Europäisches Parlament
2019-2024

Ausschuss für auswärtige Angelegenheiten

2023/0109(COD)

27.10.2023

STELLUNGNAHME

des Ausschusses für auswärtige Angelegenheiten

für den Ausschuss für Industrie, Forschung und Energie

zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Verfasser der Stellungnahme: Dragoş Tudorache

PA_Legapp

Änderungsantrag 1

Vorschlag für eine Verordnung
Erwägung 1

Vorschlag der Kommission	*Geänderter Text*
(1) Die Nutzung und Abhängigkeit von Informations- und Kommunikationstechnologien sind von grundlegender Bedeutung in allen Wirtschaftssektoren, da öffentliche Verwaltungen, Unternehmen und Bürger stärker als je zuvor branchen- und grenzübergreifend miteinander vernetzt und voneinander abhängig sind.	(1) Die Nutzung und Abhängigkeit von Informations- und Kommunikationstechnologien sind von grundlegender Bedeutung in allen Wirtschaftssektoren ***sowie im Militärbereich***, da öffentliche Verwaltungen, Unternehmen und Bürger ***sowie Akteure im Militär- und Verteidigungsbereich*** stärker als je zuvor branchen- und grenzübergreifend miteinander vernetzt und voneinander abhängig sind.

Änderungsantrag 2

Vorschlag für eine Verordnung
Erwägung 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die Tragweite, die Häufigkeit und die Auswirkungen von Cybersicherheitsvorfällen nehmen zu, was auch Cyberangriffe im Zusammenhang mit Cyberspionage, Ransomware oder Störungen einschließt. Sie stellen eine große Bedrohung für das Funktionieren von Netz- und Informationssystemen dar. Angesichts der sich wandelnden Bedrohungslandschaft ist wegen der Gefahr von Vorfällen großen Ausmaßes, die erhebliche Störungen oder Schäden an kritischen Infrastrukturen verursachen, eine erhöhte Abwehrbereitschaft auf allen Ebenen des Cybersicherheitsrahmens der Union erforderlich. ***Diese Bedrohung geht*** über die militärische Aggression Russlands gegen die Ukraine hinaus und ***wird*** angesichts der Vielzahl staatsnaher, krimineller und hacktivistischer Akteure, die an den derzeitigen geopolitischen	(2) Die Tragweite, die Häufigkeit und die Auswirkungen von Cybersicherheitsvorfällen nehmen zu, was auch Cyberangriffe im Zusammenhang mit Cyberspionage, Ransomware oder Störungen einschließt. Sie stellen eine große Bedrohung für das Funktionieren von Netz- und Informationssystemen dar. Angesichts der sich wandelnden Bedrohungslandschaft ist wegen der Gefahr von Vorfällen großen Ausmaßes, die erhebliche Störungen oder Schäden an kritischen Infrastrukturen verursachen, eine erhöhte Abwehrbereitschaft auf allen Ebenen des Cybersicherheitsrahmens der Union erforderlich. ***Mit der Rückkehr des Kriegs auf unseren Kontinent ist der Ernst dieser Bedrohungen noch deutlicher geworden. Diese Bedrohungen gehen*** über die militärische Aggression Russlands gegen die Ukraine hinaus und

Spannungen beteiligt sind, wahrscheinlich andauern. Solche Vorfälle können – auch in kritischen oder hochkritischen Sektoren – die Erbringung öffentlicher Dienstleistungen und die Ausübung wirtschaftlicher Tätigkeiten beeinträchtigen, erhebliche finanzielle Verluste verursachen, das Vertrauen der Nutzer untergraben und der Wirtschaft der Union schweren Schaden zufügen und sogar gesundheitliche oder lebensbedrohliche Folgen haben. Darüber hinaus sind Cybersicherheitsvorfälle unvorhersehbar, da sie oft innerhalb sehr kurzer Zeiträume auftreten und sich fortentwickeln, nicht auf ein bestimmtes geografisches Gebiet beschränkt sind, sondern sich gleichzeitig in vielen Ländern ereignen oder sich rasch in andere Länder ausbreiten können.	***werden*** angesichts der Vielzahl staatsnaher, krimineller und hacktivistischer Akteure, die an den derzeitigen geopolitischen Spannungen beteiligt sind, wahrscheinlich andauern. Solche Vorfälle können – auch in kritischen oder hochkritischen Sektoren – die Erbringung öffentlicher Dienstleistungen und die Ausübung wirtschaftlicher Tätigkeiten beeinträchtigen, erhebliche finanzielle Verluste verursachen, das Vertrauen der Nutzer untergraben und der Wirtschaft ***und der Sicherheit*** der Union schweren Schaden zufügen und sogar gesundheitliche oder lebensbedrohliche Folgen haben***, indem lokale oder nationale sicherheitsrelevante Anlagen beeinträchtigt werden können***. Darüber hinaus sind Cybersicherheitsvorfälle unvorhersehbar, da sie oft innerhalb sehr kurzer Zeiträume auftreten und sich fortentwickeln, nicht auf ein bestimmtes geografisches Gebiet beschränkt sind, sondern sich gleichzeitig in vielen Ländern ereignen oder sich rasch in andere Länder ausbreiten können. ***Cybersicherheit ist wichtig für den Schutz unserer europäischen Werte und gewährleistet das Funktionieren unserer Demokratie, indem unsere Wahlinfrastruktur und demokratischen Verfahren vor ausländischer Einflussnahme geschützt werden.***

Änderungsantrag 3

Vorschlag für eine Verordnung
Erwägung 2 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(2a) Cybersicherheit ist ein wesentliches Instrument zum Schutz unserer Union, mit dem – staatliche oder private – böswillige Akteure davon abgehalten werden sollen, unserer Demokratie, unserer Wirtschaft und

	unserer Sicherheit zu schaden. Es ist jedoch notwendig, eine fragmentierte Landschaft zu vermeiden, da eine solche Situation keinen angemessenen Ansatz bieten würde, insbesondere mit Blick auf die Herausforderung künftiger Cyberangriffe großen Ausmaßes, die gleichzeitig mehrere Mitgliedstaaten oder länderübergreifende kritische Infrastrukturen betreffen. Deshalb ist eine Einrichtung der EU erforderlich, die als Koordinierungsplattform für alle bestehenden und künftigen Instrumente, Fonds und Mechanismen im Bereich Cybersicherheit fungiert.

Änderungsantrag 4

Vorschlag für eine Verordnung
Erwägung 3

Vorschlag der Kommission	*Geänderter Text*
(3) Es ist notwendig, die Wettbewerbsposition der Industrie- und Dienstleistungssektoren in der Union in der gesamten digitalisierten Wirtschaft zu stärken und ihren digitalen Wandel zu unterstützen, indem das Cybersicherheitsniveau im digitalen Binnenmarkt erhöht wird. Wie in drei verschiedenen Vorschlägen der Konferenz zur Zukunft Europas[16] empfohlen, muss die Resilienz der Bürgerinnen und Bürger und der Unternehmen und Einrichtungen, die kritische Infrastrukturen betreiben, gegenüber den zunehmenden Cybersicherheitsbedrohungen, die verheerende gesellschaftliche und wirtschaftliche Auswirkungen haben können, erhöht werden. Daher sind Investitionen in Infrastrukturen und Dienste erforderlich, die eine schnellere Erkennung von Cybersicherheitsbedrohungen und -vorfällen und eine schnellere Reaktion darauf unterstützen, und die Mitgliedstaaten benötigen Unterstützung	(3) Es ist notwendig, die Wettbewerbsposition der Industrie- und Dienstleistungssektoren in der Union in der gesamten digitalisierten Wirtschaft zu stärken und ihren digitalen Wandel zu unterstützen, indem das Cybersicherheitsniveau im digitalen Binnenmarkt erhöht wird. Wie in drei verschiedenen Vorschlägen der Konferenz zur Zukunft Europas[16] empfohlen, muss die Resilienz der Bürgerinnen und Bürger und der Unternehmen und Einrichtungen, die kritische Infrastrukturen betreiben, gegenüber den zunehmenden Cybersicherheitsbedrohungen, die verheerende gesellschaftliche und wirtschaftliche Auswirkungen haben können, erhöht werden. Daher sind Investitionen in Infrastrukturen und Dienste erforderlich, die eine schnellere Erkennung von Cybersicherheitsbedrohungen und -vorfällen und eine schnellere Reaktion darauf unterstützen, und die Mitgliedstaaten benötigen Unterstützung

zur Verbesserung der Vorsorgemaßnahmen und der Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes. Auch die Union sollte ihre Kapazitäten in diesen Bereichen ausbauen, insbesondere in Bezug auf die Erhebung und Analyse von Daten über Cybersicherheitsbedrohungen und -vorfälle.

zur Verbesserung der Vorsorgemaßnahmen und der Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes. Auch die Union sollte ihre Kapazitäten in diesen Bereichen ausbauen, insbesondere in Bezug auf die Erhebung und Analyse von Daten über Cybersicherheitsbedrohungen und -vorfälle ***sowie in Bezug auf ihre Fähigkeit, vorausschauend zu handeln und bei Cybersicherheitsbedrohungen und -vorfällen entschlossen zu reagieren***.

[16] https://futureu.europa.eu/de/

[16] https://futureu.europa.eu/de/

Änderungsantrag 5

Vorschlag für eine Verordnung
Erwägung 4

Vorschlag der Kommission

(4) Die Union hat bereits eine Reihe von Rechtsakten erlassen, um Sicherheitslücken zu verringern und die Resilienz kritischer Infrastrukturen und Einrichtungen gegenüber Cybersicherheitsrisiken zu erhöhen, darunter insbesondere die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates[17], die Empfehlung (EU) 2017/1584 der Kommission[18], die Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates[19] und die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates[20]. Ferner wurden die Mitgliedstaaten in der Empfehlung des Rates für eine unionsweite koordinierte Vorgehensweise zur Stärkung der Resilienz kritischer Infrastruktur aufgefordert, unverzüglich wirksame Maßnahmen zu ergreifen und loyal, effizient, solidarisch und in koordinierter Weise mit der Kommission und anderen einschlägigen Behörden sowie den betreffenden Einrichtungen

Geänderter Text

(4) Die Union hat bereits eine Reihe von Rechtsakten erlassen, um Sicherheitslücken zu verringern und die Resilienz kritischer Infrastrukturen und Einrichtungen gegenüber Cybersicherheitsrisiken zu erhöhen, darunter insbesondere die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates[17], die Empfehlung (EU) 2017/1584 der Kommission[18], die Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates[19] und die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates[20]. Ferner wurden die Mitgliedstaaten in der Empfehlung des Rates für eine unionsweite koordinierte Vorgehensweise zur Stärkung der Resilienz kritischer Infrastruktur aufgefordert, unverzüglich wirksame Maßnahmen zu ergreifen und loyal, effizient, ***proaktiv,*** solidarisch und in koordinierter Weise mit der Kommission und anderen einschlägigen Behörden sowie den betreffenden Einrichtungen

zusammenzuarbeiten, um die Resilienz kritischer Infrastrukturen, die für die Erbringung wesentlicher Dienste im Binnenmarkt genutzt werden, zu erhöhen.

zusammenzuarbeiten, um die Resilienz kritischer Infrastrukturen, die für die Erbringung wesentlicher Dienste im Binnenmarkt genutzt werden, zu erhöhen. ***Des Weiteren hat die Union im März 2022 ihren Strategischen Kompass für Sicherheit und Verteidigung angenommen und auf den Weg gebracht, bei dem unter anderem die Stärkung der Cybersicherheit und eine Verbesserung der internationalen Zusammenarbeit mit gleichgesinnten Verbündeten und demokratischen Partnern, insbesondere in diesem Bereich, im Mittelpunkt stehen. Darüber hinaus bildet die Cybersicherheit einen Schwerpunkt in der jüngsten dritten gemeinsamen Erklärung zur Zusammenarbeit zwischen der EU und der NATO von Januar 2023. Insbesondere enthielt der abschließende Beurteilungsbericht der EU-NATO-Taskforce die Empfehlung, Synergien zwischen der EU und der NATO[1] in vollem Umfang zu nutzen, z. B. in Form eines Austauschs bewährter Verfahren zwischen zivilen und militärischen Akteuren, was die Umsetzung einschlägiger politischer Strategien und Rechtsvorschriften im Cyberbereich anbelangt.***

[1] https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_en

---

[17] 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 (ABl. L 333 vom 27.12.2022, S. 80).

[18] Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für

[17] 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 (ABl. L 333 vom 27.12.2022, S. 80).

[18] 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).

[19] 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).

[20] 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).

eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (ABl. L 239 vom 19.9.2017, S. 36).

[19] 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).

[20] 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).

