Rat der
Europäischen Union

Brüssel, den 6. Juni 2025
(OR. en)

9794/25

Interinstitutionelles Dossier:
2025/0036 (NLE)

CYBER 157
IPCR 42
RELEX 706
JAI 738
JAIEX 54
POLMIL 138
HYBRID 63
TELECOM 178
COSI 108

BERATUNGSERGEBNISSE

Absender:	Generalsekretariat des Rates
vom	6. Juni 2025
Empfänger:	Delegationen
Betr.:	Empfehlung des Rates für einen EU-Konzeptentwurf für das Cyberkrisenmanagement – Empfehlung des Rates, vom Rat auf seiner Tagung am 6. Juni 2025 gebilligt

Die Delegationen erhalten anbei die Empfehlung des Rates in der vom Rat auf seiner Tagung vom 6. Juni 2025 gebilligten Fassung.

ANLAGE

EMPFEHLUNG DES RATES

für einen EU-Konzeptentwurf für das Cyberkrisenmanagement

DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf die Artikel 114 und 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 Cybersicherheitsvorfällen 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 hybrider Kampagnen 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 Übersprungpotenzial, 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, Unternehmen und Bürgerinnen und Bürger 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) Angesichts der wechselseitigen Abhängigkeiten und Verbindungen zwischen den IKT-Umgebungen der Unionseinrichtungen und Mitgliedstaaten könnten Vorfälle bei Unionseinrichtungen ein Cybersicherheitsrisiko für Mitgliedstaaten darstellen und umgekehrt. Der Austausch einschlägiger Informationen und die Koordination hinsichtlich sowohl Cybersicherheitsvorfällen großen Ausmaßes als auch schwerwiegender Sicherheitsvorfälle gemäß Artikel 3 Nummer 8 der Verordnung (EU, Euratom) 2023/2841[1] ist im Kontext des EU-Konzeptentwurfs für das Cybersicherheitskrisenmanagement (im Folgenden „der Cyber-Konzeptentwurf“) von entscheidender Bedeutung.

[1] 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, S. 1).

(4) Im Fall einer Krise, für die die Integrierte EU-Regelung für die politische Reaktion auf Krisen (im Folgenden „IPCR" – Integrated Political Crisis Response) gemäß Durchführungsbeschluss (EU) 2018/1993 des Rates[2] (im Folgenden „IPCR-Regelung") aktiviert wurde, sollte der Cyber-Konzeptentwurf die IPCR-Regelung für Koordinierung und Reaktion vollumfänglich berücksichtigen. Die politische und strategische Koordinierung würde im Rahmen der IPCR erfolgen. Die IPCR-Regelung ist das Werkzeug für die horizontale Koordinierung und Reaktion auf der politischen Ebene der Union. Gemäß der IPCR-Regelung liegt die Entscheidung zur Aktivierung oder Deaktivierung der IPCR beim Vorsitz des Rates der Europäischen Union. Die Arbeit im Rahmen der IPCR wird sowohl im Informationsaustausch-Modus als auch im Modus der vollständigen Aktivierung durch von den Kommissionsdienststellen und dem Europäischen Auswärtigen Dienst (im Folgenden „EAD") ausgearbeitete Berichte über die „Integrierte Lageeinschätzung und -auswertung" (im Folgenden „ISAA" – Integrated Situational Awareness and Analysis) unterstützt.

(5) Die Hauptverantwortung für das Management von Cybersicherheitsvorfällen und Cyberkrisen liegt bei den Mitgliedstaaten. Allerdings 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. Das Cyberkrisenmanagement über den gesamten Lebenszyklus umfasst die Abwehrbereitschaft und die gemeinsame Lageerfassung zur Antizipation von Cybersicherheitsvorfällen von großem Ausmaß, die erforderlichen Erkennungskapazitäten für die Bestimmung der benötigten Reaktions- und Wiederherstellungsinstrumente zur Milderung und Eindämmung von Cybersicherheitsvorfällen großen Ausmaßes sowie die Reaktionskapazitäten, um vor weiteren Vorfällen abzuschrecken und diese zu verhindern.

---

[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).

(6) 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 Cybersicherheitsvorfälle großen Ausmaßes und Cyberkrisen festgelegt. Darin werden die einschlägigen Akteure auf technischer, operativer und politischer Ebene aufgeführt und es wird erläutert, wie diese in die bestehenden Mechanismen der Union für das Krisenmanagement 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. Die vorliegende Empfehlung baut auf diesen Grundprinzipien auf und soll die Empfehlung (EU) 2017/1584 ersetzen und einen neuen Rahmen der EU für das Cybersicherheitskrisenmanagement festlegen.

(7) Einige in der vorliegenden Empfehlung verwendeten Begriffsbestimmungen beruhen auf den in der der Richtlinie (EU) 2022/2555[4] verwendeten Begriffsbestimmungen und Begriffen. Die vorliegende Empfehlung hat jedoch einen anderen Anwendungsbereich als die Richtlinie (EU) 2022/2555. Mit der vorliegenden Empfehlung wird der Rahmen der EU für das Cyberkrisenmanagement vor dem Hintergrund der allgemeinen Vorbereitung der EU auf Cybersicherheitsvorfälle großen Ausmaßes und Cyberkrisen, die daraus entstehen, festgelegt – unabhängig davon, welcher Sektor oder welche Einrichtung betroffen ist. Soweit möglich, beruhen die Begriffsbestimmungen auf den Begriffsbestimmungen der Richtlinie (EU) 2022/2555.

---

[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).

[4] 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 (EU) 2016/1148 (NIS- 2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80).

(8) Es ist ein aktualisierter Cyber-Konzeptentwurf vonnöten, um klare und zugängliche Leitlinien bereitzustellen, in denen erläutert wird, was ein Cybersicherheitsvorfall großen Ausmaßes sowie eine Cyberkrise auf Unionsebene sind, wie der Rahmen für das Krisenmanagement ausgelöst wird, welche Rollen die einschlägigen Netzwerke, Akteure und Mechanismen auf Unionsebene spielen und wie diese Akteure und Mechanismen über den gesamten Lebenszyklus von Cyberkrisen interagieren sollen. Mit dem Cyber-Konzeptentwurf soll ein breiterer Rahmen für zivil-militärische Beziehungen der EU im Kontext des Cyberkrisenmanagements, unter anderem vor dem Hintergrund der Vertiefung der Beziehungen zwischen der EU und der NATO, unterstützt werden, wo möglich auch durch inklusive, wechselseitige und nichtdiskriminierende Mechanismen für verbesserten Informationsaustausch im Cyberkrisenmanagement.

(9) Das sektorübergreifende Krisenmanagement auf Unionsebene sollte verstärkt werden, um eine integrierte Krisenreaktion zu ermöglichen, insbesondere in Fällen, in denen Cybersicherheitsvorfälle großen Ausmaßes und Cyberkrisen physische Auswirkungen haben. Diese Empfehlung ergänzt die IPCR-Regelung und andere Mechanismen der Union für das Krisenmanagement, einschließlich des allgemeinen Frühwarnsystems ARGUS der Kommission, des Katastrophenschutzverfahrens der Union (im Folgenden „UCPM“ – Union Civil Protection Mechanism), das durch das im Rahmen des UCPM mit dem Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates über ein Katastrophenschutzverfahren der Union[5] (im Folgenden „UCPM-Beschluss“) eingerichtete Zentrum für die Koordination von Notfallmaßnahmen (im Folgenden „ERCC“ – Emergency Response Coordination Centre) unterstützt wird, und des Krisenreaktionsmechanismus („CRM“ –Crisis Response Mechanism) des EAD, sowie andere Prozesse, wie sie im Instrumentarium für die Cyberdiplomatie[6], im EU-Instrumentarium zur Abwehr hybrider Bedrohungen[7] und im überarbeiteten EU-Protokoll für das operative Vorgehen bei der Abwehr hybrider Bedrohungen[8] beschrieben sind. Sie ergänzt auch die Empfehlung (EU) 2024/4371 des Rates für einen Konzeptentwurf zur Koordinierung der Reaktion – auf Unionsebene – auf Störungen kritischer Infrastrukturen von erheblicher grenzüberschreitender Bedeutung[9] (im Folgenden „EU-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.

---

5 Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates vom 17. Dezember 2013 über ein Katastrophenschutzverfahren der Union (ABl. L 347 vom 20.12.2013, S. 924).

6 Schlussfolgerungen des Rates über einen Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten, Dok. 9916/17.

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

8 Gemeinsame Arbeitsunterlage – EU-Protokoll zur Abwehr hybrider Bedrohungen (SWD(2023) 116 final).

9 ABl. C, 2024/4371, 5.7.2024.

(10) Das europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (im Folgenden „EU-CyCLONe“) ist das Netzwerk für die Koordinierung des Managements von Cybersicherheitsvorfällen großen Ausmaßes und Cyberkrisen auf operativer Ebene, einschließlich sektorübergreifender Cybersicherheitsvorfälle großen Ausmaßes und sektorenübergreifender Cyberkrisen. Damit der bestehende Rahmen nicht noch komplizierter wird, sollte die Schaffung sektoraler Strukturen, die eine Dopplung der Aufgaben des EU-CyCLONe bewirken, vermieden werden. EU-CyCLONe sollte operative Informationen mit Bezug auf Cybersicherheit auch von den Sektoren erhalten und auf politischer Ebene einen Beitrag leisten.

(11) Die Mitgliedstaaten sind angehalten, die im Rahmen der einschlägigen Unionsprogramme für die Cybersicherheit bereitgestellten Finanzmittel voll ausschöpfen. Es sollte sichergestellt werden, dass diese Programme nur minimalen Verwaltungsaufwand für die Antragsteller, die Finanzmittel beantragen, verursachen und dass die Teilnahme der Mitgliedstaaten an diesen Programmen durch die Bereitstellung einschlägiger Leitlinien über geeignete finanzielle Unterstützungsmöglichkeiten erleichtert wird.

(12) Die vorliegende Empfehlung trägt im Einklang mit den in der Strategie der Union zur Krisenvorsorge verankerten Grundsätzen zu umfassenderen Vorsorgemaßnahmen bei, die für die Union angesichts sektorübergreifender Krisen erforderlich sind, nämlich zu einem gefahrenübergreifenden, ressortübergreifenden und gesamtgesellschaftlichen Ansatz, insbesondere im Hinblick auf eine Verbesserung des Bewusstseins für Risiken und Bedrohungen sowie der sektorübergreifenden Krisenreaktion —

HAT FOLGENDE EMPFEHLUNG ABGEGEBEN:

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

Ziel und Geltungsbereich

1. Mit der vorliegenden Empfehlung für einen EU-Konzeptentwurf für das Cyberkrisenmanagement (im Folgenden „Cyber-Konzeptentwurf“) wird der Rahmen der EU für das Cyberkrisenmanagement vor dem Hintergrund der allgemeinen Vorbereitung der EU auf Cybersicherheitsvorfälle von großem Umfang und Cyberkrisen festgelegt. Der Rahmen trägt der Rolle der Mitgliedstaaten und der Organe, Einrichtungen und sonstigen Stellen der Union (im Folgenden „Einrichtungen der Union“) innerhalb ihrer jeweiligen Zuständigkeiten und unter Achtung der nationalen Rechtsvorschriften und interne Regeln Rechnung, um umfassende und koordinierte Maßnahmen auf Unionsebene zu gewährleisten.

2. Der Cyber-Konzeptentwurf sollte im Einklang mit dem EU-Konzeptentwurf für kritische Infrastrukturen angewandt werden, insbesondere bei Sicherheitsvorfällen, die sowohl die physische Resilienz als auch die Cybersicherheit kritischer Infrastrukturen beeinträchtigen.[10]

3. Der Cyber-Konzeptentwurf enthält Leitlinien für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Cyberkrisen und sollte als Ergänzung zu einschlägigen sektoralen Reaktionsmechanismen wie denen in Anhang II verwendet werden. Die betroffenen Akteure im Bereich Cybersicherheit sollten beim Erreichen der Ziele dieser sektoralen Mechanismen auf nationaler Ebene und auf Unionsebene helfen und Unterstützung leisten.

4. Im Fall einer EU-weiten sektorübergreifenden Krise mit Cyberaspekten, für die die IPCR aktiviert wurde, sollte der Rat die Reaktion auf politischer Ebene der Union unter Nutzung der IPCR-Regelung koordinieren. Bei Aktivierung der IPCR sollten die Maßnahmen gemäß dem Cyber-Konzeptentwurf die Reaktion der EU auf politischer Ebene unterstützen und dabei spezifische Unterstützung im Bereich Cybersicherheit leisten.

