European Parliament
2019-2024

Committee on Industry, Research and Energy

2023/0109(COD)

22.9.2023

AMENDMENTS
46 - 216

Draft report
Lina Gálvez Muñoz
(PE752.795v01-00)

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 46
Evžen Tošenovský

Proposal for a regulation
Title 1

Text proposed by the Commission	*Amendment*
Proposal for aREGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCILlaying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents	Proposal for aREGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCILlaying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents ***(Cyber Solidarity Act)***

Or. en

Amendment 47
Ville Niinistö
on behalf of the Verts/ALE Group

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 ***and vulnerabilities*** 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.

Or. en

Justification

The need for this legal text arises form the fact that fundamental dependencies come also vulnerabilities

Amendment 48
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Recital 2

Text proposed by the Commission	*Amendment*
(2) The magnitude, frequency and impact of cybersecurity incidents are increasing, including supply chain attacks aiming at cyberespionage, ransomware or disruption. They represent a major threat to the functioning of network and information systems. In view of the fast-evolving threat landscape, the threat of possible large-scale incidents causing significant disruption or damage to critical infrastructures demands heightened preparedness at all levels of the Union's cybersecurity framework. That threat goes beyond Russia's military aggression on Ukraine, and is likely to persist given the multiplicity of state-aligned, criminal and hacktivist actors involved in current geopolitical tensions. Such incidents can impede the provision of public services and the pursuit of economic activities, including in critical or highly critical sectors, generate substantial financial losses, undermine user confidence, cause major damage to the economy of the Union, and could even 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.	(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 ***across the Union*** 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. ***Therefore, close and coordinated cooperation between the public sector, the private sector, the Member states, Union institutions or agencies, and acedemia is necessary to improve the Union's cybersecurity posture. The Union's response should be in cooperation with trusted and like-minded international partners and international institutions and aligned with international cooperation frameworks and agreements.***

Or. en

Amendment 49
Ville Niinistö
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 2

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

Or. en

Justification

The general inclusion of hacktivism along criminal activities is not reflecting the variety of such activities, including legitimate protests and whistleblowing. The text would benefit from avoiding unclairities and protecting legitimate activities.

Amendment 50
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Ioan-Rareş Bogdan, Cristian-Silviu Buşoi

Proposal for a regulation
Recital 3

Text proposed by the Commission	*Amendment*
(3) It is necessary to strengthen the competitive position of industry and services sectors in the Union across the digitised economy and support their digital transformation, by reinforcing the level of cybersecurity in the Digital Single Market. As recommended in three different proposals of the Conference on the Future of ***Europe[16]*** , it is necessary to increase the resilience of citizens, businesses and entities operating critical infrastructures against the growing cybersecurity threats, which can have devastating societal and economic impacts. Therefore, investment in infrastructures ***and*** services that will support faster detection and response to cybersecurity threats and incidents is needed, and Member States need assistance in better preparing for, as well as responding to significant and large-scale cybersecurity incidents. The Union should also increase its capacities in these areas, notably as regards the collection and analysis of data on cybersecurity threats and incidents.	(3) It is necessary to strengthen the competitive position of industry and services sectors in the Union across the digitised economy and support their digital transformation, by reinforcing the level of cybersecurity in the Digital Single Market. As recommended in three different proposals of the Conference on the Future of ***Europe16***, it is necessary to increase the resilience of citizens, businesses***, including micro-, small and medium-sized enterprises (SMEs),*** and entities operating critical infrastructures***, including local or regional authorities,*** against the growing cybersecurity threats, which can have devastating societal and economic impacts. Therefore, investment in infrastructures***,*** services***, and highly-qualified personnel with the needed skills*** 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***, also through pro-actively gathering intelligence***. The Union should also increase its capacities in these areas, notably as regards the collection and analysis of data on cybersecurity threats and incidents. ***[1] https://futureu.europa.eu/en/***

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

Or. en

Amendment 51
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Recital 5

Text proposed by the Commission	*Amendment*
(5) The growing cybersecurity risks and an overall complex threat landscape, with a clear risk of rapid spill-over of cyber incidents from one Member State to others and from a third country to the Union requires strengthened solidarity at Union level to better detect, prepare for ***and*** respond to cybersecurity threats and incidents. Member States have also invited the Commission to present a proposal on a new Emergency Response Fund for Cybersecurity in the Council Conclusions on an EU Cyber Posture[21] .	(5) The growing cybersecurity risks and an overall complex threat landscape, with a clear risk of rapid spill-over of cyber incidents from one Member State to others and from a third country to the Union requires strengthened solidarity at Union level to better detect, prepare for**,** respond to***, and recover from*** cybersecurity threats and incidents. Member States have also invited the Commission to present a proposal on a new Emergency Response Fund for Cybersecurity in the Council Conclusions on an EU Cyber Posture[21] .
[21] Council conclusions on the development of the European Union's cyber posture approved by the Council at its meeting on 23 May 2022, (9364/22)	[21] Council conclusions on the development of the European Union's cyber posture approved by the Council at its meeting on 23 May 2022, (9364/22)

Or. en

Amendment 52
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Recital 9 a (new)

Text proposed by the Commission	*Amendment*
	(9a) In light of the geopolitical developments and increasing cyber threat

landscape, the continuity and further development of the measures laid down in this Regulation, particularly the European Cyber Shield and the European Emergency Mechanism, is important. Therefore, it is necessary to ensure a specific budget line in the multiannual financial framework for 2028 to 2034. Member States should also commit to supporting all necessary measures to strengthen solidarity within the Union and to reduce cyber threats and incidents throughout the Union.