Änderungsantrag 6

Vorschlag für eine Verordnung
Erwägung 6

Vorschlag der Kommission	*Geänderter Text*
(6) In der am 10. November 2022 angenommenen Gemeinsamen Mitteilung über die EU-Cyberabwehrpolitik[22] wurde eine EU-Initiative zur Cybersolidarität mit folgenden Zielen angekündigt: Stärkung der gemeinsamen Fähigkeiten der EU zur Erkennung, Lageerfassung und Bewältigung durch Förderung des Aufbaus einer EU-Infrastruktur von Sicherheitseinsatzzentren (SOCs), Unterstützung des schrittweisen Aufbaus einer Cybersicherheitsreserve auf EU-Ebene mit Diensten vertrauenswürdiger privater Anbieter und Prüfung von kritischen Einrichtungen auf potenzielle Schwachstellen auf der Grundlage von EU-Risikobewertungen.	(6) In der am 10. November 2022 angenommenen Gemeinsamen Mitteilung über die EU-Cyberabwehrpolitik[22] wurde eine EU-Initiative zur Cybersolidarität mit folgenden Zielen angekündigt: Stärkung der gemeinsamen Fähigkeiten der EU zur Erkennung, Lageerfassung und Bewältigung durch Förderung des Aufbaus einer EU-Infrastruktur von Sicherheitseinsatzzentren (SOCs), Unterstützung des schrittweisen Aufbaus einer Cybersicherheitsreserve auf EU-Ebene mit Diensten vertrauenswürdiger privater Anbieter und Prüfung von kritischen Einrichtungen auf potenzielle Schwachstellen auf der Grundlage von EU-Risikobewertungen. ***Darüber hinaus zeigen die sich rasch verändernde Cyberbedrohungslandschaft und die***

	Geschwindigkeit der technologischen Entwicklung den Schlussfolgerungen des Rates zur Cyberabwehrpolitik der EU[1] zufolge auch, dass die Koordinierung und Zusammenarbeit zwischen zivilen und militärischen Stellen verstärkt werden muss.
	[1] Schlussfolgerungen des Rates zur Cyberabwehrpolitik der EU, die der Rat auf seiner Tagung vom 22. Mai 2023 gebilligt hat, Dok. 9618/23.
[22] Gemeinsame Mitteilung an das Europäische Parlament und den Rat – EU-Cyberabwehrpolitik, JOIN(2022) 49 final.	[22] Gemeinsame Mitteilung an das Europäische Parlament und den Rat – EU-Cyberabwehrpolitik, JOIN(2022) 49 final.

Änderungsantrag 7

Vorschlag für eine Verordnung
Erwägung 6 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(6a) Angesichts der verschwimmenden Grenzen zwischen zivilen und militärischen Angelegenheiten und des doppelten Verwendungszwecks von Cyberinstrumenten und -technologien bedarf es eines umfassenden und ganzheitlichen Konzepts für den Digitalbereich. Im Falle von Cybersicherheitsvorfällen und -krisen großen Ausmaßes, von denen mehr als ein Mitgliedstaat betroffen ist, sollte eine angemessene Krisenbewältigung und -steuerung eingerichtet werden. Diese Strukturen sollten den Austausch von Informationen, die Koordinierung und Zusammenarbeit mit den Strukturen der Union im Bereich der äußeren Sicherheit und der militärischen Krisenbewältigung sowie den für die Sicherheit und Verteidigung zuständigen Stellen der Mitgliedstaaten (Cyberabwehrgemeinschaft der EU) organisieren. Dies sollte auch für

	Missionen und Operationen im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik gelten, die von der Union durchgeführt werden, um in ihrer Nachbarschaft und darüber hinaus für Frieden und Stabilität zu sorgen.

Änderungsantrag 8

Vorschlag für eine Verordnung
Erwägung 7

Vorschlag der Kommission	*Geänderter Text*
(7) Es ist notwendig, in der gesamten Union sowohl die Erkennung und Lageerfassung im Bereich der Cyberbedrohungen und -vorfälle als auch die Solidarität zu stärken, indem die Abwehrbereitschaft und die Fähigkeiten der Mitgliedstaaten und der Union zur Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes verbessert werden. Daher sollte eine europaweite Infrastruktur von Sicherheitseinsatzzentren („europäischer Cyberschutzschild“) aufgebaut werden, um gemeinsame Fähigkeiten zur Erkennung und Lageerfassung aufzubauen und zu verbessern; ein Cybernotfallmechanismus sollte eingerichtet werden, um die Mitgliedstaaten bei der Vorsorge für, der Bewältigung von und der sofortigen Wiederherstellung nach schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes zu unterstützen; ferner sollte ein Überprüfungsmechanismus für Cybersicherheitsvorfälle eingerichtet werden, um bestimmte schwerwiegende Cybersicherheitsvorfälle bzw. Cybersicherheitsvorfälle großen Ausmaßes zu überprüfen und zu bewerten. Diese Maßnahmen lassen Artikel 107 und 108 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) unberührt.	(7) Es ist notwendig, in der gesamten Union sowohl die Erkennung und Lageerfassung im Bereich der Cyberbedrohungen und -vorfälle als auch die Solidarität zu stärken, indem die Abwehrbereitschaft und die Fähigkeiten der Mitgliedstaaten und der Union zur Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes verbessert werden. Daher sollte eine europaweite Infrastruktur von Sicherheitseinsatzzentren („europäischer Cyberschutzschild“) aufgebaut werden, um gemeinsame Fähigkeiten zur Erkennung und Lageerfassung aufzubauen und zu verbessern; ein Cybernotfallmechanismus sollte eingerichtet werden, um die Mitgliedstaaten bei der Vorsorge für, der Bewältigung von und der sofortigen Wiederherstellung nach schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes***, einschließlich Vorfällen, die mehrere Mitgliedstaaten betreffen,*** zu unterstützen; ***sofern machbar und notwendig, sollten der Informationsaustausch und die Zusammenarbeit mit den Verteidigungsbehörden der Mitgliedstaaten über einen Cybernotfallmechanismus erfolgen, der von den Organen, Einrichtungen und sonstigen Stellen***

(Cyberabwehrgemeinschaft der EU) unterstützt wird; ferner sollte ein Überprüfungsmechanismus für Cybersicherheitsvorfälle eingerichtet werden, um bestimmte schwerwiegende Cybersicherheitsvorfälle bzw. Cybersicherheitsvorfälle großen Ausmaßes zu überprüfen und zu bewerten. ***Durch diese neuen Strukturen sollten auch die GSVP-Missionen und -Operationen der EU unterstützt werden.*** Diese Maßnahmen lassen Artikel 107 und 108 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) unberührt.

Änderungsantrag 9

Vorschlag für eine Verordnung
Erwägung 11

Vorschlag der Kommission	*Geänderter Text*
(11) Um eine wirtschaftliche Haushaltsführung zu gewährleisten, sollten spezifische Vorschriften für die Übertragung nicht in Anspruch genommener Verpflichtungs- und Zahlungsermächtigungen festgelegt werden. Unter Wahrung des Grundsatzes der Jährlichkeit des Unionshaushalts sollten in dieser Verordnung angesichts des unvorhersehbaren, außergewöhnlichen und besonderen Charakters der Cybersicherheitslandschaft über die in der Haushaltsordnung festgelegten Möglichkeiten hinaus weitere Möglichkeiten vorgesehen werden, nicht verwendete Mittel zu übertragen und so die Fähigkeit des Cybernotfallmechanismus zur Unterstützung der Mitgliedstaaten bei der wirksamen Abwehr von Cyberbedrohungen zu maximieren.	(11) Um eine wirtschaftliche Haushaltsführung zu gewährleisten, sollten spezifische Vorschriften für die Übertragung nicht in Anspruch genommener Verpflichtungs- und Zahlungsermächtigungen festgelegt werden. Unter Wahrung des Grundsatzes der Jährlichkeit des Unionshaushalts sollten in dieser Verordnung angesichts des unvorhersehbaren, außergewöhnlichen und besonderen Charakters der Cybersicherheitslandschaft über die in der Haushaltsordnung festgelegten Möglichkeiten hinaus weitere Möglichkeiten vorgesehen werden, nicht verwendete Mittel zu übertragen und so die Fähigkeit des Cybernotfallmechanismus zur Unterstützung der Mitgliedstaaten bei der wirksamen Abwehr von Cyberbedrohungen zu maximieren. ***Durch diese spezifischen Vorschriften würde zudem eine längerfristige finanzielle Unterstützung für die gemeinsame Beschaffung ultrasicherer Instrumente und Infrastrukturen der nächsten Generation ermöglicht, um die kollektiven***

	Erkennungsfähigkeiten durch den Einsatz der neuesten künstlichen Intelligenz (KI) und von Datenanalysen zu verbessern.

Änderungsantrag 10

Vorschlag für eine Verordnung
Erwägung 13

Vorschlag der Kommission	*Geänderter Text*
(13) Jeder Mitgliedstaat sollte auf nationaler Ebene eine öffentliche Stelle benennen, die mit der Koordinierung von Tätigkeiten zur Erkennung von Cyberbedrohungen in diesem Mitgliedstaat betraut ist. Diese nationalen SOCs sollten auf nationaler Ebene als Bezugspunkt und Zugangstor für die Beteiligung am Europäischen Cyberschutzschild fungieren und sicherstellen, dass Informationen über Cyberbedrohungen von öffentlichen und privaten Einrichtungen auf nationaler Ebene wirksam und effizient ausgetauscht und gesammelt werden.	(13) Jeder Mitgliedstaat sollte auf nationaler Ebene eine öffentliche Stelle benennen, die mit der Koordinierung von Tätigkeiten zur Erkennung von Cyberbedrohungen in diesem Mitgliedstaat betraut ist. Diese nationalen SOCs sollten auf nationaler Ebene als Bezugspunkt und Zugangstor für die Beteiligung am Europäischen Cyberschutzschild fungieren und sicherstellen, dass Informationen über Cyberbedrohungen von öffentlichen und privaten Einrichtungen auf nationaler Ebene wirksam und effizient ausgetauscht und gesammelt werden. ***Wie in der Gemeinsamen Mitteilung über die EU-Cyberabwehrpolitik[1] dargelegt und vom Hohen Vertreter unterstützt, sollte durch die SOCs, sofern machbar und erforderlich, auch die Beteiligung des Verteidigungsbereichs ermöglicht werden, indem mit Blick auf die Governance und die Art der ausgetauschten Informationen eine „Verteidigungssäule“ eingerichtet wird.*** ***[1] Gemeinsame Mitteilung an das Europäische Parlament und den Rat – EU-Cyberabwehrpolitik, JOIN(2022) 49 final.***

Änderungsantrag 11

Vorschlag für eine Verordnung
Erwägung 14

Vorschlag der Kommission	*Geänderter Text*
(14) Im Rahmen des europäischen Cyberschutzschilds sollte eine Reihe grenzübergreifender Cybersicherheitseinsatzzentren („grenzübergreifende SOCs“) eingerichtet werden. Darin sollten sich nationale SOCs aus mindestens drei Mitgliedstaaten zusammenfinden, damit die Vorteile der grenzübergreifenden Erkennung von Bedrohungen sowie des Informationsaustauschs und -managements voll ausgeschöpft werden können. Das allgemeine Ziel grenzübergreifender SOCs sollte darin bestehen, die Kapazitäten zur Analyse, Verhütung und Erkennung von Cybersicherheitsbedrohungen zu stärken und die Gewinnung hochwertiger Erkenntnisse über Cybersicherheitsbedrohungen zu unterstützen, insbesondere durch den Austausch von Daten aus verschiedenen öffentlichen oder privaten Quellen sowie durch die Weitergabe und die gemeinsame Nutzung modernster Instrumente und die gemeinsame Entwicklung von Erkennungs-, Analyse- und Präventionsfähigkeiten in einem vertrauenswürdigen Umfeld. Sie sollten neue zusätzliche Kapazitäten bereitstellen, die auf bestehenden SOCs und Computer-Notfallteams (CSIRTs) und anderen einschlägigen Akteuren aufbauen und diese ergänzen.	(14) Im Rahmen des europäischen Cyberschutzschilds sollte eine Reihe grenzübergreifender Cybersicherheitseinsatzzentren („grenzübergreifende SOCs“) eingerichtet werden. Darin sollten sich nationale SOCs aus mindestens drei Mitgliedstaaten, ***darunter eine „Verteidigungssäule“,*** zusammenfinden, damit die Vorteile der grenzübergreifenden Erkennung von Bedrohungen sowie des Informationsaustauschs und -managements voll ausgeschöpft werden können. Das allgemeine Ziel grenzübergreifender SOCs sollte darin bestehen, die Kapazitäten zur Analyse, Verhütung und Erkennung von Cybersicherheitsbedrohungen zu stärken und die Gewinnung hochwertiger Erkenntnisse über Cybersicherheitsbedrohungen zu unterstützen, insbesondere durch den Austausch von Daten aus verschiedenen öffentlichen oder privaten ***sowie – sofern erforderlich und machbar, und mit ausreichenden Leitlinien für den Informationsaustausch – militärischen*** Quellen sowie durch die Weitergabe und die gemeinsame Nutzung modernster Instrumente und die gemeinsame Entwicklung von Erkennungs-, Analyse- und Präventionsfähigkeiten in einem vertrauenswürdigen Umfeld. Sie sollten neue zusätzliche Kapazitäten bereitstellen, die auf bestehenden SOCs und Computer-Notfallteams (CSIRTs) und anderen einschlägigen Akteuren aufbauen und diese ergänzen.

Änderungsantrag 12

Vorschlag für eine Verordnung
Erwägung 15

Vorschlag der Kommission	*Geänderter Text*
(15) Auf nationaler Ebene wird die Überwachung, Erkennung und Analyse von Cyberbedrohungen in der Regel durch SOCs öffentlicher und privater Einrichtungen in Kombination mit CSIRTs sichergestellt. Darüber hinaus tauschen die CSIRTs im Rahmen des CSIRT-Netzes Informationen gemäß der Richtlinie (EU) 2022/2555 aus. Die grenzübergreifenden SOCs-Plattformen sollten eine neue Kapazität bilden, die das CSIRTs-Netz ergänzt, indem sie Daten über Bedrohungen der Cybersicherheit von öffentlichen und privaten Einrichtungen zusammenführen und weitergeben, den Wert solcher Daten durch Expertenanalysen, gemeinsam beschaffte Infrastrukturen und modernste Instrumente steigern und zur Entwicklung der Fähigkeiten und ***technologischen Souveränität*** der Union beitragen.	(15) Auf nationaler Ebene wird die Überwachung, Erkennung und Analyse von Cyberbedrohungen in der Regel durch SOCs öffentlicher und privater Einrichtungen in Kombination mit CSIRTs sichergestellt. Darüber hinaus tauschen die CSIRTs im Rahmen des CSIRT-Netzes Informationen gemäß der Richtlinie (EU) 2022/2555 aus. Die grenzübergreifenden SOCs-Plattformen sollten eine neue Kapazität bilden, die das CSIRTs-Netz ergänzt, indem sie Daten über Bedrohungen der Cybersicherheit von öffentlichen und privaten Einrichtungen zusammenführen und weitergeben, den Wert solcher Daten durch Expertenanalysen, gemeinsam beschaffte Infrastrukturen und modernste Instrumente steigern und zur Entwicklung der Fähigkeiten und ***der Resilienz*** der Union beitragen.

