European Parliament
2019-2024

Committee on Foreign Affairs

2023/0109(COD)

27.10.2023

OPINION

of the Committee on Foreign Affairs

for the Committee on Industry, Research and Energy

on the proposal for a regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents (COM(2023/0209) – C9-0136/2023 – 2023/0109(COD))

Rapporteur for opinion: Dragoş Tudorache

PA_Legam

Amendment 1

Proposal for a regulation
Recital 1

Text proposed by the Commission	*Amendment*
(1) The use of and dependence on information and communication technologies have become fundamental aspects in all sectors of economic activity as our public administrations, companies and citizens are more interconnected and interdependent across sectors and borders than ever before.	(1) The use of and dependence on information and communication technologies have become fundamental aspects in all sectors of economic ***as well as military*** activity as our public administrations, companies and citizens***, as well as military and defence actors*** are more interconnected and interdependent across sectors and borders than ever before.

Amendment 2

Proposal for a regulation
Recital 2

Text proposed by the Commission	*Amendment*
(2) The magnitude, frequency and impact of cybersecurity incidents are increasing, including supply chain attacks aiming at cyberespionage, ransomware or disruption. They represent a major threat to the functioning of network and information systems. In view of the fast-evolving threat landscape, the threat of possible large-scale incidents causing significant disruption or damage to critical infrastructures demands heightened preparedness at all levels of the Union's cybersecurity framework. ***That threat goes*** beyond Russia's military aggression on Ukraine, and ***is*** likely to persist given the multiplicity of state-aligned, criminal and hacktivist actors involved in current geopolitical tensions. Such incidents can impede the provision of public services and the pursuit of economic activities, including in critical or highly critical sectors, generate substantial financial losses, undermine user confidence, cause major damage to the economy of the Union, and could even	(2) The magnitude, frequency and impact of cybersecurity incidents are increasing, including supply chain attacks aiming at cyberespionage, ransomware or disruption. They represent a major threat to the functioning of network and information systems. In view of the fast-evolving threat landscape, the threat of possible large-scale incidents causing significant disruption or damage to critical infrastructures demands heightened preparedness at all levels of the Union's cybersecurity framework. ***The gravity of these threats became even more relevant due to the return of war on our continent. These threats go*** beyond Russia's military aggression on Ukraine, and ***are*** likely to persist given the multiplicity of state-aligned, criminal and hacktivist actors involved in current geopolitical tensions. Such incidents can impede the provision of public services and the pursuit of economic activities, including in critical or highly critical sectors, generate substantial financial

have health or life-threatening consequences. Moreover, cybersecurity incidents are unpredictable, as they often emerge and evolve within very short periods of time, not contained within any specific geographical area, and occurring simultaneously or spreading instantly across many countries.	losses, undermine user confidence, cause major damage to the economy ***and security*** of the Union, and could even have health or life-threatening consequences ***by possibly undermining local or national security related installations***. Moreover, cybersecurity incidents are unpredictable, as they often emerge and evolve within very short periods of time, not contained within any specific geographical area, and occurring simultaneously or spreading instantly across many countries. ***Cybersecurity is important to protect our European values, and ensures the functioning of our democracies by shielding our election infrastructure and democratic procedures from any foreign interference.***

Amendment 3

Proposal for a regulation
Recital 2 a (new)

Text proposed by the Commission	*Amendment*
	(2 a) Cybersecurity is crucial to keep our Union safe and prevent malicious actors, state and non-state, from undermining our democracy, economy, and security. It is necessary to prevent a fragmented landscape as such a situation would not represent an adequate approach, in particular when faced with the challenge of future large scale cyber attack targetting several Member States at the same time or transnational critical infrastructure. Therefore, a Union body that would act as a coordination platform for all existing and future cyber security instruments, funds and mechanisms is needed.

Amendment 4

Proposal for a regulation
Recital 3

Text proposed by the Commission	*Amendment*
(3) It is necessary to strengthen the competitive position of industry and services sectors in the Union across the digitised economy and support their digital transformation, by reinforcing the level of cybersecurity in the Digital Single Market. As recommended in three different proposals of the Conference on the Future of Europe[16] , it is necessary to increase the resilience of citizens, businesses and entities operating critical infrastructures against the growing cybersecurity threats, which can have devastating societal and economic impacts. Therefore, investment in infrastructures and services that will support faster detection and response to cybersecurity threats and incidents is needed, and Member States need assistance in better preparing for, as well as responding to significant and large-scale cybersecurity incidents. The Union should also increase its capacities in these areas, notably as regards the collection and analysis of data on cybersecurity threats and incidents.	(3) It is necessary to strengthen the competitive position of industry and services sectors in the Union across the digitised economy and support their digital transformation, by reinforcing the level of cybersecurity in the Digital Single Market. As recommended in three different proposals of the Conference on the Future of Europe[16] , it is necessary to increase the resilience of citizens, businesses and entities operating critical infrastructures against the growing cybersecurity threats, which can have devastating societal and economic impacts. Therefore, investment in infrastructures and services that will support faster detection and response to cybersecurity threats and incidents is needed, and Member States need assistance in better preparing for, as well as responding to significant and large-scale cybersecurity incidents. The Union should also increase its capacities in these areas, notably as regards the collection and analysis of data on cybersecurity threats and incidents***, as well as its ability to act proactively and react decisively to cybersecurity threats and incidents***.
[16] https://futureu.europa.eu/en/	[16] https://futureu.europa.eu/en/

Amendment 5

Proposal for a regulation
Recital 4

Text proposed by the Commission	*Amendment*
(4) The Union has already taken a number of measures to reduce vulnerabilities and increase the resilience	(4) The Union has already taken a number of measures to reduce vulnerabilities and increase the resilience

of critical infrastructures and entities against cybersecurity risks, in particular Directive (EU) 2022/2555 of the European Parliament and of the Council[17] , Commission Recommendation (EU) 2017/1584[18] , Directive 2013/40/EU of the European Parliament and of the Council[19] and Regulation (EU) 2019/881 of the European Parliament and of the Council[20] . In addition, the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure invites Member States to take urgent and effective measures, and to cooperate loyally, efficiently, in solidarity and in a coordinated manner with each other, the Commission and other relevant public authorities as well as the entities concerned, to enhance the resilience of critical infrastructure used to provide essential services in the internal market.

[17] Directive (EU) 2022/2555 of the

of critical infrastructures and entities against cybersecurity risks, in particular Directive (EU) 2022/2555 of the European Parliament and of the Council[17] , Commission Recommendation (EU) 2017/1584[18] , Directive 2013/40/EU of the European Parliament and of the Council[19] and Regulation (EU) 2019/881 of the European Parliament and of the Council[20] . In addition, the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure invites Member States to take urgent and effective measures, and to cooperate loyally, efficiently, ***and proactively,*** in solidarity and in a coordinated manner with each other, the Commission and other relevant public authorities as well as the entities concerned, to enhance the resilience of critical infrastructure used to provide essential services in the internal market. ***Furthermore, the Union approved and launched its Strategic Compass for Security and Defence on March 2022, which focuses inter alia on strengthening cyber security and enhancing international cooperation with like-minded allies and democratic partners especially in this matter. Moreover, cyber-security has been a focal point of the recent Third Joint Declaration on EU-NATO Cooperation of January 2023. In particular, the final assessment report of the EU-NATO task force recommended making full use of synergies between EU and NATO[1], including the exchange of best practices between civilian and military actors on the implementation of relevant cyber-related policies and legislation.***

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

[17] Directive (EU) 2022/2555 of the

European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022).

[18] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

[19] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (J L 218, 14.8.2013, p. 8).

[20] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022).

[18] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

[19] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (J L 218, 14.8.2013, p. 8).