Or. en

Amendment 53
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Recital 12

Text proposed by the Commission	*Amendment*
(12) To more effectively prevent, assess ***and*** respond to cyber threats and incidents, it is necessary to develop more comprehensive knowledge about the threats to critical assets and infrastructures on the territory of the Union, including their geographical distribution, interconnection and potential effects in case of cyber-attacks affecting those infrastructures. A large-scale Union infrastructure of SOCs should be deployed ('the European Cyber Shield'), comprising of several interoperating cross-border platforms, each grouping together several National SOCs. That infrastructure should serve national and Union cybersecurity interests and needs, leveraging state of the art technology for advanced data collection and analytics tools, enhancing cyber detection and management capabilities and providing real-time situational awareness. That infrastructure should serve to increase detection of cybersecurity threats and	(12) To more effectively prevent, assess***,*** respond to***, and recover from*** cyber threats and incidents, it is necessary to develop more comprehensive knowledge about the threats to critical assets and infrastructures on the territory of the Union, including their geographical distribution, interconnection and potential effects in case of cyber-attacks affecting those infrastructures***, including by gathering pro-active intelligence***. A large-scale Union infrastructure of SOCs should be deployed ('the European Cyber Shield'), comprising of several interoperating cross-border platforms, each grouping together several National SOCs***. A national SOC is a centralized capacity repsonsible for continuously gathering threat intelligence information and improving the cybersecurity posture of entities under national jurisdiction by preventing, detecting, and analyzing cybersecurity threats***. That infrastructure should serve

incidents and thus complement and support Union entities and networks responsible for crisis management in the Union, notably the EU Cyber Crises Liaison Organisation Network ('EU-CyCLONe'), as defined in Directive (EU) 2022/2555 of the European Parliament and of the Council[24] .

national and Union cybersecurity interests and needs, leveraging state of the art technology for advanced data collection and analytics tools, enhancing cyber detection and management capabilities and providing real-time situational awareness. That infrastructure should serve to increase detection of cybersecurity threats and incidents and thus complement and support Union entities and networks responsible for crisis management in the Union, notably the EU Cyber Crises Liaison Organisation Network ('EU-CyCLONe'), as defined in Directive (EU) 2022/2555 of the European Parliament and of the Council[24] .

[24] 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 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

[24] 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 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

Or. en

Amendment 54
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Recital 13

Text proposed by the Commission

(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

Amendment

(13) ***In order to participate in the European Cyber Shield,*** each Member State should designate a public body at national level tasked with coordinating cyber threat detection ***and information sharing*** activities in that Member State***.*** ***Member States are strongly encouraged to incorporate the National SOC capacity into their already existing cyber structure and governance to not create additional***

level in an effective and streamlined manner.

governance layers and to align the Cyber Solidarity Act with already existing legislation, including Directive 2022/2555. These National SOCs should act as a reference point and gateway at national level for participation ***of private and public entities, particularly their SOCs,*** 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. ***National SOCs should strengthen the cooperation and information sharing between public and private entities to break up currently existing communication siloes. In doing so, they may support the creation of data exchange models and should facilitate and encourage the sharing of information in a trusted and secure environment. Close and coordinated cooperation between public and private entities is central for strengthening the Union's resilience in the cybersecurity sphere.***

Or. en

Amendment 55
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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	(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.	support the production of high-quality ***and pro-active*** 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. ***The cross-border SOCs should facilitate and encourage the sharing of information in a trusted and secure environment. ENISA should support Cross-border SOCs in matters related to operational cooperation.*** They should provide new additional capacity, ***while being incorporated in the already*** existing ***cybersecurity infrastructure, including*** SOCs and computer incident response teams ('CSIRTs') and other relevant actors.

Or. en

Amendment 56
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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	(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 ***capacity*** that is ***incorporated into the already existing cybersecurity infrastructure, particularly*** the CSIRTs network, by pooling and sharing data on cybersecurity threats from public and private entities***, in particular their SOCs***, enhancing the value of such data through expert analysis and jointly

Union capabilities and technological sovereignty.	acquired infrastructures and state of the art tools, and contributing to the development of Union capabilities and technological sovereignty***, to strengthen the Union's resilience***.

Or. en

Amendment 57
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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 ***a significant cybersecurity ecosystem with strong*** Union capabilities and ***cooperation with like-minded partners***.

Or. en

Amendment 58
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Recital 16

Text proposed by the Commission	*Amendment*
(16) The Cross-border SOCs should act as a central point allowing for a broad pooling of relevant data and cyber threat intelligence, enable the spreading of threat information among a large and diverse set of actors (e.g., Computer Emergency Response Teams ('CERTs'), CSIRTs, Information Sharing and Analysis Centers ('ISACs'), operators of critical infrastructures***). The*** information exchanged among participants in a Cross-border SOC could include data from 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.	(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 ***to facilitate the break-up of currently existing communication siloes. In doings so, cross-border SOCs could also support the creation of data exchange models across the Union.The*** information exchanged among participants in a Cross-border SOC could include data from networks and sensors, threat intelligence feeds***, including the gathering of pro-active intelligence***, 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.