Änderungsantrag 13

Vorschlag für eine Verordnung
Erwägung 16

Vorschlag der Kommission	*Geänderter Text*
(16) Die grenzübergreifenden SOCs sollten als zentrale Stelle fungieren, die eine umfassende Zusammenführung einschlägiger Daten und Erkenntnisse über Cyberbedrohungen und die Verbreitung von Informationen über Bedrohungen in einer großen und vielfältigen Gruppe von Akteuren ermöglicht (z. B. Soforteinsatzteams für IT-Sicherheitsvorfälle (CERTs), CSIRTs, Informationsaustausch- und -analysezentren (ISACs), Betreiber kritischer Infrastrukturen). Der Informationsaustausch zwischen den Teilnehmern eines grenzübergreifenden SOC könnte Daten von Netzwerken und	(16) Die grenzübergreifenden SOCs sollten als zentrale Stelle fungieren, die eine umfassende Zusammenführung einschlägiger Daten und Erkenntnisse über Cyberbedrohungen und die Verbreitung von Informationen über Bedrohungen in einer großen und vielfältigen Gruppe von Akteuren ermöglicht (z. B. Soforteinsatzteams für IT-Sicherheitsvorfälle (CERTs), CSIRTs, Informationsaustausch- und -analysezentren (ISACs), Betreiber kritischer Infrastrukturen ***sowie die Cyberabwehrgemeinschaft***). Der Informationsaustausch zwischen den Teilnehmern eines grenzübergreifenden

Sensoren sowie laufende Erkenntnisse über Bedrohungen, Kompromittierungsindikatoren und kontextualisierte Informationen über Vorfälle, Bedrohungen und Schwachstellen umfassen. Darüber hinaus sollten die grenzübergreifenden SOCs auch Kooperationsvereinbarungen mit anderen grenzübergreifenden SOCs schließen.	SOC könnte Daten von Netzwerken und Sensoren sowie laufende Erkenntnisse über Bedrohungen, Kompromittierungsindikatoren und kontextualisierte Informationen über Vorfälle, Bedrohungen und Schwachstellen umfassen. Darüber hinaus sollten die grenzübergreifenden SOCs auch Kooperationsvereinbarungen mit anderen grenzübergreifenden SOCs ***sowie mit dem noch einzurichtenden operativen Netz für milCERT (MICNET)*** schließen.

Änderungsantrag 14

Vorschlag für eine Verordnung
Erwägung 17

Vorschlag der Kommission	*Geänderter Text*
(17) Die gemeinsame Lageerfassung unter den zuständigen Behörden ist eine unabdingbare Voraussetzung für die unionsweite Abwehrbereitschaft und Koordinierung in Bezug auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes. Zur Unterstützung des koordinierten Managements von Cybersicherheitsvorfällen großen Ausmaßes und Cyberkrisen auf operativer Ebene und zur Gewährleistung eines regelmäßigen Austauschs relevanter Informationen zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union wird mit der Richtlinie (EU) 2022/2555 das EU-CyCLONe-Netz eingerichtet. Die Empfehlung (EU) 2017/1584 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen befasst sich mit der Rolle aller einschlägigen Akteure. In der Richtlinie (EU) 2022/2555 wird auch auf die Zuständigkeiten der Kommission im Rahmen des mit dem Beschluss Nr. 1313/2013/EU des Europäischen	(17) Die gemeinsame Lageerfassung unter den zuständigen Behörden ist eine unabdingbare Voraussetzung für die unionsweite Abwehrbereitschaft und Koordinierung in Bezug auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes. Zur Unterstützung des koordinierten Managements von Cybersicherheitsvorfällen großen Ausmaßes und Cyberkrisen auf operativer Ebene und zur Gewährleistung eines regelmäßigen Austauschs relevanter Informationen zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union wird mit der Richtlinie (EU) 2022/2555 das EU-CyCLONe-Netz eingerichtet. Die Empfehlung (EU) 2017/1584 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen befasst sich mit der Rolle aller einschlägigen Akteure. In der Richtlinie (EU) 2022/2555 wird auch auf die Zuständigkeiten der Kommission im Rahmen des mit dem Beschluss Nr. 1313/2013/EU des Europäischen

Parlaments und des Rates eingerichteten Katastrophenschutzverfahrens der Union (UCPM) sowie für die Bereitstellung analytischer Berichte für die Integrierte Regelung für die politische Reaktion auf Krisen (IPCR) gemäß dem Durchführungsbeschluss (EU) 2018/1993 hingewiesen. Wenn grenzübergreifende SOCs Informationen im Zusammenhang mit einem potenziellen oder andauernden Cybersicherheitsvorfall großen Ausmaßes erhalten, sollten sie daher dem EU-CyCLONe-Netz, dem CSIRTs-Netz und der Kommission einschlägige Informationen zur Verfügung stellen. Je nach Lage könnten die auszutauschenden Informationen insbesondere technische Informationen, Informationen über die Art und die Motive des tatsächlichen oder potenziellen Angreifers sowie übergeordnete nichttechnische Informationen über einen potenziellen oder andauernden Cybersicherheitsvorfall großen Ausmaßes umfassen. In diesem Zusammenhang sollte dem Grundsatz „Kenntnis nur, wenn nötig“ und dem potenziell sensiblen Charakter der ausgetauschten Informationen gebührend Rechnung getragen werden.

Parlaments und des Rates eingerichteten Katastrophenschutzverfahrens der Union (UCPM) sowie für die Bereitstellung analytischer Berichte für die Integrierte Regelung für die politische Reaktion auf Krisen (IPCR) gemäß dem Durchführungsbeschluss (EU) 2018/1993 hingewiesen. Wenn grenzübergreifende SOCs Informationen im Zusammenhang mit einem potenziellen oder andauernden Cybersicherheitsvorfall großen Ausmaßes erhalten, sollten sie daher dem EU-CyCLONe-Netz, dem CSIRTs-Netz***, der Cyberabwehrgemeinschaft*** und der Kommission einschlägige Informationen zur Verfügung stellen. Je nach Lage könnten die auszutauschenden Informationen insbesondere technische Informationen, Informationen über die Art und die Motive des tatsächlichen oder potenziellen Angreifers sowie übergeordnete nichttechnische Informationen über einen potenziellen oder andauernden Cybersicherheitsvorfall großen Ausmaßes umfassen. In diesem Zusammenhang sollte dem Grundsatz „Kenntnis nur, wenn nötig“ und dem potenziell sensiblen Charakter der ausgetauschten Informationen gebührend Rechnung getragen werden.

Änderungsantrag 15

Vorschlag für eine Verordnung
Erwägung 19

Vorschlag der Kommission	*Geänderter Text*
(19) Um den Austausch von Daten über Cybersicherheitsbedrohungen aus verschiedenen Quellen in einem vertrauenswürdigen Umfeld in großem Maßstab zu ermöglichen, sollten Stellen, die sich am europäischen Cyberschutzschild beteiligen, mit modernsten und hochsicheren Instrumenten, Ausrüstungen und Infrastrukturen ausgestattet sein. Dies	(19) Um den Austausch von Daten über Cybersicherheitsbedrohungen aus verschiedenen Quellen in einem vertrauenswürdigen Umfeld in großem Maßstab zu ermöglichen, sollten Stellen, die sich am europäischen Cyberschutzschild beteiligen, mit modernsten und hochsicheren Instrumenten, Ausrüstungen und Infrastrukturen ausgestattet sein, ***wobei***

sollte es ermöglichen, die kollektiven Datenerhebungskapazitäten zu verbessern und die Behörden und einschlägigen Einrichtungen rechtzeitig zu warnen, insbesondere durch den Einsatz der neuesten Techniken der künstlichen Intelligenz und der Datenanalyse.	***Hochrisikoanbieter von kritischen Produkten mit digitalen Elementen hiervon ausgenommen sind***. Dies sollte es ermöglichen, die kollektiven Datenerhebungskapazitäten zu verbessern und die Behörden und einschlägigen Einrichtungen rechtzeitig zu warnen, insbesondere durch den Einsatz der neuesten Techniken der künstlichen Intelligenz und der Datenanalyse. ***Beim Einsatz von KI sollte eine menschliche Aufsicht vorgesehen werden, und es sollte sichergestellt werden, dass ein ausreichendes Maß an KI-Kenntnissen, die notwendige Unterstützung und die Befugnis zur Ausübung dieser Funktion vorhanden sind.***

Änderungsantrag 16

Vorschlag für eine Verordnung
Erwägung 19 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(19a) Gemäß Verordnung [XX/XXXX (Cyberresilienzgesetz)] sollten Stellen, die sich am europäischen Cyberschutzschild beteiligen, auch die in dieser Verordnung festgelegten Anforderungen für alle Produkte mit digitalen Elementen erfüllen. Angesichts der zunehmenden Risiken infolge wirtschaftlicher Abhängigkeiten muss der Kontakt zu Hochrisikoanbietern von kritischen Produkten durch einen Gemeinsamen Strategischen Rahmen für wirtschaftliche Sicherheit in der EU minimiert werden. Von Hochrisikoanbietern von kritischen Produkten mit digitalen Elementen abhängig zu sein, stellt ein strategisches Risiko dar, mit dem sich auf Unionsebene befasst werden sollte, wobei insbesondere die Frage zu beantworten ist, ob sich ein Land an Wirtschaftsspionage oder an wirtschaftlichen Zwangsmaßnahmen beteiligt und ob es aufgrund seiner Gesetzgebung verpflichtet ist, beliebigen

	Zugang zu jeder Art von Unternehmenstätigkeiten oder -daten zu gewähren, insbesondere wenn die kritischen Produkte wesentlichen Einrichtungen im Sinne der Richtlinie (EU) 2022/2555 zur Verfügung gestellt werden sollen.

Änderungsantrag 17

Vorschlag für eine Verordnung
Erwägung 20

Vorschlag der Kommission	*Geänderter Text*
(20) Durch die Sammlung, die Weitergabe und den Austausch von Daten sollte der europäische Cyberschutzschild die technologische Souveränität der Union stärken. Die Zusammenführung hochwertiger kuratierter Daten sollte auch zur Entwicklung fortgeschrittener Techniken der künstlichen Intelligenz und der Datenanalyse beitragen. Dies sollte durch die Verbindung des europäischen Cyberschutzschilds mit der dank der Verordnung (EU) 2021/1173 des Rates[25] geschaffenen europaweiten Hochleistungsrecheninfrastruktur erleichtert werden.	(20) Durch die Sammlung, die Weitergabe und den Austausch von Daten sollte der europäische Cyberschutzschild die technologische Souveränität***, die strategische Autonomie, Wettbewerbsfähigkeit und Resilienz*** der Union stärken. Die Zusammenführung hochwertiger kuratierter Daten sollte auch zur Entwicklung fortgeschrittener Techniken der künstlichen Intelligenz und der Datenanalyse beitragen. Dies sollte durch die Verbindung des europäischen Cyberschutzschilds mit der dank der Verordnung (EU) 2021/1173 des Rates[25] geschaffenen europaweiten Hochleistungsrecheninfrastruktur erleichtert werden.
[25] Verordnung (EU) 2021/1173 des Rates vom 13. Juli 2021 zur Gründung des Gemeinsamen Unternehmens für europäisches Hochleistungsrechnen und zur Aufhebung der Verordnung (EU) 2018/1488 (ABl. L 256 vom 19.7.2021, S. 3).	[25] Verordnung (EU) 2021/1173 des Rates vom 13. Juli 2021 zur Gründung des Gemeinsamen Unternehmens für europäisches Hochleistungsrechnen und zur Aufhebung der Verordnung (EU) 2018/1488 (ABl. L 256 vom 19.7.2021, S. 3).