---

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

Leitgrundsätze

5. Für das Cyberkrisenmanagement auf Unionsebene gelten die folgenden Leitgrundsätze:

a) *Verhältnismäßigkeit*: Die meisten Cybersicherheitsvorfälle, die die Mitgliedstaaten betreffen, sind nicht so schwerwiegend, dass sie als Cybersicherheitsvorfall großen Ausmaßes oder Cyberkrise auf nationaler Ebene oder Unionsebene angesehen werden könnten. Bei Cybersicherheitsvorfällen und -bedrohungen arbeiten die Mitgliedstaaten zusammen und tauschen auf freiwilliger Basis regelmäßig Informationen im Netz der Computer-Notfallteams (im Folgenden „CSIRTs-Netzwerk“) und im EU-CyCLONe im Einklang mit den Standardarbeitsverfahren dieser Netze aus.

b) *Subsidiarität*: Bei Cybersicherheitsvorfällen, Cybersicherheitsvorfällen großen Ausmaßes oder Cyberkrisen sind in erster Linie die betroffenen Mitgliedstaaten für die Reaktion und Abhilfe zuständig. Angesichts möglicher grenzübergreifender Effekte sollten der Rat, die Kommission, der Hohe Vertreter, die Agentur der Europäischen Union für Cybersicherheit (im Folgenden „ENISA“) das IT-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der EU (im Folgenden „CERT-EU“), Europol und alle anderen einschlägigen Einrichtungen der Union während des gesamten Krisenzyklus zusammenarbeiten. Diese Rolle leitet sich aus dem Unionsrecht ab und spiegelt wider, in welchem Umfang Cybersicherheitsvorfälle großen Ausmaßes und Cyberkrisen einen oder mehr Wirtschaftssektoren im Binnenmarkt, die Sicherheit und die internationalen Beziehungen der Union oder auch die Einrichtungen der Union selbst treffen.

c) *Komplementarität*: Die vorliegende Empfehlung trägt den auf Unionsebene bestehenden Krisenmanagementmechanismen, die in Anhang II aufgeführt sind, in vollem Umfang Rechnung, insbesondere der IPCR-Regelung, ARGUS und dem CRM des EAD. Die vorliegende Empfehlung berücksichtigt die Mandate des CSIRTs-Netzwerks und EU-CyCLONe sowie die Verordnung (EU, Euratom) 2023/2841. In Fällen, in denen die IPCR aktiviert ist, sollte die Arbeit der einschlägigen Netze, Einrichtungen und aktivierter sektoraler Mechanismen fortgesetzt werden und in die politische und strategische Koordinierung, die im Rahmen der IPCR stattfindet, einfließen und diese unterstützen.

d) *Vertraulichkeit von Informationen*: Jeder Informationsaustausch im Rahmen der vorliegenden Empfehlung sollte den geltenden Sicherheits- und Datenschutzvorschriften entsprechen. Informelle Geheimhaltungsvereinbarungen wie das „Traffic Light Protocol“ für die Kennzeichnung vertraulicher Informationen sollten gegebenenfalls berücksichtigt werden. Für den Austausch von Verschlusssachen sollten unabhängig von der geltenden Einstufungsregelung die bestehenden bindenden Vorschriften und Übereinkünfte über die Verarbeitung von Verschlusssachen gemeinsam mit den verfügbaren akkreditierten Instrumenten angewandt werden.

6. Im Einklang mit oben genannten Leitgrundsätzen 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. Diese Zusammenarbeit im Rahmen des Cyber-Konzeptentwurfs wird durch die Umsetzung der Artikel 22 und 23 der Verordnung (EU, Euratom) 2023/2841 erleichtert. Insbesondere der auf Grundlage des Artikels 23 der Verordnung (EU, Euratom) 2023/2841 aufgestellte Cyberkrisenbewältigungsplan leistet unter anderem einen Beitrag zum regelmäßigen Austausch einschlägiger Informationen zwischen Einrichtungen der Union und den Mitgliedstaaten, und mit ihm werden Regelungen für die Koordinierung und den Informationsfluss zwischen Einrichtungen der Union festgelegt.

II: Begriffsbestimmungen

7. Für die Zwecke des vorliegenden Cyber-Konzeptentwurfs bezeichnet der Ausdruck

a) „Sicherheitsvorfall“ ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt;

b) „erheblicher Sicherheitsvorfall“ einen Sicherheitsvorfall, der

a. schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann;

b. andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann;

c) „Cybersicherheitsvorfall großen Ausmaßes“ einen Sicherheitsvorfall, der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt, oder der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat;

d) „Cyberkrise“ einen Cybersicherheitsvorfall, der sich zu einer echten Krise entwickelt hat, die das reibungslose Funktionieren des Binnenmarkts verhindert oder ernsthafte, die öffentliche Sicherheit betreffende Risiken für Einrichtungen und Bürger in mehreren Mitgliedstaaten oder in der gesamten Union darstellt.

III: Nationale Strukturen und Zuständigkeiten für das Cyberkrisenmanagement

8. Bei Cybersicherheitsvorfällen großen Ausmaßes oder Cyberkrisen sind in erster Linie die betroffenen Mitgliedstaaten für die Reaktion zuständig. Im Einklang mit der Richtlinie (EU) 2022/2555 verfügt jeder Mitgliedstaat über eine oder mehrere Behörden für das Cyberkrisenmanagement sowie über eines oder mehrere Computer-Notfallteams (CSIRTs).

9. Durch die Annahme der Richtlinie (EU) 2022/2555 und anderer legislativer und nichtlegislativer Instrumente im Bereich der Cybersicherheit haben die Mitgliedstaaten ihre Rahmen für die Cybersicherheit angeglichen, indem sie Mindestvorschriften für das Funktionieren des koordinierten Rechtsrahmen festgelegt, Mechanismen für die wirksame Zusammenarbeit zwischen den zuständigen Behörden in den einzelnen Mitgliedstaaten vorgeschrieben und wirksame Abhilfemaßnahmen und Durchsetzungsmaßnahmen, die für die wirksame Durchsetzung dieser Verpflichtungen von entscheidender Bedeutung sind, eingeführt haben.

10. Im Einklang mit Artikel 9 Absatz 4 der Richtlinie (EU) 2022/2555 sollte jeder Mitgliedstaat einen nationalen Plan für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen verabschieden. Diese Pläne enthalten insbesondere nationale Vorsorgenmaßnahmen, Verfahren für das Cyberkrisenmanagement sowie die zwischen den einschlägigen nationalen Behörden und Stellen vereinbarten nationalen Verfahren und Regelungen, die gewährleisten sollen, dass sich der jeweilige Mitgliedstaat wirksam am koordinierten Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen auf Unionsebene beteiligen und dieses unterstützen kann. Die Verfahren für das Cyberkrisenmanagement umfassen auch Vorschriften für deren Integration in den nationalen Rahmen für das allgemeine Krisenmanagement und für die Kanäle für den Informationsaustausch.

11. Im Einklang mit Artikel 9 Absatz 1 der Richtlinie (EU) 2022/2555 sollte jeder Mitgliedstaat die Kohärenz mit den geltenden Rahmen für das allgemeine nationale Krisenmanagement gewährleisten. Im Falle der Aktivierung der IPCR sollten die nationalen Behörden für das Krisenmanagement Informationen der Behörden für das Cyberkrisenmanagement und der nationalen sektorale Krisenmechanismen sammeln, um der IPCR als Grundlage zu dienen.

12. Im Einklang mit Artikel 9 Absatz 5 der Richtlinie (EU) 2022/2555 sollte EU-CyCLONe auf Ersuchen eines betroffenen Mitgliedstaats Informationen über die einschlägigen Teile der nationalen Pläne für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen austauschen, insbesondere über die Vorschriften zur Gewährleistung einer wirksamen Beteiligung am koordinierten Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen auf Unionsebene sowie der Unterstützung davon, um bewährte Verfahren auszutauschen und zu überprüfen, ob der allgemeine Rahmen in der Praxis funktionieren würde.

13. EU-CyCLONe und der Interinstitutionelle Cybersicherheitsbeirat (im Folgenden „IICB“ – Interinstitutional Cybersecurity Board) werden ersucht, sich gegebenenfalls über die Kohärenz zwischen dem vom IICB gemäß Artikel 23 der Verordnung (EU, Euratom) 2023/2841 ausgearbeiteten Cyberkrisenbewältigungsplans und den nationalen Plänen für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen auszutauschen.

14. EU-CyCLONe sollte – unterstützt durch ENISA als sein Sekretariat – eine aktuelle Liste nationaler Behörden für das Cyberkrisenmanagement mit Kontaktdaten von CyCLONe-Beamten und -Führungskräften führen und diese den Mitgliedern von EU-CyCLONe zur Verfügung stellen.

IV: Wichtigste Netzwerke und Akteure im Ökosystem der EU für das Cyberkrisenmanagement

15. Im Einklang mit den einschlägigen Aufgaben gemäß Artikel 15 Absatz 3 der Richtlinie (EU) 2022/2555 ist das CSIRTS-Netzwerk insbesondere im Anwendungsbereich der vorliegenden Empfehlung das wichtigste technische Netzwerk für den Austausch relevanter Informationen über Sicherheitsvorfälle. Es trägt zum Aufbau von Vertrauen zwischen den Mitgliedstaaten bei und fördert eine rasche und wirksame operative Zusammenarbeit zwischen ihnen. Der Vorsitz des CSIRTs-Netzwerks kann als Beobachter am IICB teilnehmen.

16. CERT-EU ist das IT-Notfallteam für alle Einrichtungen der Union. In Einklang mit Artikel 13 der Verordnung (EU) 2023/2841 fungiert CERT-EU als die zentrale Stelle für den Austausch von Informationen zur Cybersicherheit und die Koordinierung der Reaktion auf Sicherheitsvorfälle. CERT-EU ist ein Mitglied des CSIRTs-Netzwerks und unterstützt die Kommission im EU-CyCLONe. CERT-EU arbeitet auf technischer Ebene und ist für die Koordinierung der Bewältigung schwerwiegender Sicherheitsvorfälle, die Einrichtungen der Union betreffen, verantwortlich.

17. EU-CyCLONe dient als Vermittler zwischen der technischen und der politischen Ebene, insbesondere im Fall von Cybersicherheitsvorfällen großen Ausmaßes und Cyberkrisen. Gemäß Artikel 16 der Richtlinie (EU) 2022/2555 unterstützt es das koordinierte Management von Cybersicherheitsvorfällen großen Ausmaßes und Cyberkrisen auf operativer Ebene und gewährleistet einen regelmäßigen Austausch relevanter Informationen zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union. Der Vorsitz von EU-CyCLONe kann als Beobachter am IICB teilnehmen.

18. Die ENISA ist die Agentur der Union, die die ihr mit der Verordnung (EU) 2019/881[11] zugewiesenen Aufgaben mit dem Ziel wahrnimmt, ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union zu erreichen, unter anderem indem sie die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der Union unterstützt. Die ENISA stellt unter anderem Lageeinschätzungsdienste für das Sekretariat des CSIRTs-Netzwerks und von EU-CyCLONe bereit und unterstützt die Mitgliedstaaten durch die regelmäßige Organisation von Cybersicherheitsübungen auf Unionsebene. Im Einklang mit der Richtlinie (EU) 2022/2555 und der Verordnung (EU) 2024/2847[12] erhält die ENISA Informationen über erhebliche grenzüberschreitende Sicherheitsvorfälle und aktiv ausgenutzte Schwachstellen sowie Sicherheitsvorfälle, die sich auf digitale Produkte auswirken.

19. Der Rat der Europäischen Union (im Folgenden „der Rat“) ist gemäß Artikel 16 des Vertrags über die Europäische Union (EUV) das Unionsorgan mit politikgestaltenden und koordinierenden Aufgaben und ist deshalb mit der IPCR betraut, die die Koordinierung und die Reaktion auf der politischen Ebene der Union betrifft. Der Rat arbeitet im Rahmen der Ratsformationen, des Ausschusses der Ständigen Vertreter und der zuständigen Vorbereitungsgremien des Rates, insbesondere der Horizontalen Gruppe „Fragen des Cyberraums“, und, wo relevant, auf der Grundlage der IPCR-Regelung.

---

11 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).

12 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, S. 1).

20. Die Kommission ist als das Organ, das gemäß Artikel 17 des Vertrags über die Europäische Union die allgemeinen Interessen der Union fördert, zu diesem Zweck geeignete Initiativen ergreift und für die Anwendung der Verträge sowie der von den Organen kraft der Verträge erlassenen Maßnahmen sorgt, im Einklang mit dem UCPM-Beschluss für bestimmte allgemeine Vorsorgemaßnahmen auf Unionsebene und bestimmte Maßnahmen zur Lageeinschätzung zuständig, einschließlich der Verwaltung des Zentrums für die Koordination von Notfallmaßnahmen sowie des Gemeinsamen Kommunikations- und Informationssystems für Notfälle. Sie erleichtert auf operativer Ebene die Kohärenz und Koordinierung zwischen verbundenen Reaktionsmaßnahmen auf Unionsebene. Sie wird bei Beschlüssen, die IPCR zu aktivieren oder zu deaktivieren, konsultiert. Die Kommissiondienststellen arbeiten gemeinsam mit dem EAD die ISAA-Berichte aus. Im Fall eines potenziellen oder laufenden Cybersicherheitsvorfalls großen Ausmaßes, der erhebliche Auswirkungen auf unter den Anwendungsbereich der Richtlinie (EU) 2022/2555 fallende Dienste und Tätigkeiten hat oder wahrscheinlich haben wird, ist die Kommission Mitglied im EU-CyCLONe; in anderen Fällen fungiert sie als Beobachter. Sie ist die Kontaktstelle im IICB zu EU-CyCLONe. Sie ist Beobachter im CSIRTs-Netzwerk.

21. Der Hohe Vertreter für Außen- und Sicherheitspolitik (im Folgenden „der Hohe Vertreter“) leitet unterstützt vom EAD die Gemeinsame Außen- und Sicherheitspolitik der Union (GASP) und trägt durch seine Vorschläge zur Festlegung dieser Politik bei, einschließlich der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP). Dazu gehören diplomatische, nachrichtendienstliche und militärische Strukturen und Mechanismen insbesondere das Einheitliche Analyseverfahren (im Folgenden „SIAC“ – Single Intelligence Analysis Capacity) als zentrale Stelle für die Zusammenführung der nachrichtendienstlichen Erkenntnisse der Mitgliedstaaten, der Militärstab der EU (EUMS) als Quelle militärischer Expertise und das EU-Instrumentarium für Cyberdiplomatie sowie das Netz der EU-Delegationen, das aus externer Perspektive zum Krisenmanagement beitragen kann. Der EAD arbeitet außerdem gemeinsam mit den Kommissiondienststellen die ISAA-Berichte aus.

