Rat der
Europäischen Union

Brüssel, den 25. Februar 2025
(OR. en)

6527/25

Interinstitutionelles Dossier:
2025/0036(NLE)

CYBER 52
IPCR 11
RELEX 241
JAI 235
JAIEX 17
POLMIL 42
HYBRID 19
TELECOM 62
COSI 37

VORSCHLAG

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	24. Februar 2025
Empfänger:	Frau Thérèse BLANCHET, Generalsekretärin des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2025) 66 final
Betr.:	Vorschlag für eine EMPFEHLUNG DES RATES für einen EU-Konzeptentwurf für das Cybersicherheitskrisenmanagement

Die Delegationen erhalten in der Anlage das Dokument COM(2025) 66 final.

Anl.: COM(2025) 66 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 24.2.2025
COM(2025) 66 final

2025/0036 (NLE)

Vorschlag für eine

EMPFEHLUNG DES RATES

für einen EU-Konzeptentwurf für das Cybersicherheitskrisenmanagement

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

• Gründe und Ziele des Vorschlags

In seinen Schlussfolgerungen zur Zukunft der Cybersicherheit vom 22. Mai 2024 rief der Rat

> *„die Kommission auf, das derzeitige Konzept zur Cybersicherheit zügig zu bewerten und auf dieser Grundlage einen überarbeiteten Konzeptentwurf zur Cybersicherheit in Form einer Empfehlung des Rates vorzulegen, in der die aktuellen Herausforderungen und die komplexe Cyberbedrohungslandschaft angegangen und bestehende Netze gestärkt werden, die Zusammenarbeit verbessert und die Abschottung zwischen Organisationen aufgebrochen wird, wobei hierfür zu allererst die bestehenden Strukturen zu nutzen sind. Ferner sollte der überarbeitete Konzeptentwurf auf bewährten leitenden Grundsätzen der Zusammenarbeit beruhen (Verhältnismäßigkeit, Subsidiarität, Komplementarität und Vertraulichkeit von Informationen) und diese auf den gesamten Krisenmanagementzyklus ausdehnen sowie dazu beitragen, sichere Kommunikation im Bereich der Cybersicherheit anzugleichen und zu verbessern. Die Kompatibilität des überarbeiteten Konzeptentwurfs mit bestehenden Rechtsrahmen, wie der Integrierten EU-Regelung für die politische Reaktion auf Krisen (IPCR), dem EU-Instrumentarium für die Cyberdiplomatie, dem EU-Instrumentarium zur Abwehr hybrider Bedrohungen, dem EU-Notfallprotokoll für die Strafverfolgung (EU LE ERP), mit entstehenden Rechtsrahmen, wie dem Konzeptentwurf für kritische Infrastrukturen, mit sektorspezifischen Verfahren sowie mit allgemeinen Strukturen zum Krisenmanagement innerhalb von Einrichtungen der Union sollte gewährleistet sein, wobei auch der Hohe Vertreter und Europol einbezogen werden sollten. In diesem überarbeiteten Konzeptentwurf sollten die Rolle der Kommission, die Rolle des Hohen Vertreters und die Rolle der ENISA, entsprechend deren Zuständigkeiten, in erster Linie darauf ausgerichtet sein, die horizontale Koordinierung zu unterstützen.“*

Ziel dieses Entwurfs einer Empfehlung des Rates für einen Konzeptentwurf der Union für das Cybersicherheitskrisenmanagement (Cyberkonzeptentwurf) ist es, den Rahmen der Europäischen Union (EU) für das Cyberkrisenmanagement in klarer, einfacher und zugänglicher Weise vorzulegen. Der Rahmen für das Cyberkrisenmanagement sollte es den einschlägigen Akteuren in der Union, einschließlich einzelner Einrichtungen und Netze von Einrichtungen auf Unionsebene, ermöglichen, besser zu verstehen, wie sie zusammenwirken sollten und wie sie die bestehenden Mechanismen über den gesamten Lebenszyklus des Krisenmanagements bestmöglich nutzen können. Es soll erläutert werden, was eine Cyberkrise ist und was einen Cyberkrisenmechanismus auf Unionsebene auslöst. In der Empfehlung wird dargelegt, wie verfügbare Mechanismen wie der Cybernotfallmechanismus, einschließlich der EU-Cybersicherheitsreserve, bei der Vorbereitung der Bewältigung einer Krise infolge eines Cybersicherheitsvorfalls großen Ausmaßes, der Reaktion darauf und der Wiederherstellung danach genutzt werden können. Darüber hinaus zielt sie darauf ab, eine strukturiertere Zusammenarbeit zwischen zivilen und militärischen Akteuren, auch mit der Nordatlantikvertrags-Organisation (NATO), zu fördern, da durch einen Cybersicherheitsvorfall großen Ausmaßes, der eine zivile Infrastruktur der Union betrifft, die vom Militär ebenfalls genutzt wird, auch NATO-Reaktionsmechanismen aktiviert werden können.

Der Cyberkonzeptentwurf ist ein nicht verbindliches Instrument, das spezifische Maßnahmen für einschlägige Akteure in einer Cyberkrise festlegt und die allgemeine Wirksamkeit des Rahmens für das Cyberkrisenmanagement erhöhen kann. Er aktualisiert den in der Empfehlung (EU) 2017/1584 der Kommission für eine koordinierte Reaktion auf große

Cybersicherheitsvorfälle und -krisen dargelegten Plan und trägt den Ergebnissen und Erkenntnissen aus den seit der Annahme der Empfehlung auf Unionsebene durchgeführten Übungen Rechnung. Er ist Teil umfassenderer politischer Prioritäten in den Bereichen Abwehrbereitschaft und Sicherheit.

Im Sinne der Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie) ist ein Cybersicherheitsvorfall großen Ausmaßes ein Sicherheitsvorfall, der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt, oder der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat. Je nach Ursache und Auswirkung kann sich ein solcher Sicherheitsvorfall verschärfen und zu einer echten Krise entwickeln, die das reibungslose Funktionieren des Binnenmarkts verhindert oder ein ernsthaftes, die öffentliche Sicherheit betreffendes Risiko für Einrichtungen und Bürger in mehreren Mitgliedstaaten oder in der gesamten Union darstellt.

- **Kohärenz mit den bestehenden Vorschriften in diesem Bereich**

Der Vorschlag steht im Einklang mit den einschlägigen Instrumenten der Union im Bereich der Cybersicherheit, insbesondere mit der NIS-2-Richtlinie und der Verordnung (EU) 2023/2841 zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union. Er steht ebenfalls im Einklang mit dem Rahmen des Katastrophenschutzverfahrens der Union (UCPM), das mit dem Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates eingerichtet wurde, dem Durchführungsbeschluss (EU) 2018/1993 über die Integrierte EU-Regelung für die politische Reaktion auf Krisen (IPCR) und den sektorspezifischen Instrumenten für die Lageerfassung und das Krisenmanagement, auch im Elektrizitätssektor.

- **Kohärenz mit der Politik der Union in anderen Bereichen**

Der Cyberkonzeptentwurf ergänzt die kürzlich angenommene Empfehlung des Rates für einen Konzeptentwurf zur Koordinierung der Reaktion – auf Unionsebene – auf Störungen kritischer Infrastrukturen von erheblicher grenzüberschreitender Bedeutung und steht im Einklang mit dieser Empfehlung, da letztere Empfehlung auch Störungen im Zusammenhang mit der nicht cyberbezogenen physischen Resilienz abdeckt. Er wirkt eng mit den Krisenmanagementmechanismen und -instrumenten der Gemeinsamen Außen- und Sicherheitspolitik (GASP) und der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) im Strategischen Kompass des Rates für Sicherheit und Verteidigung zusammen. Darüber hinaus können auch Initiativen der Union zur Bekämpfung der Cyberkriminalität die mit der vorliegenden Empfehlung verfolgten Ziele unterstützen.

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄßIGKEIT

- **Rechtsgrundlage**

Der Vorschlag stützt sich auf Artikel 292 AEUV, in dem die einschlägigen Vorschriften für die Annahme von Empfehlungen festgelegt sind.

Der Vorschlag würde den auf EU-Ebene eingerichteten Gesamtrechtsrahmen für die Cybersicherheit ergänzen. In dem Vorschlag geht es nicht um den Umgang mit schwerwiegenden Sicherheitsvorfällen, die Einrichtungen der Union im Sinne der auf der Grundlage von Artikel 298 AEUV erlassenen Verordnung (EU) 2023/2841 betreffen. Er betrifft jedoch den Informationsaustausch zwischen Einrichtungen der Union und Mitgliedstaaten, einschließlich der Bestimmungen der Verordnung (EU) 2023/2841 für den Vertreter der Kommission im Interinstitutionellen Cybersicherheitsbeirat (IICB), der als Anlaufstelle fungieren soll, um den Austausch einschlägiger Informationen über

schwerwiegende Sicherheitsvorfälle mit dem europäischen Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) als Beitrag zur gemeinsamen Lageerfassung zu erleichtern.