Änderungsantrag 18

Vorschlag für eine Verordnung
Erwägung 25

Vorschlag der Kommission	*Geänderter Text*
(25) Der Cybernotfallmechanismus sollte die Mitgliedstaaten in Ergänzung ihrer eigenen Maßnahmen und Ressourcen sowie anderer bestehender Unterstützungsoptionen – wie der von der Agentur der Europäischen Union für Cybersicherheit (ENISA) im Einklang mit ihrem Mandat bereitgestellten Dienste, der koordinierten Reaktion und der Unterstützung durch das CSIRTs-Netz, der Unterstützung der Eindämmung durch das EU-CyCLONe-Netz sowie der Amtshilfe zwischen den Mitgliedstaaten, auch im Zusammenhang mit Artikel 42 Absatz 7 EUV, der SSZ-Teams für die rasche Reaktion auf Cybervorfälle***[26]*** und der Soforteinsatzteams für hybride Bedrohungen – im Falle einer Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes und deren sofortiger Bewältigung unterstützen. Er sollte der Notwendigkeit Rechnung tragen, dass spezialisierte Mittel zur Verfügung stehen müssen, um die Abwehrbereitschaft und die Reaktion auf Cybersicherheitsvorfälle in der gesamten Union und in Drittländern zu unterstützen.	(25) Der Cybernotfallmechanismus sollte die Mitgliedstaaten in Ergänzung ihrer eigenen Maßnahmen und Ressourcen sowie anderer bestehender Unterstützungsoptionen – wie der von der Agentur der Europäischen Union für Cybersicherheit (ENISA) im Einklang mit ihrem Mandat bereitgestellten Dienste, der koordinierten Reaktion und der Unterstützung durch das CSIRTs-Netz, der Unterstützung der Eindämmung durch das EU-CyCLONe-Netz sowie der Amtshilfe zwischen den Mitgliedstaaten, auch im Zusammenhang mit Artikel 42 Absatz 7 EUV, der SSZ-Teams für die rasche Reaktion auf Cybervorfälle***[1], des neuen Koordinierungszentrums für den Cyber- und Informationsraum (CIDCC) und des EU-Koordinierungszentrums für die Cyberabwehr (EUCDCC) als dessen vorgeschlagenen Nachfolgers,*** und der Soforteinsatzteams für hybride Bedrohungen – im Falle einer Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes und deren sofortiger Bewältigung unterstützen. Er sollte der Notwendigkeit Rechnung tragen, dass spezialisierte Mittel zur Verfügung stehen müssen, um die Abwehrbereitschaft und die Reaktion auf Cybersicherheitsvorfälle in der gesamten Union und in Drittländern***, insbesondere in den EU-Kandidatenländern, die sich an der Gemeinsamen Außen- und Sicherheitspolitik und der Gemeinsamen Sicherheits- und Verteidigungspolitik der EU orientieren, beim Aufbau ihrer Cyberfähigkeiten*** zu unterstützen ***und die grenzüberschreitende und regionale Zusammenarbeit zwischen diesen Kandidatenländern im Cyberbereich zu verbessern***. ***[1] Beschluss (GASP) 2017/2315 des Rates vom 11. Dezember 2017 über die***

	Begründung der Ständigen Strukturierten Zusammenarbeit (PESCO) und über die Liste der daran teilnehmenden Mitgliedstaaten.
[26] Beschluss (GASP) 2017/2315 des Rates vom 11. Dezember 2017 über die Begründung der Ständigen Strukturierten Zusammenarbeit (PESCO) und über die Liste der daran teilnehmenden Mitgliedstaaten.	[26] Beschluss (GASP) 2017/2315 des Rates vom 11. Dezember 2017 über die Begründung der Ständigen Strukturierten Zusammenarbeit (PESCO) und über die Liste der daran teilnehmenden Mitgliedstaaten.

Änderungsantrag 19

Vorschlag für eine Verordnung
Erwägung 26

Vorschlag der Kommission	*Geänderter Text*
(26) Dieses Instrument lässt die Verfahren und Rahmen für die Koordinierung der Krisenreaktion auf Unionsebene, insbesondere das UCPM[27], die IPCR[28] und die Richtlinie (EU) 2022/2555 unberührt. Es kann zu Maßnahmen beitragen oder diese ergänzen, die im Zusammenhang mit Artikel 42 Absatz 7 EUV oder in den in Artikel 222 AEUV genannten Situationen durchgeführt werden. Der Einsatz dieses Instruments sollte ***gegebenenfalls*** auch mit der Umsetzung der Maßnahmen des Instrumentariums für die Cyberdiplomatie koordiniert werden.	(26) Dieses Instrument lässt die Verfahren und Rahmen für die Koordinierung der Krisenreaktion auf Unionsebene, insbesondere das UCPM[27], die IPCR[28] und die Richtlinie (EU) 2022/2555 unberührt. Es kann zu Maßnahmen beitragen oder diese ergänzen, die im Zusammenhang mit Artikel 42 Absatz 7 EUV oder in den in Artikel 222 AEUV genannten Situationen durchgeführt werden. Der Einsatz dieses Instruments sollte auch mit der Umsetzung der Maßnahmen des Instrumentariums für die Cyberdiplomatie koordiniert werden, ***wodurch sich die strategische, operative und technische Zusammenarbeit zwischen der Cyberabwehrgemeinschaft und anderen Cybergemeinschaften verbessern würde, insbesondere zur Stärkung der Fähigkeiten zur Abwehr von Cybersicherheitsbedrohungen, die ihren Ursprung außerhalb der Union haben, einschließlich restriktiver Maßnahmen, mit denen böswillige Cyberaktivitäten verhindert werden können bzw. darauf reagiert werden kann***.

[27] 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).

[28] Integrierte Regelung für die politische Reaktion auf Krisen (IPCR) und im Einklang mit der Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen.

[27] 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).

[28] Integrierte Regelung für die politische Reaktion auf Krisen (IPCR) und im Einklang mit der Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen.

Änderungsantrag 20

Vorschlag für eine Verordnung
Erwägung 28

Vorschlag der Kommission	*Geänderter Text*
(28) Gemäß der Richtlinie (EU) 2022/2555 müssen die Mitgliedstaaten eine oder mehrere Behörden für das Cyberkrisenmanagement benennen oder einrichten und sicherstellen, dass sie über angemessene Ressourcen verfügen, um die ihnen übertragenen Aufgaben wirksam und effizient ausführen zu können. Ferner werden die Mitgliedstaaten darin dazu verpflichtet, Kapazitäten, Mittel und Verfahren zu ermitteln, die im Fall einer Krise eingesetzt werden können, sowie einen nationalen Plan für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und auf Cyberkrisen aufzustellen, in dem die Ziele und Modalitäten für das Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen festgelegt sind. Überdies sind die Mitgliedstaaten verpflichtet, ein oder mehrere CSIRTs einzurichten, die mit der Bewältigung von Sicherheitsvorfällen nach einem genau festgelegten Ablauf betraut sind und mindestens die in den Anwendungsbereich der genannten Richtlinie fallenden	(28) Gemäß der Richtlinie (EU) 2022/2555 müssen die Mitgliedstaaten eine oder mehrere Behörden für das Cyberkrisenmanagement benennen oder einrichten und sicherstellen, dass sie über angemessene Ressourcen verfügen, um die ihnen übertragenen Aufgaben wirksam und effizient ausführen zu können. Ferner werden die Mitgliedstaaten darin dazu verpflichtet, Kapazitäten, Mittel und Verfahren zu ermitteln, die im Fall einer Krise eingesetzt werden können, sowie einen nationalen Plan für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und auf Cyberkrisen aufzustellen, in dem die Ziele und Modalitäten für das Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen festgelegt sind. Überdies sind die Mitgliedstaaten verpflichtet, ein oder mehrere CSIRTs einzurichten, die mit der Bewältigung von Sicherheitsvorfällen nach einem genau festgelegten Ablauf betraut sind und mindestens die in den Anwendungsbereich der genannten Richtlinie fallenden

Sektoren, Teilsektoren und Arten von Einrichtungen abdecken, und dafür zu sorgen, dass sie mit angemessenen Ressourcen ausgestattet sind, damit sie die ihnen übertragenen Aufgaben wirksam wahrnehmen können. Diese Verordnung lässt die Rolle der Kommission bei der Gewährleistung der Einhaltung der Verpflichtungen aus der Richtlinie (EU) 2022/2555 durch die Mitgliedstaaten unberührt. Der Cybernotfallmechanismus sollte Unterstützung für Maßnahmen zur Stärkung der Abwehrbereitschaft sowie für Maßnahmen zur Reaktion auf Sicherheitsvorfälle bereitstellen, um die Auswirkungen von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes abzumildern, die sofortige Wiederherstellung zu unterstützen und/oder die Funktionsfähigkeit wesentlicher Dienste wiederherzustellen.	Sektoren, Teilsektoren und Arten von Einrichtungen abdecken, und dafür zu sorgen, dass sie mit angemessenen Ressourcen ausgestattet sind, damit sie die ihnen übertragenen Aufgaben wirksam wahrnehmen können. Diese Verordnung lässt die Rolle der Kommission bei der Gewährleistung der Einhaltung der Verpflichtungen aus der Richtlinie (EU) 2022/2555 durch die Mitgliedstaaten unberührt. Der Cybernotfallmechanismus sollte Unterstützung für Maßnahmen zur Stärkung der Abwehrbereitschaft sowie für Maßnahmen zur Reaktion auf Sicherheitsvorfälle bereitstellen, um die Auswirkungen von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes abzumildern, die sofortige Wiederherstellung zu unterstützen und/oder die Funktionsfähigkeit wesentlicher Dienste wiederherzustellen***, und dabei in geeigneter Weise auf das ganze Spektrum an Verteidigungsmöglichkeiten zurückgreifen, das den zivilen und militärischen Gemeinschaften zur Verfügung steht***.

Änderungsantrag 21

Vorschlag für eine Verordnung
Erwägung 29

Vorschlag der Kommission	*Geänderter Text*
(29) Im Rahmen der Vorsorgemaßnahmen sollten koordinierte Tests und eine entsprechende Bewertung der Cybersicherheit von in hochkritischen Sektoren tätigen Einrichtungen gemäß der Richtlinie (EU) 2022/2555 unterstützt werden, um einen kohärenten Ansatz zu fördern und die Sicherheit in der gesamten Union und ihrem Binnenmarkt zu erhöhen. Dazu sollte die Kommission mit Unterstützung der ENISA und in Zusammenarbeit mit der durch die	(29) Im Rahmen der Vorsorgemaßnahmen sollten koordinierte Tests und eine entsprechende Bewertung der Cybersicherheit von in hochkritischen Sektoren tätigen Einrichtungen gemäß der Richtlinie (EU) 2022/2555 unterstützt werden, um einen kohärenten Ansatz zu fördern und die Sicherheit in der gesamten Union und ihrem Binnenmarkt zu erhöhen. Dazu sollte die Kommission mit Unterstützung der ENISA und in Zusammenarbeit mit der durch die

Richtlinie (EU) 2022/2555 eingesetzten NIS-Kooperationsgruppe regelmäßig einschlägige Sektoren oder Teilsektoren festlegen, die für eine finanzielle Unterstützung für koordinierte Tests auf Unionsebene in Betracht kommen sollen. ***Die*** Sektoren oder Teilsektoren ***sollten*** aus Anhang I der Richtlinie (EU) 2022/2555 („Sektoren der hohen Kritikalität“) ausgewählt werden. Die koordinierten Tests sollten auf gemeinsamen Risikoszenarien und -methoden beruhen. Auch angesichts der Notwendigkeit, Doppelarbeit zu vermeiden, sollten bei der Auswahl der Sektoren und der Entwicklung von Risikoszenarien einschlägige unionsweite Risikobewertungen und -szenarien berücksichtigt werden, darunter etwa die Risikobewertung und -szenarien, zu deren Durchführung die Kommission, der Hohe Vertreter und die NIS-Kooperationsgruppe in Abstimmung mit den einschlägigen zivilen und militärischen Einrichtungen und Agenturen sowie bestehenden Netzwerken wie dem EU-CyCLONe in den Schlussfolgerungen des Rates zur Entwicklung der Cyberabwehr der Europäischen Union aufgefordert werden; dazu zählen auch die Risikobewertung von Kommunikationsnetzen und -infrastrukturen, die im gemeinsamen Ministeraufruf von Nevers gefordert und von der NIS-Kooperationsgruppe mit Unterstützung der Kommission und der ENISA und in Zusammenarbeit mit dem Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) durchgeführt wird, die gemäß Artikel 22 der Richtlinie (EU) 2022/2555 durchzuführenden koordinierten Risikobewertungen und das Testen der digitalen operationalen Resilienz gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates***[29]***. Bei der Auswahl der Sektoren sollte auch der Empfehlung des Rates für eine unionsweite koordinierte Vorgehensweise zur Stärkung

Richtlinie (EU) 2022/2555 eingesetzten NIS-Kooperationsgruppe regelmäßig einschlägige Sektoren oder Teilsektoren festlegen, die für eine finanzielle Unterstützung für koordinierte Tests auf Unionsebene in Betracht kommen sollen. ***Gegebenenfalls sollten auch der Europäische Auswärtige Dienst (EAD), insbesondere das ihm unterstellte EU-Zentrum für Informationsgewinnung und Lageerfassung (INTCEN) und die zugehörige Analyseeinheit für hybride Bedrohungen, sowie – in unterstützender Funktion – die Direktion „Aufklärung“ des Militärstabs der Europäischen Union (EUMS), die dem Einheitlichen Analyseverfahren (SIAC) untersteht, für die Bereitstellung aktueller Bewertungen hinzugezogen werden, um bei der Ermittlung der*** Sektoren oder Teilsektoren ***mitzuwirken, die*** aus Anhang I der Richtlinie (EU) 2022/2555 („Sektoren der hohen Kritikalität“) ausgewählt werden ***sollten***. Die koordinierten Tests sollten auf gemeinsamen Risikoszenarien und -methoden beruhen. ***Darüber hinaus sollten diese Tests eine wichtige Rolle bei der Verbesserung der Zusammenarbeit zwischen zivilen und militärischen Einrichtungen spielen. Daher sollten die Kommission, der EAD und die ENISA bei der Organisation von Tests systematisch in Erwägung ziehen, Akteure anderer Cybergemeinschaften, wie beispielsweise die Europäische Verteidigungsagentur (EDA) oder andere einschlägige Einrichtungen, einzubeziehen.*** Auch angesichts der Notwendigkeit, Doppelarbeit zu vermeiden, sollten bei der Auswahl der Sektoren und der Entwicklung von Risikoszenarien einschlägige unionsweite Risikobewertungen und -szenarien berücksichtigt werden, darunter etwa die Risikobewertung und -szenarien, zu deren Durchführung die Kommission, der Hohe Vertreter und die NIS-Kooperationsgruppe in Abstimmung mit den einschlägigen zivilen und militärischen Einrichtungen

der Resilienz kritischer Infrastrukturen Rechnung getragen werden.

und Agenturen sowie bestehenden Netzwerken wie dem EU-CyCLONe in den Schlussfolgerungen des Rates zur Entwicklung der Cyberabwehr der Europäischen Union aufgefordert werden; dazu zählen auch die Risikobewertung von Kommunikationsnetzen und -infrastrukturen, die im gemeinsamen Ministeraufruf von Nevers gefordert und von der NIS-Kooperationsgruppe mit Unterstützung der Kommission und der ENISA und in Zusammenarbeit mit dem Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) durchgeführt wird, die gemäß Artikel 22 der Richtlinie (EU) 2022/2555 durchzuführenden koordinierten Risikobewertungen und das Testen der digitalen operationalen Resilienz gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates***[1]***. Bei der Auswahl der Sektoren sollte auch der Empfehlung des Rates für eine unionsweite koordinierte Vorgehensweise zur Stärkung der Resilienz kritischer Infrastrukturen Rechnung getragen werden.

