Rat der
Europäischen Union

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

6527/25
ADD 1

Interinstitutionelles Dossier:
2025/0036(NLE)

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

ÜBERMITTLUNGSVERMERK

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

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

Anl.: COM(2025) 66 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 24.2.2025
COM(2025) 66 final

ANNEXES 1 to 3

ANHÄNGE

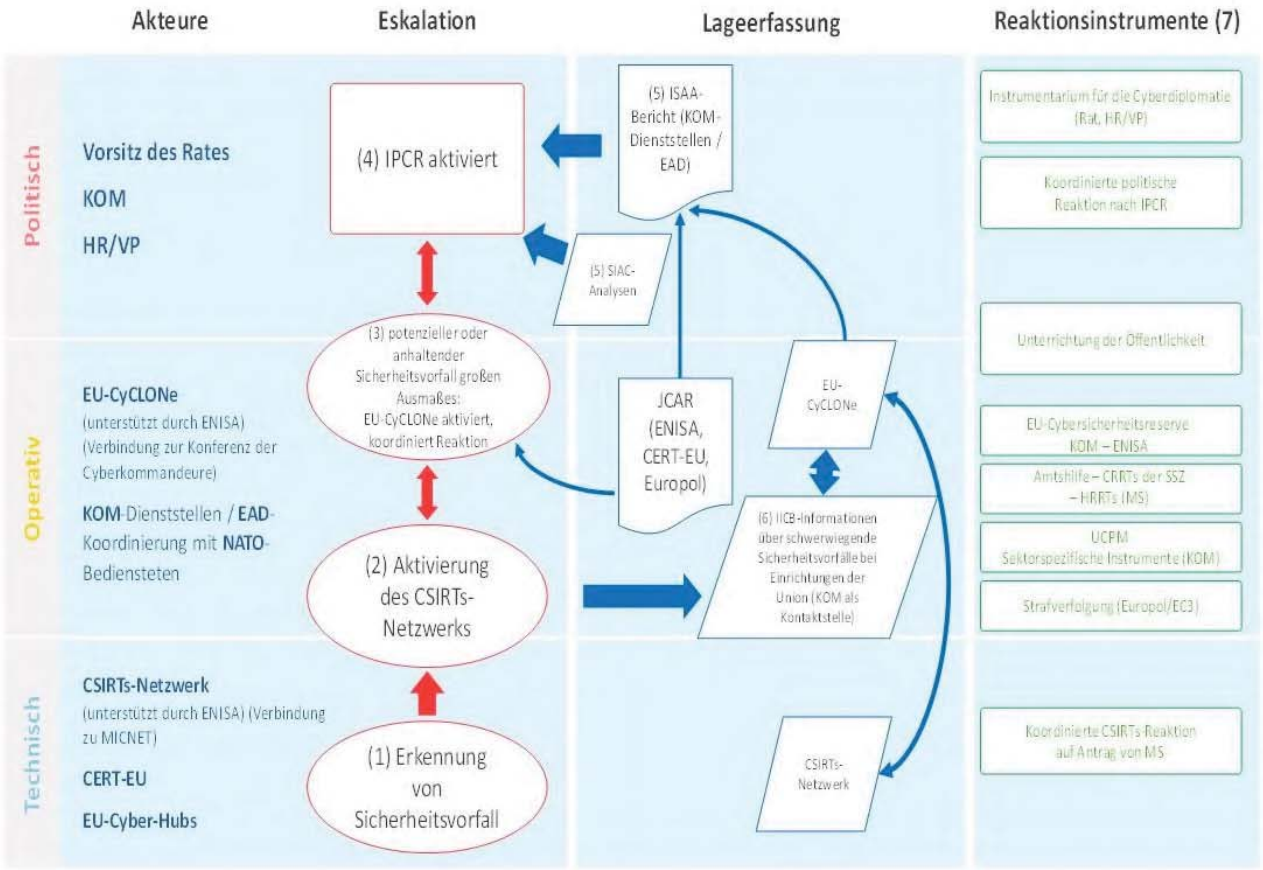
des

Vorschlags für eine EMPFEHLUNG DES RATES

für einen EU-Konzeptentwurf für das Cybersicherheitskrisenmanagement

ANHANG I – Konzeptentwurf der Union für das Cybersicherheitskrisenmanagement

Die folgende Abbildung zeigt eine Veranschaulichung und Zusammenfassung des Cyberkonzeptentwurfs der Union: wer redet mit wem in einer Cybersicherheitskrise der Union – im Einklang mit den einschlägigen Krisenmechanismen der EU, die in Anhang II aufgeführt sind. Eine solche Krise wird unweigerlich einen oder mehrere kritische Sektoren betreffen und eine enge Koordinierung zwischen der Cybergemeinschaft, sektoralen Mechanismen und Katastrophenschutzmechanismen erforderlich machen. Cybersicherheitsvorfälle können Teil umfassenderer hybrider Kampagnen sein, weshalb die Cyberabwehr mit anderen Maßnahmen im Einklang mit der Strategie für eine krisenfeste Union koordiniert werden sollte.



1) Die CSIRTs und/oder grenzübergreifenden Cyber-Hubs erkennen einen Cybersicherheitsvorfall großen Ausmaßes.
2) Das CSIRTs-Netzwerk meldet dies im Einklang mit den internen Verfahren weiter.
3) EU-CyCLONe koordiniert die operative Reaktion im Fall eines Sicherheitsvorfalls großen Ausmaßes.
4) Der Vorsitz des Rates bestimmt in Konsultation mit den Mitgliedstaaten, der Kommission und der Hohen Vertreterin, ob die IPCR-Krisenregelung der EU aktiviert oder deaktiviert wird.
5) Sofern die IPCR-Regelung aktiviert wird, fließen die von den Kommissionsdienststellen und dem EAD ausgearbeiteten ISAA-Berichte in die Erörterungen ein. EU-CyCLONe und JCAR sollten Beiträge zum ISAA leisten. Der Rat erhält darüber hinaus Informationen über SIAC-Analysen.