22. In Anhang II sind die Rollen und Zuständigkeiten der einschlägigen Akteure auf Unionsebene in Bezug auf das Cyberkrisenmanagement aufgeführt, einschließlich der wichtigsten Netzwerke und Akteure.

V: Vorsorge für Cybersicherheitsvorfälle großen Ausmaßes und Cyberkrisen

Bedrohungslandschaft

23. Die Mitgliedstaaten und einschlägigen Einrichtungen der Union sollten die notwendigen Maßnahmen ergreifen, um die Lageerfassung zu verbessern, und sich dessen bewusst sein, dass die Bedrohungslandschaft und vorfallspezifische Lageerfassung unterschiedliche Vorgehensweisen benötigen. Die Mitgliedstaaten und die einschlägigen Einrichtungen der Union sollten auf Grundlage verifizierter, zuverlässiger Daten einschließlich Trends bei Sicherheitsvorfällen, Taktiken, Techniken und Verfahren sowie aktiv ausgenutzter Schwachstellen zusammenarbeiten.

24. Beim Informationsaustausch auf EU-Ebene 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.

25. Um die gemeinsame Lageerfassung zu verbessern und die Bewertung der EU-Auswirkungen zu erleichtern, sollten EU-CyCLONe und das CSIRT-Netzwerk mit Unterstützung der ENISA intern vereinbarte Meldemechanismen verwenden, um anhand auf nationaler Ebene gesammelter Informationen einen EU-Überblick über technische und operative Aktivitäten zu erstellen.

26. 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 ihren Mitgliedern und zwischen den Netzwerken schaffen;

    c) die vorhandenen Instrumente für den Informationsaustausch mit Unterstützung der ENISA in vollem Umfang nutzen und prüfen, wie diese Instrumente verbessert werden können und die Interoperabilität zwischen den Netzwerken sichergestellt werden kann.

27. EU-CyCLONe, das CSIRTs-Netzwerk und der IICB sollten zusammenarbeiten, um einen wirksamen Austausch einschlägiger Informationen zu gewährleisten.

28. Die ENISA spielt als Sekretariat des CSIRTs-Netzwerks und von EU-CyCLONe eine zentrale Rolle bei der Unterstützung der Mitgliedstaaten und Organe, Einrichtungen und sonstigen Stellen der Union, um eine gemeinsame Lageerfassung der EU auf technischer und operativer Ebene zu erreichen, mit der die Vorsorge für Cybersicherheitsvorfälle großen Ausmaßes und Cyberkrisen unterstützt wird.

29. In Einklang mit der Richtlinie (EU) 2022/2555 und der Verordnung (EU) 2019/881 sollten sich die Mitgliedstaaten und die einschlägigen Einrichtungen der Union zur Verbesserung der Informationsweitergabe mit dem privaten Sektor, einschließlich Open-Source-Gemeinschaften und Hersteller, abstimmen. Die ENISA sollte in diesem Zusammenhang insbesondere ihr Partnerschaftsprogramm verwenden. Außerdem könnten die Mitgliedstaaten und die einschlägigen Einrichtungen der Union auf den bestehenden Informationsaustausch- und analysezentren (ISACs) auf EU- und nationaler Ebene aufbauen, um die Cybersicherheitskapazitäten auszubauen und auf Cybersicherheitsvorfälle zu reagieren, unter anderem auch durch gemeinsame Treffen des privaten Sektors mit EU- CyCLONe und dem CSIRTs-Netzwerk.

30. Um den Informationsaustausch mit und zwischen den Netzwerken auszubauen sowie die gegenseitigen Erwartungen an diesen Austausch zu präzisieren, sollte EU-CyCLONe mit Unterstützung der ENISA als Sekretariat und nach Konsultation des CSIRTs-Netzwerks sowie der NIS-Kooperationsgruppe innerhalb von 24 Monaten nach der Annahme der vorliegenden Empfehlung eine gemeinsame abgestimmte Taxonomie von Schweregraden für Sicherheitsvorfälle vereinbaren. Diese Taxonomie sollte den Vergleich der Schwere der Sicherheitsvorfälle in den Mitgliedstaaten ermöglichen, indem die Auswirkungen auf die Erbringung von Dienstleistungen, die Anzahl betroffener Einrichtungen und ihre jeweilige Relevanz, die Auswirkungen auf andere Dienste und die Infrastruktur, der finanzielle und politische Schaden sowie der Schaden für den Ruf berücksichtigt werden. Sie sollte auf bestehenden Skalen oder Taxonomien wie der universellen Taxonomie zur Einstufung von Vorfällen aufbauen.

Technische Ebene

31. Das CSIRTs-Netzwerk ist die Plattform für technische Zusammenarbeit und Informationsaustausch zwischen allen Mitgliedstaaten und über CERT-EU mit den Einrichtungen der EU.

32. Im Einklang mit der Richtlinie (EU) 2022/2555 hat jedes CSIRT die Überwachung und Analyse von Cyberbedrohungen, Schwachstellen und Sicherheitsvorfällen auf nationaler Ebene zur Aufgabe. Die CSIRTs sollten relevante Informationen über Sicherheitsvorfälle, Beinahe-Vorfälle, Cyberbedrohungen, Risiken und Schwachstellen sowohl innerhalb des CSIRTs-Netzwerks als auch bilateral austauschen, um eine gemeinsame Lageerfassung zu erreichen.

33. Um die operative Zusammenarbeit auf Unionsebene zu verbessern, sollte das CSIRTs-Netzwerk in Erwägung ziehen, mit Cybersicherheitspolitik befasste Einrichtungen und Agenturen der Union, etwa Europol, zur Teilnahme an seiner Arbeit einzuladen.

34. Im Einklang mit Verordnung 2023/2841 sollte CERT-EU Informationen über Cyberbedrohungen, Schwachstellen und Sicherheitsvorfälle betreffend nicht für Verschlusssachen genutzte IKT-Infrastrukturen verwalten und analysieren und diese Informationen mit den Einrichtungen der Union austauschen und, erforderlichenfalls dem IICB spezifische Vorschläge für Leitlinien und Empfehlungen für die Organe, Einrichtungen und sonstigen Stellen der Union vorlegen. CERT-EU sollte mit seinen Pendants in den Mitgliedstaaten zusammenarbeiten und Informationen austauschen, auch über das CSIRTs-Netzwerk.

Operative Ebene

35. Im Einklang mit der Richtlinie (EU) 2022/2555 sollte EU-CyCLONe als Plattform für die Zusammenarbeit zwischen den Behörden der Mitgliedstaaten für das Cyberkrisenmanagement und – über die Kommission – mit den einschlägigen Einrichtungen der Union dienen, mit dem Ziel, die Vorsorge im Hinblick auf das Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen zu verbessern und eine gemeinsame Lageerfassung für Cybersicherheitsvorfälle großen Ausmaßes und Krisen zu entwickeln.

36. Im Einklang mit der Richtlinie (EU) 2022/2555 und der Verordnung (EU) 2024/2847 erhält die ENISA Informationen über erhebliche grenzüberschreitende Sicherheitsvorfälle und aktiv ausgenutzte Schwachstellen sowie Sicherheitsvorfälle, die sich auf digitale Produkte auswirken. Als Sekretariat sollte ENISA das CSIRTs-Netzwerk und EU-CyCLONe beraten, um die Netzwerke bei der Feststellung zu unterstützen, ob weitere Maßnahmen ergriffen werden sollten, und zur gemeinsamen Lageerfassung beizutragen.

Politische Ebene

37. Die Mitgliedstaaten und die einschlägigen Einrichtungen der Union sollten internationale Entwicklungen verfolgen, die die Cybersicherheit betreffen (darunter Cyberbedrohungen, hybride Bedrohungen sowie Informationsmanipulation und Einflussnahme aus dem Ausland, einschließlich gegebenenfalls Desinformation). Initiativen wie die gemeinsamen technischen EU-Cybersicherheitslageberichte (JCAR), Analysen des SIAC und andere einschlägige Produkte, die spezielle Erkenntnisse bieten, sollten berücksichtigt werden.

38. Der Hohe Vertreter sollte die Mitgliedstaaten weiterhin informieren und in die diplomatischen Bemühungen der Union im Zusammenhang mit Cyberbedrohungen, insbesondere solchen mit Beteiligung staatlicher Akteure, in die Zusammenarbeit der Union mit Drittländern und internationalen Organisationen, darunter der NATO, und in die Umsetzung diplomatischer Maßnahmen, einschließlich restriktiver Maßnahmen, einbeziehen.

39. Der Vorsitz des Rates der Europäischen Union kann auf der IPCR-Internet-Plattform eine Beobachtungswebsite einrichten, auf der die Mitgliedstaaten und die Organe und Einrichtungen der EU Informationen über eine möglicherweise entstehende Krise austauschen können.

Gemeinsame Übungen

40. In Abstimmung mit dem Hohen Vertreter und unterstützt von der ENISA sollte die Kommission nach Konsultation von EU-CyCLONe und des CSIRTs-Netzwerks ein effizientes jährliches fortlaufendes Cyberübungsprogramm zusammenstellen, um sich auf Cyberkrisen vorzubereiten und die organisatorische Effizienz zu steigern. Das fortlaufende Cyberübungsprogramm sollte den Übungen des UPCM und anderen Übungen der Krisenreaktionsmechanismen auf Unionsebene, einschließlich der im EU-Konzeptentwurf für kritische Infrastrukturen beschriebenen Übung, Rechnung tragen. Das erste fortlaufende Programm sollte innerhalb von zwölf Monaten nach der Annahme des Cyber-Konzeptentwurfs ausgearbeitet werden; die nachfolgenden Programme sind bis zum 31. März jeden Jahres fertigzustellen. Das fortlaufende Programm sollte dem Rat zur Information übermittelt werden.

41. Das fortlaufende Programm sollte sich auch auf Übungen erstrecken, die unter Verwendung der Szenarien der EU-weit koordinierten Risikobewertungen entwickelt wurden. Es sollte sich auf Übungen erstrecken, bei denen alle einschlägigen Akteure einbezogen werden, insbesondere der Privatsektor und die NATO.

42. In ihrer Rolle als Sekretariat des CSIRTs-Netzwerks und von EU-CyCLONe sollte die ENISA für die systematische Erfassung der aus den Übungen gewonnenen Erkenntnisse sowie für die Bestimmung von daraus resultierenden Maßnahmen und für Vorschläge für deren Umsetzung sorgen, um so die wirksame Ausführung und die positiven Auswirkungen dieser Maßnahmen auf die gemeinsame Resilienz der EU, einschließlich entsprechender Standardarbeitsverfahren, zu gewährleisten.

43. Alle Akteure und Netze sollten die Koordinierung im Falle eines Cybersicherheitsvorfall großen Ausmaßes oder einer Cyberkrise auf der Grundlage der aus den Übungen gewonnenen Erkenntnisse verbessern. Insbesondere EU-CyCLONe und das CSIRTs-Netzwerk sollten die im Laufe der Übungen festgestellten Herausforderungen angehen, um die Koordinierung zu verbessern – vor allem jene Herausforderungen, die die Zusammenarbeit zwischen den Netzen betreffen –, und, falls erforderlich, die Standardarbeitsverfahren zügig anpassen.

44. Die NIS-Kooperationsgruppe sollte das CSIRTs-Netzwerk, EU-CyCLONe und die ENISA ersuchen, die aus den Übungen gewonnenen Erkenntnisse sowie die Bestimmung von daraus resultierenden Maßnahmen und Vorschläge für deren Umsetzung vorzulegen.

45. Der Rat kann die Vorsitze des CSIRTs-Netzwerks, von EU-CyCLONe, der NIS-Kooperationsgruppe und der ENISA ersuchen, darzulegen, wie die aus den Übungen gewonnenen Erkenntnisse umgesetzt wurden.

46. Die ENISA wird ersucht, in Zusammenarbeit mit der Kommission und dem Hohen Vertreter eine Übung zum Testen des Cyber-Konzeptentwurfs während der nächsten „CyberEurope"-Übung zu organisieren. An der Übung sollten alle einschlägigen Akteure, auch die politische Ebene, beteiligt werden. Die ENISA wird ersucht, die Beteiligung der politischen Ebene mit dem Vorsitz des Rates der Europäischen Union abzustimmen. Auch der Privatsektor und die NATO können in die Übung einbezogen werden.

VI: Erkennung von Vorfällen, die sich zu einem Cybersicherheitsvorfall großen Ausmaßes oder zu einer Cyberkrise ausweiten könnten

47. Alle Akteure sollten im Rahmen ihres jeweiligen Auftrags und nach dem gefahrenübergreifenden Ansatz Informationen übermitteln, die auf einen potenziellen Cybersicherheitsvorfall großen Ausmaßes oder eine potenzielle Cyberkrise in den betreffenden Netzen hindeuten.

48. Wenn die grenzübergreifenden Cyber-Hubs Informationen über einen potenziellen oder laufenden Cybersicherheitsvorfall großen Ausmaßes erhalten, sollten sie im Einklang mit der Verordnung (EU) 2025/38[13] zu Zwecken der gemeinsamen Lageerfassung sicherstellen, dass den Behörden der Mitgliedstaaten und der Kommission über EU-CyCLONe und das CSIRTs-Netzwerk unverzüglich relevante Informationen übermittelt werden.