- **Subsidiarität (bei nicht ausschließlicher Zuständigkeit)**

Während die Reaktion auf Störungen kritischer Infrastrukturen oder der von wesentlichen und wichtigen Einrichtungen erbrachten Dienste in erster Linie in die Zuständigkeit der Mitgliedstaaten fällt, können bestimmte böswillige grenzüberschreitende Cyberaktivitäten kritische Informationsinfrastrukturen stören und schädigen, von denen das reibungslose Funktionieren des Binnenmarkts abhängt. Daher spielt die Union im Falle eines erheblichen Sicherheitsvorfalls oder einer erheblichen Krise eine wichtige Rolle. Eine solche Störung kann sich auf mehrere oder sogar alle Wirtschaftssektoren im Binnenmarkt auswirken und könnte die Sicherheit und die internationalen Beziehungen der Union beeinträchtigen. Um das Funktionieren des Binnenmarkts zu gewährleisten, ist eine Koordinierung auf Unionsebene im Falle von Störungen kritischer Infrastrukturen mit erheblichen grenzüberschreitenden Auswirkungen nicht nur angemessen, sondern auch notwendig. Koordinierte Reaktionen auf Unionsebene werden die Reaktionen der Mitgliedstaaten auf die Störung durch eine gemeinsame Lageerfassung, eine koordinierte Kommunikation mit der Öffentlichkeit und die Abmilderung der Folgen der Störung auf den Binnenmarkt unterstützen.

- **Verhältnismäßigkeit**

Der vorliegende Vorschlag steht im Einklang mit dem in Artikel 5 Absatz 4 des Vertrags über die Europäische Union (EUV) verankerten Grundsatz der Verhältnismäßigkeit. Weder Inhalt noch Form der vorgeschlagenen Empfehlung des Rates gehen über das hinaus, was zur Erreichung ihrer Ziele notwendig ist. Die vorgeschlagenen Maßnahmen stehen in einem angemessenen Verhältnis zu den verfolgten Zielen; diese konzentrieren sich auf die Gewährleistung eines auf Unionsebene koordinierten Cyberkrisenmanagement.

- **Wahl des Instruments**

Um die oben genannten Ziele zu erreichen, sieht der AEUV insbesondere in Artikel 292 vor, dass der Rat Empfehlungen auf der Grundlage eines Vorschlags der Kommission annimmt. Empfehlungen sind gemäß Artikel 288 AEUV nicht verbindlich. Eine Empfehlung des Rates ist in diesem Fall ein geeignetes Instrument, da sie das Engagement der Mitgliedstaaten für die darin enthaltenen Maßnahmen signalisiert und eine solide Grundlage für die Zusammenarbeit bei der Koordinierung des Managements großer Cybersicherheitsvorfälle und -krisen bietet. Auf diese Weise würde die vorgeschlagene Empfehlung den verbindlichen Rechtsrahmen (insbesondere die NIS-2-Richtlinie) ergänzen.

3. ERGEBNISSE DER EX-POST-BEWERTUNG, DER KONSULTATION DER INTERESSENTRÄGER UND DER FOLGENABSCHÄTZUNG

- **Konsultation der Interessenträger**

Im Zuge der Ausarbeitung dieses Vorschlags führte die Kommission eine Konsultation zur Überprüfung des Cyberkonzeptentwurfs durch und ersuchte Mitgliedstaaten und einschlägige Einrichtungen der Union um Beiträge. Berücksichtigt wurden auch die Standpunkte der Sachverständigen der Mitgliedstaaten sowie der ENISA, die auf dem von der Kommission und Polen gemeinsam veranstalteten Workshop am 5. September 2024 in Karpacz geäußert wurden.

Die Kommission konsultierte im September 2024 Vertreter der Mitgliedstaaten im CSIRTs-Netzwerk, im EU-CyCLONe und in der NIS-Kooperationsgruppe und holte schriftliche Beiträge ein.

Die Kommission stellte den Vorschlag dem Rat in zwei besonderen Beratungen der Horizontalen Gruppe „Fragen des Cyberraums“ im Oktober und November 2024 vor und ersuchte sie um Rückmeldungen.

Die Kommission konsultierte Vertreter des Privatsektors sowie der Mitgliedstaaten, des Europäischen Auswärtigen Dienstes (EAD) und der ENISA bei einem Workshop, der von der Ständigen Vertretung Polens bei der EU im November 2024 in Brüssel ausgerichtet wurde.

Die Kommission konsultierte einschlägige Einrichtungen der Union, nämlich den EAD, die ENISA, Europol und das CERT-EU, unter anderem im Zuge hochrangiger Gespräche in den Sitzungen des Krisenstabs für Cybersicherheit[1] im Juli und November 2024.

Es wurde Einvernehmen darüber erzielt, dass ein aktuelles, klares, einfaches und operatives Dokument benötigt wird, das es den einschlägigen Akteuren ermöglicht, den Rahmen für das Cyberkrisenmanagement zu verstehen und die verfügbaren Mechanismen wirksam zu nutzen. Ebenfalls bestand Einigkeit darin, dass Doppelungen bei den Instrumenten vermieden und die auf Unionsebene bestehenden Mechanismen für die Koordinierung, den Informationsaustausch und die Reaktion sinnvoll genutzt werden müssen, ohne dass neue Strukturen geschaffen oder in die internen Standardarbeitsanweisungen bestehender Netzwerke und bestehende sektorspezifische Mechanismen eingegriffen wird.

[1] Eine Informelle Gruppe aus Vertretern von Kommissionsdienststellen und anderen EU-Dienststellen.

2025/0036 (NLE)

Vorschlag für eine

EMPFEHLUNG DES RATES

für einen EU-Konzeptentwurf für das Cybersicherheitskrisenmanagement

DER RAT DER EUROPÄISCHEN UNION —

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

auf Vorschlag der Europäischen Kommission,

in Erwägung nachstehender Gründe:

(1) Digitale Technik und globale Konnektivität bilden das Rückgrat des Wirtschaftswachstums, der Wettbewerbsfähigkeit und des Umbaus kritischer Infrastrukturen in der Union. Mit einer vernetzten und zunehmend digitalen Wirtschaft steigt jedoch auch das Risiko von Cybervorfällen und Cyberangriffen. Darüber hinaus spiegeln sich zunehmende geopolitische Spannungen, Konflikte und strategische Rivalitäten in den Auswirkungen, dem Umfang und der Komplexität böswilliger Cyberaktivitäten wider. Solche Aktivitäten können Teil mehrdimensionaler hybrider Bedrohungen oder militärischer Operationen sein. Sie können sich auch unmittelbar auf die Sicherheit, die Wirtschaft und die Gesellschaft der Union auswirken. Darüber hinaus haben sie ein Übergriffspotenzial, insbesondere wenn solche Aktivitäten auf internationale strategische Partnerländer wie Kandidatenländer oder Nachbarländer ausgerichtet sind.

(2) Ein Cybersicherheitsvorfall großen Ausmaßes kann eine Störung verursachen, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt, oder aber beträchtliche Auswirkungen mehrere Mitgliedstaaten haben. Je nach Ursache und Auswirkung könnte sich ein solcher Sicherheitsvorfall verschärfen und zu einer echten Krise entwickeln, die das reibungslose Funktionieren des Binnenmarkts verhindert oder ein ernsthaftes, die öffentliche Sicherheit betreffendes Risiko für Einrichtungen und Bürger in mehreren Mitgliedstaaten oder in der gesamten Union darstellt. Ein wirksames Krisenmanagement ist für die Aufrechterhaltung der wirtschaftlichen Stabilität und den Schutz europäischer Behörden, kritischer Infrastrukturen, der Bürgerinnen und Bürger und Unternehmen sowie zur Leistung eines Beitrags zur internationalen Sicherheit und zur Stabilität im Cyberraum unverzichtbar. Das Cyberkrisenmanagement ist daher ein fester Bestandteil des übergreifenden EU-Rahmens für das Krisenmanagement.

(3) Gemäß den im Durchführungsbeschluss (EU) 2018/1993 des Rates[2] festgelegten Verfahren fasst der Ratsvorsitz, nachdem er die betroffenen Mitgliedstaaten, die

[2] Durchführungsbeschluss (EU) 2018/1993 des Rates vom 11. Dezember 2018 über die integrierte EU-Regelung für die politische Reaktion auf Krisen (ABl. L 320 vom 17.12.2018, S. 28, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

Kommission und die Hohe Vertreterin konsultiert hat (es sei denn, die Solidaritätsklausel wurde geltend gemacht), einen Beschluss zur Aktivierung und Deaktivierung der Integrierten EU-Regelung für die politische Reaktion auf Krisen (IPCR). Darüber hinaus können das Generalsekretariat des Rates, die Kommissionsdienststellen und der EAD gemäß den IPCR-Verfahren in Absprache mit dem Vorsitz auch vereinbaren, die IPCR im Informationsaustausch-Modus zu aktivieren. Die Diskussionen im Rahmen der IPCR stützen sich auf Berichte zur Integrierten Lageeinschätzung und -auswertung, die von den Kommissionsdienststellen und dem EAD erarbeitet werden.

(4) Wenngleich die Hauptverantwortung für das Management nationaler Cyberkrisen bei den Mitgliedstaaten liegt, müssen die Mitgliedstaaten und die einschlägigen Einrichtungen der Union aufgrund des möglichen grenzüberschreitenden und sektorübergreifenden Charakters von Cybersicherheitsvorfällen auf technischer, operativer und politischer Ebene zusammenarbeiten, um eine wirksame Koordinierung in der gesamten Union zu gewährleisten. Gleichzeitig sind Krisenreaktion und die Wiederherstellung danach für die betroffenen Einrichtungen und Sektoren kostspielig. Das Krisenmanagement über den gesamten Lebenszyklus umfasst daher die Abwehrbereitschaft und die gemeinsame Lageerfassung zur Antizipation von Cybersicherheitsvorfällen, die zur Bestimmung von Cybersicherheitsvorfällen erforderlichen Erkennungskapazitäten und die erforderlichen Reaktions- und Wiederherstellungsinstrumente, um Cybersicherheitsvorfälle abzumildern, abzuwehren und einzudämmen.