[20] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

Amendment 6

Proposal for a regulation
Recital 6

Text proposed by the Commission	*Amendment*
(6) The Joint Communication on the EU Policy on Cyber Defence[22] adopted on 10 November 2022 announced an EU Cyber Solidarity Initiative with the following objectives: strengthening of common EU detection, situational awareness and response capabilities by promoting the deployment of an EU infrastructure of Security Operations Centres (‘SOCs’), supporting gradual building of an EU-level cybersecurity	(6) The Joint Communication on the EU Policy on Cyber Defence[22] adopted on 10 November 2022 announced an EU Cyber Solidarity Initiative with the following objectives: strengthening of common EU detection, situational awareness and response capabilities by promoting the deployment of an EU infrastructure of Security Operations Centres (‘SOCs’), supporting gradual building of an EU-level cybersecurity

reserve with services from trusted private providers and testing of critical entities for potential vulnerabilities based on EU risk assessments.	reserve with services from trusted private providers and testing of critical entities for potential vulnerabilities based on EU risk assessments. ***In addition, the rapidly evolving cyber threat landscape and the fast pace of technological development also demonstrate the need for enhanced civil-military coordination and cooperation, as stressed by the Council in its Conclusions on the EU Policy on Cyber Defence[1].***
	[1] Council Conclusions on the EU Policy on Cyber Defence approved by the Council at its meeting on 22 May 2023, (9618/23)
[22] Join Communication to the European Parliament and the Council EU Policy on Cyber Defence JOIN/2022/49 final	[22] Join Communication to the European Parliament and the Council EU Policy on Cyber Defence JOIN/2022/49 final

Amendment 7

Proposal for a regulation
Recital 6 a (new)

Text proposed by the Commission	*Amendment*
	(6 a) Given the blurring of lines between the realms of civilian and military matters and the dual-use nature of cyber tools and technologies, there is a need for a comprehensive and holistic approach to the digital domain. In the event of a large-scale cybersecurity incident and crisis involving more than one Member State, appropriate crisis management and governance should be established. Such structures should organise exchange of information, coordination and cooperation with the Union's external security and military crisis management structures and Member States' bodies in charge of security and defence (the cyber defence community). This should also apply to Common Security and Defence Policy

operations and missions conducted by the Union to ensure peace and stability in its neighbourhood and beyond.

Amendment 8

Proposal for a regulation
Recital 7

Text proposed by the Commission	*Amendment*
(7) It is necessary to strengthen the detection and situational awareness of cyber threats and incidents throughout the Union and to strengthen solidarity by enhancing Member States' and the Union's preparedness and capabilities to respond to significant and large-scale cybersecurity incidents. Therefore a pan-European infrastructure of SOCs (European Cyber Shield) should be deployed to build and enhance common detection and situational awareness capabilities; a Cybersecurity Emergency Mechanism should be established to support Member States in preparing for, responding to, and immediately recovering from significant and large-scale cybersecurity incidents; a Cybersecurity Incident Review Mechanism should be established to review and assess specific significant or large-scale incidents. These actions shall be without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union ('TFEU').	(7) It is necessary to strengthen the detection and situational awareness of cyber threats and incidents throughout the Union and to strengthen solidarity by enhancing Member States' and the Union's preparedness and capabilities to respond to significant and large-scale cybersecurity incidents. Therefore a pan-European infrastructure of SOCs (European Cyber Shield) should be deployed to build and enhance common detection and situational awareness capabilities; a Cybersecurity Emergency Mechanism should be established to support Member States in preparing for, responding to, and immediately recovering from significant and large-scale cybersecurity incidents***, including the incidents involving more than one Member State. When feasible and necessary, a Cybersecurity Emergency Mechanism should organise information-sharing and cooperation with Member States' defence authorities and supported by EU institutions, bodies and agencies (the EU cyber defence community)***; a Cybersecurity Incident Review Mechanism should be established to review and assess specific significant or large-scale incidents. ***Such new structures should also support EU CSDP operations and missions.*** These actions shall be without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union ('TFEU').

Amendment 9

Proposal for a regulation
Recital 11

Text proposed by the Commission	*Amendment*
(11) For the purpose of sound financial management, specific rules should be laid down for the carry-over of unused commitment and payment appropriations. While respecting the principle that the Union budget is set annually, this Regulation should, on account of the unpredictable, exceptional and specific nature of the cybersecurity landscape, provide for possibilities to carry over unused funds beyond those set out in the Financial Regulation, thus maximising the Cybersecurity Emergency Mechanism's capacity to support Member States in countering effectively cyber threats.	(11) For the purpose of sound financial management, specific rules should be laid down for the carry-over of unused commitment and payment appropriations. While respecting the principle that the Union budget is set annually, this Regulation should, on account of the unpredictable, exceptional and specific nature of the cybersecurity landscape, provide for possibilities to carry over unused funds beyond those set out in the Financial Regulation, thus maximising the Cybersecurity Emergency Mechanism's capacity to support Member States in countering effectively cyber threats. ***These specific rules would also permit longer term financial support for joint procurement of next-generation ultra-secure tools and infrastructure, to improve collective detection capabilities by using the latest artificial intelligence (AI) and data analytics.***

Amendment 10

Proposal for a regulation
Recital 13

Text proposed by the Commission	*Amendment*
(13) Each Member State should designate a public body at national level tasked with coordinating cyber threat detection activities in that Member State. These National SOCs should act as a reference point and gateway at national level for participation in the European Cyber Shield and should ensure that cyber threat information from public and private entities is shared and collected at national level in an effective and streamlined	(13) Each Member State should designate a public body at national level tasked with coordinating cyber threat detection activities in that Member State. These National SOCs should act as a reference point and gateway at national level for participation in the European Cyber Shield and should ensure that cyber threat information from public and private entities is shared and collected at national level in an effective and streamlined

manner.	manner. ***When feasible and necessary, SOCs should also allow for the participation of defence entities, establishing a 'defence pillar' in terms of governance and type of information shared, as set out in the Joint Communication on the EU Policy on Cyber Defence[1] and supported by the High Representative.***
	[1] Joint Communication to the European Parliament and the Council EU Policy on Cyber Defence JOIN/2022/49 final

Amendment 11

Proposal for a regulation
Recital 14

Text proposed by the Commission	*Amendment*
(14) As part of the European Cyber Shield, a number of Cross-border Cybersecurity Operations Centres (‘Cross-border SOCs’) should be established. These should bring together National SOCs from at least three Member States, so that the benefits of cross-border threat detection and information sharing and management can be fully achieved. The general objective of Cross-border SOCs should be to strengthen capacities to analyse, prevent and detect cybersecurity threats and to support the production of high-quality intelligence on cybersecurity threats, notably through the sharing of data from various sources, public or private, as well as through the sharing and joint use of state-of-the-art tools, and jointly developing detection, analysis and prevention capabilities in a trusted environment. They should provide new additional capacity, building upon and complementing existing SOCs and computer incident response teams (‘CSIRTs’) and other relevant actors.	(14) As part of the European Cyber Shield, a number of Cross-border Cybersecurity Operations Centres (‘Cross-border SOCs’) should be established. These should bring together National SOCs from at least three Member States, ***including a ‘defence pillar’,*** so that the benefits of cross-border threat detection and information sharing and management can be fully achieved. The general objective of Cross-border SOCs should be to strengthen capacities to analyse, prevent and detect cybersecurity threats and to support the production of high-quality intelligence on cybersecurity threats, notably through the sharing of data from various sources, public or private ***and, when necessary and feasible military with sufficient guidance for information sharing,*** , as well as through the sharing and joint use of state-of-the-art tools, and jointly developing detection, analysis and prevention capabilities in a trusted environment. They should provide new additional capacity, building upon and complementing existing SOCs and computer incident response teams

('CSIRTs') and other relevant actors.

