnehmer in die Lage versetzen, im EU-Rahmen für die Reaktion auf Cybersicherheitskrisen mit einem breiteren Spektrum von Interessenträgern zusammenzuarbeiten. Bei der Wahrnehmung ihrer Aufgaben im Rahmen ihrer Mandate sollten die Teilnehmer von einer verbesserten Abwehrbereitschaft und einer umfassenderen Lageerfassung profitieren, die alle Aspekte im Zusammenhang mit Cybersicherheitsbedrohungen und -vorfällen abdecken, und zusätzliches Fachwissen im Bereich der Cybersicherheit mobilisieren. Beispielsweise sollten die Teilnehmer regelmäßig in gemeinschaftsübergreifenden Übungen eingebunden werden, eine klar definierte Rolle im EU-Krisenreaktionsplan übernehmen, die Visibilität ihrer Maßnahmen durch gemeinsame öffentliche Kommunikation fördern und Vereinbarungen über die operative Zusammenarbeit mit dem Privatsektor schließen. Parallel dazu sollte der Beitrag zur Gemeinsamen Cyber-Einheit es den Teilnehmern ermöglichen, bestehende Netze wie das CSIRTs-Netz und EU-CyCLONe zu stärken, indem diesen sichere Instrumente für den Informationsaustausch und bessere

[13] Siehe Fußnote 5. Da der EAD und die EDA das SSZ-Sekretariat wahrnehmen, werden sie mit den Koordinatoren der einschlägigen SSZ-Projekte zusammenarbeiten.

Aufdeckungskapazitäten (Sicherheitseinsatzzentren) zur Verfügung gestellt werden, die sie in die Lage versetzen, die verfügbaren operativen Fähigkeiten der EU zu nutzen.

(12) Die Teilnehmer der Gemeinsamen Cyber-Einheit sollten sich auf die technische und operative Zusammenarbeit, einschließlich gemeinsamer Aktionen, konzentrieren. Die Teilnehmer sollten in dem nach ihrem Mandat zulässigen Umfang zu dieser Zusammenarbeit beitragen. Die Zusammenarbeit sollte auf laufenden Bemühungen aufbauen und diese ergänzen. Je nach Art der jeweiligen Zusammenarbeit können weitere Teilnehmer dazukommen.

(13) Die Plattform sollte Sachverständige für technisches und operatives Krisenmanagement aus den Mitgliedstaaten und EU-Einrichtungen zusammenbringen, um die Reaktion auf Cyberbedrohungen, Cybersicherheitsvorfälle und -krisen unter Nutzung der vorhandenen Fähigkeiten und des vorhandenen Fachwissens zu koordinieren. Sachverständige, die an der Gemeinsamen Cyber-Einheit teilnehmen, können eine viel größere Angriffsfläche überwachen und schützen, indem sie sowohl die physische als auch die virtuelle Plattform nutzen. Hierzu sollten die Teilnehmer ihre Bemühungen im Falle grenzüberschreitender Sicherheitsvorfälle und -krisen sowie die Unterstützung der von Sicherheitsvorfällen betroffenen Länder über die Plattform koordinieren.

(14) Der Aufbau der Gemeinsamen Cyber-Einheit sollte schrittweise erfolgen unter Nutzung und Konsolidierung der in dieser Empfehlung genannten bestehenden Rahmen und Strukturen, einschließlich der Kooperationsmechanismen, die im Rahmen von mitgliedstaatlich geführten Foren eingerichtet wurden (z. B. CSIRTs-Netzwerk, EU-CyCLONe, horizontale Arbeitsgruppe des Rates zu Cyberfragen, J-CAT und einschlägige SSZ-Projekte), und, aufseiten der Organe, Einrichtungen und sonstigen Stellen der EU, der strukturierten Zusammenarbeit zwischen ENISA und CERT-EU sowie der interinstitutionellen Gruppe für den Informationsaustausch im Bereich Cybersicherheit. Darüber hinaus sollten die Rahmen für hybride Bedrohungen und Katastrophenschutz[14] sowie sektorspezifische Rahmen[15] angemessen berücksichtigt werden. Ein ähnlich strukturierte Verknüpfung sollte mit der IPCR[16] hergestellt werden. So können im Krisenfall den im Rat versammelten politischen Entscheidungsträgern rasch und effizient Informationen übermittelt werden.

(15) Die Gemeinsame Cyber-Einheit sollte daher in den nächsten beiden Jahren schrittweise und transparent aufgebaut werden. Aus diesem Grund sollten die in dieser Empfehlung festgelegten Ziele in vier Stufen umgesetzt werden, die im Anhang dieser Empfehlung beschrieben sind. Im Zuge der ersten beiden Stufen sollten in einer von der Kommission einzurichtenden Arbeitsgruppe ein von der ENISA organisierter und unterstützter Vorbereitungsprozess stattfinden, an dem operative und unterstützende Teilnehmer auf EU- und Mitgliedstaatsebene beteiligt sind. Die Vorarbeit sollte sich an den Grundsätzen Zusammenarbeit, Inklusion und Konsensbildung orientieren. Das Engagement aller Teilnehmer sollte gefördert werden, damit unterschiedliche

---

14 In diesem Kontext sollten zwischen der Gemeinsamen Cyber-Einheit und dem Katastrophenschutzverfahren der Union (UCPM) Synergien geschaffen werden, um die Abwehrbereitschaft und Reaktionsfähigkeit Europas im Falle mehrschichtiger Katastrophen und Notfälle, die ein Cyberelement umfassen, zu verbessern.