(5) In der Empfehlung (EU) 2017/1584 der Kommission[3] für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen sind die Ziele und Modalitäten der Zusammenarbeit zwischen Mitgliedstaaten und Einrichtungen der Union bei der Reaktion auf große Cybersicherheitsvorfälle und Krisen festgelegt. Darin werden die einschlägigen Akteure auf technischer, operativer und politischer Ebene aufgeführt und es wird erläutert, wie diese in das umfassendere Krisenmanagement der Union wie die IPCR-Regelung integriert sind. Die in der Empfehlung (EU) 2017/1584 dargelegten Grundprinzipien der Subsidiarität, Komplementarität und Vertraulichkeit von Informationen sowie der dreistufige Ansatz (technische, operative und politische Ebene) sind nach wie vor gültig.

(6) Seit 2017 hat die Union ihren Cybersicherheitsrahmen durch mehrere Instrumente ausgebaut, die Bestimmungen enthalten, die für das Cybersicherheitskrisenmanagement relevant sind: Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates[4], Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates[5], Durchführungsverordnung (EU) 2024/2690 der

---

3 Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (ABl. L 239 vom 19.9.2017, S. 36, ELI: http://data.europa.eu/eli/reco/2017/1584/oj).

4 Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

5 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie

Kommission[6], Verordnung (EU, Euratom) 2023/2841 des Europäischen Parlaments und des Rates[7], Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates[8], Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates[9] und Verordnung (EU) 2025/38 des Europäischen Parlaments und des Rates („Cybersolidaritätsverordnung“)[10]. Zu den besonderen sektoralen Maßnahmen zur Bewältigung von Cybersicherheitskrisen gehören die Delegierte Verordnung (EU) 2024/1366 der Kommission[11] und der künftige Rahmen für die Koordinierung in Bezug auf systemische Cybervorfälle (EU-SCICF) im Zusammenhang mit der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates[12]. Die Richtlinie 2013/40/EU[13] enthält Verweise auf die Definition krimineller Tätigkeiten im Zusammenhang mit Cyberangriffen und auf die Unionsvorschriften über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln, insbesondere die Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates[14], die nach

---

(EU) 2016/1148 (NIS- 2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

6 Durchführungsverordnung (EU) 2024/2690 der Kommission vom 17. Oktober 2024 mit Durchführungsbestimmungen zur Richtlinie (EU) 2022/2555 im Hinblick auf die technischen und methodischen Anforderungen der Risikomanagementmaßnahmen im Bereich der Cybersicherheit und die Präzisierung der Fälle, in denen ein Sicherheitsvorfall in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter verwalteter Dienste, Anbieter verwalteter Sicherheitsdienste, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter als erheblich gilt (ABl. L, 2024/2690, 18.10.2024).

7 Verordnung (EU, Euratom) 2023/2841 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union (ABl. L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

8 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 (ABl. L 202 vom 8.6.2021, S. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

9 Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung) (ABl. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

10 Verordnung (EU) 2025/38 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 über Maßnahmen zur Stärkung der Solidarität für und der Kapazitäten in der Union für die Erkennung von, Vorsorge für und Bewältigung von Cyberbedrohungen und Sicherheitsvorfällen und zur Änderung der Verordnung (EU) 2021/694 (Cybersolidaritätsverordnung) (ABl. L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

11 Delegierte Verordnung (EU) 2024/1366 der Kommission vom 11. März 2024 zur Ergänzung der Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates durch Festlegung eines Netzkodex mit sektorspezifischen Vorschriften für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse (ABl. L, 2024/1366, 24.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

12 Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (ABl. L 333 vom 27.12.2022, S. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

13 Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates (ABl. L 218 vom 14.8.2013, S. 8, ELI: http://data.europa.eu/eli/dir/2013/40/oj).

14 Verordnung (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. Juli 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren (ABl.

ihrer Umsetzung Strafverfolgungsmaßnahmen in diesem Bereich erheblich erleichtern wird. In der EU-Cyberabwehrpolitik[15] sind die Aufgaben eines EU-weiten operativen Netzes der militärischen IT-Notfallteams (MICNET) und der EU-Konferenz der Cyberkommandeure dargelegt und die Einrichtung eines EU-Koordinierungszentrums für die Cyberabwehr (EUCDCC) vorgesehen. Andere, nicht cyberbezogene Mechanismen zur Lageerfassung und Krisenreaktion gibt es in einigen der in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführten kritischen Sektoren. Die Empfehlung des Rates für einen Konzeptentwurf zur Koordinierung der Reaktion – auf Unionsebene – auf Störungen kritischer Infrastrukturen von erheblicher grenzüberschreitender Bedeutung[16] sieht die Zusammenarbeit zwischen den einschlägigen Akteuren vor, wenn ein Sicherheitsvorfall sowohl physische Aspekte als auch die Cybersicherheit kritischer Infrastruktur betrifft.

(7) Auf Unionsebene gehören zu den einschlägigen für das Cyberkrisenmanagement zuständigen Akteuren die Kommission, der EAD, einschließlich des Einheitlichen Analyseverfahrens (SIAC), die Agentur der Europäischen Union für Cybersicherheit (ENISA), das IT-Notfallteam der Organe, Einrichtungen und sonstigen Stellen der EU (CERT-EU), Europol über sein Europäisches Zentrum zur Bekämpfung der Cyberkriminalität (EC3), das Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe), das Netz der Computer-Notfallteams (CSIRTs), das EU-Satellitenzentrum (SATCEN), die Galileo-Sicherheitszentrale und das Netz der Delegationen der Union. Diese Akteure der Union sollten im Einklang mit ihren Zuständigkeiten nach geltendem Recht gemeinsam Bereiche für die Zusammenarbeit festlegen und zur Umsetzung des Unionsrahmens für das Cyberkrisenmanagement beitragen.

(8) Eine aktualisierte Empfehlung für einen Konzeptentwurf für die Cybersicherheit (im Folgenden „Cyberkonzeptentwurf“) ist erforderlich, um klare und zugängliche Leitlinien bereitzustellen, in denen erläutert wird, was eine Cyberkrise auf Unionsebene ist, wie der Rahmen für das Krisenmanagement ausgelöst wird, welche Rollen die einschlägigen Akteure und Mechanismen auf Unionsebene spielen und wie diese Akteure und Mechanismen über den gesamten Lebenszyklus von Cyberkrisen interagieren sollen. Der Cyberkonzeptentwurf ist im breiteren Kontext der zivil-militärischen Beziehungen und der Beziehungen zwischen der EU und der NATO zu sehen.

(9) Diese Empfehlung ergänzt die Regelung für die integrierte politische Reaktion auf Krisen (IPCR) und umfassendere Krisenmechanismen der Union, einschließlich des allgemeinen Frühwarnsystems ARGUS der Kommission, des Katastrophenschutzverfahrens der Union (UCPM), das vom Zentrum für die Koordination von Notfallmaßnahmen (ERCC) unterstützt wird, des Krisenreaktionsmechanismus (CRM) des EAD, sowie andere Prozesse, wie sie im EU-Instrumentarium zur Abwehr hybrider Bedrohungen[17] und im überarbeiteten EU-

---

L 191 vom 28.7.2023, S. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj) und Richtlinie (EU) 2023/1544 des Europäischen Parlaments und des Rates vom 12. Juli 2023 zur Festlegung einheitlicher Regeln für die Benennung von benannten Niederlassungen und die Bestellung von Vertretern zu Zwecken der Erhebung elektronischer Beweismittel in Strafverfahren (ABl. L 191 vom 28.7.2023, S. 181, ELI: http://data.europa.eu/eli/dir/2023/1544/oj).

15 JOIN(2022) 49 final.

16 ABl. C, 2024/4371, 5.7.2024.

17 Schlussfolgerungen des Rates über einen Rahmen für eine koordinierte Reaktion der EU auf hybride Kampagnen vom 22. Juni 2022.

Protokoll für das operative Vorgehen bei der Abwehr hybrider Bedrohungen beschrieben sind. Sie ergänzt auch die Empfehlung des Rates für einen Konzeptentwurf zur Koordinierung der Reaktion – auf Unionsebene – auf Störungen kritischer Infrastrukturen von erheblicher grenzüberschreitender Bedeutung (im Folgenden „Konzeptentwurf für kritische Infrastrukturen“), die die nicht cyberbezogene physische Resilienz abdeckt und mit der die Koordinierung der Reaktion auf Unionsebene in diesem Bereich verbessert werden soll, und sollte mit ihr im Einklang stehen.

(10) Ein umfassender und integrierter Ansatz für das Krisenmanagement sollte in allen Sektoren und auf allen Regierungs- und Verwaltungsebenen gefördert werden. Das sektorübergreifende Krisenmanagement auf Unionsebene sollte verstärkt werden, um eine integrierte Krisenreaktion zu ermöglichen, insbesondere in Fällen, in denen Cybervorfälle Folgen in der realen Welt haben. Wenn Cybersicherheitsvorfälle Teil einer umfassenderen hybriden Kampagne oder Krise sind, sollten die einschlägigen Akteure die laufenden Bemühungen zur Entwicklung eines einheitlichen Lagebildes über mehrere Sektoren und Bereiche hinweg unterstützen. Die Empfehlung trägt zu umfassenderen Vorsorgemaßnahmen bei, die für die Union angesichts mehrdimensionaler hybrider Bedrohungen erforderlich sind [im Einklang mit den in der Strategie für eine krisenfeste Union verankerten Grundsätzen].