Or. en

Amendment 59
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposal for a regulation
Recital 16

Text proposed by the Commission	*Amendment*
(16) The Cross-border SOCs should act as a central point allowing for a broad pooling of relevant data and cyber threat intelligence, enable the spreading of threat information among a large and diverse set of actors (e.g., Computer Emergency Response Teams ('CERTs'), CSIRTs, Information Sharing and Analysis Centers ('ISACs'), operators of critical infrastructures). The information exchanged among participants in a Cross-	(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.	border SOC could include ***analyzed*** data from networks***,*** sensors***, logging, and telemetry***, threat intelligence feeds, indicators of compromise, and contextualised information about ***tactics, techniques and procedures (TTPs),*** incidents***, malware samples***, threats and vulnerabilities. In addition, Cross-border SOCs should also enter into cooperation agreements with other Cross-border SOCs.

Or. en

Amendment 60
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Recital 17

Text proposed by the Commission	*Amendment*
(17) Shared situational awareness among relevant authorities is an indispensable prerequisite for Union-wide preparedness and coordination with regards to significant and large-scale cybersecurity incidents. Directive (EU) 2022/2555 establishes the EU–CyCLONe to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies and agencies. Recommendation (EU) 2017/1584 on coordinated response to large-scale cybersecurity incidents and crises addresses the role of all relevant actors. Directive (EU) 2022/2555 also recalls the Commission's responsibilities in the Union Civil Protection Mechanism ('UCPM') established by Decision 1313/2013/EU of the European Parliament and of the Council, as well as for providing analytical reports for the Integrated Political Crisis Response Mechanism ('IPCR') arrangements under Implementing Decision (EU) 2018/1993.	(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.	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 line with already existing provisions under Directive (EU) 2022/2555***. 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 61
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 ***and highly-skilled personnel***. 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.

Or. en

Amendment 62
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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. The pooling of high-quality curated data should also contribute to the development of advanced artificial intelligence and data analytics technologies. It ***must be noted, however, that artificial intelligence is the most effective when paired with human analysis. Therefore, highly-skilled staff remains essential for pooling high-quality data and gathering of pro-active threat intelligence. 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 63
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposal for a regulation
Recital 20

Text proposed by the Commission	*Amendment*
(20) By collecting, sharing and	(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] .

[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).

exchanging data, the European Cyber Shield should enhance the Union's ***significant cybersecurity ecosystem***. 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).

Or. en

Amendment 64
Ville Niinistö
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 21

Text proposed by the Commission	*Amendment*
(21) While the European Cyber Shield is a civilian project, the cyber defence community could benefit from stronger civilian detection and situational awareness capabilities developed for the protection of critical infrastructure. Cross-border SOCs, with the support of the Commission and the European Cybersecurity Competence Centre ('ECCC'), and in cooperation with the High Representative of the Union for Foreign Affairs and Security Policy (the 'High Representative'), should gradually develop dedicated protocols and standards to allow for cooperation with the cyber defence community, including vetting and security conditions. The development of	(21) While the European Cyber Shield is a civilian project, the cyber defence community could benefit from stronger civilian detection and situational awareness capabilities developed for the protection of critical infrastructure. Cross-border SOCs, with the support of the Commission and the European Cybersecurity Competence Centre ('ECCC'), and in cooperation with the High Representative of the Union for Foreign Affairs and Security Policy (the 'High Representative'), should gradually develop dedicated ***access conditions and safeguards*** protocols and standards to allow for cooperation with the cyber defence community, including vetting and

the European Cyber Shield should be accompanied by a reflection enabling future collaboration with networks and platforms responsible for information sharing in the cyber defence community, in close cooperation with the High Representative.	security conditions***, respecting the civilian character of insitutions and the destination of funding, therefore using the funds available to the defence community*** . The development of the European Cyber Shield should be accompanied by a reflection enabling future collaboration with networks and platforms responsible for information sharing in the cyber defence community, in close cooperation with the High Representative ***and in full respect of rights and freedoms***.

Or. en

Justification

In the spirit of avoiding duplication and safeguarding right and freedoms, cooperation between the civilian and defense sides of cybersecurity needs to be based on safeguards, avoiding changing the destination of civilian funding.

Amendment 65
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Recital 24

Text proposed by the Commission	*Amendment*
(24) In view of the increasing risks and number of cyber incidents affecting Member States, it is necessary to set up a crisis support instrument to improve the Union's resilience to significant and large-scale cybersecurity incidents and complement Member States' actions through emergency financial support for preparedness, response and immediate recovery of essential services. That instrument should enable the rapid deployment of assistance in defined circumstances and under clear conditions and allow for a careful monitoring and evaluation of how resources have been used. Whilst the primary responsibility for preventing, preparing for and responding to	(24) In view of the increasing risks and number of cyber incidents affecting Member States, it is necessary to set up a crisis support instrument to improve the Union's resilience to significant and large-scale cybersecurity incidents and complement Member States' actions through emergency financial support for preparedness, response and immediate recovery of essential services. That instrument should enable the rapid ***and effective*** deployment of assistance in defined circumstances and under clear conditions and allow for a careful monitoring and evaluation of how resources have been used. Whilst the primary responsibility for preventing,

cybersecurity incidents and crises lies with the Member States, the Cyber Emergency Mechanism promotes solidarity between Member States in accordance with Article 3(3) of the Treaty on European Union ('TEU').	preparing for and responding to cybersecurity incidents and crises lies with the Member States, the Cyber Emergency Mechanism promotes solidarity between Member States in accordance with Article 3(3) of the Treaty on European Union ('TEU').