15 Wie jener des Finanzsektors, der in der Verordnung (EU) 2021/xx des Europäischen Parlaments und des Rates* [DORA] vorgesehen ist.

16 Siehe Erwägungsgrund 5.

Ansichten und Standpunkte zum Ausdruck gebracht und Lösungen gefunden werden können, die eine möglichst breite Unterstützung finden. Je nach Bedarf und unter gerechtfertigten Bedingungen kann der Zeitplan für die verschiedenen in dieser Empfehlung genannten Stufen angepasst werden.

(16) In der ersten Stufe sollte der Vorbereitungsprozess mit der Ermittlung der relevanten verfügbaren operativen Fähigkeiten der EU und der Einleitung einer Bewertung der Aufgaben und Zuständigkeiten der Plattformteilnehmer beginnen. Die zweite Stufe sollte die Entwicklung des EU-Plans für die Reaktion auf Cybersicherheitsvorfälle und -krisen im Einklang mit dem Blueprint[17] und dem EU-Notfallprotokoll für die Strafverfolgung, den Auftakt von Aktivitäten der Abwehrbereitschaft und Lageerfassung, die mit dem Rechtsakt zur Cybersicherheit und der Europol-Verordnung[18] im Einklang stehen, und den Abschluss der Bewertung der Aufgaben und Zuständigkeiten der Plattformteilnehmer umfassen. Die Arbeitsgruppe sollte die Ergebnisse dieser Bewertung der Kommission und dem Hohen Vertreter vorlegen, die diese Bewertung anschließend dem Rat übermitteln. Die Kommission und der Hohe Vertreter sollten auf der Grundlage dieser Bewertung gemäß ihren jeweiligen Zuständigkeiten einen gemeinsamen Bericht erstellen, und den Rat ersuchen, diesen Bericht im Wege von Schlussfolgerungen des Rates zu billigen.

(17) Nach der Billigung des Berichts durch den Rat wird die Gemeinsame Cyber-Einheit in Betrieb genommen, damit die beiden verbleibenden Stufen abgeschlossen werden können. In der dritten Stufe sollten die Teilnehmer in der Lage sein, in der Gemeinsamen Cyber-Einheit schnelle EU-Einsatzteams nach den im EU-Plan für die Reaktion auf Cybersicherheitsvorfälle und -krisen festgelegten Verfahren zu entsenden, und dafür sowohl die physische als auch die virtuelle Plattform nutzen und zu verschiedenen Aspekten der Reaktion auf Sicherheitsvorfälle beitragen (von der öffentlichen Kommunikation bis zur anschließenden Folgenbewältigung). In der vierten und letzten Stufe werden Interessenträger aus dem Privatsektor, darunter Nutzer und Anbieter von Cybersicherheitslösungen und -diensten, aufgefordert, einen Beitrag zur Plattform zu leisten, damit die Teilnehmer den Informationsaustausch verbessern und die koordinierte Reaktion der EU auf Cyberbedrohungen und Cybersicherheitsvorfälle stärken können.

(18) Nach Abschluss der vierten Stufe sollten die Teilnehmer einen Bericht über die Fortschritte bei der Umsetzung der vier in der Empfehlung dargelegten Stufen erstellen, in dem die Ergebnisse und Herausforderungen beschrieben werden und der der Kommission und dem Hohen Vertreter vorgelegt werden sollte. Auf der Grundlage dieses Berichts sollten die Kommission und der Hohe Vertreter die Ergebnisse bewerten und Schlussfolgerungen für die Zukunft der Gemeinsamen Cyber-Einheit ziehen.

(19) Die Kommission, ENISA, Europol und CERT-EU sollten der Gemeinsamen Cyber-Einheit – vorbehaltlich der Verfügbarkeit von Haushaltsmitteln und Humanressourcen – administrative, finanzielle und technische Unterstützung gemäß Abschnitt IV dieser Empfehlung leisten. Die Stärkung der operativen Cybersicherheitsfähigkeiten der einschlägigen Organe, Einrichtungen und sonstigen Stellen der EU wird von

---

17 Siehe Fußnote 3.

18 Verordnung (EU) 2016/794 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates.

entscheidender Bedeutung sein, um eine wirksame Vorbereitung der Gemeinsamen Cyber-Einheit und deren Nachhaltigkeit zu gewährleisten. Die Kommission beabsichtigt, dafür zu sorgen, dass die geplante Verordnung über gemeinsame verbindliche Cybersicherheitsvorschriften für die Organe, Einrichtungen und sonstigen Stellen der EU (Oktober 2021) im Falle des CERT-EU die Rechtsgrundlage für diesen Beitrag bildet.