[1] Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011.

---

[29] Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011.

[29] Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011.

Änderungsantrag 22

Vorschlag für eine Verordnung
Erwägung 32

Vorschlag der Kommission	*Geänderter Text*
(32) Der Cybernotfallmechanismus sollte den Mitgliedstaaten bei der Unterstützung eines von einem schwerwiegenden Cybersicherheitsvorfall oder Cybersicherheitsvorfall großen Ausmaßes betroffenen Mitgliedstaat helfen, auch mithilfe des CSIRTs-Netzes gemäß Artikel 15 der Richtlinie (EU) 2022/2555. Mitgliedstaaten, die Unterstützung leisten, sollten die Möglichkeit haben, die Erstattung der Kosten im Zusammenhang mit der Entsendung von Sachverständigenteams im Rahmen der Amtshilfe zu beantragen. Die erstattungsfähigen Kosten könnten Reise- und Unterbringungskosten sowie Tagegelder für Cybersicherheitsexperten umfassen.	(32) Der Cybernotfallmechanismus sollte den Mitgliedstaaten bei der Unterstützung eines von einem schwerwiegenden Cybersicherheitsvorfall oder Cybersicherheitsvorfall großen Ausmaßes betroffenen Mitgliedstaat helfen, auch mithilfe des CSIRTs-Netzes gemäß Artikel 15 der Richtlinie (EU) 2022/2555. Mitgliedstaaten, die Unterstützung leisten, sollten die Möglichkeit haben, die Erstattung der Kosten im Zusammenhang mit der Entsendung von Sachverständigenteams im Rahmen der Amtshilfe zu beantragen***, wodurch eine effiziente Koordinierung zwischen den einschlägigen Programmen und Instrumenten der EU, einschließlich der Europäischen Friedensfazilität (EFF), der GASP und des Instruments „NDICI/Europa in der Welt“, bei der Unterstützung von Drittländern, insbesondere der Ukraine und Moldau, sichergestellt wird***. Die erstattungsfähigen Kosten könnten Reise- und Unterbringungskosten sowie Tagegelder für Cybersicherheitsexperten umfassen.

Änderungsantrag 23

Vorschlag für eine Verordnung
Erwägung 33

Vorschlag der Kommission	*Geänderter Text*
(33) Es sollte schrittweise eine Cybersicherheitsreserve auf Unionsebene eingerichtet werden, die aus Diensten privater Anbieter verwalteter Sicherheitsdienste besteht, um die Reaktion und sofortige Wiederherstellung im Falle von schwerwiegenden	(33) Es sollte schrittweise eine Cybersicherheitsreserve auf Unionsebene eingerichtet werden, die aus Diensten privater Anbieter verwalteter Sicherheitsdienste besteht, um die Reaktion und sofortige Wiederherstellung im Falle von schwerwiegenden

Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes zu unterstützen. Die EU-Cybersicherheitsreserve sollte die Verfügbarkeit und Einsatzbereitschaft der betroffenen Dienste gewährleisten. Die Dienste der EU-Cybersicherheitsreserve sollten dazu dienen, den nationalen Behörden bei der Unterstützung betroffener in kritischen oder hochkritischen Sektoren tätiger Einrichtungen ergänzend zu ihren eigenen Maßnahmen auf nationaler Ebene zu helfen. Wenn die Mitgliedstaaten Unterstützung aus der EU-Cybersicherheitsreserve beantragen, sollten sie angeben, welche Unterstützung die betroffene Einrichtung auf nationaler Ebene erhält, und dies sollte bei der Prüfung des Antrags des Mitgliedstaats berücksichtigt werden. Die Dienste der EU-Cybersicherheitsreserve können auch dazu dienen, die Organe, Einrichtungen und sonstigen Stellen der Union unter ähnlichen Bedingungen zu unterstützen.

Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes zu unterstützen. Die EU-Cybersicherheitsreserve sollte die Verfügbarkeit und Einsatzbereitschaft der betroffenen Dienste gewährleisten. Die Dienste der EU-Cybersicherheitsreserve sollten dazu dienen, den nationalen Behörden bei der Unterstützung betroffener in kritischen oder hochkritischen Sektoren tätiger Einrichtungen ergänzend zu ihren eigenen Maßnahmen auf nationaler Ebene zu helfen. Wenn die Mitgliedstaaten Unterstützung aus der EU-Cybersicherheitsreserve beantragen, sollten sie angeben, welche Unterstützung die betroffene Einrichtung auf nationaler Ebene erhält, und dies sollte bei der Prüfung des Antrags des Mitgliedstaats berücksichtigt werden. Die Dienste der EU-Cybersicherheitsreserve können auch dazu dienen, die Organe, Einrichtungen und sonstigen Stellen der Union***, einschließlich der GSVP-Missionen,*** unter ähnlichen Bedingungen zu unterstützen.

Änderungsantrag 24

Vorschlag für eine Verordnung
Erwägung 34

Vorschlag der Kommission	*Geänderter Text*
(34) Im Hinblick auf die Auswahl privater Dienstleister für die Bereitstellung von Diensten im Rahmen der EU-Cybersicherheitsreserve muss eine Reihe von Mindestkriterien festgelegt werden, die in die Ausschreibung für die Auswahl dieser Anbieter aufgenommen werden sollten, damit die Bedürfnisse der Behörden und der in kritischen oder hochkritischen Sektoren tätigen Einrichtungen in den Mitgliedstaaten erfüllt werden.	(34) Im Hinblick auf die Auswahl privater Dienstleister für die Bereitstellung von Diensten im Rahmen der EU-Cybersicherheitsreserve muss eine Reihe von Mindestkriterien festgelegt werden, die in die Ausschreibung für die Auswahl dieser Anbieter aufgenommen werden sollten, damit die Bedürfnisse der Behörden und der in kritischen oder hochkritischen Sektoren tätigen Einrichtungen in den Mitgliedstaaten erfüllt werden***, wobei unter anderem die Risiken, die mit der Beteiligung von Anbietern aus strategischen***

Wettbewerbsländern einhergehen und so die wirtschaftliche Sicherheit gefährden könnten, sowie die Auswirkungen auf die strategische Sicherheit der EU berücksichtigt werden sollten.

Änderungsantrag 25

Vorschlag für eine Verordnung
Erwägung 36

Vorschlag der Kommission	*Geänderter Text*
(36) Um die Ziele dieser Verordnung, nämlich die Förderung einer gemeinsamen Lageerfassung, die Stärkung der Resilienz der Union und die Ermöglichung einer wirksamen Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes, zu unterstützen, sollten das EU-CyCLONe-Netz, das CSIRT-Netz oder die Kommission die ENISA beauftragen können, Bedrohungen, Schwachstellen und Eindämmungsmaßnahmen im Zusammenhang mit einem bestimmten schwerwiegenden Cybersicherheitsvorfall oder Cybersicherheitsvorfall großen Ausmaßes zu überprüfen und zu bewerten. Nach Abschluss der Überprüfung und Bewertung eines Sicherheitsvorfalls sollte die ENISA in Zusammenarbeit mit den einschlägigen Beteiligten, einschließlich Vertretern des Privatsektors, der Mitgliedstaaten, der Kommission und anderer einschlägiger Organe, Einrichtungen und sonstiger Stellen der EU, einen Bericht über die Überprüfung des Sicherheitsvorfalls erstellen. Was den Privatsektor betrifft, entwickelt die ENISA derzeit Kanäle für den Informationsaustausch mit spezialisierten Anbietern, darunter auch mit Anbietern verwalteter Sicherheitslösungen, um zur Erfüllung des Auftrags der ENISA beizutragen, ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union zu erreichen. Aufbauend auf der	(36) Um die Ziele dieser Verordnung, nämlich die Förderung einer gemeinsamen Lageerfassung, die Stärkung der Resilienz der Union und die Ermöglichung einer wirksamen Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes, zu unterstützen, sollten das EU-CyCLONe-Netz, das CSIRT-Netz oder die Kommission die ENISA beauftragen können, Bedrohungen, Schwachstellen und Eindämmungsmaßnahmen im Zusammenhang mit einem bestimmten schwerwiegenden Cybersicherheitsvorfall oder Cybersicherheitsvorfall großen Ausmaßes zu überprüfen und zu bewerten. ***Angesichts der Entwicklung eines sicheren Konnektivitätssystems, das auf der europäischen Quantenkommunikationsinfrastruktur (EuroQCI) und der staatlichen Satellitenkommunikation in der Europäischen Union (GOVSATCOM) aufbaut, insbesondere der Umsetzung des globalen Satellitennavigationssystems (GNSS) GALILEO für Nutzer im Verteidigungsbereich, sollte bei jeder möglichen künftigen Entwicklung das Aufkommen eines „Hyperkriegs“ berücksichtigt werden, bei dem der Gesellschaft durch die Kombination der Geschwindigkeit und technischen Ausgereiftheit der Quanteninformatik mit hochgradig autonomen militärischen Systemen verheerender Schaden zugefügt***

Zusammenarbeit mit Interessenträgern, einschließlich des Privatsektors, sollte der Bericht über die Überprüfung bestimmter Sicherheitsvorfälle darauf abzielen, die Ursachen, Auswirkungen und Eindämmungsmaßnahmen eines Sicherheitsvorfalls nach seinem Auftreten zu bewerten. Besonderes Augenmerk sollte auf die Beiträge und Erkenntnisse gelegt werden, die von den Anbietern verwalteter Sicherheitsdienste geteilt werden, die die in dieser Verordnung geforderten Bedingungen der größtmöglichen beruflichen Integrität, Unparteilichkeit und des erforderlichen technischen Fachwissens erfüllen. Der Bericht sollte vorgelegt werden und in die Arbeit des EU-CyCLONe-Netzes, des CSIRTs-Netzes und der Kommission einfließen. Betrifft der Vorfall ein Drittland, so sollte die Kommission den Bericht auch an den Hohen Vertreter weitergeben.

werden kann. Nach Abschluss der Überprüfung und Bewertung eines Sicherheitsvorfalls sollte die ENISA in Zusammenarbeit mit den einschlägigen Beteiligten, einschließlich Vertretern des Privatsektors, der Mitgliedstaaten, der Kommission und anderer einschlägiger Organe, Einrichtungen und sonstiger Stellen der EU, einen Bericht über die Überprüfung des Sicherheitsvorfalls erstellen. Was den Privatsektor betrifft, entwickelt die ENISA derzeit Kanäle für den Informationsaustausch mit spezialisierten Anbietern, darunter auch mit Anbietern verwalteter Sicherheitslösungen, um zur Erfüllung des Auftrags der ENISA beizutragen, ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union zu erreichen. Aufbauend auf der Zusammenarbeit mit Interessenträgern, einschließlich des Privatsektors, sollte der Bericht über die Überprüfung bestimmter Sicherheitsvorfälle darauf abzielen, die Ursachen, Auswirkungen und Eindämmungsmaßnahmen eines Sicherheitsvorfalls nach seinem Auftreten zu bewerten. Besonderes Augenmerk sollte auf die Beiträge und Erkenntnisse gelegt werden, die von den Anbietern verwalteter Sicherheitsdienste geteilt werden, die die in dieser Verordnung geforderten Bedingungen der größtmöglichen beruflichen Integrität, Unparteilichkeit und des erforderlichen technischen Fachwissens erfüllen. Der Bericht sollte vorgelegt werden und in die Arbeit des EU-CyCLONe-Netzes, des CSIRTs-Netzes und der Kommission einfließen. Betrifft der Vorfall ein Drittland, so sollte die Kommission den Bericht auch an den Hohen Vertreter***, den EAD und an alle GSVP-Missionen in dem von dem Vorfall betroffenen Land über die Missionszentrale*** weitergeben.