(11) Die Sicherheit kritischer digitaler Infrastrukturen ist für die Resilienz der Wirtschaft, der Gesellschaft und der Verteidigung der Union von wesentlicher Bedeutung. Einrichtungen, die in den Anwendungsbereich der Richtlinie (EU) 2022/2555 fallen, einschließlich solcher, die Unterseekommunikationskabel bereitstellen, müssen Maßnahmen zum Schutz der physischen und ökologischen Sicherheit von Netz- und Informationssystemen auf der Grundlage eines gefahrenübergreifenden Ansatzes, wie im Hinblick auf Systemfehler, menschliche Fehler, böswillige Handlungen oder Naturereignisse, ergreifen. Darüber hinaus sollten diese Einrichtungen Sicherheitsvorfälle, einschließlich solcher im Zusammenhang mit Unterseekommunikationskabeln, an die CSIRTs oder gegebenenfalls an die zuständige Behörde melden. Obwohl die dem Cyberkonzeptentwurf zugrunde liegenden Grundprinzipien für die Sicherheit von Seekabeln relevant sind, sind die darin festgelegten Mechanismen nicht umfassend genug, um den gesamten Krisenresilienzzyklus abzudecken. Sein besonderer Charakter rechtfertigt konzertierte und maßgeschneiderte Anstrengungen, um dem Bedarf an integrierter Bedrohungsüberwachung und Lageerfassung in den Meeresbecken rund um die EU, an strategischen Investitionen zur Schaffung von Redundanzen und an einem gemeinsamem europäischen Ansatz zur Stärkung der Reparatur- und Wiederherstellungskapazitäten gerecht zu werden. Die EU-Strategie für maritime Sicherheit umfasst Maßnahmen zur Verbesserung der Cybersicherheit im maritimen Bereich und zur Verbesserung der Überwachung und des Schutzes kritischer maritimer Infrastrukturen, einschließlich Seekabeln. Ein gangbarer Weg für das Krisenmanagement auf Unionsebene wäre der Aufbau eines spezifischen Netzes nationaler Kontaktstellen und eines engen zivil-militärischen Zusammenwirken, auch mit der NATO.

(12) Angesichts der Konvergenz der wirtschaftlichen und sicherheitspolitischen Interessen der EU macht die Krisenvorsorge eine umfassende Risikobewertung aller Gefahren und Bedrohungen erforderlich. Eine gemeinsame unionsweite Lageerfassung der Mitgliedstaaten und der Einrichtungen der Union, die durch die Einigung auf eine gemeinsame Taxonomie und sichere Kommunikationskanäle erleichtert wird, sollte

eine koordinierte und fundierte Reaktion auf potenzielle Cybersicherheitsvorfälle großen Ausmaßes sowie die Abschreckung von Akteuren, von denen eine anhaltende Bedrohung ausgeht, ermöglichen. Auf der Grundlage des Grundsatzes „Kenntnis nur, wenn nötig“ und unter Berücksichtigung der Bedeutung des Vertrauens in den Informationsaustausch könnten Gruppen von Mitgliedstaaten in verschiedenen Konfigurationen und gegebenenfalls einschlägige Einrichtungen der Union zusammenarbeiten und Informationen austauschen, die für das Management von Cybervorfällen relevant sind. Mitgliedstaaten und Einrichtungen der Union, die sich über Bedrohungen, Risiken und Lücken in der Cybersicherheitsreife austauschen, sollten das Setzen der richtigen Prioritäten für solide Investitionen und konkrete Maßnahmen ermöglichen, die dann die Cyberresilienz verbessern würden.

(13) Gemäß Artikel 7 Absatz 6 der Verordnung (EU) 2019/881 erstellt die ENISA in enger Zusammenarbeit mit den Mitgliedstaaten regelmäßig einen eingehenden technischen EU-Cybersicherheitslagebericht über Sicherheitsvorfälle und Cyberbedrohungen. Dieser Bericht wird als gemeinsamer EU-Cyberbewertungsbericht (EU-JCAR) bezeichnet; er wird gemeinsam mit Europol/EC3 und dem CERT-EU erstellt und soll die Abwehrbereitschaft der Union stärken, da er eine Lageeinschätzung auf der Grundlage einer Analyse von Sicherheitsvorfällen und Cyberbedrohungen bietet.

(14) Wichtige kritische Infrastrukturen wie Energie-, Verkehrs- und digitale Infrastrukturen, Gesundheits- oder Finanzdienstleistungen sowie die zu ihrem Schutz eingesetzten Sicherheitslösungen werden in der Regel von privaten Unternehmen betrieben. Der Schutz solcher Infrastrukturen vor Cybervorfällen großen Ausmaßes erfordert eine enge Zusammenarbeit zwischen öffentlichen und privaten Einrichtungen, einschließlich Herstellern und Open-Source-Entwicklern, auf der Grundlage von Vertrauen und klaren zweckbestimmten Verfahren für den Austausch und die Verbreitung von Informationen und die Koordinierung der Reaktion.

(15) Cyberübungen auf Unionsebene sind ein äußerst wirksames Instrument, um Verfahren und Kooperationsmechanismen zu testen und so die Abwehrbereitschaft zu verbessern. Da die Übungen ressourcenintensiv sind, muss die Übungsplanung so gestrafft und konsolidiert wie möglich sein und die Szenarien berücksichtigen, die im Zuge koordinierter Risikobewertungen der Union und anderer einschlägiger Initiativen entwickelt wurden.

(16) Europäische digitale Infrastrukturen weisen viele tief verwurzelte technische Abhängigkeiten auf. Diese sollten angegangen werden, um die Aufrechterhaltung des Betriebs im Krisenfall zu gewährleisten. Dies betrifft beispielsweise das Domänennamensystem (DNS), das eine entscheidende Komponente für den Betrieb des Internets ist. DNS-Auflösungsdienste sind für den Internetzugang, auch während einer schwerwiegenden Cyberkrise, unerlässlich, da sie Internet-Domänennamen in IP-Adressen umwandeln. Mit der Richtlinie (EU) 2022/2555 werden die einschlägigen Interessenträger dazu angehalten, eine Strategie zur Diversifizierung der DNS-Auflösung zu verfolgen. Ferner werden die Mitgliedstaaten darin aufgerufen, die Entwicklung und Nutzung eines öffentlichen und sicheren europäischen DNS-Auflösungsdienstes als Schlüsselmaßnahme zur Gewährleistung der Krisenvorsorge und -resilienz zu fördern.

(17) Um die Resilienz anderer kritischer Komponenten wie des Routing-Systems zu erhöhen und ihre Funktionsfähigkeit bei schwerwiegenden Cyberkrisen sicherzustellen, ist es darüber hinaus unabdingbar, dass entsprechende bewährte Verfahren und die neuesten bestehenden Normen zeitnah umgesetzt werden. Folglich

wird mit der Durchführungsverordnung (EU) 2024/2690 die Einrichtung eines Multi-Stakeholder-Forums zur Ermittlung der besten bestehenden Normen und Einführungstechniken für grundlegende Cybersicherheitselemente beauftragt und die Beteiligung der betreffenden Einrichtungen gefördert.

(18) Um böswillige Aktivitäten in den immer komplexeren globalen Lieferketten, die unionsweite Auswirkungen haben können, wirksam zu erkennen, ist ein koordinierter Ansatz erforderlich. Dies gilt insbesondere für Bereiche, in denen sich die Union auf Technik von Hochrisikoanbietern stützt, die der Rechtshoheit eines Drittlands unterliegen, sodass Informationen über Schwachstellen in Bezug auf Software oder Hardware an dessen Behörden übermittelt werden müssen, bevor sie überhaupt bekannt werden und ausgenutzt werden können. Staatlich geförderte Akteure können auch in kritischen Infrastrukturen einnisten, um erst zu einem späteren Zeitpunkt, z. B. während eines Konflikts, Störungen zu verursachen. Dies lässt sich anhand traditioneller Methoden nur schwer erkennen, da die Bedrohungsakteure ihr Vorgehen verschleiern, indem sie es mit legalem Verkehr verschmelzen und LOTL-Techniken (LOTL – „*Living off the land*“) einsetzen, die auf legitimen Instrumenten und Verfahren beruhen, um böswillige Aktivitäten zu verbergen. Gleiches gilt für Drittländer, wenn öffentlichen Erklärungen der Union oder ihrer Mitgliedstaaten zufolge Bedrohungsakteure, die von den Hoheitsgebieten dieser Länder aus operieren, böswillige Cyberaktivitäten gegen die Union durchführen. Lieferketten sollten resilienter und diversifizierter werden, ohne aber eine gemeinsame Basis für die Abwehrbereitschaft aufzugeben.

(19) Auf technischer Ebene spielen CSIRTs, Strafverfolgungsbehörden sowie die nationalen und grenzübergreifenden Cyber-Hubs (im Folgenden „Cyber-Hubs“), die gemäß der Verordnung (EU) 2025/38 eingerichtet werden sollen, eine wesentliche Rolle bei der Erkennung von Sicherheitsvorfällen, Cyberbedrohungen und Schwachstellen, der Unterstützung technischer Zuordnungen und der Wiederherstellung nach Cyberangriffen. Wirksame Verfahrensmodalitäten für die Zusammenarbeit zwischen dem CSIRTs-Netz und EU-CyCLONe gemäß der Richtlinie (EU) 2022/2555 sind unverzichtbar. Der Europäische Warnmechanismus für Cybersicherheit soll die Entwicklung fortgeschrittener Fähigkeiten unterstützen, um die Kapazitäten der Union zur Erkennung, Analyse und Datenverarbeitung im Zusammenhang mit Cyberbedrohungen und zur Verhütung von Sicherheitsvorfällen in der Union zu verbessern.