---

13 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 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).

49. Wird ein erheblicher Sicherheitsvorfall beobachtet, so kann dieser –vor allem wenn er unmittelbare Auswirkungen hat – einem CSIRT und auch den für das Cyberkrisenmanagement zuständigen Behörden der Mitgliedstaaten oder anderen sektoralen Behörden gemeldet oder von diesen erkannt werden. Die Mitgliedstaaten sind aufgefordert, Informationen zu diesen Vorfällen in den Netzen weiterzugeben; diese sollten geeignete Maßnahmen in Betracht ziehen. Die Aktivierung des CSIRTs-Netzwerks und von EU-CyCLONe kann unabhängig voneinander erfolgen, je nach Art des Vorfalls und der erforderlichen Reaktion. Jedoch sind beide Netze aufgefordert, die gegenseitige Zusammenarbeit auf der Grundlage der vereinbarten Verfahrensmodalitäten fortzusetzen. Der Beschluss über die Aktivierung liegt einzig und allein bei dem jeweiligen Netz.

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

51. Wie in der Richtlinie (EU) 2022/2555 angegeben, sollten sich das CSIRTs-Netzwerk und EU-CyCLONe unverzüglich auf Verfahrensmodalitäten für potenzielle oder laufende Cybersicherheitsvorfälle großen Ausmaßes einigen, um eine technisch-operative Koordinierung und eine zeitnahe und aussagekräftige Unterrichtung der politischen Ebene sicherzustellen.

VII: Reaktion auf einen Cybersicherheitsvorfall großen Ausmaßes oder eine Cyberkrise auf Unionsebene

Reaktion auf einen Cybersicherheitsvorfall großen Ausmaßes oder eine Cyberkrise, für den bzw. die die IPCR sich nicht im Modus der vollständigen Aktivierung befindet

52. Eine wirksame Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes oder auf Cyberkrisen auf EU-Ebene hängt von der wirksamen technischen, operativen und politischen Zusammenarbeit mit einem ressortübergreifenden Ansatz ab und schließt nach Möglichkeit auch die Strafverfolgung ein.

53. Auf jeder Ebene sollten die beteiligten Akteure bestimmte Tätigkeiten ausführen, um eine gemeinsame Lageerfassung und eine koordinierte Reaktion zu erreichen. Diese Maßnahmen gewährleisten eine ordnungsgemäße und wirksame Weitergabe von Informationen.

54. Die Reaktion sollte in einem angemessenen Verhältnis zu den Auswirkungen eines Cybersicherheitsvorfalls großen Ausmaßes oder einer Cyberkrise stehen. Im Einklang mit der Richtlinie (EU) 2022/2555 sollten die für das Cyberkrisenmanagement zuständigen Behörden der Mitgliedstaaten die nationale Kohärenz und Koordinierung zwischen den sektoralen Reaktionen auf die Cyberkrise sicherstellen.

55. Im Falle eines Cybersicherheitsvorfalls großen Ausmaßes oder einer Cyberkrise sollten alle Akteure und Netze in enger Zusammenarbeit wie folgt reagieren:

a) Auf technischer Ebene:

i. Die betroffenen Mitgliedstaaten und ihre CSIRTs sollten mit den betroffenen Einrichtungen zusammenarbeiten, um auf Sicherheitsvorfälle zu reagieren und gegebenenfalls Unterstützung zu leisten.

ii. Die CSIRTs sollten über das CSIRTs-Netzwerk zusammenarbeiten, um relevante technische Informationen über den Sicherheitsvorfall weiterzugeben. Die CSIRTs arbeiten bei der Analyse der verfügbaren forensischen Artefakte und anderer technischer Informationen im Zusammenhang mit dem Sicherheitsvorfall zusammen, um die Ursache festzustellen und mögliche Eindämmungsmaßnahmen zu identifizieren.

iii. Erlangt ein CSIRT oder eine für das Cyberkrisenmanagement zuständige Behörde eines Mitgliedstaats Kenntnis von einem erheblichen Sicherheitsvorfall, so ist es bzw. sie aufgefordert, dies innerhalb des CSIRTs-Netzwerks oder von EU-CyCLONe mitzuteilen.

iv. Das CSIRTs-Netzwerk sollte mit Unterstützung der ENISA eine Synthese der von den CSIRTs vorgelegten nationalen Berichte erstellen, die EU-CyCLONe vorgelegt werden sollte.

v. Hat ein Cybersicherheitsvorfall das Potenzial, sich zu einem Cybersicherheitsvorfall großen Ausmaßes oder zu einer Cyberkrise auszuweiten, so sollte das CSIRTs-Netzwerk geeignete Information an das EU-CyCLONe übermitteln. EU-CyCLONe sollte diese Informationen dazu verwenden, den Rat zu unterrichten.

vi. Das CSIRTs-Netzwerk sollte in engem Kontakt mit Europol stehen, um den Austausch relevanter technischer Informationen sicherzustellen. Das CSIRTs-Netzwerk und Europol sollten Kontaktstellen einrichten, um den Informationsaustausch auszubauen, wenn dies im Falle eines Cybersicherheitsvorfall großen Ausmaßes erforderlich sein sollte.

b) Auf operativer Ebene:

i. Die Mitgliedstaaten sollten die Auswirkungen des Sicherheitsvorfalls auf nationaler Ebene eindämmen, indem sie geeignete Maßnahmen ergreifen.

ii. Das CSIRTs-Netzwerk sollte für EU-CyCLONe technische Bewertungen des laufenden Sicherheitsvorfalls bereitstellen, die von EU-CyCLONe verwendet werden können.

iii. EU-CyCLONe sollte die Folgen und Auswirkungen einschlägiger Cybersicherheitsvorfälle großen Ausmaßes und von Cyberkrisen bewerten und mögliche Eindämmungsmaßnahmen vorschlagen; außerdem sollte es das koordinierte Management von Cybersicherheitsvorfällen großen Ausmaßes und von Cyberkrisen sowie die Beschlussfassung auf politischer Ebene unterstützen.

iv. Sollte ein Cybersicherheitsvorfall großen Ausmaßes mit sektorübergreifenden Auswirkungen die Aktivierung von Reaktionsmaßnahmen auf Unionsebene, insbesondere von in Anhang II aufgeführten einschlägigen horizontalen und sektoralen Krisenmanagementmechanismen, erfordern,

(a) so können die geeigneten Akteure je nach Art des Krisenmanagementmechanismus auf Unionsebene die Aktivierung des besagten Mechanismus fordern.

(b) Im Falle der Aktivierung eines solchen sektoralen Mechanismus unterstützen die einschlägigen Einrichtungen die sektoralen Einrichtungen bei der Eindämmung der Auswirkungen des Sicherheitsvorfalls.

(c) Die Kommission sollte 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; ferner sollte sie eine integrierte sektorübergreifende Analyse durchführen und Optionen für einen geeigneten integrierten Reaktionsplan vorschlagen.

(d) In Zusammenarbeit mit dem Hohen Vertreter sollte die Kommission, gegebenenfalls durch EU-CyCLONe, für Kohärenz und Koordinierung der operativen Maßnahmen im Cyberbereich auf EU-Ebene mit den damit verbundenen Reaktionsmaßnahmen auf Unionsebene sorgen, insbesondere in Bezug auf Amtshilfeersuchen über das UCPM.

(e) Wurde eine IPCR-Beobachtungswebsite eingerichtet, so sollten Informationen über den Sicherheitsvorfall, seine Auswirkungen und die ergriffenen Maßnahmen ebenfalls über die IPCR-Internet-Plattform zwischen den Mitgliedstaaten und den Einrichtungen der Union weitergegeben werden.

v. Die Mitgliedstaaten können im Einklang mit Artikel 15 der Verordnung (EU) 2025/38 Dienste der EU-Cybersicherheitsreserve beantragen. Unbeschadet künftiger Durchführungsrechtsakte im Rahmen der Verordnung sollten die Dienste der EU-Cybersicherheitsreserve innerhalb von 24 Stunden nach der Beantragung bereitgestellt werden.

c) Auf politischer Ebene:

i. Der Rat kann von den wichtigsten Interessenträgern, insbesondere der Kommission, dem Hohen Vertreter und EU-CyCLONe, Briefings verlangen, um eine angemessene politische und strategische Reaktion durchzuführen.

ii. Mit Unterstützung der Kommission und des Hohen Vertreters könnte der Rat die geeigneten Maßnahmen beschließen, um auf den Cybersicherheitsvorfall großen Ausmaßes zu reagieren; dazu zählen auch die möglichen diplomatischen Reaktionen gemäß Kapitel IX.

iii. Je nach Art und Auswirkungen des Sicherheitsvorfalls können die Mitgliedstaaten zusätzliche Mechanismen oder Instrumente des Cyberkrisenmanagements aktivieren.

iv. Wird die IPCR im Informationsaustausch-Modus aktiviert, so wird die ISAA-Unterstützungsfähigkeit ausgelöst; dadurch wird der Informationsaustausch über die IPCR-Internet-Plattform intensiviert und ein gemeinsamer Lageüberblick gewährleistet. Die Lageberichte von EU-CyCLONe und dem CSIRTs Netzwerk sollten die Hauptinstrumente bleiben, um die gemeinsame Lageerfassung auf der operativen bzw. der technischen Ebene dazulegen. Diese Berichte können in die ISAA-Berichte einfließen.

v. Im Falle eines Sicherheitsvorfalls, der die Aktivierung von Reaktionsmaßnahmen auf Unionsebene, insbesondere von in Anhang II aufgeführten einschlägigen horizontalen und sektoralen Krisenmanagementmechanismen, erfordert, sollte der Rat in Zusammenarbeit mit der Kommission und dem Hohen Vertreter für Kohärenz und Koordinierung zwischen den Reaktionen auf die Cyberkrise und den damit verbundenen Reaktionsmaßnahmen auf Unionsebene sorgen.

vi. Werden einschlägige Mechanismen, insbesondere die Dienste der Cybersicherheitsreserve, beantragt, sollten die Kommissionsdienststellen und gegebenenfalls der EAD sowie die einschlägigen Ratsgremien, insbesondere die Horizontale Gruppe „Fragen des Cyberraums“ beziehungsweise die Horizontale Gruppe „Stärkung der Resilienz und Abwehr hybrider Bedrohungen“ (HWP ERCHT), sich darüber abstimmen, was die Ausgestaltung und die Umsetzung von Maßnahmen sowie das geeignete Beschlussfassungsverfahren für zusätzliche Maßnahmen im Einklang mit dem Instrumentarium zur Abwehr hybrider Bedrohungen[14] betrifft, falls es sich um böswillige Cyberaktivitäten handelt, die Teil einer umfassenderen hybriden Kampagne sind.

Reaktion auf einen Cybersicherheitsvorfall großen Ausmaßes oder eine Cyberkrise, für den bzw. die die IPCR sich im Modus der vollständigen Aktivierung befindet

56. Die im obigen Abschnitt *„Reaktion auf einen Cybersicherheitsvorfall großen Ausmaßes oder eine Cyberkrise, für den bzw. die die IPCR sich nicht im Modus der vollständigen Aktivierung befindet“* aufgeführten Schritte sollten durchgeführt werden.

57. Befindet sich die IPCR im Modus der vollständigen Aktivierung, dienen die ISAA-Berichte der Gewährleistung einer gemeinsamen Lageerfassung auf politischer Ebene. Die Lageberichte von EU-CyCLONe und dem CSIRTs Netzwerk sollten die Hauptinstrumente bleiben, um die gemeinsame Lageerfassung auf der operativen bzw. der technischen Ebene dazulegen. Diese Berichte können in die ISAA-Berichte einfließen.

58. Im Falle eines Cybersicherheitsvorfalls großen Ausmaßes oder einer Cyberkrise, der bzw. die zur Aktivierung der IPCR im Modus der vollständigen Aktivierung führt, sollten alle Akteure in enger Abstimmung im Rahmen eines ressortübergreifenden Ansatzes wie folgt reagieren:

a) Die Koordinierung der Reaktion auf politischer Ebene der Union erfolgt durch den Rat unter Nutzung der IPCR-Regelung.

---

14 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.

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 einen Beitrag zu den ISAA-Berichten leisten.

c) Zusätzlich zur ISAA-Fähigkeit würde der Vorsitz des Rates der Europäischen Union IPCR-Rundtischsitzungen einberufen, um die politische und strategische Koordinierung der EU-Reaktion zu ermöglichen, wobei die Maßnahmen gemäß dem Cyber-Konzeptentwurf und die Arbeit einschlägiger sektoraler Mechanismen in die Arbeit im Rahmen der IPCR einfließen. Bei den Rundtischsitzungen können darüber hinaus einige spezifische Lücken in der Reaktion ermittelt werden, und spezifische EU-Akteure können aufgefordert werden, diese Lücken anzugehen und bei künftigen Rundtischsitzungen Bericht zu erstatten, um die politische und strategische Koordinierung im Rahmen der IPCR zu unterstützen.

d) Der Vorsitz des Rates der Europäischen Union sollte in Erwägung ziehen, EU-CyCLONe zu einschlägigen Sitzungen, einschließlich Rundtischsitzungen im Rahmen der IPCR-Regelung, und zu anderen einschlägigen Tagungen des Rates einzuladen.

e) Die für das Cyberkrisenmanagement zuständigen Behörden der Mitgliedstaaten sollten für Kohärenz und Koordinierung zwischen den sektoralen Reaktionen auf die Cyberkrise, die von den Behörden für das Cyberkrisenmanagement unterstützt werden, sorgen.

f) Die möglichen diplomatischen Reaktionen sollten gemäß Kapitel IX in Erwägung gezogen und durchgeführt werden.