Änderungsantrag 26

Vorschlag für eine Verordnung
Erwägung 37

Vorschlag der Kommission	*Geänderter Text*
(37) Angesichts des unvorhersehbaren Charakters von Cybersicherheitsangriffen und der Tatsache, dass sie häufig nicht auf ein bestimmtes geografisches Gebiet beschränkt sind und ein hohes Ausbreitungsrisiko bergen, trägt die Stärkung der Resilienz von Nachbarländern und ihrer Fähigkeit, wirksam auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes zu reagieren, auch zum Schutz der Union als Ganzes bei. Daher ***können*** Drittländer, die mit dem Programm Digitales Europa assoziiert sind, aus der EU-Cybersicherheitsreserve unterstützt werden***, sofern dies im jeweiligen Assoziierungsabkommen mit dem Programm Digitales Europa vorgesehen ist***. Die Fördermittel für assoziierte Drittländer sollten von der Union im Rahmen einschlägiger Partnerschafts- und Finanzierungsinstrumente für diese Länder gewährt werden. Die Unterstützung sollte Dienste im Bereich der Reaktion und sofortigen Wiederherstellung im Falle von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes abdecken. Die in dieser Verordnung festgelegten Bedingungen für die EU-Cybersicherheitsreserve und für vertrauenswürdige Anbieter sollten auch bei der Unterstützung der mit dem Programm Digitales Europa assoziierten Drittländer gelten.	(37) Angesichts des unvorhersehbaren Charakters von Cybersicherheitsangriffen und der Tatsache, dass sie häufig nicht auf ein bestimmtes geografisches Gebiet beschränkt sind und ein hohes Ausbreitungsrisiko bergen, trägt die Stärkung der Resilienz von Nachbarländern***, insbesondere der Ukraine und Moldau,*** und ihrer Fähigkeit, wirksam auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes zu reagieren, auch zum Schutz der Union als Ganzes bei. Daher ***sollten*** Drittländer, die mit dem Programm Digitales Europa assoziiert sind, aus der EU-Cybersicherheitsreserve unterstützt werden***. Die Unterstützung sollte auch für Drittländer gelten, in die eine GSVP-Mission mit dem konkreten Auftrag entsandt wurde, die Resilienz gegenüber hybriden Bedrohungen, auch Cyberbedrohungen, zu stärken, oder in denen eine EFF-Unterstützungsmaßnahme zur Stärkung der Cyberresilienz des Landes eingeführt wurde.*** Die Fördermittel für assoziierte Drittländer sollten von der Union im Rahmen einschlägiger Partnerschafts- und Finanzierungsinstrumente für diese Länder gewährt werden. Die Unterstützung sollte Dienste im Bereich der Reaktion und sofortigen Wiederherstellung im Falle von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes abdecken. Die in dieser Verordnung festgelegten Bedingungen für die EU-Cybersicherheitsreserve und für vertrauenswürdige Anbieter sollten auch bei der Unterstützung der mit dem Programm Digitales Europa assoziierten

Drittländer gelten.

Änderungsantrag 27

Vorschlag für eine Verordnung
Artikel 1 – Absatz 1 – Buchstabe c

Vorschlag der Kommission	*Geänderter Text*
c) die Einrichtung eines europäischen Überprüfungsmechanismus für Cybersicherheitsvorfälle zur Überprüfung und Bewertung von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes.	c) die Einrichtung eines europäischen Überprüfungsmechanismus für Cybersicherheitsvorfälle zur Überprüfung und Bewertung von schwerwiegenden Cybersicherheitsvorfällen ***oder -bedrohungen*** und Cybersicherheitsvorfällen ***oder -bedrohungen*** großen Ausmaßes.

Änderungsantrag 28

Vorschlag für eine Verordnung
Artikel 1 – Absatz 2 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) Stärkung der gemeinsamen Fähigkeiten der Union zur Erkennung und Lageerfassung im Bereich der Cyberbedrohungen und -vorfälle, um so in der gesamten digitalen Wirtschaft der Union eine Stärkung der Wettbewerbsfähigkeit der Industrie- und Dienstleistungszweige zu ermöglichen und zur technologischen ***Souveränität*** der Union im Bereich der Cybersicherheit beizutragen;	a) Stärkung der gemeinsamen Fähigkeiten der Union zur Erkennung und Lageerfassung im Bereich der Cyberbedrohungen und -vorfälle, um so in der gesamten digitalen Wirtschaft der Union eine Stärkung der Wettbewerbsfähigkeit der Industrie- und Dienstleistungszweige zu ermöglichen und zur technologischen ***Resilienz*** der Union im Bereich der Cybersicherheit beizutragen;

Änderungsantrag 29

Vorschlag für eine Verordnung
Artikel 1 – Absatz 2 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) Stärkung der Abwehrbereitschaft der in kritischen und hochkritischen	b) Stärkung der Abwehrbereitschaft der in kritischen und hochkritischen

Sektoren tätigen Einrichtungen in der gesamten Union und Stärkung der Solidarität durch den Aufbau gemeinsamer Kapazitäten für die Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes, indem u. a. die Unionsunterstützung für die Bewältigung von Cybersicherheitsvorfällen auch Drittländern, die mit dem Programm Digitales Europa (DEP) assoziiert sind, zur Verfügung gestellt wird;	Sektoren tätigen Einrichtungen in der gesamten Union und Stärkung der Solidarität durch den Aufbau gemeinsamer Kapazitäten für die Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes, indem u. a. die Unionsunterstützung für die Bewältigung von Cybersicherheitsvorfällen auch Drittländern, die mit dem Programm Digitales Europa (DEP) assoziiert sind, ***oder Drittländern, die Kandidaten für den Beitritt zur Europäischen Union sind und den Sicherheits- und Verteidigungsinteressen der Union und ihrer Mitgliedstaaten, wie sie in der GASP gemäß Titel V EUV festgelegt sind, nicht zuwiderhandeln,*** zur Verfügung gestellt wird; ***Im Rahmen ihrer nationalen Cybersicherheitsstrategie sollten die Mitgliedstaaten ein Programm der aktiven Cyberabwehr in Betracht ziehen, wozu regelmäßige gemeinsame Schulungsmaßnahmen unter Mitgliedstaaten und unter Einbeziehung internationaler Organisationen gehören. Ein solches Programm sollte die Möglichkeit bieten, Bedrohungen synchronisiert und in Echtzeit zu entdecken, zu erkennen, zu analysieren und zu mindern.***

Änderungsantrag 30

Vorschlag für eine Verordnung
Artikel 1 – Absatz 2 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	2a. Senkung der systemischen Cybersicherheitsrisiken durch Abhängigkeiten von kritischen Ausrüstungen aus Ländern, die den Sicherheits- und Verteidigungsinteressen der Union und ihrer Mitgliedstaaten, wie sie im Rahmen der GASP gemäß Titel V EUV festgelegt sind, zuwiderlaufen

würden;

Änderungsantrag 31

Vorschlag für eine Verordnung
Artikel 2 – Absatz 2 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	Die „Cyberabwehrgemeinschaft“ bezeichnet die Verteidigungsbehörden der Mitgliedstaaten und wird von den Organen, Einrichtungen und sonstigen Stellen der EU gemäß der Gemeinsamen Mitteilung über die EU-Cyberabwehrpolitik[1] unterstützt.
	[1] Gemeinsame Mitteilung an das Europäische Parlament und den Rat – EU-Cyberabwehrpolitik, JOIN(2022) 49 final.

Änderungsantrag 32

Vorschlag für eine Verordnung
Artikel 3 – Absatz 2 – Unterabsatz 1 – Buchstabe b a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ba) Unterstützung der Modernisierung der gesamten Cyberabwehrsysteme, Verbesserung der Qualität der Fähigkeiten im Bereich der Cyberabwehr durch den Einsatz von KI-Systemen und Beschleunigung des Informationsaustausches zwischen den nationalen SOCs und den grenzübergreifenden SOCs;

Änderungsantrag 33

Vorschlag für eine Verordnung
Artikel 3 – Absatz 2 – Unterabsatz 1 – Buchstabe d a (neu)

Vorschlag der Kommission	*Geänderter Text*
	da) Überprüfung und Bewertung kritischer Cybersicherheitstechnologien und -ausrüstungen, die von SOC bei der Reaktion auf Cybersicherheitsvorfälle eingesetzt werden, im Hinblick auf systemische Risiken durch die Kontrolle von Hochrisikoanbietern durch Länder, die den Sicherheits- und Verteidigungsinteressen der Union und ihrer Mitgliedstaaten, wie sie im Rahmen der GASP gemäß Titel V EUV festgelegt sind, zuwiderlaufen würde.

Änderungsantrag 34

Vorschlag für eine Verordnung
Artikel 4 – Absatz 1 – Unterabsatz 2

Vorschlag der Kommission	*Geänderter Text*
Es muss in der Lage sein, als Bezugspunkt und Zugangstor zu anderen öffentlichen und privaten Organisationen auf nationaler Ebene für die Sammlung und Auswertung von Informationen über Cybersicherheitsbedrohungen und -vorfälle zu fungieren und zu einem grenzübergreifenden SOC beizutragen. Es wird mit modernster Technik ausgestattet, die es ermöglicht, Daten in Bezug auf Cybersicherheitsbedrohungen und -vorfälle zu erkennen, zu aggregieren und zu analysieren.	Es muss in der Lage sein, als Bezugspunkt und Zugangstor zu anderen öffentlichen und privaten ***sowie gegebenenfalls militärischen*** Organisationen auf nationaler Ebene für die Sammlung und Auswertung von Informationen über Cybersicherheitsbedrohungen und -vorfälle zu fungieren und zu einem grenzübergreifenden SOC beizutragen. Es wird mit modernster Technik ausgestattet, die es ermöglicht, Daten in Bezug auf Cybersicherheitsbedrohungen und -vorfälle zu erkennen, zu aggregieren und zu analysieren.

Änderungsantrag 35

Vorschlag für eine Verordnung
Artikel 4 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Im Anschluss an eine Aufforderung zur Interessenbekundung wählt das	(2) Im Anschluss an eine Aufforderung zur Interessenbekundung wählt das

Europäische Kompetenzzentrum für Cybersicherheit (ECCC) nationale SOCs zur Teilnahme an einer gemeinsamen Beschaffung von Instrumenten und Infrastrukturen mit dem ECCC aus. Das ECCC kann den ausgewählten nationalen SOCs Finanzhilfen zur Finanzierung des Betriebs dieser Instrumente und Infrastrukturen gewähren. Der Finanzbeitrag der Union deckt bis zu 50 % der Beschaffungskosten der Instrumente und Infrastrukturen und bis zu 50 % der Betriebskosten; die verbleibenden Kosten trägt der betreffende Mitgliedstaat. Bevor das Verfahren für die Beschaffung der Instrumente und Infrastrukturen eingeleitet wird, schließen das ECCC und das nationale SOC eine Aufnahme- und Nutzungsvereinbarung, in der die Verwendung der Instrumente und Infrastrukturen geregelt wird.

Europäische Kompetenzzentrum für Cybersicherheit (ECCC) nationale SOCs zur Teilnahme an einer gemeinsamen Beschaffung von Instrumenten und Infrastrukturen mit dem ECCC aus. Das ECCC kann den ausgewählten nationalen SOCs Finanzhilfen zur Finanzierung des Betriebs dieser Instrumente und Infrastrukturen ***unter der strengen Voraussetzung*** gewähren***, dass diese Instrumente und Infrastrukturen durch vertrauenswürdige Anbieter im Sinne von Artikel 16 bereitgestellt werden***. Der Finanzbeitrag der Union deckt bis zu 50 % der Beschaffungskosten der Instrumente und Infrastrukturen und bis zu 50 % der Betriebskosten; die verbleibenden Kosten trägt der betreffende Mitgliedstaat. Bevor das Verfahren für die Beschaffung der Instrumente und Infrastrukturen eingeleitet wird, schließen das ECCC und das nationale SOC eine Aufnahme- und Nutzungsvereinbarung, in der die Verwendung der Instrumente und Infrastrukturen geregelt wird.

Änderungsantrag 36

Vorschlag für eine Verordnung
Artikel 5 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Im Anschluss an eine Aufforderung zur Interessenbekundung wählt das ECCC ein Aufnahmekonsortium zur Teilnahme an einer gemeinsamen Beschaffung von Instrumenten und Infrastrukturen mit dem ECCC aus. Das ECCC kann dem Aufnahmekonsortium eine Finanzhilfe zur Finanzierung des Betriebs der Instrumente und Infrastrukturen gewähren. Der Finanzbeitrag der Union deckt bis zu 75 % der Beschaffungskosten der Instrumente und Infrastrukturen und bis zu 50 % der Betriebskosten; die verbleibenden Kosten trägt das Aufnahmekonsortium. Bevor das Verfahren für die Beschaffung der	(2) Im Anschluss an eine Aufforderung zur Interessenbekundung wählt das ECCC ein Aufnahmekonsortium zur Teilnahme an einer gemeinsamen Beschaffung von Instrumenten und Infrastrukturen mit dem ECCC aus. Das ECCC kann dem Aufnahmekonsortium eine Finanzhilfe zur Finanzierung des Betriebs der Instrumente und Infrastrukturen ***unter der strengen Voraussetzung*** gewähren***, dass diese Instrumente und Infrastrukturen durch vertrauenswürdige Anbieter im Sinne von Artikel 16 bereitgestellt werden***. Der Finanzbeitrag der Union deckt bis zu 75 % der Beschaffungskosten der Instrumente

Instrumente und Infrastrukturen eingeleitet wird, schließen das ECCC und das Aufnahmekonsortium eine Aufnahme- und Nutzungsvereinbarung, in der die Verwendung der Instrumente und Infrastrukturen geregelt wird.	und Infrastrukturen und bis zu 50 % der Betriebskosten; die verbleibenden Kosten trägt das Aufnahmekonsortium. Bevor das Verfahren für die Beschaffung der Instrumente und Infrastrukturen eingeleitet wird, schließen das ECCC und das Aufnahmekonsortium eine Aufnahme- und Nutzungsvereinbarung, in der die Verwendung der Instrumente und Infrastrukturen geregelt wird.

Änderungsantrag 37

Vorschlag für eine Verordnung
Artikel 5 – Absatz 2 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	2a. Infrastruktur und Lieferanten aus Drittländern mit hohem Risiko werden automatisch ausgeschlossen.