Amendment 12

Proposal for a regulation
Recital 15

Text proposed by the Commission	*Amendment*
(15) At national level, the monitoring, detection and analysis of cyber threats is typically ensured by SOCs of public and private entities, in combination with CSIRTs. In addition, CSIRTs exchange information in the context of the CSIRT network, in accordance with Directive (EU) 2022/2555. The Cross-border SOCs should constitute a new capability that is complementary to the CSIRTs network, by pooling and sharing data on cybersecurity threats from public and private entities, enhancing the value of such data through expert analysis and jointly acquired infrastructures and state of the art tools, and contributing to the development of Union capabilities and ***technological sovereignty***.	(15) At national level, the monitoring, detection and analysis of cyber threats is typically ensured by SOCs of public and private entities, in combination with CSIRTs. In addition, CSIRTs exchange information in the context of the CSIRT network, in accordance with Directive (EU) 2022/2555. The Cross-border SOCs should constitute a new capability that is complementary to the CSIRTs network, by pooling and sharing data on cybersecurity threats from public and private entities, enhancing the value of such data through expert analysis and jointly acquired infrastructures and state of the art tools, and contributing to the development of Union capabilities and ***resilience***.

Amendment 13

Proposal for a regulation
Recital 16

Text proposed by the Commission	*Amendment*
(16) The Cross-border SOCs should act as a central point allowing for a broad pooling of relevant data and cyber threat intelligence, enable the spreading of threat information among a large and diverse set of actors (e.g., Computer Emergency Response Teams ('CERTs'), CSIRTs, Information Sharing and Analysis Centers ('ISACs'), operators of critical infrastructures). The information exchanged among participants in a Cross-border SOC could include data from	(16) The Cross-border SOCs should act as a central point allowing for a broad pooling of relevant data and cyber threat intelligence, enable the spreading of threat information among a large and diverse set of actors (e.g., Computer Emergency Response Teams ('CERTs'), CSIRTs, Information Sharing and Analysis Centers ('ISACs'), operators of critical infrastructures***, as well as the cyber defence community***. The information exchanged among participants in a Cross-

networks and sensors, threat intelligence feeds, indicators of compromise, and contextualised information about incidents, threats and vulnerabilities. In addition, Cross-border SOCs should also enter into cooperation agreements with other Cross-border SOCs.

border SOC could include data from networks and sensors, threat intelligence feeds, indicators of compromise, and contextualised information about incidents, threats and vulnerabilities. In addition, Cross-border SOCs should also enter into cooperation agreements with other Cross-border SOCs ***and operational network for milCERTs (MICNET) when established***.

Amendment 14

Proposal for a regulation
Recital 17

Text proposed by the Commission	*Amendment*
(17) Shared situational awareness among relevant authorities is an indispensable prerequisite for Union-wide preparedness and coordination with regards to significant and large-scale cybersecurity incidents. Directive (EU) 2022/2555 establishes the EU–CyCLONe to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies and agencies. Recommendation (EU) 2017/1584 on coordinated response to large-scale cybersecurity incidents and crises addresses the role of all relevant actors. Directive (EU) 2022/2555 also recalls the Commission's responsibilities in the Union Civil Protection Mechanism ('UCPM') established by Decision 1313/2013/EU of the European Parliament and of the Council, as well as for providing analytical reports for the Integrated Political Crisis Response Mechanism ('IPCR') arrangements under Implementing Decision (EU) 2018/1993. Therefore, in situations where Cross-border SOCs obtain information related to a potential or ongoing large-scale cybersecurity incident, they should provide relevant information to EU-CyCLONe, the	(17) Shared situational awareness among relevant authorities is an indispensable prerequisite for Union-wide preparedness and coordination with regards to significant and large-scale cybersecurity incidents. Directive (EU) 2022/2555 establishes the EU–CyCLONe to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies and agencies. Recommendation (EU) 2017/1584 on coordinated response to large-scale cybersecurity incidents and crises addresses the role of all relevant actors. Directive (EU) 2022/2555 also recalls the Commission's responsibilities in the Union Civil Protection Mechanism ('UCPM') established by Decision 1313/2013/EU of the European Parliament and of the Council, as well as for providing analytical reports for the Integrated Political Crisis Response Mechanism ('IPCR') arrangements under Implementing Decision (EU) 2018/1993. Therefore, in situations where Cross-border SOCs obtain information related to a potential or ongoing large-scale cybersecurity incident, they should provide relevant information to EU-CyCLONe, the

CSIRTs network and the Commission. In particular, depending on the situation, information to be shared could include technical information, information about the nature and motives of the attacker or potential attacker, and higher-level non-technical information about a potential or ongoing large-scale cybersecurity incident. In this context, due regard should be paid to the need-to-know principle and to the potentially sensitive nature of the information shared.	CSIRTs network ***the cyber defence community*** and the Commission. In particular, depending on the situation, information to be shared could include technical information, information about the nature and motives of the attacker or potential attacker, and higher-level non-technical information about a potential or ongoing large-scale cybersecurity incident. In this context, due regard should be paid to the need-to-know principle and to the potentially sensitive nature of the information shared.

Amendment 15

Proposal for a regulation
Recital 19

Text proposed by the Commission	*Amendment*
(19) In order to enable the exchange of data on cybersecurity threats from various sources, on a large-scale basis, in a trusted environment, entities participating in the European Cyber Shield should be equipped with state-of-the-art and highly-secure tools, equipment and infrastructures. This should make it possible to improve collective detection capacities and timely warnings to authorities and relevant entities, notably by using the latest artificial intelligence and data analytics technologies.	(19) In order to enable the exchange of data on cybersecurity threats from various sources, on a large-scale basis, in a trusted environment, entities participating in the European Cyber Shield should be equipped with state-of-the-art and highly-secure tools, equipment and infrastructures***, excluding high-risk suppliers of critical products with digital elements***. This should make it possible to improve collective detection capacities and timely warnings to authorities and relevant entities, notably by using the latest artificial intelligence and data analytics technologies. ***Human oversight should be provided for when using AI, and sufficient level of AI literacy, necessary support and authority to exercise that function should be ensured.***

Amendment 16

Proposal for a regulation
Recital 19 a (new)

Text proposed by the Commission	*Amendment*
	(19 a) In accordance with Regulation [XX/XXXX (Cyber Resilience Act)] entities participating in the European Cyber Shield should also cover the requirements laid down in this Regulation for all products with digital elements. In view of the increasing risks coming from economic dependencies, it is necessary to minimise the exposure to high-risk suppliers of critical products, through a common strategic framework for EU economic security. Dependencies on high-risk suppliers of critical products with digital elements pose a strategic risk that should be addressed at Union level, in particular whether a country engages in economic espionage or economic coercion and its legislation obliges arbitrary access to any kind of company operations or data, especially when the critical products are intended for the use by essential entities referred to in Directive (EU) 2022/2555.

Amendment 17

Proposal for a regulation
Recital 20

Text proposed by the Commission	*Amendment*
(20) By collecting, sharing and exchanging data, the European Cyber Shield should enhance the Union's technological sovereignty. The pooling of high-quality curated data should also contribute to the development of advanced artificial intelligence and data analytics technologies. It should be facilitated through the connection of the European Cyber Shield with the pan-European High Performance Computing infrastructure established by Council Regulation (EU) 2021/1173[25] .	(20) By collecting, sharing and exchanging data, the European Cyber Shield should enhance the Union's technological sovereignty***, its strategic autonomy, competitiveness and resilience***. The pooling of high-quality curated data should also contribute to the development of advanced artificial intelligence and data analytics technologies. It should be facilitated through the connection of the European Cyber Shield with the pan-European High Performance Computing infrastructure established by Council

Regulation (EU) 2021/1173[25] .

[25] Council Regulation (EU) 2021/1173 of 13 July 2021 on establishing the European High Performance Computing Joint Undertaking and repealing Regulation (EU) 2018/1488 (OJ L 256, 19.7.2021, p. 3).