(20) Dank ihres erweiterten Mandats gemäß der Verordnung (EU) 2019/881 (Cybersicherheitsverordnung) ist die ENISA in der einzigartigen Position, die Vorbereitung der gemeinsamen Cyber-Einheit sowohl zu organisieren und zu unterstützen als auch zu ihrer Operationalisierung beizutragen. Im Einklang mit der Cybersicherheitsverordnung richtet die ENISA derzeit ein Büro in Brüssel ein, um ihre strukturierte Zusammenarbeit mit dem CERT-EU zu unterstützen. Diese strukturierte Zusammenarbeit, einschließlich nebeneinander liegender Büros, bietet günstige Rahmenbedingungen, die die Errichtung der Gemeinsamen Cyber-Einheit erleichtert, einschließlich der Einrichtung ihrer physischen Räumlichkeiten, die bei Bedarf den Teilnehmern sowie Mitarbeitern anderer einschlägiger Organe, Einrichtungen und sonstiger Stellen der EU zur Verfügung gestellt werden sollten. Die physische Plattform sollte mit einer virtuellen Plattform in Form von Instrumenten für die Zusammenarbeit und den sicheren Informationsaustausch kombiniert werden. Diese Instrumente erschließen eine Fülle von Informationen, die über den europäischen Cyberschutzschild[19], einschließlich der Sicherheitseinsatzzentren (SOC) und der Informationsaustausch- und -analysezentren (ISAC), gesammelt wurden.

(21) Im EU-Notfallprotokoll für die Strafverfolgung, das der Rat 2018 verabschiedet hat, wird dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3)[20] von Europol als Teil des Blueprint-Rahmens eine zentrale Rolle zugewiesen. Dieses Protokoll ermöglicht es den Strafverfolgungsbehörden der EU, sieben Tage die Woche rund um die Uhr rasch auf mutmaßlich böswillige grenzüberschreitende Cyberangriffe großen Ausmaßes zu reagieren und sie zu bewerten und rechtzeitig und sicher kritische Informationen auszutauschen, um die Reaktionen darauf zu koordinieren. Das Protokoll enthält weitere Einzelheiten über die Zusammenarbeit mit anderen EU-Einrichtungen und über EU-weite Krisenprotokolle sowie über die Krisenzusammenarbeit mit dem Privatsektor. Die Strafverfolgungsgemeinschaft sollte – gegebenenfalls mit Unterstützung von Europol – zur Gemeinsamen Cyber-Einheit beitragen, indem sie während des gesamten Ermittlungszyklus im Einklang mit dem strafrechtlichen Rahmen und den jeweiligen Verfahren für die elektronische Beweisführung die erforderlichen Schritte unternimmt. Seit der Errichtung des EC3 im Jahr 2013 leistet Europol operative Unterstützung und erleichtert die operative Zusammenarbeit bei der Bekämpfung von Cyberbedrohungen. Europol sollte die Plattform gemäß seinem Mandat und dem Konzept der erkenntnisgestützten Polizeiarbeit unterstützen und gleichzeitig sämtliche internen Fachkenntnisse, Produkte, Instrumente und Dienste einsetzen, die für die Reaktion auf einen Sicherheitsvorfall oder eine Krise relevant sind.

---

19 JOIN/2020/18 final, Abschnitt 1.2.

20 Errichtet mit der Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates.

(22) Gemäß der Richtlinie 2013/40/EU über Angriffe auf Informationssysteme müssen die Mitgliedstaaten ferner sicherstellen, dass sie über eine operative nationale Kontaktstelle verfügen, die sieben Tage die Woche rund um die Uhr für den Austausch von Informationen über die in der Richtlinie definierten Straftaten zur Verfügung steht. Das Netz der operativen nationalen Kontaktstellen sollte ebenfalls zur Gemeinsamen Cyber-Einheit beitragen, indem es gegebenenfalls die Einbindung der Strafverfolgungsbehörden der Mitgliedstaaten sicherstellt.

(23) Die EU-Cyberdiplomatiegemeinschaft trägt dazu bei, einen globalen, offenen, stabilen und sicheren Cyberraum zu fördern und zu schützen sowie entsprechende böswillige Cyberaktivitäten zu verhindern, abzuschrecken und darauf zu reagieren. 2017 verabschiedete die EU einen Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten (Cyber Diplomacy Toolbox). Dieser Rahmen ist Teil der umfassenderen Cyberdiplomatiepolitik der EU. Er trägt zur Konfliktprävention und zu mehr Stabilität in den internationalen Beziehungen bei. Der Rahmen ermöglicht es der EU und den Mitgliedstaaten, gegebenenfalls in Zusammenarbeit mit internationalen Partnern alle Maßnahmen der Gemeinsamen Außen- und Sicherheitspolitik (GASP) im Einklang mit den jeweiligen Verfahren für die Verwirklichung ihrer Ziele zu nutzen, um die Zusammenarbeit zu fördern, Bedrohungen zu mindern und Einfluss auf das derzeitige und etwaige künftige böswillige Verhalten im Cyberraum zu nehmen. Die Cyberdiplomatiegemeinschaft sollte unter der Gemeinsamen Cyber-Einheit kooperieren, indem sie die Ausschöpfung des gesamten Spektrums an diplomatischen Maßnahmen insbesondere im Bereich öffentliche Kommunikation unterstützt und so die gemeinsame Lageerfassung und die Zusammenarbeit mit Drittländern im Krisenfall fördert.