Änderungsantrag 38

Vorschlag für eine Verordnung
Artikel 6 – Absatz 1 – Buchstabe b a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ba) durch diesen Informationsaustausch die Stärkung der Kapazitäten der teilnehmenden Länder im Militär- und Verteidigungsbereich direkt unterstützt oder eine direkte, unmittelbare Bedrohung ihrer Sicherheit verhindert wird. Da durch die Ausnutzung von Schwachstellen im Verteidigungsbereich erhebliche Störungen und Schäden verursacht werden können, sind im Bereich der Cybersicherheit der Verteidigungsindustrie besondere Maßnahmen erforderlich, um die Sicherheit von Lieferketten, insbesondere von weiter unten in der Lieferkette stehenden Einrichtungen, die keinen Zugang zu Verschlusssachen benötigen, aber ernsthafte Risiken für den gesamten

	Sektor bergen könnten, sicherzustellen. Den Auswirkungen von Verstößen sowie der Bedrohung durch potenzielle Manipulationen von Netzwerkdaten, durch die kritische Verteidigungsanlagen unbrauchbar gemacht oder sogar ihre Betriebssysteme ausgeschaltet werden könnten, sodass sie anfällig sind für eine Übernahme, sollte besondere Aufmerksamkeit gewidmet werden.

Änderungsantrag 39

Vorschlag für eine Verordnung
Artikel 6 – Absatz 1 – Buchstabe b a (neu)

Vorschlag der Kommission	*Geänderter Text*
	bb) die Stärkung der Kapazitäten der teilnehmenden Länder im Verteidigungsbereich unterstützt oder eine direkte, unmittelbare Bedrohung ihrer Sicherheit verhindert wird, wobei die Sicherheit von Lieferketten, insbesondere von weiter unten in der Lieferkette stehenden Einrichtungen, die keinen Zugang zu Verschlusssachen benötigen, aber ernsthafte Risiken für den gesamten Sektor bergen könnten, sichergestellt wird.

Änderungsantrag 40

Vorschlag für eine Verordnung
Artikel 7 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Wenn die grenzübergreifenden SOCs Informationen über einen potenziellen oder andauernden Cybersicherheitsvorfall großen Ausmaßes erhalten, stellen sie dem EU-CyCLONe-Netz, dem CSIRTs-Netz und der Kommission im Hinblick auf ihre jeweiligen Krisenmanagementaufgaben unverzüglich alle einschlägigen	(1) Wenn die grenzübergreifenden SOCs Informationen über einen potenziellen oder andauernden Cybersicherheitsvorfall großen Ausmaßes erhalten, stellen sie dem EU-CyCLONe-Netz, dem CSIRTs-Netz und der Kommission***, ferner dem Hohen Vertreter und dem EAD, wenn ein Drittland betroffen ist,*** im Hinblick auf ihre

Informationen im Einklang mit der Richtlinie (EU) 2022/2555 zur Verfügung.	jeweiligen Krisenmanagementaufgaben unverzüglich alle einschlägigen Informationen im Einklang mit der Richtlinie (EU) 2022/2555 zur Verfügung.

Änderungsantrag 41

Vorschlag für eine Verordnung
Artikel 8 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Die am europäischen Cyberschutzschild beteiligten Mitgliedstaaten gewährleisten ein hohes Maß an Datensicherheit und physischer Sicherheit der Infrastruktur des europäischen Cyberschutzschilds und stellen sicher, dass die Infrastruktur angemessen verwaltet und kontrolliert wird, um sie vor Bedrohungen zu schützen und ihre Sicherheit sowie die Sicherheit der Systeme und der über die Infrastruktur ausgetauschten Daten zu gewährleisten.	(1) Die am europäischen Cyberschutzschild beteiligten Mitgliedstaaten gewährleisten ein hohes Maß an Datensicherheit und physischer Sicherheit der Infrastruktur des europäischen Cyberschutzschilds und stellen sicher, dass die Infrastruktur angemessen verwaltet und kontrolliert wird, um sie vor Bedrohungen zu schützen und ihre Sicherheit sowie die Sicherheit der Systeme ***zu gewährleisten, indem sie den technischen Vorsprung der EU in kritischen Sektoren fördern und die damit im Zusammenhang stehenden Risiken mindern, beispielsweise durch Maßnahmen zur Beschränkung oder zum Ausschluss von Hochrisikoanbietern,*** und ***die Sicherheit*** der über die Infrastruktur ausgetauschten Daten zu gewährleisten.

Änderungsantrag 42

Vorschlag für eine Verordnung
Artikel 8 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die am europäischen Cyberschutzschild beteiligten Mitgliedstaaten stellen sicher, dass durch den Informationsaustausch innerhalb des europäischen Cyberschutzschilds mit Einrichtungen, die keine öffentlichen Stellen der Mitgliedstaaten sind, die Sicherheitsinteressen der Union nicht	(2) Die am europäischen Cyberschutzschild beteiligten Mitgliedstaaten stellen sicher, dass durch den Informationsaustausch innerhalb des europäischen Cyberschutzschilds mit Einrichtungen, die keine öffentlichen Stellen der Mitgliedstaaten sind, die Sicherheitsinteressen der Union nicht

beeinträchtigt werden.	beeinträchtigt werden***, dass ein etwaiger Informationsaustausch mit Hochrisikoanbietern beschränkt wird und dass die Sicherheit und die strategischen Interessen der Union durch diesen Informationsaustausch keinen Schaden nehmen***.

Änderungsantrag 43

Vorschlag für eine Verordnung
Artikel 8 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) Die Kommission kann Durchführungsrechtsakte erlassen, in denen sie technische Anforderungen festgelegt, nach denen die Mitgliedstaaten ihrer Verpflichtung gemäß den Absätzen 1 und 2 nachkommen müssen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 21 Absatz 2 dieser Verordnung genannten Prüfverfahren erlassen. Dabei berücksichtigt die Kommission mit Unterstützung des Hohen Vertreters einschlägige Sicherheitsstandards auf Verteidigungsebene, um die Zusammenarbeit mit militärischen Akteuren zu erleichtern.	(3) Die Kommission kann Durchführungsrechtsakte erlassen, in denen sie technische Anforderungen festgelegt, nach denen die Mitgliedstaaten ihrer Verpflichtung gemäß den Absätzen 1 und 2 nachkommen müssen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 21 Absatz 2 dieser Verordnung genannten Prüfverfahren erlassen. Dabei berücksichtigt die Kommission mit Unterstützung des Hohen Vertreters einschlägige Sicherheitsstandards auf Verteidigungsebene, um die Zusammenarbeit mit militärischen Akteuren zu erleichtern***, wobei sie das gesamte Spektrum der Möglichkeiten nutzt, die den zivilen und militärischen Gemeinschaften im Verteidigungsbereich für die Sicherheit und Verteidigung der EU im weiteren Sinne zur Verfügung stehen, und setzt das Europäische Parlament in Kenntnis***.

Änderungsantrag 44

Vorschlag für eine Verordnung
Artikel 9 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Maßnahmen zur Umsetzung des	(2) Maßnahmen zur Umsetzung des

Cybernotfallmechanismus werden mit Mitteln aus dem Programm Digitales Europa unterstützt und im Einklang mit der Verordnung (EU) 2021/694 und insbesondere deren spezifischen Ziel 3 durchgeführt.	Cybernotfallmechanismus werden mit Mitteln aus dem Programm Digitales Europa unterstützt, im Einklang mit der Verordnung (EU) 2021/694 und insbesondere deren spezifischen Ziel 3 durchgeführt ***und von der Europäischen Friedensfazilität (EFF) im Rahmen ihrer Unterstützungsmaßnahmen für Drittländer, insbesondere die Ukraine und Moldau, gefördert***.

Änderungsantrag 45

Vorschlag für eine Verordnung
Artikel 10 – Absatz 1 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) Vorsorgemaßnahmen, einschließlich koordinierter Tests der Abwehrbereitschaft der in hochkritischen Sektoren tätigen Einrichtungen in der gesamten Union;	a) Vorsorgemaßnahmen, einschließlich koordinierter Tests der Abwehrbereitschaft der in hochkritischen Sektoren tätigen Einrichtungen***, wie in den Bereichen öffentliche Infrastruktur, Wahlinfrastruktur, Verkehr, Gesundheitswesen, Finanzwesen, Telekommunikation, Lebensmittelversorgung und Sicherheit,*** in der gesamten Union;

Änderungsantrag 46

Vorschlag für eine Verordnung
Artikel 10 – Absatz 1 – Buchstabe c

Vorschlag der Kommission	*Geänderter Text*
c) Amtshilfe, die darin besteht, dass nationale Behörden eines Mitgliedstaats einen anderen Mitgliedstaat unterstützen, insbesondere gemäß Artikel 11 Absatz 3 Buchstabe f der Richtlinie (EU) 2022/2555**.**	c) Amtshilfe, die darin besteht, dass nationale Behörden eines Mitgliedstaats einen anderen Mitgliedstaat unterstützen, insbesondere gemäß Artikel 11 Absatz 3 Buchstabe f der Richtlinie (EU) 2022/2555 ***und im Sinne von Artikel 42 Absatz 7 EUV und Artikel 222 AEUV***.

Änderungsantrag 47

Vorschlag für eine Verordnung
Artikel 10 – Absatz 1 – Buchstabe c a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ca) Austausch und schrittweise Abschaffung kritischer Ausrüstungen von Hochrisikoanbietern, die den Sicherheits- und Verteidigungsinteressen der Union und ihrer Mitgliedstaaten, wie sie im Rahmen der GASP gemäß Titel V EUV festgelegt sind, zuwiderlaufen würden.

Änderungsantrag 48

Vorschlag für eine Verordnung
Artikel 11 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die NIS-Kooperationsgruppe entwickelt in Zusammenarbeit mit der Kommission, der ENISA ***und*** dem Hohen Vertreter gemeinsame Risikoszenarien und -methoden für die Durchführung der koordinierten Tests.	(2) Die NIS-Kooperationsgruppe entwickelt in Zusammenarbeit mit der Kommission, der ENISA***,*** dem Hohen Vertreter***, dem EAD und gegebenenfalls der EDA*** gemeinsame Risikoszenarien und -methoden für die Durchführung der koordinierten Tests.

Änderungsantrag 49

Vorschlag für eine Verordnung
Artikel 12 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die EU-Cybersicherheitsreserve besteht aus Sicherheitsvorfall-Notdiensten vertrauenswürdiger Anbieter, die nach den in Artikel 16 festgelegten Kriterien ausgewählt wurden. Die Reserve umfasst vorab zugesagte Dienste. Die Dienste müssen in allen Mitgliedstaaten durchführbar sein.	(2) Die EU-Cybersicherheitsreserve besteht aus Sicherheitsvorfall-Notdiensten vertrauenswürdiger Anbieter, die nach den in Artikel 16 festgelegten Kriterien ausgewählt wurden. Die Reserve umfasst vorab zugesagte Dienste. Die Dienste müssen in allen Mitgliedstaaten ***sowie in Drittländern, die die geltenden Anforderungen dieser Verordnung***

erfüllen, durchführbar sein.

Änderungsantrag 50

Vorschlag für eine Verordnung
Artikel 12 – Absatz 3 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) die Organe, Einrichtungen und sonstigen Stellen der Union.	b) die Organe, Einrichtungen und sonstigen Stellen der Union***, einschließlich der GSVP-Missionen***.

Änderungsantrag 51

Vorschlag für eine Verordnung
Artikel 12 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
(4) Die in Absatz 3 Buchstabe a genannten Nutzer nehmen die Dienste der EU-Cybersicherheitsreserve in Anspruch, um auf schwerwiegende Sicherheitsvorfälle oder Sicherheitsvorfälle großen Ausmaßes, von denen in kritischen und hochkritischen Sektoren tätige Einrichtungen betroffen sind, zu reagieren oder die Reaktion darauf und die anschließende sofortige Wiederherstellung zu unterstützen.	(4) Die in Absatz 3 Buchstabe a genannten Nutzer nehmen die Dienste der EU-Cybersicherheitsreserve in Anspruch, um auf schwerwiegende Sicherheitsvorfälle oder Sicherheitsvorfälle großen Ausmaßes, von denen in kritischen und hochkritischen Sektoren tätige Einrichtungen betroffen sind***, wie etwa in den Bereichen öffentliche Infrastruktur, Wahlinfrastruktur, Verkehr, Gesundheitswesen, Finanzwesen, Telekommunikation, Lebensmittelversorgung und Sicherheit***, zu reagieren oder die Reaktion darauf und die anschließende sofortige Wiederherstellung zu unterstützen.

Änderungsantrag 52

Vorschlag für eine Verordnung
Artikel 12 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
(5) Die Kommission trägt die Gesamtverantwortung für die Umsetzung	(5) Die Kommission trägt die Gesamtverantwortung für die Umsetzung

der EU-Cybersicherheitsreserve. Die Kommission legt die Prioritäten und die Entwicklung der EU-Cybersicherheitsreserve im Einklang mit den Anforderungen der in Absatz 3 genannten Nutzer fest; sie überwacht ihre Umsetzung und sorgt für Komplementarität, Kohärenz, Synergien und Verbindungen mit anderen Unterstützungsmaßnahmen im Rahmen dieser Verordnung sowie mit anderen Maßnahmen und Programmen der Union.	der EU-Cybersicherheitsreserve. Die Kommission legt die Prioritäten und die Entwicklung der EU-Cybersicherheitsreserve im Einklang mit den Anforderungen der in Absatz 3 genannten Nutzer fest; sie überwacht ihre Umsetzung und sorgt für Komplementarität, Kohärenz, Synergien und Verbindungen mit anderen Unterstützungsmaßnahmen im Rahmen dieser Verordnung sowie mit anderen Maßnahmen***,*** Programmen ***und Zielen*** der Union***, insbesondere mit dem strategischen Ziel, die Abhängigkeit von Hochrisikoanbietern zu verringern, die den Sicherheits- und Verteidigungsinteressen der Union und ihrer Mitgliedstaaten, wie sie im Rahmen der GASP gemäß Titel V EUV festgelegt sind, zuwiderlaufen würde***.