6) CERT-EU ist für die operative Reaktion auf Krisen, die Einrichtungen der Union betreffen, zuständig; relevante Informationen können EU-CyCLONe durch den IICB über die Kommission als Kontaktstelle übermittelt werden.
7) Der Rat, EU-CyCLONe und das CSIRTs-Netzwerk haben die Aufsicht über die Reaktionen auf politischer, operativer bzw. technischer Ebene.

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

(1) Einschlägige Akteure auf Unionsebene während des gesamten Lebenszyklus des Cyberkrisenmanagements

Ebene/Stufe	Krisenvorsorge	Erkennung	Reaktion	Wiederherstellung
Politisch	• Rat • Kommission • EAD		• Rat • Kommission • EAD	
Operativ	• EU-CyCLONe • ENISA • Kommission • Europol		• EU-CyCLONe • Kommission • ENISA • CERT-EU (für Sicherheits-vorfälle, die Einrich-tungen der Union betreffen) • Europol	• ENISA
Technisch	• CSIRTs-Netzwerk • Grenzübergreifende Cyber-Hubs • CERT-EU	• CSIRTs-Netzwerk • Grenzübergreifende Cyber-Hubs • CERT-EU	• CSIRTs-Netzwerk • CERT-EU	• CSIRTs-Netzwerk • CERT-EU

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

Akteur	Ebene/ Stufe	Rolle und Zuständigkeit	Verweis
CERT-EU	Tech-nisch/ Operativ	Koordiniert die Reaktion und Bewältigung schwerwiegender Sicherheitsvorfälle, die Einrichtungen der Union betreffen.	Verordnung (EU, Euratom) 2023/2841

		Mitglied des CSIRTs-Netzwerks. Unterstützt die Kommission in EU-CyCLONe. 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 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.	
Vorsitz des Rates der EU	Politisch	Beschließt (außer in den Fällen, in denen die Solidaritätsklausel gemäß Artikel 222 des Vertrags über die Arbeitsweise der Europäischen Union aktiviert wird) über die Aktivierung oder Deaktivierung der IPCR-Regelung auf Antrag eines Mitgliedstaats und gegebenenfalls in Absprache mit den betroffenen Mitgliedstaaten sowie der Kommission und der Hohen Vertreterin sowie über die Herauf- oder Herabstufung von einem Aktivierungsmodus zum anderen.	Artikel 16 des Vertrags über die Europäische Union, Durchführungsbeschluss (EU) 2018/1993 des Rates