[25] Council Regulation (EU) 2021/1173 of 13 July 2021 on establishing the European High Performance Computing Joint Undertaking and repealing Regulation (EU) 2018/1488 (OJ L 256, 19.7.2021, p. 3).

Amendment 18

Proposal for a regulation
Recital 25

Text proposed by the Commission	*Amendment*
(25) The Cyber Emergency Mechanism should provide support to Member States complementing their own measures and resources, and other existing support options in case of response to and immediate recovery from significant and large-scale cybersecurity incidents, such as the services provided by the European Union Agency for Cybersecurity ('ENISA') in accordance with its mandate, the coordinated response and the assistance from the CSIRTs network, the mitigation support from the EU-CyCLONe, as well as mutual assistance between Member States including in the context of Article 42(7) of TEU, the PESCO Cyber Rapid Response Teams***[26]*** and Hybrid Rapid Response Teams. It should address the need to ensure that specialised means are available to support preparedness and response to cybersecurity incidents across the Union and in third countries.	(25) The Cyber Emergency Mechanism should provide support to Member States complementing their own measures and resources, and other existing support options in case of response to and immediate recovery from significant and large-scale cybersecurity incidents, such as the services provided by the European Union Agency for Cybersecurity ('ENISA') in accordance with its mandate, the coordinated response and the assistance from the CSIRTs network, the mitigation support from the EU-CyCLONe, as well as mutual assistance between Member States including in the context of Article 42(7) of TEU, the PESCO Cyber Rapid Response Teams***[1], the new PESCO-project Cyber Information Domain Coordination Centre (CIDCC) and its proposed successor the EU Cyber Defence Coordination Centre (EUCDCC),*** and Hybrid Rapid Response Teams. It should address the need to ensure that specialised means are available to support preparedness and response to cybersecurity incidents across the Union and in third countries***, especially those EU candidate countries aligned with the EU Common Foreign and Security Policy and Common Security and Defence Policy, supporting them in building up their cyber capabilities and enhancing cross-***

border and regional cooperation among those candidate countries in the field of cyber.

[1] COUNCIL DECISION (CFSP) 2017/ 2315 - of 11 December 2017 - establishing permanent structured cooperation (PESCO) and determining the list of participating Member States.

---

[26] COUNCIL DECISION (CFSP) 2017/ 2315 - of 11 December 2017 - establishing permanent structured cooperation (PESCO) and determining the list of participating Member States.

---

[26] COUNCIL DECISION (CFSP) 2017/ 2315 - of 11 December 2017 - establishing permanent structured cooperation (PESCO) and determining the list of participating Member States.

Amendment 19

Proposal for a regulation
Recital 26

Text proposed by the Commission	*Amendment*
(26) This instrument is without prejudice to procedures and frameworks to coordinate crisis response at Union level, in particular the UCPM[27] , IPCR[28] , and Directive (EU) 2022/2555. It may contribute to or complement actions implemented in the context of Article 42(7) of TEU or in situations defined in Article 222 of TFEU. The use of this instrument should also be coordinated with the implementation of Cyber Diplomacy Toolbox's measures, ***where appropriate***.	(26) This instrument is without prejudice to procedures and frameworks to coordinate crisis response at Union level, in particular the UCPM[27] , IPCR[28] , and Directive (EU) 2022/2555. It may contribute to or complement actions implemented in the context of Article 42(7) of TEU or in situations defined in Article 222 of TFEU. The use of this instrument should also be coordinated with the implementation of Cyber Diplomacy Toolbox's measures, ***enhancing cooperation at the strategic, operational and technical level between cyber defence and other cyber communities, particularly in order to strengthen capabilities against cybersecurity threats from outside the Union, including restrictive measures, that can be used to prevent and respond to malicious cyber activities***.

---

[27] Decision No 1313/2013/EU of the European Parliament and of the Council of

---

[27] Decision No 1313/2013/EU of the European Parliament and of the Council of

17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924).

[28] Integrated Political Crisis Response arrangements (IPCR) and in accordance with Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises.

17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924).

[28] Integrated Political Crisis Response arrangements (IPCR) and in accordance with Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises.

Amendment 20

Proposal for a regulation
Recital 28

Text proposed by the Commission	*Amendment*
(28) Directive (EU) 2022/2555 requires Member States to designate or establish one or more cyber crisis management authorities and ensure they have adequate resources to carry out their tasks in an effective and efficient manner. It also requires Member States to identify capabilities, assets and procedures that can be deployed in the case of a crisis as well as to adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. Member States are also required to establish one or more CSIRTs tasked with incident handling responsibilities in accordance with a well-defined process and covering at least the sectors, subsectors and types of entities under the scope of that Directive, and to ensure they have adequate resources to carry out effectively their tasks. This Regulation is without prejudice to the Commission's role in ensuring the compliance by Member States with the obligations of Directive (EU) 2022/2555. The Cyber Emergency Mechanism should provide assistance for actions aimed at reinforcing preparedness as well as incident response actions to mitigate the	(28) Directive (EU) 2022/2555 requires Member States to designate or establish one or more cyber crisis management authorities and ensure they have adequate resources to carry out their tasks in an effective and efficient manner. It also requires Member States to identify capabilities, assets and procedures that can be deployed in the case of a crisis as well as to adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. Member States are also required to establish one or more CSIRTs tasked with incident handling responsibilities in accordance with a well-defined process and covering at least the sectors, subsectors and types of entities under the scope of that Directive, and to ensure they have adequate resources to carry out effectively their tasks. This Regulation is without prejudice to the Commission's role in ensuring the compliance by Member States with the obligations of Directive (EU) 2022/2555. The Cyber Emergency Mechanism should provide assistance for actions aimed at reinforcing preparedness as well as incident response actions to mitigate the

impact of significant and large-scale cybersecurity incidents, to support immediate recovery and/or restore the functioning of essential services.

impact of significant and large-scale cybersecurity incidents, to support immediate recovery and/or restore the functioning of essential services***, making appropriate use of the whole range of defensive options available to the civilian and military communities***.

Amendment 21

Proposal for a regulation
Recital 29

Text proposed by the Commission	*Amendment*
(29) As part of the preparedness actions, to promote a consistent approach and strengthen security across the Union and its internal market, support should be provided for testing and assessing cybersecurity of entities operating in highly critical sectors identified pursuant to Directive (EU) 2022/2555 in a coordinated manner. For this purpose, the Commission, with the support of ENISA and in cooperation with the NIS Cooperation Group established by Directive (EU) 2022/2555, should regularly identify relevant sectors or subsectors, which should be eligible to receive financial support for coordinated testing at Union level. ***The*** sectors or subsectors should be selected from Annex I to Directive (EU) 2022/2555 ('Sectors of High Criticality'). The coordinated testing exercises should be based on common risk scenarios and methodologies. The selection of sectors and development of risk scenarios should take into account relevant Union-wide risk assessments and risk scenarios, including the need to avoid duplication, such as the risk evaluation and risk scenarios called for in the Council conclusions on the development of the European Union's cyber posture to be conducted by the Commission, the High Representative and the NIS Cooperation Group, in coordination with relevant civilian and	(29) As part of the preparedness actions, to promote a consistent approach and strengthen security across the Union and its internal market, support should be provided for testing and assessing cybersecurity of entities operating in highly critical sectors identified pursuant to Directive (EU) 2022/2555 in a coordinated manner. For this purpose, the Commission, with the support of ENISA and in cooperation with the NIS Cooperation Group established by Directive (EU) 2022/2555, should regularly identify relevant sectors or subsectors, which should be eligible to receive financial support for coordinated testing at Union level. ***When appropriate, the European External Action Service (EEAS), in particular through the EU Intelligence Centre (INTCEN) and its Hybrid Fusion Cell, with the support of the Intelligence Directorate of the European Union Military Staff (EUMS) under the Single Intelligence Analysis Capability (SIAC), should also be associated to provide up-to-date assessments and thus contribute to the identification of the*** sectors or subsectors ***that*** should be selected from Annex I to Directive (EU) 2022/2555 ('Sectors of High Criticality'). The coordinated testing exercises should be based on common risk scenarios and methodologies. ***These exercises should***

military bodies and agencies and established networks, including the EU CyCLONe, as well as the risk assessment of communications networks and infrastructures requested by the Joint Ministerial Call of Nevers and conducted by the NIS Cooperation Group, with the support of the Commission and ENISA, and in cooperation with the Body of European Regulators for Electronic Communications (BEREC), the coordinated risk assessments to be conducted under Article 22 of Directive (EU) 2022/2555 and digital operational resilience testing as provided for in Regulation (EU) 2022/2554 of the European Parliament and of the Council***[29]*** . The selection of sectors should also take into account the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.