Or. en

Amendment 66
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Recital 27

Text proposed by the Commission	*Amendment*
(27) Assistance provided under this Regulation should be in support of, and complementary to, the actions taken by Member States at national level. To this end, close cooperation and consultation between the Commission and the affected Member State should be ensured. When requesting support under the Cyber Emergency Mechanism, the Member State should provide relevant information justifying the need for support.	(27) Assistance provided under this Regulation should be in support of, and complementary to, the actions taken by Member States at national level. To this end, close cooperation and consultation between the Commission***, ENISA*** and the affected Member State should be ensured. When requesting support under the Cyber Emergency Mechanism, the Member State should provide relevant information justifying the need for support.

Or. en

Amendment 67
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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	(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.

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***, while reinforcing the Union's resilience and competitiveness, including the participation of European managed security service providers that are SMEs. Trusted providers, including SMEs, should be able to cooperate with one another to fulfil the criteria above***. 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***. Where possible, the services should be based on state-of-the-art technologies, including cloud and artificial intelligence. Therefore, the Cybersecurity Reserve should incentivize investment in research and innovation to boost the development of these technologies. Where appropriate, common exercises with the trusted providers and potential users of the Cybersecurity Reserve could be conducted to ensure efficient functioning of the Reserve when needed***. 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.

Or. en

Amendment 68
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposal for a regulation
Recital 33

Text proposed by the Commission	*Amendment*
(33) A Union-level Cybersecurity Reserve should gradually be set up, ***consisting*** of services from private providers of managed security services to support response and immediate recovery actions in cases of significant or large-scale cybersecurity incidents. The EU Cybersecurity Reserve should ensure the availability and readiness of services. The services from the EU Cybersecurity Reserve should serve to support national authorities in providing assistance to affected entities operating in critical or highly critical sectors as a complement to their own actions at national level. When requesting support from the EU Cybersecurity Reserve, Member States should specify the support provided to the affected entity at the national level, which should be taken into account when assessing the Member State request. The services from the EU Cybersecurity Reserve may also serve to support Union institutions, bodies and agencies, under similar conditions.	(33) A Union-level Cybersecurity Reserve should gradually be set up, ***with initial funding of 10 million euro under this Regulation until the Evaluation. It consists*** 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. ***The Commission shall ensure that it will not duplicate similar initiatives within NATO.***

Or. en

Justification

The Commission foresees a "gradual set up" of the Reserve but this is not reflected in the rest of the proposed Regulation. This amendment therefore proposes to reduce the initial budget for the Reserve from 36 million to 10 million euro until the evaluation of this Regulation. This would return 26 million euro to the Digital Europe Program - Special Objective 4 on Advanced Digital Skills (of the 35 million taken from it). Developing a EU Cybersecurity Reserve next to an existing NATO cyber reserve comes with a high risk of duplication and should not be at the expense of investing more in developing and attracting cybersecurity talent in Europe.

Amendment 69
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Recital 35

Text proposed by the Commission	*Amendment*
(35) To support the establishment of the EU Cybersecurity Reserve, the Commission ***could consider requesting*** ENISA to prepare a candidate certification scheme pursuant to Regulation (EU) 2019/881 for managed security services in the areas covered by the Cyber Emergency Mechanism.	(35) To support the establishment of the EU Cybersecurity Reserve, the Commission ***should request*** ENISA to prepare a candidate certification scheme pursuant to Regulation (EU) 2019/881 for managed security services in the areas covered by the Cyber Emergency Mechanism.

Or. en

Amendment 70
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen, Nicola Danti

Proposal for a regulation
Recital 35 a (new)

Text proposed by the Commission	*Amendment*
	(35a) In light of the additional tasks provided for in this Regulation as well as in the [Proposal for horizontal cybersecurity requirements for products with digital elements], ENISA should be provided with the necessary human and financial resources under the Union budget.

Or. en

Amendment 71
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Recital 37 a (new)

Text proposed by the Commission	*Amendment*
	(37a) Incident response service providers

from third countries, including third countries associated to the DEP or NATO members or other like-minded international partner countries, may be needed for the provision of specific services in the EU Cybersecurity Reserve. To strengthen the Union's resilience and sovereignty and to safeguard the Union's strategic assets, interests or security, it may be necessary to restrict or exclude the participation of legal entities established in or controlled by non-associated countries.