Grenzübergreifende Cyber-Hubs	Tech-nisch	Bestehen aus drei oder mehr nationalen Cyber-Hubs und gewährleisten den Austausch wichtiger Informationen im Zusammenhang mit Cyberbedrohungen, Beinahe-Vorfällen, Kompromittierungs-indikatoren und Cybersicherheitswarnungen innerhalb des grenzübergreifenden Cyber-Hubs. Arbeiten eng mit dem CSIRTs-Netzwerk zusammenarbeiten, um Informationen auszutauschen. Geben Informationen über einen potenziellen oder anhaltenden Cybersicherheitsvorfall großen Ausmaßes an die Behörden der Mitgliedstaaten und die Kommission über EU-CyCLONe und das CSIRTs-Netzwerk weiter.	Verordnung (EU) 2025/38
CSIRTs-Netzwerk	Tech-nisch	Tauscht relevante Informationen über Sicherheitsvorfälle, Beinahe-Vorfälle, Cyberbedrohungen, Risiken und Schwachstellen aus. 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 umsetzen, der im Zuständigkeitsbereich eines antragstellenden Mitglieds festgestellt wurde.	Artikel 15 der Richtlinie (EU) 2022/2555

		Erhält von den Mitgliedstaaten Informationen über deren Anträge an die EU-Cybersicherheitsreserve.	
Konferenz der Cyberkommandeure		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), des Europäischen Auswärtigen Dienstes (EAD) und des Militärstabs der EU (EUMS) organisiert.	Gemeinsame Mitteilung zur EU-Cyberabwehrpolitik
Kommission	Operativ / Politisch	Gewährleistet das reibungslose Funktionieren des Binnenmarkts. Legt Analyseberichte (ISAA) für den IPCR-Mechanismus vor. Ergreift allgemeine Vorsorgemaßnahmen, einschließlich Verwaltung des Zentrums für die Koordination von Notfallmaßnahmen und des Gemeinsamen Kommunikations- und Informationssystems für Notfälle. Beobachter im EU-CyCLONe und Mitglied im Falle eines potenziellen oder anhaltenden	Artikel 17 des Vertrags über die Europäische Union, Durchführungs-beschluss (EU) 2018/1993 des Rates Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates Richtlinie (EU) 2022/2555 Verordnung (EU) 2025/38, Verordnung (EU, Euratom) 2023/2841

		Sicherheitsvorfalls großen Ausmaßes. Beobachter im CSIRTs-Netzwerk. Trägt die Gesamtverantwortung für die Umsetzung der EU-Cybersicherheitsreserve. Kontaktstelle des Interinstitutionellen Cybersicherheitsbeirats (IICB) für den Austausch einschlägiger Informationen über schwerwiegende Sicherheitsvorfälle mit EU-CyCLONe. Führt die strategische Aufsicht über die Galileo-Sicherheitszentrale (GSMC). Wird vom Vorsitz des Rates zu Beschlüssen über die Aktivierung oder Deaktivierung der IPCR-Regelung konsultiert. Die Kommissiondienststellen arbeiten gemeinsam mit dem EAD den ISAA-Bericht aus.	
Europäische Cybersicherheitsagentur (ENISA)	Tech-nisch/ Operativ	Stellt das Sekretariat für das CSIRTs-Netzwerk und EU-CyCLONe. Trägt zur Entwicklung einer gemeinsamen Reaktion auf grenzüberschreitende Sicherheitsvorfälle oder Krisen großen Ausmaßes bei, indem sie Berichte aus nationalen Quellen zusammenfasst und auswertet, den Informationsfluss zwischen technischer, operativer und politischer Ebene gewährleistet, den Umgang mit Sicherheitsvorfällen	NIS-2-Richtlinie (Richtlinie (EU) 2022/2555) Verordnung (EU) 2019/881 Verordnung (EU) 2025/38 Verordnung (EU) 2024/2847