also play an important role in improving cooperation between civilian and military entities. When organising exercises, the Commission, the EEAS and ENISA should therefore systematically consider including participants from other cyber communities, as such the European Defence Agency (EDA) and other relevant entities. The selection of sectors and development of risk scenarios should take into account relevant Union-wide risk assessments and risk scenarios, including the need to avoid duplication, such as the risk evaluation and risk scenarios called for in the Council conclusions on the development of the European Union's cyber posture to be conducted by the Commission, the High Representative and the NIS Cooperation Group, in coordination with relevant civilian and military bodies and agencies and established networks, including the EU CyCLONe, as well as the risk assessment of communications networks and infrastructures requested by the Joint Ministerial Call of Nevers and conducted by the NIS Cooperation Group, with the support of the Commission and ENISA, and in cooperation with the Body of European Regulators for Electronic Communications (BEREC), the coordinated risk assessments to be conducted under Article 22 of Directive (EU) 2022/2555 and digital operational resilience testing as provided for in Regulation (EU) 2022/2554 of the European Parliament and of the Council***[1]***. The selection of sectors should also take into account the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.

[1] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU)

	No 600/2014, (EU) No 909/2014 and (EU) 2016/1011
[29] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011	[29] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

Amendment 22

Proposal for a regulation
Recital 32

Text proposed by the Commission	*Amendment*
(32) The Cyber Emergency Mechanism should support assistance provided by Member States to a Member State affected by a significant or large-scale cybersecurity incident, including by the CSIRTs network set out in Article 15 of Directive (EU) 2022/2555. Member States providing assistance should be allowed to submit requests to cover costs related to dispatching of expert teams in the framework of mutual assistance. The eligible costs could include travel, accommodation and daily allowance expenses of cybersecurity experts.	(32) The Cyber Emergency Mechanism should support assistance provided by Member States to a Member State affected by a significant or large-scale cybersecurity incident, including by the CSIRTs network set out in Article 15 of Directive (EU) 2022/2555. Member States providing assistance should be allowed to submit requests to cover costs related to dispatching of expert teams in the framework of mutual assistance***, ensuring efficient coordination among the EU's relevant programmes and instruments, including the European Peace Facility (EPF), CFSP and NDICI, when providing assistance to third countries, particularly Ukraine and Moldova.***. The eligible costs could include travel, accommodation and daily allowance expenses of cybersecurity experts.

Amendment 23

Proposal for a regulation
Recital 33

Text proposed by the Commission	*Amendment*
(33) A Union-level Cybersecurity Reserve should gradually be set up, consisting of services from private providers of managed security services to support response and immediate recovery actions in cases of significant or large-scale cybersecurity incidents. The EU Cybersecurity Reserve should ensure the availability and readiness of services. The services from the EU Cybersecurity Reserve should serve to support national authorities in providing assistance to affected entities operating in critical or highly critical sectors as a complement to their own actions at national level. When requesting support from the EU Cybersecurity Reserve, Member States should specify the support provided to the affected entity at the national level, which should be taken into account when assessing the Member State request. The services from the EU Cybersecurity Reserve may also serve to support Union institutions, bodies and agencies, under similar conditions.	(33) A Union-level Cybersecurity Reserve should gradually be set up, consisting of services from private providers of managed security services to support response and immediate recovery actions in cases of significant or large-scale cybersecurity incidents. The EU Cybersecurity Reserve should ensure the availability and readiness of services. The services from the EU Cybersecurity Reserve should serve to support national authorities in providing assistance to affected entities operating in critical or highly critical sectors as a complement to their own actions at national level. When requesting support from the EU Cybersecurity Reserve, Member States should specify the support provided to the affected entity at the national level, which should be taken into account when assessing the Member State request. The services from the EU Cybersecurity Reserve may also serve to support Union institutions, bodies and agencies, ***including CSDP missions*** under similar conditions.

Amendment 24

Proposal for a regulation
Recital 34

Text proposed by the Commission	*Amendment*
(34) For the purpose of selecting private service providers to provide services in the context of the EU Cybersecurity Reserve, it is necessary to establish a set of minimum criteria that should be included in the call for tenders to select these providers, so as to ensure that the needs of Member States' authorities and entities operating in critical or highly critical sectors are met.	(34) For the purpose of selecting private service providers to provide services in the context of the EU Cybersecurity Reserve, it is necessary to establish a set of minimum criteria that should be included in the call for tenders to select these providers, so as to ensure that the needs of Member States' authorities and entities operating in critical or highly critical sectors are met***, taking also into account the risks associated with the participation of providers from strategic competitor countries, which may***

give rise to economic security risks, as well as the implications for the strategic security of the Union.

Amendment 25

Proposal for a regulation
Recital 36

Text proposed by the Commission	*Amendment*
(36) In order to support the objectives of this Regulation of promoting shared situational awareness, enhancing Union's resilience and enabling effective response to significant and large-scale cybersecurity incidents, the EU=CyCLONe, the CSIRTs network or the Commission should be able to ask ENISA to review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. After the completion of a review and assessment of an incident, ENISA should prepare an incident review report, in collaboration with relevant stakeholders, including representatives from the private sector, Member States, the Commission and other relevant EU institutions, bodies and agencies. As regards the private sector, ENISA is developing channels for exchanging information with specialised providers, including providers of managed security solutions and vendors, in order to contribute to ENISA's mission of achieving a high common level of cybersecurity across the Union. Building on the collaboration with stakeholders, including the private sector, the review report on specific incidents should aim at assessing the causes, impacts and mitigations of an incident, after it has occurred. Particular attention should be paid to the input and lessons shared by the managed security service providers that fulfil the conditions of highest professional integrity, impartiality and requisite technical expertise as required by this	(36) In order to support the objectives of this Regulation of promoting shared situational awareness, enhancing Union's resilience and enabling effective response to significant and large-scale cybersecurity incidents, the EU=CyCLONe, the CSIRTs network or the Commission should be able to ask ENISA to review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. ***In view of the development of a secure connectivity system, building on the European quantum communication infrastructure (EuroQCI) and the European Union Governmental Satellite Communication (GOVSATCOM), in particular the implementation of GALILEO GNSS for defence users, any future possible development should take into account the advent of 'hyperwar' which merges the speed and sophistication of quantum computing with highly autonomous military systems*** After the completion of a review and assessment of an incident, ENISA should prepare an incident review report, in collaboration with relevant stakeholders, including representatives from the private sector, Member States, the Commission and other relevant EU institutions, bodies and agencies. As regards the private sector, ENISA is developing channels for exchanging information with specialised providers, including providers of managed security solutions and vendors, in order to contribute to ENISA's mission of

Regulation. The report should be delivered and feed into the work of the EU=CyCLONe, the CSIRTs network and the Commission. When the incident relates to a third country, it will also be shared by the Commission with the High Representative.	achieving a high common level of cybersecurity across the Union. Building on the collaboration with stakeholders, including the private sector, the review report on specific incidents should aim at assessing the causes, impacts and mitigations of an incident, after it has occurred. Particular attention should be paid to the input and lessons shared by the managed security service providers that fulfil the conditions of highest professional integrity, impartiality and requisite technical expertise as required by this Regulation. The report should be delivered and feed into the work of the EU=CyCLONe, the CSIRTs network and the Commission. When the incident relates to a third country, it will also be shared by the Commission with the High Representative***, the EEAS and any CSDP Mission in the country affected by the incident through their headquarters***.