Or. en

Amendment 72
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Recital 38 a (new)

Text proposed by the Commission	*Amendment*
	(38a) Highly-skilled personnel, that is able to reliably deliver the relevant cybersecurity services at highest standards, is imperative for the effective implementation of the European Cyber Shield and the Cyber Emergency Mechanism. It is therefore concerning that the Union is faced with a talent gap, characterized by a shortage of skilled professionals, while facing a rapidly evolving threat landscape as acknowledged in the Commission communication of 18 April 2023 on the Cyber Skills Academy. It is important to bridge this talent gap by strengthening cooperation and coordination among the different stakeholders, including the private sector, academia, Member States, the Commission and ENISA to scale up and create synergies for the investment in education and training, the development of public-private partnerships, support of research and innovation initiatives, the

development and mutual recognition of common standards and certification of cybersecurity skills, including through the European Cyber Security Skills Framework. This should also facilitate the mobility of cybersecurity professionals within the Union. This Regulation should aim to promote a more diverse cybersecurity workforce.

Or. en

Amendment 73
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Recital 38 b (new)

Text proposed by the Commission	*Amendment*
	(38b) Member States' capacity building is essential for a Union-wide coordinated approach to strengthening the resilience of the Union's cybersecurity posture. As emphasized in the Commission communication of 18 April 2023 on the Cyber Skills Academy, the security of the Union cannot be guaranteed without the Union's most valuable asset: its people. The European Cyber Security Skills Framework can help to better understand the composition of the Union's workforce, including the current and required competences within participating entities.

Or. en

Amendment 74
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Recital 39

Text proposed by the Commission	*Amendment*
(39) The objective of this Regulation can be better achieved at Union level than by the Member States. Hence, the Union may adopt measures, in accordance with the principles of subsidiarity and proportionality as set out in Article 5 of the Treaty on European Union. This Regulation does not go beyond what is necessary in order to achieve that objective.	(39) The objective of this Regulation***, namely to break up communication silos and reinforce the Union's cyber threat prevention, detection, response and recover capacities,*** can be better achieved at Union level than by the Member States. Hence, the Union may adopt measures, in accordance with the principles of subsidiarity and proportionality as set out in Article 5 of the Treaty on European Union. This Regulation does not go beyond what is necessary in order to achieve that objective.

Or. en

Amendment 75
Nicola Danti

Proposal for a regulation
Recital 39 a (new)

Text proposed by the Commission	*Amendment*
	(39a) In light of the additional tasks provided for in this Regulation as well as in the [Proposal for horizontal cybersecurity requirements for products with digital elements], ENISA should be provided with the necessary human and financial resources under the Union budget.

Or. en

Amendment 76
Johan Nissinen

Proposal for a regulation
Article 1 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. This Regulation lays down	1. This Regulation lays down

measures to strengthen capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents, in particular through the following actions:	measures to strengthen capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents, ***while respecting that national security, including in the cyber domain, remains the sole responsibility of each Member State, as noted in article 4(2) TEU,*** in particular through the following actions:
	Or. en

Amendment 77
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
(a) the deployment ***of a pan-European infrastructure*** of Security Operations Centres (***'European Cyber Shield'***) to build and enhance common detection and situational awareness capabilities;	(a) the ***strenghtening of Computer security incident response teams (CSIRTs), referred to in Article 10 of Directive (EU) 2022/2555, and of the CSIRTs Network referred to in Article 15 of Directive (EU) 2022/2555, and*** deployment of Security Operations Centres (***SOCs***) to build and enhance ***national and*** common detection and situational awareness capabilities ***('European Cyber Shield')***;
	Or. en

Amendment 78
Evžen Tošenovský

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

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

Or. en

Amendment 79
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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***, including SMEs,*** and services sectors in the Union across the digital economy and contribute to the Union's technological sovereignty in the area of cybersecurity;

Or. en

Amendment 80
Johan Nissinen

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 ***voluntary*** 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;

Or. en

Amendment 81
Johan Nissinen

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

Text proposed by the Commission	*Amendment*
(b) to reinforce preparedness of entities operating in critical and highly critical sectors across the Union and strengthen ***solidarity*** by developing common response capacities against significant or large-scale cybersecurity incidents, including by making Union cybersecurity incident response support available for third countries associated to the Digital Europe Programme ('DEP');	(b) to reinforce preparedness of entities operating in critical and highly critical sectors across the Union and strengthen ***voluntary cooperation*** by developing common response capacities against significant or large-scale cybersecurity incidents, including by making Union cybersecurity incident response support available for third countries associated to the Digital Europe Programme ('DEP');

Or. en

Amendment 82
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
(c) to enhance Union resilience and contribute to effective response by reviewing and assessing significant or large-scale incidents, including drawing lessons learned and, where appropriate, recommendations..	***deleted***

Or. en

Amendment 83
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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

Text proposed by the Commission	*Amendment*
	(ca) to develop and improve skills and

competences of the workforce in the cybersecurity sector in a coordinated way, by cooperating with the Cyber Skills Academy to provide training and opportunities with the goal of closing the talent gap in the cybersecurity sector.

Or. en

Amendment 84
Johan Nissinen

Proposal for a regulation
Article 1 – paragraph 3

Text proposed by the Commission	*Amendment*
3. This Regulation is without prejudice to the Member States' primary responsibility for national security, public security, and the prevention, investigation, detection and prosecution of criminal offences.	3. This Regulation is without prejudice to the Member States' primary responsibility for national security, public security, and the prevention, investigation, detection and prosecution of criminal offences ***and avoids unnecessary duplication with existing initiatives***.