(24) Gemäß dem Blueprint-Rahmen sollte der Hohe Vertreter auch über das INTCEN zur Gemeinsamen Cyber-Einheit beitragen, indem er für eine kontinuierliche, erkenntnisgestützte gemeinsame Lageerfassung für bestehende und sich abzeichnende Bedrohungen sorgt, einschließlich jeglicher notwendigen strategischen Lageerfassung.

(25) Ziel der EU und der Mitgliedstaaten ist es, auch im Hinblick auf Missionen und Operationen im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) die Cyberabwehrfähigkeiten zu stärken und Synergien, Koordinierung und Zusammenarbeit zwischen den einschlägigen Organen, Einrichtungen und sonstigen Stellen der EU sowie mit und zwischen den Mitgliedstaaten weiter auszubauen. Grundlage der Gemeinschaftsfunktionen sind eine zwischenstaatliche Governance auf EU-Ebene, nationale militärische Befehlsstrukturen sowie militärische Fähigkeiten und Mittel bzw. Fähigkeiten und Mittel mit doppeltem Verwendungszweck. Angesichts ihrer unterschiedlichen Natur sollten spezifische Schnittstellen mit der Gemeinsamen Cyber-Einheit eingerichtet werden, um den Austausch von Informationen mit der Cyberabwehrgemeinschaft zu ermöglichen[21].

(26) Die Ständige Strukturierte Zusammenarbeit (SSZ) ist ein Rechtsrahmen, der mit dem Vertrag von Lissabon[22] eingeführt und 2017 in den Unionsrahmen aufgenommen wurde. Im Rahmen der SSZ wurde eine Reihe von Projekten im Cyberbereich

---

21 Insbesondere über den EAD, um eine angemessene Beteiligung der Cyberabwehrgemeinschaft zu ermöglichen, die auf den freiwilligen nationalen Beiträgen beruht.

22 Artikel 42 Absatz 6, Artikel 46 und Protokoll Nr. 10.

gestartet, die zur Erfüllung der Verpflichtung 11[23] „verstärkte Anstrengungen bei der Zusammenarbeit im Bereich der Cyberabwehr zu gewährleisten, wie etwa Informationsaustausch, Ausbildung und operative Unterstützung“ beitragen. Der EAD, einschließlich des Militärstabs der EU und der EDA, nimmt das SSZ-Sekretariat wahr, das innerhalb des Unionsrahmens eine zentrale Anlaufstelle für alle SSZ-Angelegenheiten bildet und alle unterstützenden und koordinierenden Funktionen im Zusammenhang mit SSZ-Projekten ausübt (z. B. Bewertung neuer Projektvorschläge, Vorbereitung der Fortschrittsberichte der Projekte usw.). Vertreter einschlägiger SSZ-Projekte sollten die Gemeinsame Cyber-Einheit insbesondere bei Lageerfassung und Abwehrbereitschaft unterstützen.

(27) Über die Gemeinsame Cyber-Einheit sollten die Teilnehmer die Interessenträger des Privatsektors, einschließlich der Anbieter und Nutzer von Cybersicherheitslösungen und -diensten, angemessen einbeziehen, um den europäischen Cyberkrisenmanagementrahmen unter gebührender Berücksichtigung des Rechtsrahmens für Datenaustausch und Informationssicherheit zu unterstützen. Cybersicherheitsanbieter sollten zu der Initiative beitragen, indem sie Bedrohungsanalysen austauschen und Sicherheitsvorfallmelder bereitstellen, um die Kapazität der Cyber-Einheit, auf Angriffe und Krisen großen Ausmaßes zu reagieren, rasch zu erweitern. Vor allem die Nutzer von Cybersicherheitsprodukten und -diensten, die in den Anwendungsbereich der NIS-Richtlinie fallen, sollten über einen – derzeit noch fehlenden – strukturierten Kanal, der mit den Informationsaustausch- und Analysezentren auf EU-Ebene (ISAC)[24] verbunden ist, Hilfe und Beratung erhalten können. Die Plattform könnte auch zur Stärkung der Zusammenarbeit mit internationalen Partnern beitragen.

(28) Die Entwicklung und Aufrechterhaltung der Lageerfassung erfordert modernste Angriffserkennungs- und -präventionskapazitäten. Die Gemeinsame Cyber-Einheit sollte sich auf ein modernes Netz stützen, das böswillige Cybersicherheitsbedrohungen und -vorfälle, die sich auf maßgebliche Kommunikations- und Informationssysteme in der gesamten Union auswirken können, analysieren kann. Dies bedeutet, dass unter anderem Bedrohungswissen aus Kommunikationsnetzen, die von nationalen, sektoralen und grenzübergreifenden Sicherheitseinsatzzentren überwacht werden, an die Gemeinsame Cyber-Einheit übermittelt werden sollte, damit die Plattformteilnehmer die Bedrohungslage in der EU besser abschätzen können.

(29) Um den Austausch operativer Informationen sowie gegebenenfalls vertraulichen Materials zu unterstützen, sollte die Plattform hinreichend sichere Kommunikationskanäle nutzen. Diese Kanäle könnten auch auf der bestehenden Infrastruktur wie z. B. der von Europol und der Strafverfolgungsgemeinschaft genutzten Netzanwendung für sicheren Informationsaustausch (SIENA) aufbauen. Wie in der Cybersicherheitsstrategie angekündigt, sollten die von Organen, Einrichtungen und sonstigen Stellen der EU verwendeten Instrumente den Vorschriften zur Informationssicherheit entsprechen, die die Kommission in Kürze vorschlagen wird.