Amendment 26

Proposal for a regulation
Recital 37

Text proposed by the Commission	*Amendment*
(37) Taking into account the unpredictable nature of cybersecurity attacks and the fact that they are often not contained in a specific geographical area and pose high risk of spill-over, the strengthening of resilience of neighbouring countries and their capacity to respond effectively to significant and large-scale cybersecurity incidents contributes to the protection of the Union as a whole. Therefore, third countries associated to the DEP ***may*** be supported from the EU Cybersecurity Reserve***,*** where ***this is provided for in the respective association agreement to DEP***. The funding for associated third countries should be supported by the Union in the framework of relevant partnerships and funding	(37) Taking into account the unpredictable nature of cybersecurity attacks and the fact that they are often not contained in a specific geographical area and pose high risk of spill-over, the strengthening of resilience of neighbouring countries***, particularly Ukraine and Moldova,*** and their capacity to respond effectively to significant and large-scale cybersecurity incidents contributes to the protection of the Union as a whole. Therefore, third countries associated to the DEP ***should*** be supported from the EU Cybersecurity Reserve***. The support should also apply to those third countries*** where ***a CSDP Mission is deployed with a specific mandate to strengthen the resilience to hybrid threats including***

instruments for those countries. The support should cover services in the area of response to and immediate recovery from significant or large-scale cybersecurity incidents. The conditions set for the EU Cybersecurity Reserve and trusted providers in this Regulation should apply when providing support to the third countries associated to DEP.	***cyber or where an EPF Assistance Measure has been adopted to strengthen the cyber resilience of the country***. The funding for associated third countries should be supported by the Union in the framework of relevant partnerships and funding instruments for those countries. The support should cover services in the area of response to and immediate recovery from significant or large-scale cybersecurity incidents. The conditions set for the EU Cybersecurity Reserve and trusted providers in this Regulation should apply when providing support to the third countries associated to DEP.

Amendment 27

Proposal for a regulation
Article 1 – paragraph 1 – point c

Text proposed by the Commission	*Amendment*
(c) the establishment of a European Cybersecurity Incident Review Mechanism to review and assess significant or large-scale incidents.	(c) the establishment of a European Cybersecurity Incident Review Mechanism to review and assess significant or large-scale incidents ***or threats***.

Amendment 28

Proposal for a regulation
Article 1 – paragraph 2 – point a

Text proposed by the Commission	*Amendment*
(a) to strengthen common Union detection and situational awareness of cyber threats and incidents thus allowing to reinforce the competitive position of industry and services sectors in the Union across the digital economy and contribute to the Union's technological ***sovereignty*** in the area of cybersecurity;	(a) to strengthen common Union detection and situational awareness of cyber threats and incidents thus allowing to reinforce the competitive position of industry and services sectors in the Union across the digital economy and contribute to the Union's technological ***resilience*** in the area of cybersecurity;

Amendment 29

Proposal for a regulation
Article 1 – paragraph 2 – point b

Text proposed by the Commission	*Amendment*
(b) to reinforce preparedness of entities operating in critical and highly critical sectors across the Union and strengthen solidarity by developing common response capacities against significant or large-scale cybersecurity incidents, including by making Union cybersecurity incident response support available for third countries associated to the Digital Europe Programme ('DEP');	(b) to reinforce preparedness of entities operating in critical and highly critical sectors across the Union and strengthen solidarity by developing common response capacities against significant or large-scale cybersecurity incidents, including by making Union cybersecurity incident response support available for third countries associated to the Digital Europe Programme ('DEP') ***or those third countries which are candidates for accession and do not contravene the security and defence interests of the Union and its Member States as established in the framework of the CFSP pursuant to Title V of the TEU; Member States should consider an active cyber defence programme to be part of their national cybersecurity strategy that incorporates regular joint training exercises between Member States and across international organisations. Such a programme should provide a synchronised, real-time capability to discover, detect, analyse, and mitigate threats***;

Amendment 30

Proposal for a regulation
Article 1 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2 a. to reduce systemic cybersecurity risks posed by dependencies on critical equipment from countries, which would contravene the security and defence interests of the Union and its Member States as established in the framework of the CFSP pursuant to Title V of the

TEU;.

Amendment 31

Proposal for a regulation
Article 2 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	'cyber defence community' means Member States' defence authorities and supported by EU institutions, bodies and agencies as sets out in the Joint Communication on EU Policy on Cyber Defence[1]
	[1] Joint Communication to the European Parliament and the Council EU Policy on Cyber Defence JOIN/2022/49 final

Amendment 32

Proposal for a regulation
Article 3 – paragraph 2 – subparagraph 1 – point b a (new)

Text proposed by the Commission	*Amendment*
	(b a) help modernise the entire cyber defence systems, increasing the quality of cyber defence capabilities through the deployment of AI systems and to accelerate the exchange of information among the National SOCs and Cross-border SOCs;

Amendment 33

Proposal for a regulation
Article 3 – paragraph 2 – subparagraph 1 – point d a (new)

Text proposed by the Commission	*Amendment*
	(d a) review and evaluate critical cybersecurity technologies and equipment deployed by SOCs in responding to cybersecurity incidents for systemic risks

	from control over high-risk providers by countries which would contravene the security and defence interests of the Union and its Member States as established in the framework of the CFSP pursuant to Title V of the TEU.

Amendment 34

Proposal for a regulation
Article 4 – paragraph 1 – subparagraph 2

Text proposed by the Commission	*Amendment*
It shall have the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing information on cybersecurity threats and incidents and contributing to a Cross-border SOC. It shall be equipped with state-of-the-art technologies capable of detecting, aggregating, and analysing data relevant to cybersecurity threats and incidents.	It shall have the capacity to act as a reference point and gateway to other public and private organisations***, and when necessary military,*** at national level for collecting and analysing information on cybersecurity threats and incidents and contributing to a Cross-border SOC. It shall be equipped with state-of-the-art technologies capable of detecting, aggregating, and analysing data relevant to cybersecurity threats and incidents.

Amendment 35

Proposal for a regulation
Article 4 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Following a call for expression of interest, National SOCs shall be selected by the European Cybersecurity Competence Centre ('ECCC') to participate in a joint procurement of tools and infrastructures with the ECCC. The ECCC may award grants to the selected National SOCs to fund the operation of those tools and infrastructures. The Union financial contribution shall cover up to 50% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Member State. Before	2. Following a call for expression of interest, National SOCs shall be selected by the European Cybersecurity Competence Centre ('ECCC') to participate in a joint procurement of tools and infrastructures with the ECCC. The ECCC may award grants to the selected National SOCs to fund the operation of those tools and infrastructures***, under the strict condition that such tools and infrastructure are provided by trusted providers in accordance with Art. 16***. The Union financial contribution shall cover up to 50% of the acquisition costs of the tools

launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the National SOC shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.	and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Member State. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the National SOC shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

Amendment 36

Proposal for a regulation
Article 5 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Following a call for expression of interest, a Hosting Consortium shall be selected by the ECCC to participate in a joint procurement of tools and infrastructures with the ECCC. The ECCC may award to the Hosting Consortium a grant to fund the operation of the tools and infrastructures. The Union financial contribution shall cover up to 75% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Hosting Consortium. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the Hosting Consortium shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.	2. Following a call for expression of interest, a Hosting Consortium shall be selected by the ECCC to participate in a joint procurement of tools and infrastructures with the ECCC. The ECCC may award to the Hosting Consortium a grant to fund the operation of the tools and infrastructures***, under the strict condition that such tools and infrastructure are provided by trusted providers in accordance with Art. 16***. The Union financial contribution shall cover up to 75% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Hosting Consortium. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the Hosting Consortium shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

Amendment 37

Proposal for a regulation
Article 5 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*

2a. Any infrastructure or provider originating in a high-risk third country shall be automatically excluded.