Or. en

Amendment 85
Evžen Tošenovský

Proposal for a regulation
Article 1 – paragraph 3

Text proposed by the Commission	*Amendment*
3. This Regulation is without prejudice to the Member States' ***primary responsibility for*** national security, public security, and the prevention, investigation, detection and prosecution of criminal offences.	3. This Regulation is without prejudice to the Member States' ***exclusive competence in*** national security, public security, and the prevention, investigation, detection and prosecution of criminal offences.

Or. en

Amendment 86
Nicola Danti

Proposal for a regulation
Article 1 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	3a. Every year when presenting the Draft Budget for the following year, the Commission shall submit a detailed assessment of ENISA's tasks under this Regulation as well as [the proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements] and other Union legislation and shall detail the financial and human resources needed to fulfil those tasks.

Or. en

Amendment 87
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
(1) 'Cross-border Security Operations Centre' ("Cross-border SOC") means a multi-country platform, that brings together in a coordinated network structure national SOCs from at least three Member States who form a Hosting Consortium, and that is designed to prevent cyber threats and incidents and to support the production of high-quality intelligence, notably through the exchange of data from various sources, public and private, as well as through the sharing of state-of-the-art tools and jointly developing cyber detection, analysis, and prevention and protection capabilities in a trusted environment;	***deleted***

Or. en

Amendment 88
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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

Text proposed by the Commission	*Amendment*
(1) 'Cross-border Security Operations Centre' ("Cross-border SOC") means a multi-country platform, that brings together in a coordinated network structure national SOCs from at least three Member States who form a Hosting Consortium, and that is designed to ***prevent*** cyber threats and incidents and to support the production of high-quality intelligence, notably through the exchange of data from various sources, public and private, as well as through the sharing of state-of-the-art tools and jointly developing cyber detection, analysis, and prevention and protection capabilities in a trusted environment;	(1) 'Cross-border Security Operations Centre' ("Cross-border SOC") means a multi-country platform, that brings together in a coordinated network structure national SOCs from at least three Member States who form a Hosting Consortium, and that is designed to ***detect and analyze*** cyber threats and ***prevent*** incidents and to support the production of high-quality intelligence, notably through the exchange of data from various sources, public and private, as well as through the sharing of state-of-the-art tools and jointly developing cyber detection, analysis, and prevention and protection capabilities in a trusted environment;

Or. en

Amendment 89
Johan Nissinen

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

Text proposed by the Commission	*Amendment*
(1) 'Cross-border Security Operations Centre' ("Cross-border SOC") means a multi-country platform, that brings together in a coordinated network structure national SOCs from at least three Member States who form a Hosting Consortium, and that is designed to prevent cyber threats and incidents and to support the production of high-quality intelligence, notably through the exchange of data from various sources, public and private, as well as through the	(1) 'Cross-border Security Operations Centre' ("Cross-border SOC") means a multi-country platform, that brings together in a coordinated network structure national SOCs from at least three Member States who form a Hosting Consortium, and that is designed to prevent cyber threats and incidents and to support the production of high-quality intelligence, notably through the ***voluntary*** exchange of data from various sources, public and private, as well

sharing of state-of-the-art tools and jointly developing cyber detection, analysis, and prevention and protection capabilities in a trusted environment;	as through the sharing of state-of-the-art tools and jointly developing cyber detection, analysis, and prevention and protection capabilities in a trusted environment;

Or. en

Amendment 90
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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

Text proposed by the Commission	*Amendment*
	(1a) "Security Operations Centre" ("SOC") means a centralized capacity, which can be in-house or outsourced, responsible for continuously monitoring and improving the cybersecurity posture of an entity to prevent, detect, analyse, and respond to cybersecurity threats.

Or. en

Amendment 91
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
	(1a) 'Security Operations Centre' ("SOC") means a centre, set up by private and public entities or national authorities, constantly monitoring and analysing the communication networks and computer systems to detect intrusions and anomalies in real time.

Or. en

Amendment 92
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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

Text proposed by the Commission	*Amendment*
	(1b) 'National Security Operations Centre' ("National SOC") means a centralized capacity responsible for continuously gathering threat intelligence and improving the cybersecurity posture of entities under national jurisdiction by preventing, detecting and analyzing, cybersecurity threats to be able to better respond to cybersecurity threats. This capacity shall, where applicable, be incorporated in already existing national structures such as CSIRTs as established under Directive 2022/2555.

Or. en

Amendment 93
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
(2) 'public ***body***' means a ***body governed by*** public ***law*** as defined in Article ***2((1)***, point ***(4),***), of Directive ***2014/24/EU of the European Parliament and the Council***[30] ;	(2) 'public ***administration entity***' means a public ***administration entity*** as defined in Article ***6***, point ***(35***), of Directive ***(EU) 2022/2555***;
[30] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94 28.3.2014, p. 65).	