VIII: Öffentlichkeitsarbeit

59. Die Kommunikation über einen laufenden Cybersicherheitsvorfall großen Ausmaßes oder eine Cyberkrise an die Bevölkerung eines einzelnen Mitgliedstaats, auch als Teil der Sensibilisierung, fällt zwar in die nationale Zuständigkeit, jedoch sollte es Ziel der Mitgliedstaaten, der Kommission und des Hohen Vertreters sein, ihre öffentliche Kommunikation weitestgehend aufeinander abzustimmen. Das informelle IPCR-Krisenkommunikationsnetz kann gegebenenfalls einbezogen werden.

60. Zur Vorbereitung auf Cybersicherheitsvorfälle großen Ausmaßes und Cyberkrisen werden die Mitgliedstaaten und gegebenenfalls die Kommission und CERT-EU ersucht, sich über ihre Öffentlichkeitsarbeit innerhalb von EU-CyCLONe und des CSIRTs-Netzwerks auszutauschen, auch über bewährte Verfahren wie Ratgeber oder Sensibilisierungskampagnen. Die ENISA sollte Instrumente zur Unterstützung dieses Austauschs und zur Sicherstellung eines einfachen Zugangs bereitstellen.

61. Die Mitgliedstaaten werden im Falle eines Cybersicherheitsvorfalls großen Ausmaßes oder einer Cyberkrise ersucht, über EU-CyCLONe Informationen über ihre Öffentlichkeitsarbeit weiterzugeben, um eine gemeinsame Sensibilisierung zu schaffen und die Maßnahmen zu koordinieren. EU-CyCLONe kann auf eigene Initiative oder auf Antrag des Rates einen Überblick über diese Ansätze an den Rat übermitteln.

IX: Diplomatische Reaktion und Zusammenarbeit mit strategischen Partnern

62. Der Hohe Vertreter sollte in enger Zusammenarbeit mit der Kommission und anderen einschlägigen Einrichtungen der Union

a) die Beschlussfassung im Rat über mögliche Maßnahmen im Rahmen des EU-Instrumentariums für die Cyberdiplomatie, unter anderem durch Analysen, Berichte und Vorschläge, unterstützen. Dadurch wird die Nutzung des gesamten verfügbaren Spektrums der Unionsinstrumente zur Vorbeugung, Abschreckung und Reaktion im Hinblick auf böswillige Cyberaktivitäten ermöglicht und somit die Cyberabwehr der Union gestärkt sowie weltweit Frieden, Sicherheit und Stabilität im Cyberraum gefördert;

b) bei Feststellung eines relevanten Sicherheitsvorfalls den Fluss der erforderlichen Informationen mit strategischen Partnern, gegebenenfalls auch mit der NATO, erleichtern;

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

63. Die Mitgliedstaaten, der Hohe Vertreter, 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.

64. Die Zusammenarbeit zwischen der Europäischen Union und der NATO sollte im Einklang mit den vereinbarten Leitgrundsätzen der Inklusivität, der Gegenseitigkeit und der Transparenz sowie unter vollständiger Achtung der Entscheidungsautonomie der Union erfolgen.

65. Die Kommission und der Hohe Vertreter sollten unter Berücksichtigung bestehender Vereinbarungen wie der technischen Vereinbarung CERT-EU/NATO von 2016 Kontaktstellen für die Koordinierung mit der NATO im Falle einer Cyberkrise einrichten, damit benötigte Informationen über die Lage und die Nutzung der Krisenreaktionsmechanismen ausgetauscht werden können, um dadurch die Zusammenarbeit im Hinblick auf die Reaktion zu verbessern und die Wirksamkeit der Reaktion zu erhöhen. Zu diesem Zweck sollte die Union prüfen, wie der Informationsaustausch mit der NATO auf inklusive, wechselseitige und nichtdiskriminierende Weise verbessert werden kann, insbesondere indem dafür gesorgt wird, dass Instrumente für eine sichere Kommunikation vorhanden sind; dabei sind die Standards für den Informationsaustausch der verschiedenen Mitgliedstaaten zu berücksichtigen.

66. Als Teil des in Kapitel V genannten fortlaufenden Cyberübungsprogramms sollten die Kommissionsdienststellen und der EAD erwägen, eine Übung auf Mitarbeiterebene mit der NATO zu organisieren, um die Zusammenarbeit zwischen zivilen und militärischen Einrichtungen im Falle eines Cybersicherheitsvorfalls großen Ausmaßes oder einer Cyberkrise zu testen, in dessen bzw. deren Verlauf die Mitgliedstaaten oder die NATO-Bündnispartner Lösungen für einen Cyberangriff auf ihre Sicherheit suchen. Die Übung sollte auf inklusive und nichtdiskriminierende Weise und unter vollständiger Achtung der vereinbarten Grundsätze für die Parameter der Zusammenarbeit zwischen der EU und der NATO durchgeführt werden. Die Übung sollte im Rahmen der Übung „EU Integrated Resolve“ (parallele und koordinierte Übung – PACE) durchgeführt werden. Es sollten alle erforderlichen Maßnahmen ergriffen werden, um die Teilnahme aller im Cyber-Konzeptentwurf genannten Akteure sicherzustellen.

67. Gemeinsame Cyberübungen auf Unionsebene mit den Ländern des westlichen Balkans, der Republik Moldau, der Ukraine sowie anderen strategischer Partnern und gleichgesinnten Drittländern sollten ebenfalls erwogen werden, in Absprache mit dem Rat, der Kommission und dem Hohen Vertreter.

X. Koordinierung des Cyberkrisenmanagements mit militärischen Akteuren auf EU-Ebene

68. Die Mitgliedstaaten sollten weiterhin die Zusammenarbeit zwischen zivilen und militärischen Cyberakteuren auf nationaler Ebene stärken.

69. EU-CyCLONe und das CSIRTs Netzwerk sollten mögliche Arten und Verfahren für die Zusammenarbeit mit den einschlägigen militärischen Akteuren der EU, wie der EU-Konferenz der Cyberkommandeure und dem Operativen Netz für die militärischen IT-Notfallteams (MICNET), ermitteln, um die Vorteile einer gemeinsamen militärischen und zivilen Perspektive zu nutzen, insbesondere durch gemeinsame Treffen. EU-CyCLONe und das CSIRTs Netzwerk sollten den Rat über die Fortschritte bezüglich dieser Zusammenarbeit informieren.

70. Der betroffene Mitgliedstaat wird ersucht, EU-CyCLONe und den EAD zu informieren, wenn einschlägige nationale oder multinationale militärische Reaktionsfähigkeiten im Zusammenhang mit einem Cybersicherheitsvorfall großen Ausmaßes oder einer Cyberkrise genutzt werden und zwischen dem Nutzer und dem Anbieter dieser Reaktionsfähigkeit gegenseitiges Einvernehmen über die Bereitstellung dieser Informationen besteht.

71. Als Teil des in Kapitel V genannten fortlaufenden Cyberübungsprogramms sollten die Kommission und der Hohe Vertreter erwägen, eine gemeinsame Übung zu organisieren, um die Zusammenarbeit zwischen zivilen und militärischen Cyberakteuren im Falle eines Cybersicherheitsvorfalls großen Ausmaßes oder einer Cyberkrise, der bzw. die Mitgliedstaaten betrifft, zu testen.

XI: Wiederherstellung und gewonnene Erkenntnisse nach einer Cyberkrise

72. Die Mitgliedstaaten, die einschlägigen Einrichtungen der Union und die Netze sollten während der Wiederherstellungsphase zusammenarbeiten, um für eine rasche Wiederherstellung der Kernfunktionen zu sorgen. Der Strafverfolgungsbehörden sollte ebenfalls, sofern relevant, in diese Zusammenarbeit eingebunden werden. In dieser Phase ist die Zusammenarbeit mit dem Privatsektor entscheidend, insbesondere für die Ermöglichung der Wiederherstellung von Daten und Systemen. Bei der wirksamen Abstimmung unter den Interessenträgern sollte die Priorität darauf liegen, die Störungen auf ein Mindestmaß zu reduzieren und für die Aufrechterhaltung des Betriebs zu sorgen.

73. Die Mitgliedstaaten, die einschlägigen Einrichtungen der Union und die Netze sollten in der Wiederherstellungsphase zusammenarbeiten und sich dabei auf aus Cyberkrisen oder bewältigten Cybersicherheitsvorfällen in der Vergangenheit gewonnene Erkenntnisse sowie auf Berichte über Sicherheitsvorfälle stützen, und zwar insbesondere im Rahmen des mit der Verordnung (EU) 2025/38 eingerichteten Europäischen Überprüfungsmechanismus für Cybersicherheitsvorfälle.

74. EU-CyCLONe sollte für das CSIRTs-Netzwerk, die NIS-Kooperationsgruppe und den Rat eine umfassende Liste von aus Cyberkrisen oder bewältigten Cybersicherheitsvorfällen in der Vergangenheit gewonnenen Erkenntnissen und von bewährten Verfahren bereitstellen. Die ENISA sollte sicherstellen, dass diese gewonnenen Erkenntnisse effektiv in künftige Vorsorgemaßnahmen und in die Planungen künftiger Übungen einfließen.

XII: Sichere Kommunikation

75. Ausgehend von der Bestandsaufnahme der vorhandenen sicheren Kommunikationsinstrumente[15] sollte die Kommission bis Ende 2026 eine interoperable Reihe sicherer Kommunikationslösungen vorschlagen. Der Rat, die Kommission, der Hohe Vertreter, EU-CyCLONe und das CSIRTs-Netzwerk sollten sich bis Ende 2027 auf diese Reihe verständigen. Diese Lösungen sollten von den Maßnahmen im Bereich der sicheren Kommunikation profitieren, die die EU-Organe im Rahmen der EU-Strategie für eine krisenfeste Union ergreifen könnten, und sollten das gesamte Spektrum der erforderlichen Kommunikationsarten abdecken (Sprache, Daten, Video- und Telekonferenzen, Nachrichtenübermittlung, Zusammenarbeit sowie Weitergabe und Konsultation von Dokumenten). Die Lösungen sollten gemeinsam festgelegte Anforderungen an den Schutz von nicht als vertraulich eingestuften sensiblen Informationen erfüllen. Es sollten Lösungen verwendet werden, die auf einem offenen Protokoll mit Implementierungen von Open-Source-Software, die für Echtzeitkommunikation geeignet sind, beruhen und von einer in der EU ansässigen Einrichtung verwaltet werden.

76. Für den Zweck des Austauschs von Informationen, die als RESTREINT UE/EU RESTRICTED eingestuft sind, sollten EU-CyCLONe und das CSIRTs-Netzwerk bei Bedarf sichere Kommunikationskanäle verwenden können, die für die Organe, Einrichtungen und sonstigen Stellen der EU den Austausch von Verschlusssachen untereinander und mit den Mitgliedstaaten erlauben.

---

15 Dok. WK 862/2023.

77. Das durch die Verordnung (EU) 2021/887[16] 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 sicherer Kommunikationsinstrumente zu unterstützen. Jegliche Doppelung von Investitionen in interoperable gesicherte Systeme ist zu vermeiden.

78. 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.

79. Es sollten – vor allem auf technischer Ebene – Mechanismen für die Kommunikation und den Informationsaustausch zwischen Strafverfolgungs- und Cybersicherheitsnetzen eingerichtet werden, um eine wirksame Reaktion auf eine Cyberkrise zu ermöglichen. Diese Mechanismen sollten die Rolle der einzelnen Beteiligten beachten, nicht in laufende Operationen eingreifen und die Redundanz der Kommunikation gewährleisten. Dem Europäischen System für kritische Kommunikation , das sich zur Zeit in der Entwicklung befindet, würde ein gemeinsames Vorgehen mit einschlägigen Cybergemeinschaften zugutekommen.

XIII: Schlussbestimmungen

80. EU-CyCLONe sollte in Zusammenarbeit mit dem CSIRTs-Netzwerk und anderen wichtigen Akteuren im Ökosystem der EU für das Cyberkrisenmanagement und mit Unterstützung der ENISA innerhalb eines Jahres nach der Veröffentlichung dieser Empfehlung detaillierte Ablaufdiagramme entwickeln, in denen die Informationsflüsse zwischen den einschlägigen Akteuren, Beschlussfassungsverfahren und Berichten aufgezeigt werden, die während des Managements eines Cybersicherheitsvorfalls großen Ausmaßes oder einer Cyberkrise, wie in dieser Empfehlung beschrieben, entwickelt wurden. Die Ablaufdiagramme sollten verschiedene Arten und Schichten der Zusammenarbeit abdecken. Sie sind erforderlichenfalls zu aktualisieren.

---

16 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).

81. Zur Unterstützung der wirksamen Anwendung des überarbeiteten Cyber-Konzeptentwurfs und aufbauend auf der Erfahrung, die durch die in dessen Rahmen durchgeführten gemeinsamen Cyberübungen gewonnen wurde, kann der Rat bei Bedarf eine Reihe von Umsetzungsleitlinien entwickeln. Mit diesen Leitlinien könnten die praktischen Herausforderungen angegangen werden, die im Laufe der Übungen ermittelt wurden, und die festgestellten Lücken und fehlenden Verbindungen bei der Koordinierung, Kommunikation und operativen Interaktion geschlossen werden.