---

23 Jeder der an der SSZ teilnehmenden Mitgliedstaaten geht 20 Einzelverpflichtungen ein, die in die fünf Schlüsselkategorien untergegliedert sind, die in Artikel 2 des Protokolls Nr. 10 zum Vertrag über die Europäische Union über die Ständige Strukturierte Zusammenarbeit genannt sind.

24 Beispiele für bereits bestehende ISAC, die dabei mitwirken könnten, sind das Europäische Energie-ISAC (EE-ISAC) und das Europäische Finanzinstitute-ISAC (FI-ISAC).

(30) Die Kommission wird vor allem über das Programm „Digitales Europa“ die notwendigen Investitionen zur Errichtung der physischen und virtuellen Plattform, zum Aufbau und Betrieb sicherer Kommunikationskanäle und Schulungskapazitäten sowie zur Entwicklung und Einführung von Detektionsfähigkeiten unterstützen. Darüber hinaus könnten auch aus dem Europäischen Verteidigungsfonds Mittel zur Finanzierung von Schlüsseltechnologien für die Cyberabwehr und von Cyberabwehrkapazitäten bereitgestellt werden, die die Abwehrbereitschaft der Mitgliedstaaten im Bereich der Cyberabwehr verbessern würden —

HAT FOLGENDE EMPFEHLUNG ABGEGEBEN:

I ZWECK DIESER EMPFEHLUNG

(1) Zweck dieser Empfehlung ist es, die Maßnahmen zu ermitteln, die erforderlich sind, um die Bemühungen der EU zur Verhütung, Aufdeckung, Abschreckung, Abschwächung und Bewältigung von Cybersicherheitsvorfällen und -krisen großen Ausmaßes durch eine gemeinsame Cyber-Einheit zu koordinieren. Hierzu enthält diese Empfehlung auch Festlegungen zu dem Prozess, zu den Etappenzielen und zur Zeitleiste, die die Mitgliedstaaten und die einschlägigen Organe, Einrichtungen und sonstigen Stellen der EU bei Einrichtung und Ausbau dieser Plattform befolgen sollten.

(2) Die Mitgliedstaaten sowie die einschlägigen Organe, Einrichtungen und sonstigen Stellen der EU sollten dafür sorgen, dass sie im Falle von Cybersicherheitsvorfällen und -krisen großen Ausmaßes ihre Bemühungen über eine gemeinsame Cyber-Einheit koordinieren, die das Fachwissen der Behörden der Mitgliedstaaten und der einschlägigen Organe, Einrichtungen und sonstigen Stellen der EU bündelt und gegenseitige Unterstützung[25] bereitstellt. Außerdem sollte die Gemeinsame Cyber-Einheit den Teilnehmern gestatten, mit dem Privatsektor zu kooperieren.

II BEGRIFFSBESTIMMUNGEN

(3) Für die Zwecke dieser Empfehlung gelten folgende Begriffsbestimmungen:

a) „EU-Plan für die Reaktion auf Cybersicherheitsvorfälle und -krisen“: eine Zusammenstellung von Aufgaben, Modalitäten und Verfahren, die der Vervollständigung des EU-Rahmens für die Reaktion auf Cybersicherheitskrisen dienen, der in Nummer 1 der Empfehlung der Kommission vom 13.9.2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen („Konzeptentwurf“) beschrieben ist;

b) „Cybersicherheitsgemeinschaften“: kooperative Gruppen der Zivilgesellschaft, der Strafverfolgung, Diplomatie und Verteidigung, die sowohl die Mitgliedstaaten als auch die einschlägigen Organe, Einrichtungen und

[25] In Übereinstimmung mit dem Ansatz und den Grundsätzen der Richtlinie (EU) 2016/1148 und des Artikels 222 AEUV. Unbeschadet des Artikels 42 Absatz 7 des Vertrags über die Europäische Union.

sonstigen Stellen der EU vertreten und Informationen austauschen, um gemeinsame Ziele, Interessen und Missionen im Bereich der Cybersicherheit zu verfolgen;

c) „Teilnehmer aus dem Privatsektor“: Vertreter von Einrichtungen des Privatsektors, die Cybersicherheitslösungen[26] und -dienste[27] anbieten oder nutzen;

d) „Sicherheitsvorfall großen Ausmaßes“: ein Sicherheitsvorfall im Sinne von Artikel 4 Absatz 7 der Richtlinie (EU) 2016/1148 mit erheblichen Auswirkungen in mindestens zwei Mitgliedstaaten;

e) „Integrierter EU-Cybersicherheitslagebericht“: ein Bericht, in dem die Beiträge der Teilnehmer der Gemeinsamen Cyber-Einheit zusammengetragen werden und der auf dem technischen EU-Cybersicherheitslagebericht nach Artikel 7 Absatz 6 der Verordnung (EU) 2019/881 aufbaut;

f) „Schnelles EU-Einsatzteam für Cybersicherheit“: ein Team, das sich aus anerkannten Cybersicherheitsexperten, insbesondere aus den CSIRT der Mitgliedstaaten zusammensetzt und von ENISA, CERT-EU sowie Europol unterstützt wird und das bereit ist, Teilnehmer, die von Sicherheitsvorfällen und -krisen großen Ausmaßes betroffen sind, aus der Ferne zu unterstützen;

g) „Absichtserklärung“: eine Vereinbarung zwischen den Teilnehmern, die als Grundlage für die gegenseitige Unterstützung dient, in der die notwendigen Modalitäten für die Zusammenarbeit festgelegt werden, einschließlich einer Definition der Mittel und Verfahren für die Einrichtung und Mobilisierung schneller EU-Einsatzteams für Cybersicherheit.