(20) Die den Mitgliedstaaten zur Verfügung stehenden Mechanismen umfassen die EU-Cybersicherheitsreserve und Maßnahmen zur Unterstützung der Amtshilfe gemäß der Verordnung (EU) 2025/38, Teams für die rasche Reaktion auf hybride Bedrohungen (HTTRs) und Teams für die rasche Reaktion auf Cybervorfälle (CRRTs) im Rahmen der Ständigen Strukturierten Zusammenarbeit (SSZ) sowie die für NATO-Verbündete vorgesehenen Mechanismen. Darüber hinaus unterstützt das EU-Notfallprotokoll für die Strafverfolgung (EU LE ERP) die Strafverfolgungsbehörden der EU bei der sofortigen Reaktion auf große grenzüberschreitende Cyberangriffe durch eine rasche Bewertung, den sicheren und zeitnahen Austausch kritischer Informationen und die wirksame Koordinierung der internationalen Aspekte ihrer Ermittlungen, einschließlich der Beilegung von Konflikten auf der Ebene der Strafverfolgung und der Koordinierung mit Partnern außerhalb der Strafverfolgung. Durch ein klares Bild davon, welche Reaktionsmöglichkeiten bei Cybervorfällen und hybriden Tätigkeiten zur Verfügung stehen und wie diese genutzt werden, kann eine effiziente Ressourcenzuteilung sichergestellt und Doppelarbeit vermieden werden.

Dementsprechend sind die Mitgliedstaaten gemäß der Verordnung (EU) 2025/38 verpflichtet, das CSIRTs-Netz und EU-CyCLONe zu unterrichten, wenn sie Dienste der EU-Cybersicherheitsreserve beantragen.

(21) Die wirksame Bekämpfung der Cyberkriminalität ist für die Cybersicherheit wesentlich. Abschreckung kann nicht allein durch Resilienz erreicht werden, sondern erfordert auch, dass Straftäter erkannt und verfolgt werden und ihnen etwas entgegengesetzt wird. Die Zusammenarbeit mithilfe angepasster technischer Systeme und Plattformen und der Austausch einschlägiger Informationen zwischen Akteuren im Bereich der Cybersicherheit, Einrichtungen der Cyberdiplomatie und der Strafverfolgung sind daher unerlässlich, um ein umfassendes Verständnis der Bedrohungslage zu gewährleisten und in kohärenter und koordinierter Weise reagieren zu können.

(22) Krisen schaffen Unsicherheit, die von Gegnern leicht ausnutzt werden kann, um Desinformation zu verbreiten und Misstrauen zu schüren. Um dem entgegenzuwirken, ist eine klare und kohärente öffentliche Kommunikation über die Lage und die Schritte, die unternommen werden, um Abhilfe zu schaffen, äußerst wichtig. Eine koordinierte strategische Kommunikation kann auch diplomatische Maßnahmen gegenüber Akteuren, von denen eine anhaltende Bedrohung ausgeht, und die Entwicklung eines Narrativs über Bedrohungen für die Union, ihre Abschreckungsmaßnahmen und die Notwendigkeit, ein verantwortungsvolles staatliches Handeln im Cyberraum zu fördern, unterstützen.

(23) Für ein wirksames Krisenmanagement ist es erforderlich, gemeinsame sichere Kommunikationslösungen für den Cyberbereich zu bestimmen und in der gesamten Union umzusetzen, gegebenenfalls auch für den Austausch von EU-Verschlusssachen. Auf Ersuchen des Rates erstellten die Kommission und andere einschlägige Einrichtungen der Union eine Bestandsaufnahme der bestehenden sicheren Kommunikationsinstrumente und legten die Ergebnisse im Dezember 2022 vor. Es bestehen mehrere voneinander getrennte Anstrengungen der Einrichtungen der Union zum Aufbau sicherer Kommunikationskapazitäten im Fall einer Krise, die eine bessere Koordinierung und Hebelwirkung erfordern. Dazu gehört die Einrichtung eines EU-Systems für kritische Kommunikation (EUCCS), um die Resilienz der öffentlichen Kommunikationsinfrastruktur gegenüber böswilligen Eingriffen zu verbessern und die tägliche operative Zusammenarbeit, auch über Grenzen hinweg, zu verbessern.

(24) Das Sicherheitsumfeld der Union erfordert einen gefahrenübergreifenden, ressortübergreifenden und gesamtgesellschaftlichen Ansatz für die zivile und militärische Krisenvorsorge und Abwehrbereitschaft. Militärische Einrichtungen stützen sich auf kritische zivile Infrastrukturen wie die für Kommunikation, Energie, Gesundheit, Verkehr und Logistik. Dementsprechend und wie in der EU-Cyberabwehrpolitik[18] hervorgehoben, erfordert die Cybersicherheit der EU eine stärkere Zusammenarbeit und Synergien zwischen den Vorsorge- und Reaktionskapazitäten ziviler und militärischer Netze, auch im Falle eines bewaffneten Angriffs. Die Akteure im Bereich der Cybersicherheit sollten über institutionelle und operative Bereiche hinweg zusammenarbeiten, um die Bedrohung durch sektorübergreifende, mehrdimensionale Störungen im Einklang mit den in der Strategie für eine krisenfeste Union verankerten Grundsätzen zu antizipieren und zu bewältigen. Darüber hinaus spielen böswillige Cyberaktivitäten bei umfassenderen

[18] EU-Cyberabwehrpolitik, JOIN(2022) 49 final.

hybriden Kampagnen gegen die Union, ihre Mitgliedstaaten und strategische Partner eine immer wichtigere Rolle. Daher ist eine engere Zusammenarbeit zwischen der Union und der NATO erforderlich.

(25) Im militärischen Bereich gelten das künftige EU-Koordinierungszentrum für die Cyberabwehr und das Einheitliche Analyseverfahren (SIAC) innerhalb des Europäischen Auswärtigen Dienstes, das operative Netz der militärischen IT-Notfallteams (MICNET) und die von der Europäischen Verteidigungsagentur (EDA) unterstützte EU-Konferenz der Cyberkommandeure sowie einschlägige Projekte im Rahmen der Ständigen Strukturierten Zusammenarbeit (SSZ) als wichtige Akteure und Initiativen für die Koordinierung und Zusammenarbeit bei der Abwehrbereitschaft im Hinblick auf die Erkennung, Abschreckung und Abwehr von Cyberbedrohungen, von denen die Union und die Mitgliedstaaten betroffen sind, sowie für die Wiederherstellung danach. Daher sollte die Zusammenarbeit zwischen zivilen und militärischen Akteuren gefördert werden, beispielsweise die Zusammenarbeit zwischen EU-CyCLONe und der EU-Konferenz der Cyberkommandeure sowie die mögliche Zusammenarbeit zwischen dem MICNET und dem CSIRTs-Netz.

(26) Die Zusammenarbeit mit internationalen strategischen Partnerländern und -organisationen außerhalb der Union stärkt auch die Cybersicherheitskapazitäten der Union. Durch die Förderung der internationalen Zusammenarbeit können die Union und ihre Partner für eine gemeinsame Lageerfassung und Kohärenz beim Cyberkrisenmanagement und eine solide Cyberabwehr sorgen und so zu einem globalen, offenen, stabilen, sicheren und resilienten Cyberraum beitragen. Diese Zusammenarbeit sollte auf Vertrauen und dem gemeinsamen Ziel beruhen, kritische Infrastrukturen und wesentliche Dienste vor Cyberbedrohungen zu schützen, unter anderem durch die Förderung eines verantwortungsvollen staatlichen Handelns im Cyberraum auf der Grundlage des Rahmens der Vereinten Nationen (VN) und indem Bedrohungsakteure für ihr unverantwortliches und rechtswidriges Verhalten im Cyberraum zur Rechenschaft gezogen werden. Maßnahmen der Cyberdiplomatie tragen zur Abschreckung von böswilligen Cyberaktivitäten und zur Reaktion darauf bei und sorgen für die Koordinierung zwischen und Zusammenarbeit mit internationalen strategischen Partnerländern —

HAT FOLGENDE EMPFEHLUNG ABGEGEBEN:

I Ziel, Anwendungsbereich und Grundsätze des EU-Rahmens für das Cyberkrisenmanagement

1. In dieser Empfehlung wird der Unionsrahmen für das Cybersicherheitskrisenmanagement im Zusammenhang mit der allgemeinen Abwehrbereitschaft der EU gegenüber mehrdimensionalen hybriden Bedrohungen beschrieben. In Anhang 1 wird dargelegt und zusammengefasst, wie sich ein Vorfall zu einem Sicherheitsvorfall großen Ausmaßes und somit zu einer Krise auf EU-Ebene ausweiten kann, selbst wenn ein solcher Vorfall mit anderen hybriden Bedrohungen zusammenfällt, die ein Ineinandergreifen der gebotenen Reaktionsmaßnahmen erfordern. Der Rahmen für das Cyberkrisenmanagement sollte es den einschlägigen Akteuren auf Unionsebene, einschließlich der Einrichtungen und Netzwerke, ermöglichen, besser zu verstehen, wie sie zusammenwirken sollten und wie sie die in Anhang II aufgeführten bestehenden Mechanismen über den gesamten Lebenszyklus des Krisenmanagements bestmöglich nutzen können. Darüber hinaus werden diesen Akteuren auf Unionsebene Empfehlungen gegeben, wie die Wirksamkeit der bestehenden Mechanismen verbessert werden kann.