Or. en

Amendment 94
Evžen Tošenovský

Proposal for a regulation
Article 2 – paragraph 1 – point 3

Text proposed by the Commission	*Amendment*
(3) 'Hosting Consortium' means a consortium composed of participating states, represented by National SOCs, that have agreed to establish and contribute to the acquisition of tools and infrastructure for, and operation of, a Cross-border SOC ;	***deleted***

Or. en

Amendment 95
Evžen Tošenovský

Proposal for a regulation
Article 2 – paragraph 1 – point 5 a (new)

Text proposed by the Commission	*Amendment*
	(5a) 'incident handling' means a incident handling as defined in Article 6, point (8), of Directive (EU) 2022/2555;

Or. en

Amendment 96
Evžen Tošenovský

Proposal for a regulation
Article 2 – paragraph 1 – point 5 b (new)

Text proposed by the Commission	*Amendment*
	(5b) 'risk' means a risk as defined in Article 6, point (9), of Directive (EU) 2022/2555;

Or. en

Amendment 97
Evžen Tošenovský

Proposal for a regulation
Article 2 – paragraph 1 – point 6 a (new)

Text proposed by the Commission	*Amendment*
	(6a) 'significant cyber threat' means a cyber threat as defined in Article 6, point (11), of Directive (EU) 2022/2555;

Or. en

Amendment 98
Evžen Tošenovský

Proposal for a regulation
Article 2 – paragraph 1 – point 9

Text proposed by the Commission	*Amendment*
(9) 'preparedness' means a state of readiness and capability to ensure an effective rapid response to a significant or large-scale cybersecurity incident, obtained as a result of risk assessment and monitoring actions taken in advance;	***deleted***

Or. en

Amendment 99
Evžen Tošenovský

Proposal for a regulation
Article 2 – paragraph 1 – point 10

Text proposed by the Commission	*Amendment*
(10) 'response' means action in the event of a significant or large-scale cybersecurity incident, or during or after such an incident, to address its immediate	***deleted***

and short-term adverse consequences;

Or. en

Amendment 100
Evžen Tošenovský

Proposal for a regulation
Article 2 – paragraph 1 – point 11

Text proposed by the Commission	*Amendment*
(11) 'trusted providers' means managed security service providers as defined in Article 6, point (40), of Directive (EU) 2022/2555 selected in accordance with Article 16 of this Regulation.	(11) 'trusted ***managed security service*** providers' means managed security service providers as defined in Article 6, point (40), of Directive (EU) 2022/2555 selected ***to be included in the EU Cybersecurity Reserve*** in accordance with Article 16 of this Regulation.

Or. en

Amendment 101
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposal for a regulation
Article 3 – paragraph 1 – subparagraph 1

Text proposed by the Commission	*Amendment*
An interconnected pan-European infrastructure of Security Operations Centres ('European Cyber Shield') shall be established to develop advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union. It shall consist of all National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs').	An interconnected pan-European infrastructure of Security Operations Centres ('European Cyber Shield') shall be established to develop advanced capabilities for the Union to detect, analyse and process data on cyber threats and ***prevent*** incidents in the Union. It shall consist of all National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs').

Or. en

Amendment 102
Johan Nissinen

Proposal for a regulation
Article 3 – paragraph 2 – subparagraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) pool and share data on cyber threats and incidents from various sources through cross-border SOCs;	(a) pool and share data on cyber threats and incidents from various sources through ***voluntary sharing of information from*** cross-border SOCs;

Or. en

Amendment 103
Evžen Tošenovský

Proposal for a regulation
Article 3 – paragraph 2 – subparagraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) pool and share data on cyber threats and incidents from various sources through cross-border SOCs;	(a) pool and share data on cyber threats and incidents from various sources through cross-border SOCs ***both at national and EU level***;

Or. en

Amendment 104
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 3 – paragraph 2 – subparagraph 1 – point c

Text proposed by the Commission	*Amendment*
(c) contribute to better protection and response to cyber threats;	(c) contribute to better protection and response to cyber threats***, including by providing concrete recommendations to entities***;

Or. en

Amendment 105
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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

Text proposed by the Commission	*Amendment*
(d) contribute to faster detection of cyber threats and situational awareness across the Union;	(d) contribute to faster detection of cyber threats and situational awareness across the Union***, including by gathering pro-active intelligence***;

Or. en

Amendment 106
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposal for a regulation
Article 3 – paragraph 2 – subparagraph 1 – point e

Text proposed by the Commission	*Amendment*
(e) provide services and activities for the cybersecurity community in the Union, including contributing to the development advanced artificial intelligence and data analytics tools.	(e) provide services and activities for the cybersecurity community in the Union, including contributing to the development ***of*** advanced artificial intelligence and data analytics tools.

Or. en

Amendment 107
Evžen Tošenovský

Proposal for a regulation
Article 4 – title

Text proposed by the Commission	*Amendment*
National ***Security Operations Centres***	***Strengthened cooperation and information sharing at*** national ***level***

Or. en

Amendment 108
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
In order to ***participate in*** the European Cyber Shield, each Member State shall designate ***at least one National SOC. The National SOC shall be a public body***.	In order to ***contribute to*** the European Cyber Shield, each Member State shall designate ***one of its Computer security incident response teams (CSIRTs), referred to in Article 10 of Directive (EU) 2022/2555, as a Information Sharing and Analysis Centre (ISAC)***.

Or. en

Amendment 109
Evžen Tošenovský

Proposal for a regulation
Article 4 – paragraph 1 – subparagraph 1 a (new)

Text proposed by the Commission	*Amendment*
	Private and public organisations or national authorities, particularly entities operating in critical or highly critical sectors, shall be encouraged to establish and operate their autonomous or shared SOCs.