		unterstützt, Einrichtungen der Union bei der öffentlichen Kommunikation unterstützt, Kapazitäten zur Reaktion auf Sicherheitsvorfälle testet. Betreibt und verwaltet ganz oder teilweise die EU-Cybersicherheitsreserve, wie in der Cybersolidaritätsverordnung vorgesehen. Überprüft und bewertet Bedrohungen, bekannte Schwachstellen und Eindämmungsmaßnahmen für einen bestimmten schwerwiegenden Cybersicherheitsvorfall oder Cybersicherheitsvorfall großen Ausmaßes. Erstellt einen Bericht über die Überprüfung des Sicherheitsvorfalls.	
Europäisches Netzwerk der Verbindungs-organisationen für Cyberkrisen (EU-CyCLONe)	Operativ	Unterstützt das koordinierte Management von Cybersicherheitsvorfällen und -krisen großen Ausmaßes 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 Cybersicherheits-vorfällen und -krisen großen Ausmaßes und unterstützt die Entscheidungsfindung auf politischer Ebene in Bezug auf solche Sicherheitsvorfälle und Krisen. Bewertet die Folgen und Auswirkungen relevanter	Richtlinie (EU) 2022/2555 Verordnung (EU) 2025/38

		Cybersicherheitsvorfälle und -krisen großen Ausmaßes und schlägt mögliche Abhilfemaßnahmen vor. Entwickelt gemeinsam mit der ENISA 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 anhaltenden Cybersicherheitsvorfall großen Ausmaßes von den grenzübergreifenden Cyber-Hubs oder vom CSIRTs-Netzwerk.	
Hohe Vertreterin der Union für Außen- und Sicherheitspolitik mit Unterstützung durch den Europäischen Auswärtigen Dienst	Politisch	Leitet und koordiniert die Bemühungen der Union zur Abwehr von Bedrohungen der äußeren Sicherheit im Zusammenhang mit hybriden Bedrohungen und der Cybersicherheit. Ist verantwortlich für die Cyberdiplomatie und die Cyberabwehrinstrumente der Union, um 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	Beschluss 2010/427/EU des Rates

		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. Wird vom Vorsitz des Rates zu Beschlüssen über die Aktivierung oder Deaktivierung der IPCR-Regelung konsultiert. Der EAD arbeitet gemeinsam mit den Kommissionsdienststellen den ISAA-Bericht aus.	
Europol	Operativ	Leistet den zuständigen Behörden der Mitgliedstaaten operative und technische Unterstützung bei der Prävention und Abschreckung von Cyberkriminalität.	Verordnung (EU) 2016/794, einschließlich aller Änderungen
Interinstitutioneller Cybersicherheitsbeirat		Nimmt den interinstitutionellen Cyberkrisenmanagementplan der Einrichtungen der Union an. 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 der militärischen IT-Notfallteams (MICNET)	Tech-nisch	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; eingerichtet und unterstützt von der Europäischen Verteidigungsagentur.	Gemeinsame Mitteilung von 2022 zur EU-Cyberabwehrpolitik
Einheitliches Analyseverfahren (SIAC)		Besteht aus 1) dem EU-Zentrum für Informationsgewinnung und Lageerfassung (EU INTCEN), das zivile und quelloffene Erkenntnisse auswertet und strategische nachrichtendienstliche Erkenntnisse über Außenpolitik, Terrorismus und hybride Bedrohungen bereitstellt, und 2) der Abteilung Aufklärung des Militärstabs der EU (EUMS INT), die militärische Erkenntnisse für GSVP-Missionen auswertet und Verteidigungs- und Krisenbewältigungsoperationen der Union unterstützt. Untersteht der Hohen Vertreterin.	Artikel 38 und Artikel 42 bis 46 des Vertrags über die Europäische Union Gemeinsame Aktion 2001/555/GASP des Rates Beschluss 2010/461/GASP des Rates