2. Bei der Bewältigung einer Krise infolge eines Cybersicherheitsvorfalls großen Ausmaßes im Sinne des Artikels 6 Nummer 7 der Richtlinie (EU) 2022/2555, der das reibungslose Funktionieren des Binnenmarkts beeinträchtigt oder ernsthafte, die öffentliche Sicherheit betreffende Risiken für Einrichtungen und Bürger in mehreren Mitgliedstaaten oder in der gesamten Union birgt (im Folgenden „Cyberkrise"), sollten die Union und ihre Mitgliedstaaten dem Cyberkonzeptentwurf folgen.

3. Wenn ein Cybersicherheitsvorfall, der auf technischer Ebene von einem CSIRT oder einem Cyber-Hub erkannt wird, zu einer Eskalation im Rahmen der internen Verfahren des CSIRTs-Netzwerks führt, dann sollten auch geeignete Informationen gemäß den einschlägigen Verfahrensmodalitäten an das EU-CyCLONe übermittelt werden, das seinerseits prüfen sollte, ob es sich um einen potenziellen oder andauernden Sicherheitsvorfall großen Ausmaßes im Sinne des Artikels 6 Nummer 7 der Richtlinie (EU) 2022/2555 handelt. Die Feststellung, ob infolge dieses Sicherheitsvorfalls großen Ausmaßes eine Cyberkrise besteht oder nicht mehr besteht, sollte im Einklang mit dem Durchführungsbeschluss (EU) 2018/1993, insbesondere dessen Artikeln 4 und 5, erfolgen.

4. Im Einklang mit den in Anhang III genannten Grundsätzen der Verhältnismäßigkeit, Subsidiarität, Komplementarität und Vertraulichkeit von Informationen sollten die Mitgliedstaaten und Einrichtungen der Union ihre Zusammenarbeit beim Cyberkrisenmanagement vertiefen, indem sie das gegenseitige Vertrauen fördern und auf bestehenden Netzwerken und Mechanismen aufbauen. Der Cyberkonzeptentwurf greift zwar nicht die Art und Weise ein, wie die Einrichtungen ihre internen Verfahren festlegen, doch sollte jede Einrichtung die Schnittstellen für ihre Zusammenarbeit mit anderen Einrichtungen eindeutig festlegen. Diese Schnittstellen sollten von den betreffenden Einrichtungen gemeinsam vereinbart und eindeutig dokumentiert werden.

5. Der Cyberkonzeptentwurf sollte im Einklang mit dem Konzeptentwurf für kritische Infrastrukturen angewandt werden, insbesondere bei Sicherheitsvorfällen, die sowohl die physische Resilienz als auch die Cybersicherheit kritischer Infrastrukturen beeinträchtigen[19]. Soweit es sektorale Krisenmanagementmaßnahmen gibt, die sich auf Cybersicherheitsvorfälle beziehen, sollten solche Maßnahmen im Einklang mit dieser Empfehlung umgesetzt werden.

II Vorbereitung auf eine Cyberkrise auf Unionsebene

a) Lageerfassung und Informationsweitergabe

6. Verifizierte, zuverlässige Daten, einschließlich Trends bei Sicherheitsvorfällen, Taktiken, Techniken und Verfahren sowie aktiv ausgenutzter Schwachstellen, sollten die Grundlage für eine gemeinsame Lageerfassung der Mitgliedstaaten und Einrichtungen der Union in Bezug auf die Cyberbedrohungslandschaft bilden. Dieses gemeinsame Wissen sollte von den Mitgliedstaaten und Einrichtungen der Union im Einklang mit ihren jeweiligen Zuständigkeitsbereichen genutzt werden, um Cyberangriffe zu antizipieren, sich darauf vorzubereiten und sie aufzudecken. Diese gemeinsame Lageerfassung sollte

   a) alle in der Richtlinie (EU) 2022/2555 aufgeführten kritischen Sektoren erfassen, darunter insbesondere Kommunikation, digitale Infrastruktur,

[19] . In dem Konzeptentwurf für kritische Infrastrukturen (Anhang Teil I Abschnitt 4) wird näher ausgeführt, wie die Koordinierung in solchen Fällen aussehen soll.

Energie, Verkehr, Finanzen, Weltraum und Gesundheit, und sollte sich – über das CERT-EU – auch auf die Netze und Systeme der Einrichtungen der Union gemäß der Verordnung (EU, Euratom) 2023/2841 erstrecken;

b) auf hochwertigen, diversifizierten und integrierten Datensätzen beruhen, die in Echtzeit gesammelt, verarbeitet und weitergegeben werden;

c) im gemeinsamen Cyberbewertungsbericht (*Joint Cyber Assessment Report*, JCAR) und anderen relevanten Unterlagen berücksichtigt werden;

d) damit verbundene hybride Bedrohungen, einschließlich Informationsmanipulation und Einflussnahme aus dem Ausland (FIMI) und Desinformation, berücksichtigen;

e) ein kurzfristiges Eingreifen und Gegenmaßnahmen unterstützen und in die langfristige politische Planung im Hinblick auf die Abwehrbereitschaft und Abschreckung einfließen;

f) [mit anderen Risiko- und Bedrohungsanalysen verknüpft werden, die regelmäßig erstellt und durch die Strategie für eine krisenfeste Union untermauert werden, um Synergien zu erreichen und die Berichtspflichten der Mitgliedstaaten zu vereinfachen.]

7. EU-CyCLONe und das CSIRTs-Netzwerk sollten

a) zusammenarbeiten, um den Informationsaustausch zwischen technischer und operativer Ebene und die Lageerfassung insgesamt zu verbessern;

b) weiterhin ein Klima des Vertrauens zwischen den Mitgliedern schaffen;

c) die vorhandenen Instrumente für den Informationsaustausch in vollem Umfang nutzen.

8. Mitgliedstaaten und einschlägige Einrichtungen der Union sollten die Möglichkeiten der Koordinierung und Zusammenarbeit mit dem Privatsektor, darunter auch mit Open-Source-Gemeinschaften und Herstellern, verbessern, um die Informationsweitergabe auf EU- und nationaler Ebene mithilfe bestehender Informationsaustausch- und Analysezentren zu verbessern, die Cybersicherheitskapazitäten auszubauen und auf Cybersicherheitsvorfälle zu reagieren, unter anderem auch durch Rundtischgespräche mit EU-CyCLONe und dem CSIRTs-Netzwerk.

9. Um die Zusammenarbeit zu fördern und das Vertrauen zu stärken, könnten Mitgliedstaaten und einschlägige Einrichtungen der Union aufbauend auf den Vereinbarungen über den Austausch von Informationen im Bereich der Cybersicherheit gemäß der Richtlinie (EU) 2022/2555 und den Bestimmungen der Verordnung (EU) 2025/38 über Cyber-Hubs beschließen, freiwillige Kooperationscluster nach dem Grundsatz „Kenntnis nur, wenn nötig“ zu schaffen, wenn es um gemeinsame Anliegen geht, wie etwa die Abschreckung, Erkennung oder Reaktion in Bezug auf eine bestimmte Art von Bedrohung, mit der sie in besonderer Weise konfrontiert sind. Solche Cluster sollten dem jeweiligen Auftrag der einschlägigen Akteure sowie den bereits bestehenden Strukturen Rechnung tragen. Solche Kooperationscluster könnten sich an Einrichtungen der Union wenden, damit diese ihre Zusammenarbeit – auch über eine geeignete Infrastruktur – erleichtern.

10. Die Mitgliedstaaten sollten im Rahmen der durch die Richtlinie (EU) 2022/2555 eingesetzten NIS-Kooperationsgruppe innerhalb von 12 Monaten nach Annahme des Cyberkonzeptentwurfs eine gemeinsame Taxonomie für das Cyberkrisenmanagement aufstellen und einen Leitfaden für die sichere Behandlung und Weitergabe von Informationen über Cybersicherheitsvorfälle und -krisen vorlegen, der auch einen Abschnitt über die Bestimmung des Vertraulichkeitsgrads dieser Informationen (Kategorisierung) enthält.

11. Bei der Bestimmung des Vertraulichkeitsgrads der vorhandenen Informationen sollten Mitgliedstaaten und einschlägige Einrichtungen der Union die möglichen Folgen einer allzu strengen Einstufung auf den freiwilligen Informationsaustausch und das Erreichen eines gemeinsamen Lagebewusstseins berücksichtigen. Beim Austausch nicht als vertraulich eingestufter Informationen sollten die Mitgliedstaaten die bestehenden Plattformen für die technische und operative Zusammenarbeit, wie sie vom CSIRTs-Netzwerk und von EU-CyCLONe verwendet werden, in vollem Umfang nutzen.

b) Gemeinsame Übungen

12. Mitgliedstaaten und einschlägige Einrichtungen der Union sollten einen effizienten fortlaufenden Cyberübungszyklus aufbauen, um sich auf Cyberkrisen vorzubereiten und die organisatorische Effizienz zu steigern. Diese Übungen sollten auf den Szenarien beruhen, die auf der Grundlage von EU-weit koordinierten Risikobewertungen, einschließlich solcher für sektorübergreifende Krisen, entwickelt wurden. Der fortlaufende Cyberübungszyklus sollte dem Katastrophenschutzverfahren der Union und anderen Krisenreaktionsmechanismen auf Unionsebene Rechnung tragen. Er sollte sicherstellen, dass die aus den Übungen gewonnenen Erkenntnisse auch wirksam umgesetzt werden.