Amendment 38

Proposal for a regulation
Article 6 – paragraph 1 – point b a (new)

Text proposed by the Commission	*Amendment*
	(b a) directly supports stregthening the military and defence capabilities of the participating members or prevents a direct and imminent threat to their security. While the exploitation of vulnerabilities in defence sector may cause significant disruption and harm, cyber security of defence industry requires special measures to ensure the security of the supply chains, particularly entities lower in supply chains, which do not require access to classified information, but that could carry serious risks to the entire sector. Special consideration should be given to the impact any breach could have and the threat of any potential manipulation of network data that could render critical defence assets useless or even override their operating systems making them vulnerable to hijacking.

Amendment 39

Proposal for a regulation
Article 6 – paragraph 1 – point b a (new)

Text proposed by the Commission	*Amendment*
	(b b) supports strengthening the defence capabilities of the participating members or prevents a direct and imminent threat to their security, ensuring the security of the supply chains, in particular those entities lower in supply chains, which do not require access to classified information, but that could

carry serious risks to the entire sector.

Amendment 40

Proposal for a regulation
Article 7 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Where the Cross-border SOCs obtain information relating to a potential or ongoing large-scale cybersecurity incident, they shall provide relevant information to EU=CyCLONe, the CSIRTs network and the Commission, in view of their respective crisis management roles in accordance with Directive (EU) 2022/2555 without undue delay.	1. Where the Cross-border SOCs obtain information relating to a potential or ongoing large-scale cybersecurity incident, they shall provide relevant information to EU=CyCLONe, the CSIRTs network and the Commission, ***including the High Representative and EEAS when it concerns a third country,*** in view of their respective crisis management roles in accordance with Directive (EU) 2022/2555 without undue delay.

Amendment 41

Proposal for a regulation
Article 8 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States participating in the European Cyber Shield shall ensure a high level of data security and physical security of the European Cyber Shield infrastructure, and shall ensure that the infrastructure shall be adequately managed and controlled in such a way as to protect it from threats and to ensure its security and that of the systems, including ***that*** of data exchanged through the infrastructure.	1. Member States participating in the European Cyber Shield shall ensure a high level of data security and physical security of the European Cyber Shield infrastructure, and shall ensure that the infrastructure shall be adequately managed and controlled in such a way as to protect it from threats and to ensure its security and that of the systems, ***de-risking and promoting EU's technological edge in critical sectors,*** including ***measures to restrict or exclude high-risk suppliers, as well as protect the security*** of data exchanged through the infrastructure.

Amendment 42

Proposal for a regulation
Article 8 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States participating in the European Cyber Shield shall ensure that the sharing of information within the European Cyber Shield with entities which are not Member State public bodies does not negatively affect the security interests of the Union.	2. Member States participating in the European Cyber Shield shall ensure that the sharing of information within the European Cyber Shield with entities which are not Member State public bodies does not negatively affect the security interests of the Union ***and that any information sharing with high-risk providers is limited in scope and does not bring prejudice to the security and strategic interests of the Union***.

Amendment 43

Proposal for a regulation
Article 8 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The Commission may adopt implementing acts laying down technical requirements for Member States to comply with their obligation under paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation. In doing so, the Commission, supported by the High Representative, shall take into account relevant defence-level security standards, in order to facilitate cooperation with military actors.	3. The Commission may adopt implementing acts laying down technical requirements for Member States to comply with their obligation under paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation. In doing so, the Commission, supported by the High Representative, shall take into account relevant defence-level security standards, in order to facilitate cooperation with military actors***, making appropriate use of the whole range of defensive options available to the civilian and military communities for the broader security and defence of the EU, and shall inform the European Parliament***.

Amendment 44

Proposal for a regulation
Article 9 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Actions implementing the Cyber Emergency Mechanism shall be supported by funding from DEP and implemented in accordance with Regulation (EU) 2021/694 and in particular Specific Objective 3 thereof.	2. Actions implementing the Cyber Emergency Mechanism shall be supported by funding from DEP and implemented in accordance with Regulation (EU) 2021/694 and in particular Specific Objective 3 thereof ***and by European Peace Facility (EPF) when providing assistance measures to third countries, particularly Ukraine and Moldova;***

Amendment 45

Proposal for a regulation
Article 10 – paragraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) preparedness actions, including the coordinated preparedness testing of entities operating in highly critical sectors across the Union;	(a) preparedness actions, including the coordinated preparedness testing of entities operating in highly critical sectors***, such as public infrastructure, election infrastructure, transport, healthcare financial, telecommunication, food supply and security*** across the Union;

Amendment 46

Proposal for a regulation
Article 10 – paragraph 1 – point c

Text proposed by the Commission	*Amendment*
(c) mutual assistance actions consisting of the provision of assistance from national authorities of one Member State to another Member State, in particular as provided for in Article 11(3), point (f), of Directive (EU) 2022/2555**.**	(c) mutual assistance actions consisting of the provision of assistance from national authorities of one Member State to another Member State, in particular as provided for in Article 11(3), point (f), of Directive (EU) 2022/2555 ***and in the context of Article 42(7) TEU and Article 222 TFEU;***

Amendment 47

Proposal for a regulation
Article 10 – paragraph 1 – point c a (new)

Text proposed by the Commission	*Amendment*
	(c a) replacement and phasing out of critical equipment from high-risk suppliers, which would contravene the security and defence interests of the Union and its Member States as established in the framework of the CFSP pursuant to Title V of the TEU.

Amendment 48

Proposal for a regulation
Article 11 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The NIS Cooperation Group in cooperation with the Commission, ENISA, ***and*** the High Representative, shall develop common risk scenarios and methodologies for the coordinated testing exercises.	2. The NIS Cooperation Group in cooperation with the Commission, ENISA, the High Representative, ***EEAS and, when relevant, the EDA*** shall develop common risk scenarios and methodologies for the coordinated testing exercises.

Amendment 49

Proposal for a regulation
Article 12 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The EU Cybersecurity Reserve shall consist of incident response services from trusted providers selected in accordance with the criteria laid down in Article 16. The Reserve shall include pre-committed services. The services shall be deployable in all Member States.	2. The EU Cybersecurity Reserve shall consist of incident response services from trusted providers selected in accordance with the criteria laid down in Article 16. The Reserve shall include pre-committed services. The services shall be deployable in all Member States ***and third countries, which satisfy the applicable requirements of this Regulation***.

Amendment 50

Proposal for a regulation
Article 12 – paragraph 3 – point b

Text proposed by the Commission	*Amendment*
(b) Union institutions, bodies and agencies.	(b) Union institutions, bodies and agencies***, including CSDP missions***.

Amendment 51

Proposal for a regulation
Article 12 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Users referred to in paragraph 3, point (a), shall use the services from the EU Cybersecurity Reserve in order to respond or support response to and immediate recovery from significant or large-scale incidents affecting entities operating in critical or highly critical sectors.	4. Users referred to in paragraph 3, point (a), shall use the services from the EU Cybersecurity Reserve in order to respond or support response to and immediate recovery from significant or large-scale incidents affecting entities operating in critical or highly critical sectors***, such as public infrastructure, election infrastructure, transport, healthcare financial, telecommunication, food supply and security***.