Änderungsantrag 53

Vorschlag für eine Verordnung
Artikel 12 – Absatz 7

Vorschlag der Kommission	*Geänderter Text*
(7) Zur Unterstützung der Kommission bei der Einrichtung der EU-Cybersicherheitsreserve arbeitet die ENISA nach Konsultation der Mitgliedstaaten und der Kommission eine Aufstellung der benötigten Dienste aus. Die ENISA arbeitet nach Konsultation der Kommission eine ähnliche Aufstellung aus, um den Bedarf von Drittländern zu ermitteln, die nach Artikel 17 Unterstützung aus der EU-Cybersicherheitsreserve erhalten können. Dabei konsultiert die Kommission gegebenenfalls den Hohen Vertreter.	(7) Zur Unterstützung der Kommission bei der Einrichtung der EU-Cybersicherheitsreserve arbeitet die ENISA nach Konsultation der Mitgliedstaaten und der Kommission eine Aufstellung der benötigten Dienste aus. Die ENISA arbeitet nach Konsultation der Kommission eine ähnliche Aufstellung aus, um ***mit Unterstützung des EAD*** den Bedarf von Drittländern zu ermitteln, die nach Artikel 17 Unterstützung aus der EU-Cybersicherheitsreserve erhalten können. Dabei konsultiert die Kommission gegebenenfalls den Hohen Vertreter.

Änderungsantrag 54

Vorschlag für eine Verordnung
Artikel 14 – Absatz 2 – Buchstabe a a (neu)

Vorschlag der Kommission	*Geänderter Text*
	aa) Auswirkungen des Vorfalls auf die Sicherheit und Verteidigung der Union;

Änderungsantrag 55

Vorschlag für eine Verordnung
Artikel 15 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) Die Unterstützung des Cybernotfallmechanismus kann in Absprache mit dem Hohen Vertreter die im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik und der Gemeinsamen Sicherheits- und Verteidigungspolitik geleistete Hilfe ergänzen, auch durch die Teams für die rasche Reaktion auf Cybervorfälle. Sie kann auch die Hilfe ergänzen, die ein Mitgliedstaat einem anderen Mitgliedstaat gemäß Artikel 42 Absatz 7 des Vertrags über die Europäische Union gewährt, oder dazu beitragen.	(3) Die Unterstützung des Cybernotfallmechanismus kann in Absprache mit dem Hohen Vertreter die im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik und der Gemeinsamen Sicherheits- und Verteidigungspolitik geleistete Hilfe ergänzen, auch durch die Teams für die rasche Reaktion auf Cybervorfälle***, um die Mitgliedstaaten der EU, die GSVP-Missionen und -Operationen und die Drittländer, die sich bei ihren Bemühungen um den Aufbau von Kapazitäten im Bereich der Cyberabwehr an der Gemeinsamen Außen- und Sicherheitspolitik und der Gemeinsamen Sicherheits- und Verteidigungspolitik der EU orientieren, insbesondere die Ukraine und Moldau, besser zu unterstützen***. Sie kann auch die Hilfe ergänzen, die ein Mitgliedstaat einem anderen Mitgliedstaat gemäß Artikel 42 Absatz 7 des Vertrags über die Europäische Union gewährt, oder dazu beitragen.

Änderungsantrag 56

Vorschlag für eine Verordnung
Artikel 16 – Absatz 2 – Buchstabe b a (neu)

Vorschlag der Kommission	*Geänderter Text*
	aa) Der Anbieter muss nachweisen, dass seine Entscheidungs- und Verwaltungsstrukturen frei von ungebührlicher Einflussnahme durch Regierungen von Staaten sind, die den Sicherheits- und Verteidigungsinteressen der Union und ihrer Mitgliedstaaten, wie sie im Rahmen der GASP gemäß Titel V EUV festgelegt sind, zuwiderlaufen würde.

Änderungsantrag 57

Vorschlag für eine Verordnung
Artikel 16 – Absatz 2 – Buchstabe f

Vorschlag der Kommission	*Geänderter Text*
f) Der Anbieter verfügt über die technische Hardware- und Softwareausrüstung, die zur Unterstützung des angeforderten Dienstes erforderlich ist.	f) Der Anbieter verfügt über die technische Hardware- und Softwareausrüstung, die zur Unterstützung des angeforderten Dienstes erforderlich ist***, und erfüllt die Anforderungen gemäß Artikel X der Verordnung XX/XXXX (Cyberresilienzgesetz)***.

Änderungsantrag 58

Vorschlag für eine Verordnung
Artikel 16 – Absatz 2 – Buchstabe j a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ja) Anbieter aus Drittländern mit hohem Risiko werden nicht zugelassen.

Änderungsantrag 59

Vorschlag für eine Verordnung
Artikel 16 – Absatz 2 – Buchstabe j b (neu)

Vorschlag der Kommission	*Geänderter Text*

	jb) Der Anbieter arbeitet, soweit möglich, eng mit den betreffenden KMU zusammen.

Änderungsantrag 60

Vorschlag für eine Verordnung
Artikel 17 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Drittländer können Unterstützung aus der EU-Cybersicherheitsreserve beantragen, wenn die Assoziierungsabkommen über ihre Teilnahme am Programm Digitales Europa dies vorsehen.	(1) Drittländer können Unterstützung aus der EU-Cybersicherheitsreserve beantragen, wenn***:***
	a) die Assoziierungsabkommen über ihre Teilnahme am Programm Digitales Europa dies vorsehen***;***
	b) in diese Drittländer eine GSVP-Mission mit dem konkreten Auftrag entsandt wurde, die Resilienz gegenüber hybriden Bedrohungen, auch Cyberbedrohungen, zu stärken, oder wenn in diesen Drittländern eine EFF-Unterstützungsmaßnahme zur Stärkung der Cyberresilienz des Landes eingeführt wurde.

Änderungsantrag 61

Vorschlag für eine Verordnung
Artikel 17 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die Unterstützung aus der EU-Cybersicherheitsreserve erfolgt im Einklang mit dieser Verordnung und unterliegt allen besonderen Bedingungen, die in den in Absatz ***1*** genannten Assoziierungsabkommen festgelegt sind.	(2) Die Unterstützung aus der EU-Cybersicherheitsreserve erfolgt im Einklang mit dieser Verordnung und unterliegt allen besonderen Bedingungen, die in den in Absatz genannten Assoziierungsabkommen festgelegt sind, ***mit Ausnahme derjenigen Drittländer, für die die in Absatz 1 Buchstabe b genannten***

Bestimmungen gelten.

Änderungsantrag 62

Vorschlag für eine Verordnung
Artikel 18 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Auf Ersuchen der Kommission, des EU-CyCLONe-Netzes oder des CSIRTs-Netzes nimmt die ENISA eine Überprüfung und Bewertung von Bedrohungen, Schwachstellen und Eindämmungsmaßnahmen im Zusammenhang mit einem bestimmten schwerwiegenden Cybersicherheitsvorfall oder Cybersicherheitsvorfall großen Ausmaßes vor. Nach Abschluss der Überprüfung und Bewertung eines Sicherheitsvorfalls legt die ENISA dem CSIRTs-Netz, dem EU-CyCLONe-Netz und der Kommission einen Bericht über die Überprüfung des Sicherheitsvorfalls vor, um sie – insbesondere auch im Hinblick auf die in den Artikeln 15 und 16 der Richtlinie (EU) 2022/2555 festgelegten Aufgaben – bei der Wahrnehmung ihrer Aufgaben zu unterstützen. Soweit dies zweckmäßig ist, gibt die Kommission den Bericht an den Hohen Vertreter weiter.	(1) Auf Ersuchen der Kommission, des EU-CyCLONe-Netzes oder des CSIRTs-Netzes nimmt die ENISA eine Überprüfung und Bewertung von Bedrohungen, Schwachstellen und Eindämmungsmaßnahmen im Zusammenhang mit einem bestimmten schwerwiegenden Cybersicherheitsvorfall oder Cybersicherheitsvorfall großen Ausmaßes vor. Nach Abschluss der Überprüfung und Bewertung eines Sicherheitsvorfalls legt die ENISA dem CSIRTs-Netz, dem EU-CyCLONe-Netz und der Kommission einen Bericht über die Überprüfung des Sicherheitsvorfalls vor, um sie – insbesondere auch im Hinblick auf die in den Artikeln 15 und 16 der Richtlinie (EU) 2022/2555 festgelegten Aufgaben – bei der Wahrnehmung ihrer Aufgaben zu unterstützen. Soweit dies zweckmäßig ist, ***insbesondere wenn der Vorfall ein Drittland betrifft,*** gibt die Kommission den Bericht an den Hohen Vertreter ***und den EAD*** weiter.

Änderungsantrag 63

Vorschlag für eine Verordnung
Artikel 18 – Absatz 3 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	3a. Der Bericht wird im Einklang mit den Rechtsvorschriften der Union oder der Mitgliedstaaten über den Schutz als Verschlusssache eingestufter vertraulicher Informationen dem

Europäischen Parlament übermittelt.

Änderungsantrag 64

Vorschlag für eine Verordnung
Artikel 19 – Absatz 1 – Nummer 1 – Buchstabe a – Ziffer 1
Verordnung (EU) 2021/694
Artikel 6 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
aa) Unterstützung des Aufbaus eines EU-Cyberschutzschilds, einschließlich der Entwicklung, der Einführung und des Betriebs nationaler und grenzübergreifender SOC-Plattformen, die zur Lageerfassung in der Union und zur Erweiterung der Kapazitäten der Union zur Gewinnung von Erkenntnissen über Cyberbedrohungen beitragen;	aa) Unterstützung des Aufbaus eines EU-Cyberschutzschilds, einschließlich der Entwicklung, der Einführung und des Betriebs nationaler und grenzübergreifender SOC-Plattformen, die zur Lageerfassung in der Union und zur Erweiterung der Kapazitäten der Union zur Gewinnung von Erkenntnissen über Cyberbedrohungen beitragen***, und Verringerung der Abhängigkeit der Union von Hochrisikoanbietern von kritischen Cybersicherheitsausrüstungen oder -komponenten, die den Sicherheits- und Verteidigungsinteressen der Union und ihrer Mitgliedstaaten, wie sie im Rahmen der GASP gemäß Titel V EUV festgelegt sind, zuwiderlaufen würde***;

Änderungsantrag 65

Vorschlag für eine Verordnung
Artikel 20 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
Bis zum [***vier*** Jahre nach dem Datum des Geltungsbeginns dieser Verordnung] legt die Kommission dem Europäischen Parlament und dem Rat einen Bericht über die Bewertung und Überprüfung dieser Verordnung vor.	Bis zum [***drei*** Jahre nach dem Datum des Geltungsbeginns dieser Verordnung ***und danach alle zwei Jahre***] legt die Kommission dem Europäischen Parlament und dem Rat einen Bericht über die Bewertung und Überprüfung dieser Verordnung vor.

VERFAHREN DES MITBERATENDEN AUSSCHUSSES

Titel	Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen
Bezugsdokumente – Verfahrensnummer	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Federführender Ausschuss Datum der Bekanntgabe im Plenum	ITRE 1.6.2023
Stellungnahme von Datum der Bekanntgabe im Plenum	AFET 1.6.2023
Verfasser der Stellungnahme Datum der Benennung	Dragoş Tudorache 16.6.2023
Prüfung im Ausschuss	18.9.2023
Datum der Annahme	24.10.2023
Ergebnis der Schlussabstimmung	+: 39 –: 4 0: 0
Zum Zeitpunkt der Schlussabstimmung anwesende Mitglieder	Alexander Alexandrov Yordanov, Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Włodzimierz Cimoszewicz, Katalin Cseh, Michael Gahler, Giorgos Georgiou, Sunčana Glavak, Bernard Guetta, Sandra Kalniete, Dietmar Köster, Andrius Kubilius, David Lega, Leopoldo López Gil, Jaak Madison, Pedro Marques, David McAllister, Vangelis Meimarakis, Sven Mikser, Francisco José Millán Mon, Matjaž Nemec, Demetris Papadakis, Kostas Papadakis, Tonino Picula, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Jordi Solé, Sergei Stanishev, Tineke Strik, Dominik Tarczyński, Dragoş Tudorache, Thomas Waitz, Bernhard Zimniok, Željana Zovko
Zum Zeitpunkt der Schlussabstimmung anwesende Stellvertreter	Attila Ara-Kovács, Lars Patrick Berg, Andrey Kovatchev, Georgios Kyrtsos, Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace

NAMENTLICHE SCHLUSSABSTIMMUNG IM MITBERATENDEN AUSSCHUSS

39	+
ECR	Lars Patrick Berg, Dominik Tarczyński
ID	Anna Bonfrisco, Jaak Madison
PPE	Alexander Alexandrov Yordanov, Traian Băsescu, Michael Gahler, Sunčana Glavak, Sandra Kalniete, Andrey Kovatchev, Andrius Kubilius, David Lega, Leopoldo López Gil, David McAllister, Vangelis Meimarakis, Francisco José Millán Mon, Željana Zovko
Renew	Petras Auštrevičius, Katalin Cseh, Bernard Guetta, Georgios Kyrtsos, Dragoş Tudorache
S&D	Attila Ara-Kovács, Włodzimierz Cimoszewicz, Dietmar Köster, Pedro Marques, Sven Mikser, Matjaž Nemec, Demetris Papadakis, Tonino Picula, Giuliano Pisapia, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Sergei Stanishev
Verts/ALE	Sergey Lagodinsky, Jordi Solé, Tineke Strik, Thomas Waitz

4	–
ID	Bernhard Zimniok
NI	Kostas Papadakis
The Left	Giorgos Georgiou, Mick Wallace

0	0

Erklärung der benutzten Zeichen:
+ : dafür
– : dagegen
0 : Enthaltung