13. Die einschlägigen Akteure der Union könnten kleinere Übungen durchführen, um ihr Zusammenwirken und ihre Schnittstellen im Falle ausufernder Cybersicherheitsvorfälle zu testen.

14. Kommissionsdienststellen, EAD und ENISA werden ersucht, innerhalb von 18 Monaten nach Annahme des Cyberkonzeptentwurfs eine Übung zu dessen Erprobung zu organisieren, an der sich alle einschlägigen Akteure, einschließlich des Privatsektors, beteiligen.

c) DNS-Auflösungsfähigkeiten

15. Mitgliedstaaten, einschlägige Einrichtungen der Union sowie private Einrichtungen wie z. B. Betreiber kritischer Infrastrukturen sollten ihre Diversifizierungsstrategie für die Namenauflösung in den Domänennamensystemen (DNS) verbessern und mindestens eine in der Union ansässige DNS-Infrastruktur wie DNS4EU verwenden, um auch bei schweren Krisen eine zuverlässige DNS-Auflösung sicherzustellen. ENISA und EU-CyCLONe sollten Notfall-Leitlinien zur Ausfallsicherung ausarbeiten und bereitstellen, in denen die Schritte für den Wechsel zu einer in der Union ansässigen DNS-Infrastruktur im Falle eines Ausfalls anderer DNS-Dienste beschrieben werden, um die Kontinuität kritischer Dienste während einer Krise zu gewährleisten.

16. Darüber hinaus sollten nationale Cyber-Hubs und grenzübergreifende Cyber-Hubs wichtige Informationen über Bedrohungen im Zusammenhang mit solchen in der Union ansässigen DNS-Infrastrukturen austauschen, um sie bei der Gewährleistung eines hohen Maßes an Schutz vor unionsspezifischen Bedrohungen zu unterstützen

und so die Fähigkeiten zur Erkennung und Abmilderung unionsspezifischer Bedrohungen weiter zu steigern.

17. Zur allgemeinen Erhöhung der Sicherheit und Verfügbarkeit kritischer Internetinfrastrukturen – auch in Krisenzeiten – sollten die Mitgliedstaaten die Einbeziehung aller einschlägigen Interessenträger – auch derjenigen, die nicht direkt unter die NIS-2-Durchführungsverordnung fallen – in das damit beauftragte Multi-Stakeholder-Forum, dessen Aufgabe es ist, die besten bestehenden Normen und Einführungstechniken für wichtige Netzsicherheitsmaßnahmen zu ermitteln, aktiv fördern. Darüber hinaus sollten die Mitgliedstaaten erwägen, sich ebenfalls an dem Forum zu beteiligen und die empfohlenen Leitlinien selbst anzunehmen.

d) Mittelverwendung

18. Die Mitgliedstaaten sollten die im Rahmen der einschlägigen Unionsprogramme für die Cybersicherheit bereitgestellten Finanzmittel voll ausschöpfen.

III Erkennung von Vorfällen, die sich zu einer Cyberkrise ausweiten könnten

19. Um der zunehmenden Komplexität von Cybersicherheitsvorfällen und den wachsenden Problemen bei ihrer Erkennung zu begegnen, sollten sowohl öffentliche als auch private Einrichtungen Bedrohungserkennungsstrategien in allen ihren digitalen Infrastrukturen umsetzen, um mögliche vorbereitende Handlungen aufzudecken, die dann später für Störungszwecke ausgenutzt werden können. Wenn verdeckte Operationen aufgedeckt werden, sollten die Einrichtungen frühzeitig und proaktiv relevante Informationen mit ihren Partnern austauschen, bevor sich eine Situation überhaupt zur Krise ausweitet.

20. Alle Akteure sollten im Rahmen ihres jeweiligen Auftrags und nach dem gefahrenübergreifenden Ansatz Informationen übermitteln, die auf eine potenzielle Cyberkrise in den betreffenden Netzen hindeuten.

21. Das CSIRTs-Netzwerk und EU-CyCLONe sollten Verfahrensmodalitäten für potenzielle oder anhaltende Cybersicherheitsvorfälle großen Ausmaßes festlegen, um eine technisch-operative Koordinierung und eine zeitnahe und aussagekräftige Unterrichtung der politischen Ebene sicherzustellen.

22. Das CSIRTs-Netzwerk sollte EU-CyCLONe in der Frage beraten, ob ein beobachteter Cybersicherheitsvorfall als potenzieller oder anhaltender Sicherheitsvorfall großen Ausmaßes zu betrachten ist.

23. Die grenzübergreifenden Cyber-Hubs, die im Rahmen der Verordnung (EU) 2025/38 bereits eingerichtet wurden oder noch einzurichten sind, sollten mit einschlägigen Informationen zu den auf Unionsebene bestehenden Mechanismen beitragen, wenn nach dem gefahrenübergreifenden Ansatz ein potenzieller oder anhaltender Cybersicherheitsvorfall großen Ausmaßes vorliegt, der physische Schäden an kritischen Infrastrukturen umfasst, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen.

24. Wenn ein potenzieller Cybersicherheitsvorfall oder ein Cybersicherheitsvorfall großen Ausmaßes mit sektorübergreifenden Auswirkungen festgestellt wird,

    a) sollte die Kommission den Fluss der erforderlichen Informationen zwischen den Anlaufstellen für die in Anhang II aufgeführten einschlägigen horizontalen

und sektoralen Krisenmechanismen auf Unionsebene und EU-CyCLONe erleichtern;

b) sollten die einschlägigen Einrichtungen der Union EU-CyCLONe bei der Bewertung der Folgen für die Sektoren und die Bevölkerung unterstützen.

IV Reaktion auf eine Cyberkrise auf Unionsebene

25. Im Falle einer Cyberkrise, die im Rahmen der IPCR-Regelung festgestellt wird, sollten alle Beteiligten in enger Abstimmung mit anderen Einrichtungen, die weiter gefasste hybride Bedrohungen abwehren, im Rahmen eines ressortübergreifenden Ansatzes wie folgt reagieren:

a) die betroffenen Mitgliedstaaten und das CSIRTs-Netzwerk sollten zusammenarbeiten, um beeinträchtigte Systeme rasch wiederherzustellen und die Betriebsstörung so gering wie möglich zu halten;

b) EU-CyCLONe sollte der politischen Ebene in Zusammenarbeit mit dem CSIRTs-Netzwerk eindeutige Informationen über Auswirkungen, mögliche Folgen und Reaktions- und Abhilfemaßnahmen im Zusammenhang mit dem Vorfall geben und unter anderem im Rahmen der IPCR-Regelung einen Beitrag zur Integrierten Lageeinschätzung und -auswertung (ISAA) leisten;

c) die Kommission sollte – gegebenenfalls in Zusammenarbeit mit der Hohen Vertreterin – für Kohärenz und Koordinierung zwischen den Krisenreaktionen und den damit verbundenen Reaktionsmaßnahmen auf Unionsebene sorgen, insbesondere den in Anhang 2 aufgeführten einschlägigen sektoralen Krisenmanagementmechanismen auf Unionsebene und in Bezug auf die Anforderung von Hilfe im Rahmen des Katastrophenschutzverfahrens der Union;

d) der Ratsvorsitz sollte in Erwägung ziehen, den Vorsitz von EU-CyCLONe zu informellen Rundtischsitzungen und anderen einschlägigen Tagungen des Rates im Rahmen der IPCR-Regelung einzuladen;

e) der Rat sollte – mit Unterstützung von EU-CyCLONe und einschlägigen Einrichtungen der Union – die öffentliche Kommunikation koordinieren, damit die Krisensituation nicht zur Verbreitung unrichtiger Informationen genutzt wird;

f) die Hohe Vertreterin sollte – in enger Zusammenarbeit mit der Kommission und anderen einschlägigen Einrichtungen der Union – die Beschlussfassung im Rat über mögliche Maßnahmen im Rahmen des Instrumentariums für die Cyberdiplomatie, unter anderem durch Analysen und Berichte, unterstützen. Dadurch wird die Nutzung des gesamten Spektrums der Unionsinstrumente zur Vorbeugung, Abschreckung und Reaktion im Hinblick auf böswillige Cyberaktivitäten ermöglicht, um die Cyberabwehr der Union zu stärken, den Weltfrieden zu bewahren und die Sicherheit und Stabilität im Cyberraum zu fördern;

g) die Kommission, die Hohe Vertreterin und die Mitgliedstaaten sollten auch wirtschaftliche Instrumente wie Handelsverbote wirksamer einsetzen, um anhaltenden böswilligen Cyberaktivitäten staatlicher Akteure besser vorzubeugen, davon abzuschrecken und darauf zu reagieren.

26. Wenn ein Nutzer der von der EU-Cybersicherheitsreserve erbrachten Dienste[20] solche Dienste der EU-Cybersicherheitsreserve gemäß Artikel 15 der Verordnung (EU) 2025/38 beantragt, so sollten unbeschadet künftiger Durchführungsrechtsakte im Rahmen der Verordnung

   a) die Dienste innerhalb von 24 Stunden nach der Beantragung bereitgestellt werden,

   b) die Kommission und die Hohe Vertreterin die Koordinierung mit zusätzlichen Maßnahmen im Einklang mit dem EU-Instrumentarium zur Abwehr hybrider Bedrohungen[21] sicherstellen, falls es sich um böswillige Cyberaktivitäten handelt, die Teil einer umfassenderen hybriden Kampagne sind,

   c) die beantragenden Mitgliedstaaten im Falle böswilliger Cyberaktivitäten mit militärischer Dimension die EU-Konferenz der Cyberkommandeure von ihrem Antrag unterrichten.