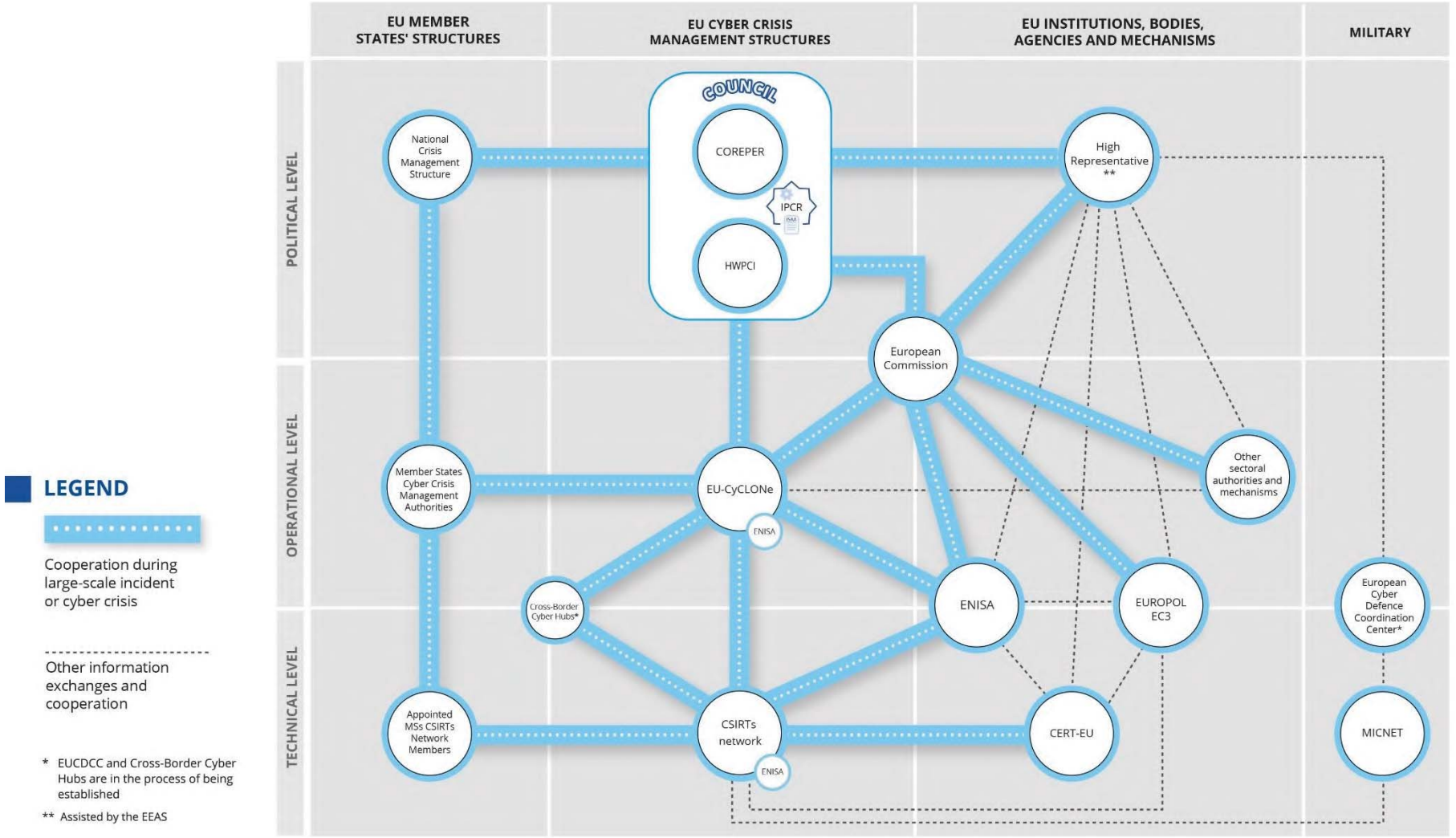
82. Diese Empfehlung sollte von der Kommission in Zusammenarbeit mit den Mitgliedstaaten mindestens alle vier Jahr nach ihrer Veröffentlichung überprüft werden. Nach jeder Überprüfung sollte die Kommission einen Bericht veröffentlichen und dem Rat vorlegen. Die Kommission und die Mitgliedstaaten sollten die Auswirkungen der sich ändernden Bedrohungslandschaft, die Ergebnisse gemeinsamer Übungen und Änderungen der Gesetzgebung berücksichtigen – insbesondere mögliche Änderungen, die sich aus der Überarbeitung der Verordnung (EU) 2019/881 ergeben.

Geschehen zu Brüssel am

Im Namen des Rates

Der Präsident/Die Präsidentin

ANHANG I – Konzeptentwurf der Union für das Cybersicherheitskrisenmanagement



ANHANG II – EINSCHLÄGIGE AKTEURE AUF UNIONSEBENE (EINRICHTUNGEN UND NETZE) UND KRISENMANAGEMENTMECHANISMEN

(1) Einbeziehung der Hauptakteure während des gesamten Lebenszyklus des Cyberkrisenmanagements (Cybersicherheitsvorfälle großen Ausmaßes und Cyberkrisen)

	Krisenvorsorge	Erkennung	Reaktion auf einen Cybersicherheitsvorfall großen Ausmaßes oder eine Cyberkrise				öffentliche Kommunikation	Wiederherstellung und gewonnene Erkenntnisse
			auf technischer Ebene	auf operativer Ebene	auf politischer Ebene			
Mitgliedstaaten	X	X	X	X	X		X	X
Kommission	X			X	X		X	
Hoher Vertreter mit Unterstützung des EAD	X			X	X		X	
Rat	X				X		X	X
ENISA	X		X	X				
CERT-EU	X	X	X	X			X	X
CSIRTs-Netzwerk	X	X	X					X
EU-CyCLONe	X			X	X			X

(2) Rollen und Zuständigkeiten der einschlägigen Akteure und Mechanismen auf Unionsebene (in alphabetischer Reihenfolge) in Bezug auf das Cyberkrisenmanagement

Akteur	**Ebene/ Stufe**	**Rolle und Zuständigkeit**	**Verweis**
CERT-EU	Technisch / Operativ	Koordiniert die Krisenreaktion auf technischer Ebene und die Bewältigung schwerwiegender Sicherheitsvorfälle, die Einrichtungen der Union betreffen. Führt ein Verzeichnis der verfügbaren technischen Fachkenntnisse, die für die Reaktion auf solche schwerwiegenden Sicherheitsvorfälle notwendig sind, und unterstützt den IICB bei der Koordinierung der Cyberkrisenmanagementpläne der Einrichtungen der Union für schwerwiegende Sicherheitsvorfälle. Mitglied des CSIRTs-Netzwerks. Unterstützt die Kommission in EU-CyCLONe beim koordinierten Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen. Handelt als zentrale Stelle für den Austausch von Informationen zur Cybersicherheit und die Koordinierung der Reaktion auf Sicherheitsvorfälle und erleichtert den Austausch von Informationen über Sicherheitsvorfälle, Cyberbedrohungen, Schwachstellen und	Verordnung (EU, Euratom) 2023/2841 Verordnung (EU) 2025/38

Akteur	Ebene/ Stufe	Rolle und Zuständigkeit	Verweis
		Beinahe-Vorfälle zwischen Einrichtungen der Union und deren Pendants. Beantragt den Einsatz der EU-Cybersicherheitsreserve im Namen von Einrichtungen der Union. Arbeitet mit dem NATO-Cybersicherheitszentrum auf der Grundlage des betreffenden technischen NATO-Übereinkommens zusammen.	
Rat der Europäischen Union	Politisch	Aufgaben der Festlegung der Politik und der Koordinierung. Ist mit der IPCR betraut, die die Koordinierung und die Reaktion auf der politischen Ebene der Union betrifft.	Artikel 16 des Vertrags über die Europäische Union
Vorsitz des Rates der Europäischen Union	Politisch	Beschließt (außer in den Fällen, in denen die Solidaritätsklausel gemäß Artikel 222 des Vertrags über die Arbeitsweise der Europäischen Union geltend gemacht wird) über die Aktivierung der IPCR, in Absprache der Kommission und dem Hohen Vertreter sowie gegebenenfalls mit den betroffenen Mitgliedstaaten.	Artikel 16 des Vertrags über die Europäische Union Durchführungsbeschluss (EU) 2018/1993 des Rates
Grenzübergreifende Cyber-Hubs	Technisch	Ein grenzübergreifender Cyber-Hub ist eine durch eine schriftliche Konsortialvereinbarung eingerichtete länderübergreifende Plattform, auf der nationale Cyber-Hubs aus mindestens drei	Verordnung (EU) 2025/38

Akteur	Ebene/ Stufe	Rolle und Zuständigkeit	Verweis
		Mitgliedstaaten in einer koordinierten Netzstruktur zusammenarbeiten und die dazu bestimmt ist, die Überwachung, Erkennung und Analyse von Cyberbedrohungen zu verbessern, um Cybersicherheitsvorfälle zu verhindern und die Gewinnung von Erkenntnissen in Bezug auf Cyberbedrohungen zu unterstützen, insbesondere durch den Austausch relevanter – gegebenenfalls anonymisierter – Daten und Informationen sowie durch die gemeinsame Nutzung modernster Instrumente und die gemeinsame Entwicklung von Erkennungs-, Analyse-, Präventions- und Schutzfähigkeiten gegenüber Cyberangriffen in einem vertrauenswürdigen Umfeld; Arbeiten eng mit dem CSIRTs-Netzwerk zusammen, um Informationen auszutauschen. Geben Informationen über einen potenziellen oder laufenden Cybersicherheitsvorfall großen Ausmaßes an die Behörden der Mitgliedstaaten und die Kommission über EU-CyCLONe und das CSIRTs-Netzwerk weiter.	

Akteur	Ebene/ Stufe	Rolle und Zuständigkeit	Verweis
CSIRTs-Netzwerk	Technisch	Trägt zum Aufbau von Vertrauen zwischen den Mitgliedstaaten bei und fördert eine rasche und wirksame operative Zusammenarbeit zwischen ihnen. Ist das wichtigste Netzwerk zum Austausch relevanter Informationen über Sicherheitsvorfälle, Beinahe-Vorfälle, Cyberbedrohungen, Risiken und Schwachstellen. Tauscht auf Antrag eines potenziell von einem Sicherheitsvorfall betroffenen Mitglieds Informationen über diesen Sicherheitsvorfall und damit verbundene Cyberbedrohungen aus und erörtert diese. Das Netzwerk kann auch eine koordinierte Reaktion auf einen Sicherheitsvorfall erleichtern, der im Zuständigkeitsbereich eines antragstellenden Mitglieds festgestellt wurde. Unterstützt die Mitgliedstaaten bei der Bewältigung grenzübergreifender Sicherheitsvorfälle und prüft weitere Formen der Zusammenarbeit, einschließlich der Amtshilfe. Erhält von den Mitgliedstaaten Informationen über deren Anträge an die	Richtlinie (EU) 2022/2555 Verordnung (EU) 2025/38

Akteur	Ebene/ Stufe	Rolle und Zuständigkeit	Verweis
		EU-Cybersicherheitsreserve.	
Konferenz der Cyber-kommandeure		Ein Forum für Cyberkommandeure auf nationaler Ebene in den Mitgliedstaaten zur Zusammenarbeit und zum Austausch wichtiger Informationen über laufende Operationen im Cyberraum und Strategien zur Eindämmung von Cybervorfällen großen Ausmaßes. Sie wird vom turnusmäßig wechselnden Vorsitz des Rates der Europäischen Union mit Unterstützung der Europäischen Verteidigungsagentur (EDA) und des Europäischen Auswärtigen Dienstes (EAD), einschließlich des Militärstabs der EU (EUMS), organisiert.	Gemeinsame Mitteilung über die EU-Cyberabwehrpolitik (2022).
Kommission	Operativ / Politisch	Exekutivorgan der Europäischen Union. Gewährleistet das reibungslose Funktionieren des Binnenmarkts. Erleichtert die Kohärenz und Koordinierung zwischen verbundenen Reaktionsmaßnahmen auf Unionsebene. Ergreift bestimmte allgemeine Vorsorgemaßnahmen auf Unionsebene im Rahmen des UPCM-Beschlusses, einschließlich Verwaltung des Zentrums für die Koordination von Notfallmaßnahmen	Artikel 17 des Vertrags über die Europäische Union Durchführungsbeschluss (EU) 2018/1993 Beschluss Nr. 1313/2013/EU Richtlinie (EU) 2022/2555 Verordnung (EU) 2025/38

Akteur	Ebene/ Stufe	Rolle und Zuständigkeit	Verweis
		und des Gemeinsamen Kommunikations- und Informationssystems für Notfälle. Beobachter im EU-CyCLONe und Mitglied im Falle eines potenziellen oder laufenden Sicherheitsvorfalls großen Ausmaßes, der erhebliche Auswirkungen auf unter den Anwendungsbereich der Richtlinie (EU) 2022/2555 fallende Dienste und Tätigkeiten hat oder wahrscheinlich haben wird. Beobachter im CSIRTs-Netzwerk. Trägt die Gesamtverantwortung für die Umsetzung der EU-Cybersicherheitsreserve. Kontaktstelle im Interinstitutionellen Cybersicherheitsbeirat (IICB) für den Austausch einschlägiger Informationen über schwerwiegende Sicherheitsvorfälle mit EU-CyCLONe. Wird vom Vorsitz des Rates zu Beschlüssen über die Aktivierung oder Deaktivierung der IPCR konsultiert (außer in den Fällen, in denen die Solidaritätsklausel gemäß Artikel 222 AEUV geltend gemacht wird).	Verordnung (EU, Euratom) 2023/2841