III ZIEL DER GEMEINSAMEN CYBER-EINHEIT

(4) Die Mitgliedstaaten und die einschlägigen Organe, Einrichtungen und sonstigen Stellen der EU sollten eine **koordinierte Reaktion der EU** auf Cybersicherheitsvorfälle und -krisen sowie eine koordinierte Folgenbewältigung gewährleisten. Insbesondere sollte sichergestellt sein, dass die operativen Teilnehmer, d. h. die ENISA, Europol, der CERT-EU, die Kommission, der Europäische Auswärtige Dienst (einschließlich INTCEN), das CSIRT-Netz und EU-CyCLONe, sowie die unterstützenden Teilnehmer, d. h. der Vorsitz der NIS-Kooperationsgruppe, der Vorsitz der horizontalen Gruppe „Fragen des Cyberraums“ des Rates, die Europäische Verteidigungsagentur und ein Vertreter der jeweiligen SSZ-Projekte[28] ihre Reaktion in diesem Sinne koordinieren. Die operativen Teilnehmer sollten in der Lage sein, innerhalb der Gemeinsamen Cyber-Einheit rasch und effektiv operative Ressourcen für die gegenseitige Unterstützung zu mobilisieren. Hierzu sollten im Rahmen der Gemeinsamen Cyber-Einheit die

26 Einschließlich Software-Anbieter.
27 Einschließlich Bedrohungsanalysen.
28 Koordinierungszentrum für den Cyber- und Informationsraum (CIDCC) und „Teams für die rasche Reaktion auf Cybervorfälle und die gegenseitige Unterstützung im Bereich der Cybersicherheit“ (CRRT)

Mechanismen für die gegenseitige Unterstützung abhängig davon, ob ein oder mehrere Mitgliedstaaten um Hilfe bitten, koordiniert werden.

(5) Im Sinne einer effektiven koordinierten Reaktion sollten die in Nummer 4 genannten operativen und unterstützenden Teilnehmer in der Lage sein, in dem Umfang, wie es ihr Mandat zulässt, bewährte Verfahren weiterzugeben, die **gemeinsame Lageerfassung** stetig zu nutzen und die erforderliche **Abwehrbereitschaft** zu gewährleisten. Diese Teilnehmer sollten die in verschiedenen Cybersicherheitsgemeinschaften bereits vorhandenen Prozesse und das dort vorhandene Fachwissen berücksichtigen.

IV FESTLEGUNG DER FUNKTIONSWEISE DER GEMEINSAMEN CYBER-EINHEIT

(6) Die Mitgliedstaaten und die einschlägigen Organe, Einrichtungen und sonstigen Stellen der EU sollten, aufbauend auf dem ENISA-Beitrag nach Artikel 7 Absatz 7 der Verordnung (EU) 2019/881, mit folgenden Maßnahmen für eine **koordinierte Reaktion** der EU auf Cybersicherheitsvorfälle und -krisen sowie eine koordinierte Folgenbewältigung sorgen:

a) Einrichtung, Schulung, Erprobung und koordinierter Einsatz des **schnellen EU-Einsatzteams für Cybersicherheit** unter Rückgriff auf Artikel 7 Absatz 4 der Verordnung (EU) 2019/881 und die Artikel 3 und 4 der Verordnung (EU) 2016/794;

b) koordinierter Aufbau einer **virtuellen und physischen Plattform** unter Bezugnahme auf die strukturierte Zusammenarbeit zwischen der ENISA und dem CERT-EU nach Artikel 7 Absatz 4 der Verordnung (EU) 2019/881, als unterstützende Infrastruktur für die technische und operative Zusammenarbeit zwischen den Teilnehmern, die dafür zuständig sein sollte, die einschlägigen personellen und sonstigen Beiträge der Teilnehmer zusammenzuführen;

c) Erstellung und Pflege eines die Cybersicherheitsgemeinschaften[29] in der Union umfassenden Verzeichnisses von **in der EU vorhandenen operativen und technischen Fähigkeiten**, die im Falle von Cybersicherheitsvorfällen oder -krisen großen Ausmaßes eingesetzt werden können;

d) Berichterstattung an die Kommission und den Hohen Vertreter über die bei der **operativen Zusammenarbeit im Bereich der Cybersicherheit** innerhalb und zwischen den Cybersicherheitsgemeinschaften gesammelten Erfahrungen.

