European Parliament
2019-2024

Committee on Foreign Affairs

2023/0109(COD)

22.9.2023

AMENDMENTS
56 - 119

Draft opinion
Dragoş Tudorache
(PE750.145v01-00)

Laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents

Proposal for a regulation
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Amendment 56
Željana Zovko

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.

Or. en

Amendment 57
Attila Ara-Kovács, Sven Mikser

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	(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 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.

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 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. ***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.***

Or. en

Amendment 58
Željana Zovko

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	(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 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.

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 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.

Or. en

Amendment 59
Attila Ara-Kovács, Sven Mikser

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,	(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.

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 in such instances***.

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

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

Or. en

Amendment 60
Tom Vandenkendelaere

Proposal for a regulation
Recital 4

Text proposed by the Commission

(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.

Amendment

(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. ***Futhermore, the Union approved and launched its Strategic Compass for Security and Defence last year which focuses inter alia on strengthening cyber security, including intensified cooperation***

with NATO in a broader context of hybrid warfare and the need to reinforce our resilience in all relevant aspects.

[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).

[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).

Or. en

Amendment 61
Attila Ara-Kovács, Sven Mikser

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.

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. ***Furthermore, the final assessment report of the EU-NATO task force recommended making full use of synergies between EU and NATO, including the exchange of best practices between civilian and military actors on the implementation of relevant cyber-related policies and legislation.***

---

[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,

[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).

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).

Or. en

Amendment 62
Markéta Gregorová
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 4 a (new)

Text proposed by the Commission	*Amendment*
	(4a) Welcomes the fact that the Union is developing its cyber security policy and has several instruments and mechanisms at its disposal or is developing them. Believes, however, that it is important 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.

Or. en

Amendment 63
Željana Zovko

Proposal for a regulation
Recital 4 a (new)

Text proposed by the Commission	*Amendment*

(4a) Cooperation on cyber-security has been a focal point of EU-NATO Cooperation and has also specifically been mentioned in the recent Third Joint Declaration on EU-NATO Cooperation of January 2023.

Or. en

Amendment 64
Markéta Gregorová
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 4 b (new)

Text proposed by the Commission	*Amendment*
	(4b) Stresses the importance of defining a Union body that would act as a coordination platform for all existing and future cyber security instruments, funds and mechanisms. Believes that it would be important to gurantee that all cyber security instruments, measures, funds and arragements are linked and interlocked in order to create synergies and prevent a fragmented landscape.

Or. en

Amendment 65
Željana Zovko

Proposal for a regulation
Recital 6 a (new)

Text proposed by the Commission	*Amendment*
	(6a) Enhanced international cooperation with like-minded allies and democratic partners around the globe is needed to ensure a coherent international response and preparedness on how to deal with these growing cybersecurity risks.

Or. en

Amendment 66
Željana Zovko

Proposal for a regulation
Recital 6 b (new)

Text proposed by the Commission	*Amendment*
	(6b) Highlighting the growing dual-use nature of technologies in the cyber domain, there is clear need to enhance "civ-mil" coordination when it comes to setting up new structures and regulations.

Or. en

Amendment 67
Witold Jan Waszczykowski

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.	(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; a Cybersecurity Emergency Mechanism should organise***

These actions shall be without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union ('TFEU').	***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').

Or. en

Amendment 68
Witold Jan Waszczykowski

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 manner.	(13) ***It is recommended that*** each Member State ***designates*** a public body at national level tasked with coordinating cyber threat detection activities in that Member State. These National SOCs ***could*** act as a reference point and gateway at national level for participation in the European Cyber Shield and ***would*** ensure that cyber threat information from public and private entities is shared and collected at national level in an effective and streamlined manner.

Or. en

Amendment 69
Witold Jan Waszczykowski

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, so that the benefits of cross-border threat detection and information sharing and management can be fully achieved***. The initial phase of Cross-border SOCs should be launched as an enhanced cooperation procedure according to the Article 20 of the Treaty on the European Union and Title III of the Treaty on the Functioning of the EU***. 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.

Or. en

Amendment 70
Attila Ara-Kovács, Sven Mikser

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	(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.	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 ***and if applicable***, ***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.

Or. en

Amendment 71
Attila Ara-Kovács, Sven Mikser

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,	(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.

and contributing to the development of Union capabilities***, resilience*** and technological sovereignty.

Or. en

Amendment 72
Nathalie Loiseau

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***,*** technological sovereignty ***and resilience***.

Or. en

Amendment 73
Witold Jan Waszczykowski

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	(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 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.

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 Member States' defence authorities and supported by EU institutions, bodies and agencies (the EU cyber defence community***). The information exchanged among participants in a Cross-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***.