27. Falls ein Cybersicherheitsvorfall großen Ausmaßes das ordnungsgemäße Funktionieren von Weltraumdiensten beeinträchtigt, die für die Sicherheit der Union oder ihrer Mitgliedstaaten wesentlich sind, sollte EU-CyCLONe die Hohe Vertreterin davon unterrichten, damit eine mögliche Reaktion mit der gemäß dem Beschluss (GASP) 2021/698 des Rates eingerichteten Architektur für die Reaktion auf Bedrohungen im Weltraum koordiniert werden kann.

V Wiederherstellung nach einer Cyberkrise

28. Mitgliedstaaten, einschlägige Einrichtungen und Netzwerke der Union sollten in der Wiederherstellungsphase zusammenarbeiten und sich dabei auf Erfahrungen aus durchgeführten Übungen sowie auf Berichte über Sicherheitsvorfälle stützen, und zwar insbesondere im Rahmen des mit der Verordnung (EU) 2025/38 eingerichteten Europäischen Überprüfungsmechanismus für Cybersicherheitsvorfälle.

VI Sichere Kommunikation

29. Ausgehend von der Bestandsaufnahme der vorhandenen sicheren Kommunikationsinstrumente[22] sollten sich die Kommission, die Hohe Vertreterin, EU-CyCLONe, das CSIRTs-Netzwerk und die einschlägigen Einrichtungen der Union bis Ende 2026 auf eine interoperable Reihe sicherer Kommunikationslösungen für die einschlägigen Akteure der Union verständigen. Diese Lösungen sollten das gesamte Spektrum der erforderlichen Kommunikationsarten abdecken (Sprache, Daten, Video- und Telekonferenzen (VTC), Nachrichtenübermittlung, Zusammenarbeit sowie Weitergabe und Konsultation von Dokumenten). Die Lösungen sollten wichtige Grundsätze wie die Sicherheitsinteressen der Union, die technologische Souveränität und die Vertraulichkeit widerspiegeln sowie Merkmale

---

[20] Die EU-Cybersicherheitsreserve ist ein Mechanismus, der aus Diensten vertrauenswürdiger Anbieter verwalteter Sicherheitsdienste besteht und auf Antrag die Reaktion und anfängliche Wiederherstellung im Falle von schwerwiegenden Cybersicherheitsvorfällen, Cybersicherheitsvorfällen großen Ausmaßes oder einem Cybersicherheitsvorfall großen Ausmaßes gleichwertigen Sicherheitsvorfällen mit Auswirkungen auf die Mitgliedstaaten, die Organe, Einrichtungen oder sonstigen Stellen der Union oder mit dem Programm „Digitales Europa“ assoziierte Drittländer unterstützt.

[21] Das Instrumentarium zur Abwehr hybrider Bedrohungen ist ein Rahmen für eine koordinierte Reaktion auf gegen die EU und ihre Mitgliedstaaten gerichtete hybride Kampagnen; es umfasst beispielsweise Präventiv-, Kooperations-, Stabilisierungs- und Wiederherstellungsmaßnahmen sowie restriktive Maßnahmen und soll die Solidarität und gegenseitige Unterstützung stärken.

[22] HWPCI WK 862/23.

wie Nutzbarkeit, konzeptintegrierte Sicherheit, Zertifizierung durch europäische Informationssicherheitsstellen, End-zu-End-Verschlüsselung, Authentifizierung, Verfügbarkeit und Post-Quanten-Kryptographie aufweisen. Die Lösungen sollten gemeinsam festgelegten Anforderungen an den Schutz von nicht als vertraulich eingestuften sensiblen Informationen erfüllen und Instrumente für den Austausch von Verschlusssachen des Geheimhaltungsgrades RESTREINT UE/EU RESTRICTED umfassen.

30. Auf dieser Grundlage sollten die Akteure auf Unionsebene Lösungen verwenden, die auf dem Matrix-Protokoll für die Echtzeitkommunikation beruhen. Das durch die Verordnung (EU) 2021/887 eingerichtete Europäische Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (ECCC) sollte unbeschadet des künftigen mehrjährigen Finanzrahmens eine Finanzierung über das Programm Digitales Europa in Betracht ziehen, um die Mitgliedstaaten beim Einsatz dieser Instrumente zu unterstützen.

31. Insbesondere sollten EU-Einrichtungen und Mitgliedstaaten Notfallvorkehrungen für schwere Krisen entwickeln, in denen normale Kommunikationskanäle, die auf das Internet oder auf Telekommunikationsnetze angewiesen sind, gestört oder nicht verfügbar sind.

32. Mittelfristig sollten – vor allem auf technischer Ebene – Mechanismen für die Kommunikation und den Informationsaustausch zwischen Strafverfolgungs- und Cybersicherheitsnetzen eingerichtet werden, um eine wirksame Krisenreaktion zu ermöglichen. Solche Mechanismen sollten die Rolle der einzelnen Beteiligten beachten und nicht in laufende Operationen eingreifen. Die Kommission arbeitet zusammen mit den Mitgliedstaaten am Aufbau des Europäischen Systems für kritische Kommunikation (EUCCS), das bis 2030 die Kommunikationsnetze für Strafverfolgung und Katastrophenschutz im gesamten Schengen-Raum miteinander verbinden soll, damit kritische Kommunikationsausrüstungen auch im Hoheitsgebiet anderer Mitgliedstaaten verwendet werden können. Dem EUCCS würde daher auch ein gemeinsames Vorgehen mit einschlägigen Cybergemeinschaften zugutekommen. Dieses System sollte auch Reserve-Kommunikationswege unterstützen, wie z. B. über Satellitenkommunikation.

VII Koordinierung mit militärischen Akteuren im Fall von Cyberkrisen

33. EU-CyCLONe, die EU-Konferenz der Cyberkommandeure, MICNET, das CSIRTs-Netzwerk sowie ein künftiges EU-Koordinierungszentrum für die Cyberabwehr und seine zivilen Partner in der Union sollten alle zusammenarbeiten, um ein gemeinsames Lagebewusstsein zwischen zivilen und militärischen Akteuren zu entwickeln.

34. Die Union sollte sich unter Berücksichtigung bestehender Vereinbarungen wie der technischen Vereinbarung CERT-EU/NATO von 2016 darum bemühen, Kontaktstellen für die Koordinierung mit der NATO im Falle einer Cyberkrise einzurichten, damit benötigte Informationen über die Lage und die Nutzung der Krisenreaktionsmechanismen ausgetauscht werden können. Zu diesem Zweck sollte die Union prüfen, wie die Kapazitäten für den Informationsaustausch mit der NATO verbessert werden können, unter anderem auch durch eine mögliche Vernetzung ihrer jeweiligen Kommunikations- und Informationssysteme.

35. Wenn ein Mitgliedstaat im Zusammenhang mit einem Cybersicherheitsvorfall auf einschlägige Verteidigungsinitiativen wie die CRRTs der SSZ oder andere

einschlägige Initiativen wie die EU-Teams für die rasche Reaktion auf hybride Bedrohungen (HRRTs) zurückgreift, sollte er EU-CyCLONe sowie die EU-Konferenz der Cyberkommandeure hierüber informieren.

VIII Zusammenarbeit mit strategischen Partnern

36. Die Hohe Vertreterin sollte in enger Zusammenarbeit mit der Kommission und anderen einschlägigen Einrichtungen der Union

    a) bei Feststellung eines relevanten Sicherheitsvorfalls den Fluss der erforderlichen Informationen mit strategischen Partnern erleichtern;

    b) im Zusammenhang mit der Reaktion auf anhaltende böswillige Cyberaktivitäten von Akteuren, von denen eine anhaltende Bedrohung ausgeht, die Koordinierung mit strategischen Partnern verbessern, insbesondere auch beim Einsatz des Instrumentariums für die Cyberdiplomatie im Einklang mit dessen Umsetzungsleitlinien.

37. Die Mitgliedstaaten, die Hohe Vertreterin, die Kommission und andere einschlägige Einrichtungen der Union sollten mit strategischen Partnern und internationalen Organisationen zusammenarbeiten, um bewährte Verfahren und ein verantwortungsvolles staatliches Handeln im Cyberraum zu fördern und eine rasche und koordinierte Reaktion auf potenzielle Cybersicherheitsvorfälle oder Cybersicherheitsvorfälle großen Ausmaßes sicherzustellen.

38. Im Rahmen des in Abschnitt II genannten fortlaufenden Cyberübungszyklus sollten die Kommissionsdienststellen und der EAD die Organisation einer gemeinsamen Stabsübung in Erwägung ziehen, um die Zusammenarbeit zwischen zivilen und militärischen Komponenten im Falle eines Cybersicherheitsvorfalls großen Ausmaßes, der die Mitgliedstaaten der Union und die NATO-Bündnispartner betrifft, zu testen, auch für den Fall, dass Artikel 4 oder Artikel 5 des NATO-Vertrags ausgelöst wird oder wahrscheinlich ausgelöst werden könnte.

39. Angesichts der Gefährdung von Kandidatenländern und angesichts des Potenzials von Cybersicherheitsvorfällen, die sich in der Nachbarschaft der Union ereignen, sollten gemeinsame Übungen unter Einbeziehung von Kandidatenländern in Betracht gezogen werden.

Geschehen zu Brüssel am

Im Namen des Rates

Der Präsident /// Die Präsidentin