(7) Mit Blick auf die in Artikel 7 der Verordnung (EU) 2019/881 und in Artikel 3 der Verordnung (EU) 2016/794 festgelegten Ziele sollten die Mitgliedstaaten und die einschlägigen Organe, Einrichtungen und sonstigen Stellen der EU sicherstellen, dass die Gemeinsame Cyber-Einheit innerhalb und zwischen den Cybersicherheitsgemeinschaften stets für eine gemeinsame **Lageerfassung** und **Abwehrbereitschaft** gegen durch den Cyberraum ermöglichte Krisen sorgt. Hierzu sollten die Mitgliedstaaten und die einschlägigen Organe, Einrichtungen und sonstigen Stellen der EU gemäß der Verordnung (EU) 2019/881 und der Verordnung

[29] Gegebenenfalls einschließlich der Cyberabwehrgemeinschaft.

(EU) 2016/794 die Voraussetzungen für die Umsetzung der folgenden **unterstützenden** Tätigkeiten schaffen:

a) Ausarbeitung des **integrierten EU-Cybersicherheitslageberichts** durch Zusammenführung und Auswertung aller relevanten Informationen und Bedrohungsanalysen;

b) Einsatz geeigneter und sicherer **Instrumente** im Einklang mit Artikel 7 Absatz 1 der Verordnung (EU) 2019/881 für den raschen Informationsaustausch zwischen Teilnehmern und anderen Stellen;

c) Austausch – mit Unterstützung der ENISA nach Artikel 7 Absatz 2 der Verordnung (EU) 2019/881 – von **Informationen und Fachkenntnissen**, die erforderlich sind, damit die Union auf die Bewältigung von durch den Cyberraum ermöglichten Sicherheitsvorfällen und -krisen großen Ausmaßes vorbereitet ist;

d) Annahme und Erprobung nationaler **Pläne für die Reaktion auf Cybersicherheitsvorfälle und -krisen**[30] nach Artikel 7 Absätze 2, 5 und 7 der Verordnung (EU) 2019/881;

e) Entwicklung, Management und Erprobung – auch im Rahmen gemeinschaftsübergreifender Übungen und Schulungen – des **EU-Plans für die Reaktion auf Cybersicherheitsvorfälle und -krisen** im Einklang mit der „Konzeptentwurf"-Empfehlung und aufbauend auf Artikel 7 Absatz 3 des Vorschlags der Kommission für eine Überarbeitung der Richtlinie (EU) 2016/1148 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union[31];

f) Hilfe für die Teilnehmer – mit Unterstützung der ENISA nach Artikel 7 Absatz 1 der Verordnung (EU) 2019/881 – beim Abschluss von Vereinbarungen über den Informationsaustausch und von Vereinbarungen über die operative Zusammenarbeit mit **privatwirtschaftlichen Stellen**, die unter anderem Bedrohungsanalysen und Sicherheitsvorfall-Notdienste bereitstellen;

g) Aufbau strukturierter Synergien mit nationalen, sektoralen und grenzübergreifenden **Monitoring- und Detektionsfähigkeiten**, insbesondere mit Sicherheitseinsatzzentren;

h) Unterstützung der Teilnehmer beim **Management** von Sicherheitsvorfällen und -krisen großen Ausmaßes im Einklang mit der unterstützenden Rolle der ENISA nach Artikel 7 der Verordnung (EU) 2019/881. Dies beinhaltet einen Beitrag zu einer gemeinsamen Lageerfassung, die Unterstützung der Diplomatie, die politische Zuordnung sowie auch die Zuordnung im Rahmen strafrechtlicher Ermittlungen, auch über Europol[32], die Abstimmung der öffentlichen Kommunikation und die Erleichterung der Folgenbewältigung.

---

30 Vorgeschlagen in Artikel 7 Absatz 3 der Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148, COM(2020) 823 final, 2020/0359(COD).

31 COM(2020) 823 final.

32 Im Einklang mit der Verordnung (EU) 2016/794.

(8) Mit Blick auf die Umsetzung der Nummern 6 und 7 sollten die Mitgliedstaaten und die einschlägigen Organe, Einrichtungen und sonstigen Stellen der EU Folgendes gewährleisten:

a) Die Festlegung der organisatorischen Aspekte der Gemeinsamen Cyber-Einheit sowie der **Aufgaben und Zuständigkeiten** der operativen und unterstützenden Teilnehmer innerhalb der Plattform, damit die Plattform im Einklang mit den im Anhang dieser Empfehlung dargelegten Aspekten und Grundsätzen wirksam funktionieren kann;

b) den Abschluss von **Absichtserklärungen**, in denen die unter Nummer 4 genannten Modalitäten der Zusammenarbeit zwischen den Teilnehmern festgelegt sind.

(9) Nach Artikel 7 der Verordnung (EU) 2019/881 sollte die ENISA die Koordinierung und Unterstützung der Mitgliedstaaten und der einschlägigen Organe, Einrichtungen und sonstigen Stellen der EU innerhalb der Gemeinsamen Cyber-Einheit sicherstellen, auch indem sie als Sekretariat fungiert, Sitzungen organisiert und zur Umsetzung der Maßnahmen sowohl auf Ebene der Mitgliedstaaten als auch auf EU-Ebene beiträgt. Die ENISA sollte sowohl eine sichere virtuelle Plattform als auch einen physischen Raum für Sitzungen einrichten und die Umsetzung der notwendigen Maßnahmen erleichtern.