Or. en

Amendment 74
Witold Jan Waszczykowski

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	(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.

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***, Member States' defence authorities and supported by EU institutions, bodies and agencies (the EU cyber defence community), as well as*** 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.

Or. en

Amendment 75
Attila Ara-Kovács, Sven Mikser

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	(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.	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.***

Or. en

Amendment 76
Željana Zovko

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. 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. ***However, given the sensitivity of the data, suppliers originating from high-risk third countries should be excluded.***

Or. en

Amendment 77
Witold Jan Waszczykowski

Proposal for a regulation
Recital 19 a (new)

Text proposed by the Commission	*Amendment*
	(19a) In accordance with Regulation [XX/XXXX (Cyber Resilience Act)] 2022/2555, critical products with digital elements shall be subject to specific conformity assessment procedures, reflecting their cybersecurity risk.

Or. en

Amendment 78
Nathalie Loiseau

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 competitiveness and its 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).

Or. en

Amendment 79
Attila Ara-Kovács, Sven Mikser

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 ***and open strategic autonomy***. 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).

Or. en

Amendment 80
Željana Zovko

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	(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.

('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. ***A particular focus should be given to the EU candidate countries in this regard to support them in building up their cyber capabilities and enhancing cross-border and regional cooperation among those candidate countries in the field of cyber.***

[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.

Or. en

Amendment 81
Witold Jan Waszczykowski

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	(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***.	Toolbox's measures, ***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 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924).	[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.	[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.

Or. en

Amendment 82
Witold Jan Waszczykowski

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)	(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***

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 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.

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 regular joint training exercises thus contributing 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. 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[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.

[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

Or. en

Amendment 83
Attila Ara-Kovács, Sven Mikser

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	(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 ***as well as contributions from the EEEAS and in particulalar through the EU Intelligence Centre (INTCEN) and with the support of the Intelligence Directorate of the European Union Military Staff (EUMS)***

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[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.	***under the Single Intelligence Analysis Capability (SIAC)***, 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[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.
[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

Or. en

Amendment 84
Witold Jan Waszczykowski

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. Moreover, third country breaches can spill over into servers and networks throughout the Union, creating a need to enhance resilience, detection and response capabilities in third countries with intertwined digital networks***. The eligible costs could include travel, accommodation and daily allowance expenses of cybersecurity experts.

Or. en

Amendment 85
Witold Jan Waszczykowski

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	(33) A Union-level Cybersecurity Reserve should gradually be set up, consisting of services from ***trusted*** private providers of managed security services to support response and immediate recovery actions in cases of significant or large-scale cybersecurity incidents***. To ensure a high***

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.

level of trust, the Commission should consider the options of supporting the development of cybersecurity certification schemes for such private cybersecurity companies, as sets out in the Joint Communication on EU Policy on Cyber Defence. 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.

Or. en

Amendment 86
Attila Ara-Kovács, Sven Mikser

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	(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.	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***,*** agencies ***and CSDP missions***, under similar conditions.

Or. en

Amendment 87
Željana Zovko

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. ***Providers originating from high-risk third countries should hence systematically be excluded.***

Or. en

Amendment 88
Witold Jan Waszczykowski

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 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.

(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 that have the capacity to devastate society and thus Member States must ensure that the protection of entire electronic communications infrastructure such as space, land and submarine network systems are prioritized. In addition,*** 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 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.

Or. en

Amendment 89
Željana Zovko

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	(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 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.	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. ***Coordination with the EEAS is particularly relevant when recalling that EU Delegations and EU CSDP Missions are also affected by such incidents.***

Or. en

Amendment 90
Witold Jan Waszczykowski

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***	(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***. The support should also apply to those third countries***

agreement to DEP. 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.

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 with an emphasis on capacity building and joint trainings***. The funding for associated third countries***, particularly Ukraine and Moldova,*** 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.

Or. en

Amendment 91
Attila Ara-Kovács, Sven Mikser

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	(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***. Support should also be extended to third countries hosting CSDP missions with a specific mandate to strengthen their resilience to cyber threats or where related EPF Assistance Measure has been adopted to that aim***. Therefore, third

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.

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 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.

Or. en

Amendment 92
Željana Zovko

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 instruments for those countries. The support should cover services in the area of response to and immediate recovery from	(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***, in particular candidate 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 instruments for those countries. The support should cover services in the area of

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.	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.