(3) Einschlägige Krisenmechanismen auf Unionsebene

Mechanismus	Horizontal/Sektoral/Cyberspezifisch	Beschreibung	Verweis
ARGUS	Horizontal	Ermöglicht der Kommission den Austausch einschlägiger Informationen über neu auftretende sektorübergreifende Krisen und über	Mitteilung der Kommission COM(2005) 662

Mechanismus	Horizontal/Sektoral/Cyberspezifisch	Beschreibung	Verweis
		absehbare oder unmittelbar bevorstehende Bedrohungen, die Maßnahmen auf Unionsebene erfordern.	
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 und Lageerfassung und stützt sich dabei auf engagierte Fachkräfte vor Ort in den Delegationen der Union.	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)
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 (Cybersolidaritätsverordnung) (ABl. L, 15.1.2025)
Instrumentarium für die Cyberdiplomatie (Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten)	Cyberspezifisch	Gewährleistet die gemeinsame diplomatische Reaktion der Union auf böswillige Cyberaktivitäten und trägt zur Konfliktverhütung, zur Eindämmung von Cybersicherheits-bedrohungen und zu größerer Stabilität in den internationalen Beziehungen bei.	Schlussfolgerungen des Rates vom 19. Juni 2017 Überarbeitete Umsetzungsleitlinien, Dok. 10289/23, 8.6.2023

Mechanismus	Horizontal/Sektoral/Cyberspezifisch	Beschreibung	Verweis
Europäische Cyberreserve	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
Netzkodex mit sektorspezifischen Regeln für Cybersicherheitsaspekte bei grenzübergreifenden Stromflüssen	Sektoral	Sieht ein regelmäßig anzuwendendes Verfahren zur Bewertung von Cybersicherheitsrisiken im Elektrizitätssektor vor, enthält besondere Bestimmungen für das Krisenmanagement und Verbindungen zum CSIRTs-Netzwerk und zu EU-CyCLONe.	Delegierte Verordnung (EU) 2024/1366 der Kommission
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 von 2022 zur EU-Cyberabwehrpolitik
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
Teams für die rasche Reaktion auf hybride Bedrohungen	Horizontal	Als Teil des EU-Instrumentariums zur Abwehr hybrider Bedrohungen greifen die EU-Teams für die rasche Reaktion auf hybride Bedrohungen	Orientierungsrahmen für die praktische Einrichtung der EU-Teams für die rasche

Mechanismus	Horizontal/Sektoral/Cyberspezifisch	Beschreibung	Verweis
(EU HRRTs)		auf einschlägige sektorspezifische zivile und militärische Sachkenntnis auf nationaler 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.	Reaktion auf hybride Bedrohungen (21. Mai 2024)
IPCR	Horizontal	Unterstützt eine rasche und koordinierte Beschlussfassung auf politischer Ebene der Union in Bezug auf schwere und komplexe Krisen, einschließlich Terroranschlägen. Der Beschluss über die Aktivierung und Deaktivierung wird vom Vorsitz des Rates gefasst, der die betroffenen Mitgliedstaaten, die Kommission und die Hohe Vertreterin 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 im Informationsaustausch-Modus zu aktivieren. Die Diskussionen stützen sich auf den ISAA-Bericht, der von den Kommissionsdienststellen und dem EAD erstellt wird. Der Bericht basiert auch auf relevanten Informationen und Auswertungen, die von den Mitgliedstaaten (z. B. den einschlägigen nationalen Krisenzentren) insbesondere über die Internet-Plattform und von Unionsagenturen bereitgestellt werden.	Durchführungsbeschluss (EU) 2018/1993 des Rates