Amendment 52

Proposal for a regulation
Article 12 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The Commission shall have overall responsibility for the implementation of the EU Cybersecurity Reserve. The Commission shall determine the priorities and evolution of the EU Cybersecurity Reserve, in line with the requirements of the users referred to in paragraph 3, and shall supervise its implementation, and ensure complementarity, consistency,	5. The Commission shall have overall responsibility for the implementation of the EU Cybersecurity Reserve. The Commission shall determine the priorities and evolution of the EU Cybersecurity Reserve, in line with the requirements of the users referred to in paragraph 3, and shall supervise its implementation, and ensure complementarity, consistency,

synergies and links with other support actions under this Regulation as well as other Union actions and programmes.	synergies and links with other support actions under this Regulation as well as other Union actions and programmes ***and objectives, in particular the strategic objective of reducing dependencies on high-risk suppliers, which would contravene the security and defence interests of the Union and its Member States as established in the framework of the CFSP pursuant to Title V of the TEU***.

Amendment 53

Proposal for a regulation
Article 12 – paragraph 7

Text proposed by the Commission	*Amendment*
7. In order to support the Commission in establishing the EU Cybersecurity Reserve, ENISA shall prepare a mapping of the services needed, after consulting Member States and the Commission. ENISA shall prepare a similar mapping, after consulting the Commission, to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve pursuant to Article 17. The Commission, where relevant, shall consult the High Representative.	7. In order to support the Commission in establishing the EU Cybersecurity Reserve, ENISA shall prepare a mapping of the services needed, after consulting Member States and the Commission. ENISA shall prepare a similar mapping, after consulting the Commission, to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve pursuant to Article 17***, supported by the EEAS***. The Commission, where relevant, shall consult the High Representative.

Amendment 54

Proposal for a regulation
Article 14 – paragraph 2 – point a a (new)

Text proposed by the Commission	*Amendment*
	(aa) the impact of the incident on the security and defence of the Union;

Amendment 55

Proposal for a regulation
Article 15 – paragraph 3

Text proposed by the Commission	*Amendment*
3. In consultation with the High Representative, support under the Cyber Emergency Mechanism may complement assistance provided in the context of the Common Foreign and Security Policy and Common Security and Defence Policy, including through the Cyber Rapid Response Teams. It may also complement or contribute to assistance provided by one Member State to another Member State in the context of Article 42(7) of the Treaty on the European Union.	3. In consultation with the High Representative, support under the Cyber Emergency Mechanism may complement assistance provided in the context of the Common Foreign and Security Policy and Common Security and Defence Policy, including through the Cyber Rapid Response Teams ***(CRRTs) in order to better support EU Member States, CSDP missions and operations and those third countries aligned with the EU Common Foreign and Security Policy and Common Security and Defence Policy in their cyber defence capacity building efforts, particularly Ukraine and Moldova***. It may also complement or contribute to assistance provided by one Member State to another Member State in the context of Article 42(7) of the Treaty on the European Union.

Amendment 56

Proposal for a regulation
Article 16 – paragraph 2 – point b a (new)

Text proposed by the Commission	*Amendment*
	(a a) the provider shall demonstrate that its decision and management structures are free from any undue influence by governments of states, which would contravene the security and defence interests of the Union and its Member States as established in the framework of the CFSP pursuant to Title V of the TEU;

Amendment 57

Proposal for a regulation
Article 16 – paragraph 2 – point f

Text proposed by the Commission	*Amendment*
(f) the provider shall be equipped with the hardware and software technical equipment necessary to support the requested service;	(f) the provider shall be equipped with the hardware and software technical equipment necessary to support the requested service ***and meets the requirements set out in Article X of the Regulation XX/XXXX (Cyber Resilience Act)***;

Amendment 58

Proposal for a regulation
Article 16 – paragraph 2 – point j a (new)

Text proposed by the Commission	*Amendment*
	(j a) No provider originating in a high-risk third country shall be admissible.

Amendment 59

Proposal for a regulation
Article 16 – paragraph 2 – point j b (new)

Text proposed by the Commission	*Amendment*
	(j b) the provider shall be in close cooperation with relevant SMEs, where possible;

Amendment 60

Proposal for a regulation
Article 17 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Third countries may request support from the EU Cybersecurity Reserve where Association Agreements concluded regarding their participation in DEP provide for this.	1. Third countries may request support from the EU Cybersecurity Reserve where***:***
	a) Association Agreements concluded

	regarding their participation in DEP provide for this***;***
	b) those third countries where a CSDP Mission is deployed with a specific mandate to strengthen the resilience to hybrid threats including cyber or where an EPF Assistance Measure has been adopted to strengthen the cyber resilience of the country.

Amendment 61

Proposal for a regulation
Article 17 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Support from the EU Cybersecurity Reserve shall be in accordance with this Regulation, and shall comply with any specific conditions laid down in the Association Agreements referred to in paragraph ***1***.	2. Support from the EU Cybersecurity Reserve shall be in accordance with this Regulation, and shall comply with any specific conditions laid down in the Association Agreements referred to in paragraph ***except for those third countries covered by the provisions set out in paragraph 1(b)***.

Amendment 62

Proposal for a regulation
Article 18 – paragraph 1

Text proposed by the Commission	*Amendment*
1. At the request of the Commission, the EU-CyCLONe or the CSIRTs network, ENISA shall review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. Following the completion of a review and assessment of an incident, ENISA shall deliver an incident review report to the CSIRTs network, the EU-CyCLONe and the Commission to support them in carrying out their tasks, in particular in view of those set out in Articles 15 and 16 of	1. At the request of the Commission, the EU-CyCLONe or the CSIRTs network, ENISA shall review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. Following the completion of a review and assessment of an incident, ENISA shall deliver an incident review report to the CSIRTs network, the EU-CyCLONe and the Commission to support them in carrying out their tasks, in particular in view of those set out in Articles 15 and 16 of

Directive (EU) 2022/2555. Where relevant, the Commission shall share the report with the High Representative.	Directive (EU) 2022/2555. Where relevant, ***especially when the incident relates to a third country*** the Commission shall share the report with the High Representative ***and the EEAS***.

Amendment 63

Proposal for a regulation
Article 18 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3a. The report shall be shared with the European Parliament in accordance with Union or national law the protection of sensitive classified information.

Amendment 64

Proposal for a regulation
Article 19 – paragraph 1 – point 1 – point a – point 1
Regulation (EU) 2021/694
Article 6, paragraph 1

Text proposed by the Commission	*Amendment*
(aa) support the development of an EU Cyber Shield, including the development, deployment and operation of National and Cross-border SOCs platforms that contribute to situational awareness in the Union and to enhancing the cyber threat intelligence capacities of the Union;	(aa) support the development of an EU Cyber Shield, including the development, deployment and operation of National and Cross-border SOCs platforms that contribute to situational awareness in the Union and to enhancing the cyber threat intelligence capacities of the Union ***and reducing the Union's dependency on high-risk providers of critical cybersecurity equipment or components, which would contravene the security and defence interests of the Union and its Member States as established in the framework of the CFSP pursuant to Title V of the TEU***;

Amendment 65

Proposal for a regulation
Article 20 – paragraph 1

Text proposed by the Commission	*Amendment*
By [***four*** years after the date of application of this Regulation], the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council.	By [***three*** years after the date of application of this Regulation ***and every two years after***], the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council.

PROCEDURE – COMMITTEE ASKED FOR OPINION

Title	Laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents
References	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Committee responsible Date announced in plenary	ITRE 1.6.2023
Opinion by Date announced in plenary	AFET 1.6.2023
Rapporteur for the opinion Date appointed	Dragoş Tudorache 16.6.2023
Discussed in committee	18.9.2023
Date adopted	24.10.2023
Result of final vote	+: 39 –: 4 0: 0
Members present for the final vote	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
Substitutes present for the final vote	Attila Ara-Kovács, Lars Patrick Berg, Andrey Kovatchev, Georgios Kyrtsos, Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

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

Key to symbols:
+ : in favour
- : against
0 : abstention