Akteur	Ebene/ Stufe	Rolle und Zuständigkeit	Verweis
		Die Kommissionsdienststellen arbeiten gemeinsam mit dem EAD die ISAA-Berichte aus.	
Agentur der Europäischen Union für Cybersicherheit (ENISA)	Technisch / Operativ	Nimmt Aufgaben wahr zu dem Zweck, ein hohes Cybersicherheitsniveau in der gesamten Union zu erreichen, auch durch aktive Unterstützung für die Mitgliedstaaten und die Organe der Union. Stellt das Sekretariat für das CSIRTs-Netzwerk und EU-CyCLONe. Erstellt regelmäßig einen technischen EU-Cybersicherheitslagebericht über Sicherheitsvorfälle und Cyberbedrohungen (mit EC3 und dem CERT-EU und in enger Zusammenarbeit mit den Mitgliedstaaten). Trägt zur Entwicklung einer gemeinsamen Reaktion auf grenzüberschreitende Sicherheitsvorfälle großen Ausmaßes oder Krisen bei, vor allem indem sie - Berichte aus nationalen Quellen zusammenfasst und auswertet,	Richtlinie (EU) 2022/2555 Verordnung (EU) 2019/881 Verordnung (EU) 2025/38 Verordnung (EU) 2024/2847

Akteur	Ebene/ Stufe	Rolle und Zuständigkeit	Verweis
		- den Informationsfluss zwischen technischer, operativer und politischer Ebene gewährleistet, - auf Antrag die Bewältigung von Sicherheitsvorfällen unterstützt, - Einrichtungen der Union bei der öffentlichen Kommunikation unterstützt, - auf Antrag die Mitgliedstaaten bei der öffentlichen Kommunikation unterstützt, - Kapazitäten zur Reaktion auf Sicherheitsvorfälle testet und regelmäßig Cybersicherheitsübungen organisiert, Handelt als öffentlicher Auftraggeber in den Fällen, in denen sie ganz oder teilweise mit dem Betrieb und der Verwaltung der EU-Cybersicherheitsreserve betraut wurde. Organisiert alle zwei Jahre eine umfassende Cybersicherheitsübung großen Ausmaßes auf Unionsebene mit technischen, operativen und strategischen Elementen. Erstellt in Zusammenarbeit mit dem betroffenen Mitgliedstaat und anderen einschlägigen Interessenträgern einen Bericht über die Überprüfung des Sicherheitsvorfalls, um die Ursachen, Auswirkungen und Maßnahmen zur Eindämmung eines Sicherheitsvorfalls zu bewerten (auf Antrag der Kommission oder	

Akteur	Ebene/ Stufe	Rolle und Zuständigkeit	Verweis
		von EU-CyCLONe und mit Zustimmung des betroffenen Mitgliedstaats). Informiert EU-CyCLONe darüber, ob Informationen, die im Rahmen der Berichtspflichten der Cyberresilienz-Verordnung bereitgestellt werden, für das koordinierte Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen auf operativer Ebene relevant sind.	
Europäisches Netzwerk der Verbindungs-organisationen für Cyberkrisen (EU-CyCLONe)	Operativ	Unterstützt das koordinierte Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen auf operativer Ebene. Gewährleistet einen regelmäßigen Austausch einschlägiger Informationen zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU. Koordiniert das Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen und unterstützt die Entscheidungsfindung auf politischer Ebene in Bezug auf solche Sicherheitsvorfälle und Krisen.	Richtlinie (EU) 2022/2555 Verordnung (EU) 2025/38

Akteur	Ebene/ Stufe	Rolle und Zuständigkeit	Verweis
		Bewertet die Folgen und Auswirkungen relevanter Cybersicherheitsvorfälle großen Ausmaßes und Krisen und schlägt mögliche Abhilfemaßnahmen vor. Erörtert auf Ersuchen eines betroffenen Mitgliedstaats nationale Pläne für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen. Entwickelt gemeinsam mit der ENISA und der Kommission ein Muster, um das Beantragen von Unterstützung aus der EU-Cybersicherheitsreserve zu erleichtern. Erhält von den Mitgliedstaaten Informationen über deren Anträge an die EU-Cybersicherheitsreserve. Erhält Informationen über einen potenziellen oder laufenden Cybersicherheitsvorfall großen Ausmaßes von den grenzübergreifenden Cyber-Hubs oder vom CSIRTs-Netzwerk.	
Hoher Vertreter der Union für Außen- und Sicherheitspolitik mit Unterstützung	Politisch	Leitet und koordiniert die Bemühungen der Union zur Abwehr von äußeren Sicherheitsbedrohungen im Zusammenhang mit hybriden Bedrohungen und der Cybersicherheit.	Beschluss 2010/427/EU des Rates

Akteur	Ebene/ Stufe	Rolle und Zuständigkeit	Verweis
durch den Europäischen Auswärtigen Dienst		Ist verantwortlich für die Instrumente der Cyberdiplomatie und der Cyberabwehr der Union, um unter anderem mithilfe der Instrumentarien der Union zur Abwehr hybrider Bedrohungen und für die Cyberdiplomatie von externen Bedrohungen abzuschrecken und darauf zu reagieren. Arbeitet mit externen Partnern zusammen, auch im Rahmen der GASP-Tätigkeiten. Trägt zur Abwehrbereitschaft der Union sowie zur Lageerfassung und Reaktionsfähigkeit der Mitgliedstaaten in Bezug auf hybride Bedrohungen und Cyberbedrohungen bei, z. B. durch praktische Übungen, Schulungen und Vernetzung. Befasst sich mit den sicherheits- und verteidigungspolitischen Auswirkungen der Weltraumressourcen der Union, insbesondere im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) der Union. Unterstützt die EU-Konferenz der Cyberkommandeure.	

Akteur	Ebene/ Stufe	Rolle und Zuständigkeit	Verweis
		Unterstützt das operative Netz für die militärischen IT-Notfallteams (MICNET) der EU. Wird vom Vorsitz des Rates zu Beschlüssen über die Aktivierung oder Deaktivierung der IPCR konsultiert (außer in den Fällen, in denen die Solidaritätsklausel gemäß Artikel 222 AEUV geltend gemacht wird). Der EAD arbeitet gemeinsam mit dem Kommissiondienststellen die ISAA-Berichte aus.	
EU-Koordinierungszentrum für die Cyberabwehr	Horizontal	Sein Ziel besteht zunächst in erster Linie darin, die gemeinsame Lageerfassung der Union und ihrer Mitgliedstaaten in Bezug auf böswillige Aktivitäten im Cyberraum zu verbessern, insbesondere im Hinblick auf militärische Missionen und Operationen im Rahmen der GSVP.	Gemeinsame Mitteilung über die EU-Cyberabwehrpolitik (2022).
Europol	Operativ	Leistet den zuständigen Behörden der Mitgliedstaaten operative und technische Unterstützung bei der Prävention und Abschreckung von Cyberkriminalität. Unterstützt die zuständigen Behörden der Mitgliedstaaten auf deren Ersuchen bei der Reaktion auf vermutlich kriminell motivierte Cyberangriffe.	Verordnung (EU) 2016/794, einschließlich aller Änderungen

Akteur	Ebene/ Stufe	Rolle und Zuständigkeit	Verweis
Interinstitutioneller Cybersicherheitsbeirat		Stellt einen Plan für das Cyberkrisenmanagement auf, um auf operativer Ebene die koordinierte Bewältigung schwerwiegender Sicherheitsvorfälle, die Einrichtungen der Union betreffen, zu unterstützen und einen Beitrag zum regelmäßigen Austausch einschlägiger Informationen zu leisten. Koordiniert die Annahme der Pläne der einzelnen Einrichtungen der Union für das Cyberkrisenmanagement. Nimmt auf Vorschlag des CERT-EU Leitlinien oder Empfehlungen für die Zusammenarbeit bei der Reaktion auf erhebliche Sicherheitsvorfälle, die Einrichtungen der Union betreffen, an.	Verordnung (EU, Euratom) 2023/2841
Operatives Netz für die militärischen IT-Notfallteams (MICNET)	Technisch	Fördert eine robustere und koordiniertere Reaktion auf Cyberbedrohungen, die die Verteidigungssysteme in der Union betreffen, einschließlich solcher, die bei militärischen Missionen und Operationen im Rahmen der GSVP verwendet werden; unterstützt von der Europäischen Verteidigungsagentur.	Gemeinsame Mitteilung von 2022 über die Cyberabwehrpolitik

Akteur	Ebene/ Stufe	Rolle und Zuständigkeit	Verweis
Einheitliches Analyse-verfahren (SIAC)		Besteht aus 1) dem EU-Zentrum für Informationsgewinnung und Lageerfassung (EU INTCEN) und 2) der Abteilung Aufklärung des Militärstabs der EU (EUMS INT) SIAC. Stellt strategische nachrichtendienstliche Erkenntnisse über Außenpolitik, Terrorismus, Cyberbedrohungen und hybride Bedrohungen bereit und wertet militärische Erkenntnisse für GSVP-Missionen aus und unterstützt Verteidigungs- und Krisenbewältigungsoperationen der Union. Untersteht dem Hohen Vertreter.	Artikel 38 und 42 bis 46 des Vertrags über die Europäische Union

(3) Einschlägige Krisenmanagementmechanismen und -plattformen auf Unionsebene

Mechanismus	Horizontal / Sektoral / Cyberspezifisch	Beschreibung	Verweis
ARGUS	Horizontal	Koordinierungsprozess und allgemeines Alarmsystem der Kommission für eine kohärente Reaktion im Falle einer schwerwiegenden grenzüberschreitenden Krise, die Maßnahmen auf EU-Ebene erfordert. Setzt sich aus allen einschlägigen Dienststellen und Kabinetten zusammen, um Maßnahme zu beschließen und zu koordinieren. Ermöglicht der Kommission den Austausch einschlägiger Informationen über neu auftretende sektorübergreifende Krisen und über absehbare oder unmittelbar bevorstehende Bedrohungen, die Maßnahmen auf Unionsebene erfordern.	Mitteilung der Kommission COM(2005) 662
EAD-Krisenreaktions-zentrum (CRC)	Horizontal	Zentrale Anlaufstelle des EAD für alle krisenbezogenen Fragen und rund um die Uhr besetzte, ständige Krisenreaktionsfähigkeit für Notfälle, die die Sicherheit des Personals in den EU-Delegationen bedrohen, und/oder für die Reaktion auf Krisen, von denen Unionsbürgerinnen und -bürger im Ausland betroffen sind. Bündelt Experten für Sicherheit, Konsularfragen	Ein Strategischer Kompass für Sicherheit und Verteidigung – Für eine Europäische Union, die ihre Bürgerinnen und Bürger, Werte und Interessen schützt und zu Weltfrieden und internationaler

Mechanismus	Horizontal / Sektoral / Cyberspezifisch	Beschreibung	Verweis
		und Lageerfassung und stützt sich dabei auf engagierte Fachkräfte vor Ort in den Delegationen der Union.	Sicherheit beiträgt (21. März 2022)
Konzeptentwurf für kritische Infrastrukturen	Horizontal	Koordiniert die Reaktion auf Unionsebene auf Störungen kritischer Infrastrukturen von erheblicher grenzüberschreitender Bedeutung.	Empfehlung C/2024/4371 des Rates
Warnsystem für Cybersicherheit	Cyberspezifisch	Gewährleistet fortgeschrittene Fähigkeiten der Union zur Verbesserung der Erkennungs-, Analyse- und Datenverarbeitungskapazitäten im Zusammenhang mit Cyberbedrohungen und zur Verhütung von Sicherheitsvorfällen in der Union.	Verordnung (EU) 2025/38
Instrumentarium für die Cyberdiplomatie (Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten)	Cyberspezifisch	Ermöglicht eine gemeinsame diplomatische Reaktion der Union auf böswillige Cyberaktivitäten und trägt zur Konfliktverhütung, zur Eindämmung von Cybersicherheitsbedrohungen und zu größerer Stabilität in den internationalen Beziehungen bei.	Schlussfolgerungen des Rates vom 19. Juni 2017 Überarbeitete Umsetzungsleitlinien, Dok. 10289/23, 8. Juni 2023
EU-Cybersicherheits-reserve	Cyberspezifisch	Mobilisiert Cybersicherheitsexperten und -ressourcen in Krisenzeiten zur Unterstützung der Reaktionsbemühungen in den Mitgliedstaaten und den Organen, Einrichtungen oder sonstigen Stellen der Union.	Verordnung (EU) 2025/38