V AUFBAU DER GEMEINSAMEN CYBER-EINHEIT

(10) Die Mitgliedstaaten und die einschlägigen Organe, Einrichtungen und sonstigen Stellen der EU sollten sicherstellen, dass die Gemeinsame Cyber-Einheit ab dem **30. Juni 2022** in ihre operative Phase eintritt. Zu diesem Zeitpunkt sollten die operativen Teilnehmer operative Fähigkeiten und Experten zur Verfügung stellen, die die Grundlage der schnellen EU-Einsatzteams für Cybersicherheit bilden können. Die Pläne für eine physische und virtuelle Plattform sollten weit fortgeschritten sein.

(11) Die Mitgliedstaaten und die einschlägigen Organe, Einrichtungen und sonstigen Stellen der EU sollten dazu beitragen, dass die Gemeinsame Cyber-Einheit bis zum **30. Juni 2023** reibungslos funktioniert und vollständig einsatzbereit ist. Dies sollte durch vier aufeinanderfolge Stufen geschehen, die auf den Abschluss folgender Tätigkeiten abzielen:

a) Stufe 1 – Bewertung der organisatorischen Aspekte der Gemeinsamen Cyber-Einheit und Ermittlung der in der EU verfügbaren operativen Fähigkeiten bis zum **31. Dezember 2021**;

b) Stufe 2 – Ausarbeitung von Plänen für die Reaktion auf Cybersicherheitsvorfälle und -krisen sowie Umsetzung gemeinsamer Maßnahmen für die Abwehrbereitschaft bis zum **30. Juni 2022**;

c) Stufe 3 – Aufnahme der Tätigkeit der Gemeinsamen Cyber-Einheit bis zum **31. Dezember 2022**;

d) Stufe 4 – Ausweitung der Zusammenarbeit innerhalb der Gemeinsamen Cyber-Einheit auf private Einrichtungen und Berichterstattung über die bis zum **30. Juni 2023** erzielten Fortschritte.

Weitere Einzelheiten zu den Maßnahmen, die im Rahmen der vier aufeinanderfolgenden Stufen ergriffen werden sollten, sind im Anhang zu dieser Empfehlung aufgeführt.

(12) Im Rahmen der ersten beiden Stufen sollte die ENISA die Vorbereitung der Gemeinsamen Cyber-Einheit organisieren und unterstützen. Die Kommissionsdienststellen sollten eine Arbeitsgruppe einsetzen, in der operative und unterstützende Teilnehmer gemeinsam diese Vorbereitungsarbeiten abschließen. Für den Vorsitz der Arbeitsgruppe sollten die Kommissionsdienststellen einen Vertreter benennen und einen vom Hohen Vertreter benannten sowie einen von den Mitgliedstaaten ausgewählten Vertreter ersuchen, den Ko-Vorsitz zu übernehmen. Die von den Kommissionsdienststellen und vom Hohen Vertreter benannten Vertreter sollten im Rahmen ihrer jeweiligen Zuständigkeiten Tagesordnungspunkte einbringen.

(13) Am Ende von Stufe 2 sollte die Arbeitsgruppe ihre Bewertung der organisatorischen Aspekte der Gemeinsamen Cyber-Einheit sowie der Aufgaben und Zuständigkeiten der operativen Teilnehmer innerhalb dieser Plattform abgeschlossen haben. Die Arbeitsgruppe sollte die Ergebnisse dieser Bewertung der Kommission und dem Hohen Vertreter vorlegen, die diese Bewertung dann dem Rat übermitteln sollten. Die Kommission und der Hohe Vertreter sollten auf der Grundlage dieser Bewertung einen gemeinsamen Bericht erstellen und den Rat ersuchen, diesen Bericht im Wege der Schlussfolgerungen des Rates zu billigen.

(14) Die gemeinsame Cyber-Einheit sollte ab Stufe 3 einsatzbereit sein.

(15) Die ENISA und die Kommission sollten dafür sorgen, dass die im Rahmen der EU-Finanzierungsprogramme, vor allem des Programms „Digitales Europa“, vorhandenen Ressourcen im Einklang mit den geltenden Vorschriften für die Festlegung der jeweiligen Arbeitsprogramme verwendet werden, damit den Teilnehmern der Gemeinsamen Cyber-Einheit zusätzliche Fähigkeiten für Schulungen und Kommunikation sowie eine Infrastruktur für den sicheren Informationsaustausch zur Verfügung gestellt werden können, die den Austausch von Verschlusssachen auch zwischen verschiedenen Gemeinschaften ermöglichen.

VI ÜBERPRÜFUNG

(16) Die Mitgliedstaaten sollten mit der Kommission und dem Hohen Vertreter, im Rahmen derer jeweiligen Zuständigkeiten, zusammenarbeiten, um die Wirksamkeit und Effizienz der Gemeinsamen Cyber-Einheit bis zum **30. Juni 2025** im Hinblick darauf zu bewerten, welche Schlussfolgerungen sich daraus für die Zukunft der Gemeinsamen Cyber-Einheit ziehen lassen. Bei dieser Bewertung sollte die Umsetzung der genannten vier Stufen berücksichtigt werden.

Brüssel, den 23.6.2021

Für die Kommission
Thierry BRETON
Mitglied der Kommission

BEGLAUBIGTE AUSFERTIGUNG
Für die Generalsekretärin

Martine DEPREZ
Direktorin
Entscheidungsprozess & Kollegialität
EUROPÄISCHE KOMMISSION