Mechanismus	Horizontal/Sektoral/Cyberspezifisch	Beschreibung	Verweis
EU-Notfallprotokoll für die Strafverfolgung	Horizontal	Ein Hilfsmittel 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 auf große Cybersicherheits-vorfälle und -krisen
Teams für die rasche Reaktion auf Cybervorfälle (CRRTs) im Rahmen der SSZ	Cyberspezifisch	Einsatz spezialisierter Teams zur raschen Reaktion auf schwerwiegende Cybersicherheitsvorfälle und zur Durchführung von Präventivmaßnahmen wie z. B. Schwachstellenbeurteilungen und Wahlbeobachtung. Initiative der Mitgliedstaaten, die teilweise aus der Fazilität „Connecting Europe“ finanziert wird.	Artikel 42 Absatz 6, Artikel 46 und Protokoll 10 des Vertrags über die Europäische Union
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 von der Hohen Vertreterin 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
Koordinierungs-rahmen für betreffende Behörden in Bezug auf systemische Cybersicherheits-vorfälle (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,	Empfehlung des Europäischen Ausschusses für Systemrisiken vom 2. Dezember 2021 zu einem europaweiten Koordinierungsrahmen für betreffende Behörden in Bezug auf systemische

Mechanismus	Horizontal/Sektoral/Cyberspezifisch	Beschreibung	Verweis
		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.	Cybersicherheits-vorfälle (ESRB/2021/17)
Katastrophen-schutzverfahren der Union (UCPM)	Horizontal	Gewährleistet die Zusammenarbeit im Katastrophenschutz, um die Katastrophenprävention, -vorsorge und -bewältigung zu verbessern.	Beschluss Nr. 1313/2013/EU
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
Finanzmarktinfra-strukturen		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)
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
Abfallbewirtschaf-tung		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 3 – GRUNDSÄTZE

Die im Konzeptentwurf für die Cybersicherheit von 2017 dargelegten Grundsätze sind nach wie vor relevant.

Verhältnismäßigkeit: Die meisten Cybersicherheitsvorfälle, die die Mitgliedstaaten betreffen, sind nicht so schwerwiegend, dass sie als Krise auf nationaler Ebene oder Unionsebene angesehen werden könnten. Bei Cybersicherheitsvorfällen arbeiten die Mitgliedstaaten im Rahmen des CSIRTs-Netzwerks und von EU-CyCLONe im Einklang mit ihren jeweiligen Verfahren zusammen.

Subsidiarität: Bei Cybersicherheitsvorfällen oder -krisen großen Ausmaßes sind in erster Linie die betroffenen Mitgliedstaaten für die Reaktion zuständig. Die Kommission, der Europäische Auswärtige Dienst, die ENISA, das CERT-EU, Europol und alle anderen einschlägigen Einrichtungen der Union spielen während des gesamten Krisenzyklus eine wichtige Rolle. Diese Rolle ist in der IPCR-Regelung definiert, leitet sich aber auch aus dem Unionsrecht ab und spiegelt wider, in welchem Umfang Cybersicherheitsvorfälle und -krisen einen oder mehr Wirtschaftssektoren im Binnenmarkt, die Sicherheit und die internationalen Beziehungen der Union oder auch die Organe selbst treffen.

Komplementarität: Diese Empfehlung trägt den auf Unionsebene bestehenden Krisenmanagementmechanismen, insbesondere der IPCR-Regelung, ARGUS und dem Krisenreaktionsmechanismus des EAD, in vollem Umfang Rechnung. Sie berücksichtigt die veränderten Rollen des CSIRTs-Netzwerks und von EU-CyCLONe gemäß den seit 2017 angenommenen Vorschriften zur größtmöglichen Ausschöpfung von Synergien und zur Minimierung von Doppelarbeit sowie die Annahme des EU-Notfallprotokolls für die Strafverfolgung.

Vertraulichkeit von Informationen: Der gesamte Informationsaustausch im Rahmen dieser Empfehlung muss mit den geltenden Sicherheits- und Datenschutzvorschriften sowie mit dem „Traffic Light Protocol“-System für die Klassifizierung vertraulicher Informationen im Einklang stehen. Für den Austausch von Verschlusssachen sollten unabhängig von der angewandten Klassifizierungsregelung die verfügbaren akkreditierten Instrumente verwendet werden. In Bezug auf die Verarbeitung personenbezogener Daten sind die anwendbaren Unionsvorschriften einzuhalten, insbesondere die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[1], die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates[2] und die Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates[3].

---

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

2 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

3 Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).