Mechanismus	Horizontal / Sektoral / Cyberspezifisch	Beschreibung	Verweis
Netzkodex mit sektorspezifischen Regeln für Cybersicherheits-aspekte bei grenzüber-greifenden Stromflüssen	Sektoral	Sieht ein regelmäßig anzuwendendes Verfahren zur Bewertung von Cybersicherheitsrisiken im Elektrizitätssektor vor, auf Ebene der Union, der Mitgliedstaaten, der Regionen und der Einrichtungen. Enthält besondere Bestimmungen für das Krisenmanagement und die Zusammenarbeit mit dem CSIRTs-Netzwerk und mit EU-CyCLONe in Fällen, in denen ein Cybersicherheitsvorfall großen Ausmaßes Auswirkungen auf andere Sektoren hat, die abhängig von der Stromversorgungssicherheit sind.	Delegierte Verordnung (EU) 2024/1366 der Kommission
Instrumentarium zur Abwehr hybrider Bedrohungen	Horizontal	Enthält eine Reihe von Bestimmungen, um einen Überblick darüber zu erhalten, was auf EU-Ebene als Reaktionsmaßnahmen auf alle Arten hybrider Bedrohungen und deren koordinierten Einsatz zur Verfügung steht, und um die Kohärenz der Maßnahmen in allen Bereichen zu gewährleisten. Das Instrumentarium trägt dazu bei, dass Entscheidungen auf der Grundlage eines umfassenden Lagebewusstseins und der gezogenen Lehren getroffen werden.	Schlussfolgerungen des Rates über einen Rahmen für eine koordinierte Reaktion der EU auf hybride Kampagnen, 22. Juni 2022 Durchführungsleitlinien für den Rahmen für eine koordinierte Reaktion auf hybride Kampagnen, 14. Dezember 2022

Mechanismus	Horizontal / Sektoral / Cyberspezifisch	Beschreibung	Verweis
Teams für die rasche Reaktion auf hybride Bedrohungen (EU HRRTs)	Horizontal	Als Teil des EU-Instrumentariums zur Abwehr hybrider Bedrohungen greifen die EU-Teams für die rasche Reaktion auf hybride Bedrohungen auf einschlägige sektorspezifische zivile und militärische Sachkenntnis auf nationaler Ebene und EU-Ebene zurück, um den Mitgliedstaaten, den Missionen und Operationen im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik sowie den Partnerländer maßgeschneiderte und gezielte kurzfristige Unterstützung bei der Abwehr hybrider Bedrohungen und Kampagnen zu leisten.	Orientierungsrahmen für die praktische Einrichtung der EU-Teams für die rasche Reaktion auf hybride Bedrohungen (21. Mai 2024) Operative Leitlinien für die Entsendung von Teams für die rasche Reaktion auf hybride Bedrohungen, vom AStV am 4. Dezember 2024 gebilligt
IPCR	Horizontal	Unterstützt eine rasche und koordinierte Beschlussfassung auf politischer Ebene der Union in Bezug auf schwere und komplexe Krisen. Der Beschluss über die Aktivierung und Deaktivierung wird vom Vorsitz des Rates gefasst, der die betroffenen Mitgliedstaaten, die Kommission und den Hohen Vertreter konsultiert (außer in Fällen, in denen die Solidaritätsklausel geltend gemacht wird). Das Generalsekretariat des Rates, die Kommissionsdienststellen und der EAD können in Absprache mit dem Ratsvorsitz auch vereinbaren, die IPCR	Durchführungs-beschluss (EU) 2018/1993 des Rates

Mechanismus	Horizontal / Sektoral / Cyberspezifisch	Beschreibung	Verweis
		im Informationsaustausch-Modus zu aktivieren. Die Arbeit der IPCR stützt sich auf die ISAA-Berichte, die von den Kommissionsdienststellen und dem EAD ausgearbeitet werden. Diese Berichte basieren auch auf relevanten Informationen und Analysen, die von den Mitgliedstaaten (z. B. den einschlägigen nationalen Krisenzentren) und den einschlägigen Stellen und Einrichtungen der Union bereitgestellt werden.	
EU-Notfallprotokoll für die Strafverfolgung	Horizontal	Ein Instrument zur Unterstützung der Strafverfolgungsbehörden der Union bei der sofortigen Reaktion auf große grenzüberschreitende Cyberangriffe durch eine rasche Bewertung, den sicheren und zeitnahen Austausch kritischer Informationen und eine wirksame Koordinierung der internationalen Aspekte ihrer Ermittlungen.	Schlussfolgerungen des Rates vom 26. Juni 2018 zu einer koordinierten Reaktion der EU auf große Cybersicherheitsvorfälle und -krisen
Teams für die rasche Reaktion auf Cybervorfälle (CRRTs) im Rahmen der SSZ	Cyberspezifisch	Die CRRTs im Rahmen der SSZ sind eine von den EU-Mitgliedstaaten gemeinsam entwickelte zivil-militärische Cyberabwehrfähigkeit zur raschen Reaktion auf schwerwiegende Cybersicherheitsvorfälle und	Artikel 42 Absatz 6, Artikel 46 und Protokoll 10 des Vertrags über die Europäische Union

Mechanismus	Horizontal / Sektoral / Cyberspezifisch	Beschreibung	Verweis
		Cyberkrisen und zur Durchführung von Präventivmaßnahmen wie z. B. Schwachstellenbeurteilungen und Wahlbeobachtung. Aufgabe der CRRTs im Rahmen der SSZ ist die Bereitstellung von Cyberunterstützung – auf Antrag – an die EU-Mitgliedstaaten, an die Organe, Einrichtungen und sonstigen Stellen der EU, an die militärischen Missionen und Operationen der EU im Rahmen der GSVP sowie an Partnerländer.	

Architektur für die Reaktion auf Bedrohungen im Weltraum (STRA)	Sektoral (Weltraumbedrohungen, auch cyberbezogen)	Architektur für die Reaktion auf Bedrohungen im Weltraum (STRA) mit Zuständigkeiten, die vom Rat und vom Hohen Vertreter wahrgenommen werden, um eine Bedrohung abzuwehren, die sich aus Einrichtung, Betrieb oder Nutzung der im Rahmen des Weltraumprogramms der Union geschaffenen Systeme und Dienste ergibt.	Beschluss (GASP) 2021/698 des Rates
Koordinierungsrahmen in Bezug auf systemische Cybersicherheitsvorfälle (EU-SCICF)	Sektoral	Ein im Aufbau befindlicher Rahmen für die Kommunikation und Koordinierung, der dazu dient, potenzielle systemische Cyberereignisse im Finanzsektor anzugehen und zu bewältigen. Er wird auf einer der in der Verordnung (EU) 2022/2554 vorgesehenen Aufgaben der Europäischen Aufsichtsbehörden (ESAs) aufbauen, nämlich schrittweise eine wirksame koordinierte Reaktion auf Unionsebene zu ermöglichen, sofern es zu einem schwerwiegenden grenzüberschreitenden IKT-bezogenen Vorfall oder einer vergleichbaren Bedrohung kommt, die systemische Auswirkungen auf den gesamten Finanzsektor der Union mit sich bringt.	Empfehlung des Europäischen Ausschusses für Systemrisiken vom 2. Dezember 2021 zu einem europaweiten Koordinierungsrahmen für betreffende Behörden in Bezug auf systemische Cybersicherheitsvorfälle (ESRB/2021/17)
Katastrophenschutzverfahren der Union (UCPM)	Horizontal	Gewährleistet die Zusammenarbeit im Katastrophenschutz, um die Katastrophenprävention, -vorsorge	Beschluss Nr. 1313/2013/EU

		und -bewältigung zu verbessern.	
Gemeinsamer Informationsraum (CISE)	Speziell für den Seeverkehr, erfasst sieben Sektoren.	CISE ist ein Netz, das Systeme von EU-/EWR-Behörden, die für die Seeverkehrsüberwachung zuständig sind, miteinander verbindet. CISE ermöglicht grenzüberschreitend und über verschiedene Sektoren hinweg den nahtlosen und automatisierten Austausch einschlägiger Informationen.	Ein Strategischer Kompass für Sicherheit und Verteidigung – Für eine Europäische Union, die ihre Bürgerinnen und Bürger, Werte und Interessen schützt und zu Weltfrieden und internationaler Sicherheit beiträgt (21. März 2022)

(4) Sektoren mit hoher Kritikalität und andere kritische Sektoren gemäß der Richtlinie (EU) 2022/2555 und sektorale Krisenmechanismen auf Unionsebene (falls zutreffend)		
Sektor	**Teilsektor**	**Anwendbare sektorale Krisenmechanismen**
Energie	Elektrizität	Koordinierungsgruppe „Strom“
	Fernwärme und -kälte	entfällt
	Erdöl	Koordinierungsgruppe „Erdöl“ EU-Gruppe der für Offshore-Erdöl- und -Erdgasaktivitäten zuständigen Behörden (EUOAG)
	Erdgas	Koordinierungsgruppe „Erdgas“
	Wasserstoff	entfällt
Verkehr	Luftfahrt	Europäische Koordinierungszelle für Luftfahrtkrisensituationen (EACCC)
	Schienenverkehr	entfällt
	Schifffahrt	Europäische Fischereiaufsichtsagentur (EFCA) SafeSeaNet (SSN) Integrierte Seeverkehrsdienste (IMS) Rechenzentrum des Systems der Fernidentifizierung und -verfolgung von Schiffen (LRIT) EMSA-Unterstützungsdienste für den Seeverkehr

	Straßenverkehr	entfällt
	Horizontal	Netz der Kontaktstellen für den Verkehr, eingerichtet durch den Notfallplan für den Verkehr (COM(2022) 211)
Bankwesen		EU-SCICF
Finanzmarktinfrastrukturen		EU-SCICF Europäischer Finanzstabilisierungsmechanismus

Gesundheitswesen		Frühwarn- und Reaktionssystem (EWRS) Zentrum für das Management von gesundheitlichen Krisensituationen (HEOF) Schnellwarnsystem für Gewebe, Zellen und Blutbestandteile (RATC/RAB) Rahmen für gesundheitliche Notlagen Schnellwarnsystem für chemische Vorfälle (RASCHEM) Europäisches Überwachungsportal für Infektionskrankheiten Krisenvorsorge und -reaktion bei gesundheitlichen Notlagen (HERA) Medizinisches Gesundheitsinformationssystem (MediSys) Hochrangige Lenkungsgruppe für Engpässe bei Medizinprodukten (MDSSG) Pharmakovigilanz-Schnellwarnsystem EU-Gesundheits-Taskforce (EUHTF) Gesundheitssicherheitsausschuss
Trinkwasser		Entfällt

Abwasser		entfällt
Digitale Infrastruktur		entfällt
Verwaltung von IKT-Diensten		entfällt
Öffentliche Verwaltung		entfällt
Weltraum		Architektur für die Reaktion auf Bedrohungen im Weltraum (STRA)
Post- und Kurierdienste		entfällt
Abfallbewirtschaftung		entfällt
Produktion, Herstellung und Handel mit chemischen Stoffen		Schnellwarnsystem für chemische Vorfälle (RASCHEM)

Produktion, Verarbeitung und Vertrieb von Lebensmitteln		Europäisches System für das Kulturpflanzen-Monitoring Weltweite Erkennung von Anomalien in der Agrarproduktion (ASAP) Europäisches Netzwerk der Pflanzengesundheitsinformationssysteme (EUROPHYT) EU-Veterinär-Notfallteams (EUVET) Schnellwarnsystem für Lebens- und Futtermittel (RASFF) Europäischer Mechanismus zur Krisenvorsorge und Krisenreaktion im Bereich der Ernährungssicherheit (EFSCM) Binnenmarkt-Notfall- und Resilienzgesetz (IMERA)
Verarbeitendes Gewerbe / Herstellung von Waren	Medizinprodukte	entfällt
	Datenverarbeitungsgeräte, elektronische und optische Erzeugnisse	entfällt
	Maschinenbau	entfällt
	Herstellung von Kraftwagen und Kraftwagenteilen	entfällt
	Sonstiger Fahrzeugbau	entfällt

Anbieter digitaler Dienste		entfällt
Forschung		entfällt

ANHANG III – EU-Rahmen für das Cybersicherheitskrisenmanagement und damit zusammenhängende Instrumente

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[1],
- Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates[2],
- Durchführungsverordnung 2024/2690 der Kommission[3], Verordnung (EU/Euratom) 2023/2841 des Europäischen Parlaments und des Rates[4],
- Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates[5],
- Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates[6] und
- Verordnung (EU) 2025/38 des Europäischen Parlaments und des Rates („Cybersolidaritätsverordnung“)[7].

Zu den besonderen sektoralen Maßnahmen zur Bewältigung von Cybersicherheitskrisen gehören die Delegierte Verordnung (EU) 2024/1366 der Kommission[8] und der künftige Rahmen für die Koordinierung in Bezug auf systemische Cybersicherheitsvorfälle (EU-SCICF) im Zusammenhang mit der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates[9].

Die Richtlinie 2013/40/EU[10] 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[11], die nach ihrer Umsetzung Strafverfolgungsmaßnahmen in diesem Bereich erheblich erleichtern wird.

In der EU-Cyberabwehrpolitik[12] 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.

In der Empfehlung des Rates für einen Konzeptentwurf zur Koordinierung der Reaktion – auf Unionsebene – auf Störungen kritischer Infrastrukturen von erheblicher grenzüberschreitender Bedeutung[13] ist die Zusammenarbeit zwischen den einschlägigen Akteuren vorgesehen, wenn ein Sicherheitsvorfall sowohl physische Aspekte als auch die Cybersicherheit kritischer Infrastruktur betrifft.

[1] 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).

[2] 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 (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).

[3] 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). ELI: https://data.europa.eu/eli/reg/2024/2690/oj).

[4] 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).

[5] 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).

[6] 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).

[7] 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 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).

[8] 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).

[9] Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Betriebsstabilität digitaler Systeme 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).

[10] 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).

[11] 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 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. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

[12] JOIN(2022) 49 final. https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52022JC0049

[13] *ABl. C, 2024/4371, 5.7.2024.* https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:C_202404371