Or. en

Amendment 93
Nathalie Loiseau

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 sovereignty ***and resilience*** in the area of cybersecurity;

Or. en

Amendment 94
Witold Jan Waszczykowski

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	(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, ***Member States should consider an active cyber defence programme to be part of their national cybersecurity strategy that incorporates***

Programme (‘DEP’)*;*	***regular joint training exercises between Member States and across international organizations. Such a programme should provide a synchronised, real-time capability to discover, detect, analyse, and mitigate threats. Active cyber defence operates at network speed using sensors, software and intelligence to detect and stop malicious activity ideally before it can affect networks and systems. This can be further aided*** by making Union cybersecurity incident response support available for third countries associated to the Digital Europe Programme (‘DEP’)***, particularly Ukraine and Moldova.***

Or. en

Amendment 95
Attila Ara-Kovács, Sven Mikser

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

Text proposed by the Commission	*Amendment*
	(ba) 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;

Or. en

Amendment 96
Witold Jan Waszczykowski

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	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.	and private organisations at national level for collecting and analysing information on cybersecurity threats and incidents and contributing to a Cross-border SOC ***under an enhanced cooperation procedure according to the Article 20 of the Treaty on the European Union and Title III of the Treaty on the Functioning of the EU***. It shall be equipped with state-of-the-art technologies capable of detecting, aggregating, and analysing data relevant to cybersecurity threats and incidents.

Or. en

Amendment 97
Attila Ara-Kovács

Proposal for a regulation
Article 4 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2a. 1. The Union shall establish a dedicated Committee for Oversight of Security Operation Centres (COSOC) as part of the ECCC. The COSOC shall be composed of representatives designated by the Member States from the National SOCs and representative of relevant EU agencies. The COSOC shall have the following tasks:
	to enhance transparency and ensure the efficient functioning of security operation centre's (SOCs) across member states;
	to oversee and asses the operations of Security Operation Centres operating in every member state within the Union;
	to scrutinize their functions, protocols, and data gathering provided by the body to guarantee full transparency and compliance;
	to draw up an annual report on the activities of SOCs; and submit it to the European Commission, and the High Representative of the EU, Council and the

European Parliament;

Or. en

Amendment 98
Željana Zovko

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.

Or. en

Amendment 99
Witold Jan Waszczykowski

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

Text proposed by the Commission	*Amendment*
	(ba) directly supports streghtening 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.

Or. en

Amendment 100
Attila Ara-Kovács, Sven Mikser

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, ***the High Representative of EU 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.

Or. en

Amendment 101
Željana Zovko

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, including that of data exchanged through the infrastructure. ***As such entity or element originating in a high-risk third country shall be excluded.***

Or. en

Amendment 102
Željana Zovko

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. ***Cooperation in this field with like-minded allies and democratic partners around the globe shall be intensified in the context of the EU's bilateral relations with those partners.***

Or. en

Amendment 103
Attila Ara-Kovács, Sven Mikser

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 any related parties, including Member States and European agencies, bodies and institutions are notified of the information-sharing***.

Or. en

Amendment 104

Attila Ara-Kovács, Sven Mikser

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***.

Or. en

Amendment 105
Nathalie Loiseau

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	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.	military actors***, making appropriate use of the whole range of civilian responses available for the broader security and defence of the EU, and shall inform the European Parliament***.

Or. en

Amendment 106
Witold Jan Waszczykowski

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***.

Or. en

Amendment 107
Attila Ara-Kovács, Sven Mikser

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*** across the Union;

Or. en

Amendment 108
Attila Ara-Kovács, Sven Mikser

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***.

Or. en

Amendment 109
Attila Ara-Kovács, Sven Mikser

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**,** agencies ***and CSDP missions and operations***.

Or. en

Amendment 110
Attila Ara-Kovács, Sven Mikser

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	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.	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***.

Or. en

Amendment 111
Attila Ara-Kovács, Sven Mikser

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

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

Or. en

Amendment 112
Witold Jan Waszczykowski

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 ***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.

Or. en

Amendment 113
Attila Ara-Kovács, Sven Mikser

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

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

Or. en

Amendment 114
Attila Ara-Kovács, Sven Mikser

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

Text proposed by the Commission	*Amendment*
	(ba) 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 frameworkd of the CFSP pursuant to Title V of the TEU;

Or. en

Amendment 115
Željana Zovko

Proposal for a regulation

Article 16 – paragraph 2 – point j a (new)

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

Or. en

Amendment 116
Attila Ara-Kovács, Sven Mikser

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.

Or. en

Amendment 117
Željana Zovko

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,	1. At the request of the Commission***, the EEAS***, the EU-CyCLONe or the CSIRTs network, ENISA shall review and

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.	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.

Or. en

Amendment 118
Attila Ara-Kovács, Sven Mikser

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.

Or. en

Amendment 119
Attila Ara-Kovács, Sven Mikser

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 year after***], the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council.

Or. en