Or. en

Amendment 110
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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 contributing to a Cross-border SOC. It shall be equipped with state-of-the-art technologies capable of detecting, aggregating, and analysing data relevant to cybersecurity threats and incidents. ***It or the national CSIRT may request telemetry, sensor or logging data that pertain to sectors of high criticality as defined in 2022/2555 from trusted providers or managed security service providers. This data may only be shared to support the tasks and responsibilities of the national SOC or CSIRT in detecting and preventing cybersecurity incidents.***
	Or. en

Amendment 111
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
It shall have the capacity to act as a reference point and gateway ***to*** other public and private organisations at national level for collecting and analysing information on cybersecurity threats and incidents ***and contributing to a Cross-border SOC***. It shall be equipped with state-of-the-art technologies capable of detecting, aggregating, and analysing data relevant to cybersecurity threats and incidents***.***	It shall have the capacity to act as a reference point and gateway ***primarily to SOCs established by private and public entities or national authorities, other CSIRTs of the same Member State, coordinator for the management of large-scale cybersecurity incidents and crises, as well as for*** other public and private organisations at national level for collecting and analysing information on cybersecurity threats and incidents***, and, where relevant, sharing those information with other members of the CSIRTs network***. 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 112
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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

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

Or. en

Amendment 113
Evžen Tošenovský

Proposal for a regulation
Article 4 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Following a call for expression of interest, National SOCs shall be selected by the European Cybersecurity Competence Centre ('ECCC') to participate in a joint procurement of tools and infrastructures with the ECCC. The ECCC may award grants to the selected National SOCs to fund the operation of those tools and infrastructures. The Union financial contribution shall cover up to 50% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Member State. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the	***deleted***

National SOC shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

Or. en

Amendment 114
Ville Niinistö
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 4 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Following a call for expression of interest, National SOCs ***shall*** be selected by the European Cybersecurity Competence Centre ('ECCC') to participate in a joint procurement of tools and infrastructures with the ECCC. The ECCC may award grants to the selected National SOCs to fund the operation of those tools and infrastructures. The Union financial contribution shall cover up to 50% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Member State. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the National SOC shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.	2. Following a call for expression of interest, National SOCs ***may*** be selected by the European Cybersecurity Competence Centre ('ECCC') to participate in a joint procurement of tools and infrastructures with the ECCC. The ECCC may award grants to the selected National SOCs to fund the operation of those tools and infrastructures. The Union financial contribution shall cover up to 50% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Member State. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the National SOC shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

Or. en

Justification

The mandatory nature of "shall", empties the content from the notion of call for expression of interest and selection processes. Naturally the SOCs may participate and may be selected.

Amendment 115
Evžen Tošenovský

Proposal for a regulation

Article 4 – paragraph 3

Text proposed by the Commission	*Amendment*
3. A National SOC selected pursuant to paragraph 2 shall commit to apply to participate in a Cross-border SOC within two years from the date on which the tools and infrastructures are acquired, or on which it receives grant funding, whichever occurs sooner. If a National SOC is not a participant in a Cross-border SOC by that time, it shall not be eligible for additional Union support under this Regulation.	***deleted***

Or. en

Amendment 116
Evžen Tošenovský

Proposal for a regulation
Article 5 – title

Text proposed by the Commission	*Amendment*
Cross-border Security Operations Centres	***Joint procurement of tools and infrastructures***

Or. en

Amendment 117
Evžen Tošenovský

Proposal for a regulation
Article 5 – paragraph 1

Text proposed by the Commission	*Amendment*
1. A Hosting Consortium consisting of at least three Member States, represented by National SOCs, committed to working together to coordinate their cyber-detection and threat monitoring activities shall be eligible to participate in actions to establish a Cross-border SOC.	***deleted***

Or. en

Amendment 118
Evžen Tošenovský

Proposal for a regulation
Article 5 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Following a call for expression of interest, a ***Hosting Consortium shall*** be selected by the ECCC to participate in a joint procurement of tools and infrastructures with the ECCC. The ECCC may award to ***the Hosting Consortium*** a grant to fund the operation of the tools and infrastructures. The Union financial contribution shall cover up to 75% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by ***the Hosting Consortium***. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and ***the Hosting Consortium*** shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.	2. Following a call for expression of interest, a ***CSIRTs-ISACs may*** be selected by the ECCC to participate in a joint procurement of tools and infrastructures with the ECCC. The ECCC may award to ***CSIRTs-ISACs*** a grant to fund the operation of the tools and infrastructures. The Union financial contribution shall cover up to 75% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by ***CSIRTs-ISACs***. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and ***participating CSIRT-ISAC*** shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures***, including their usage by other CSIRTs and SOCs in that Member State***.

Or. en

Amendment 119
Ville Niinistö
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 5 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Following a call for expression of interest, a Hosting Consortium ***shall*** be selected by the ECCC to participate in a joint procurement of tools and	2. Following a call for expression of interest, a Hosting Consortium ***may*** be selected by the ECCC to participate in a joint procurement of tools and

infrastructures with the ECCC. The ECCC may award to the Hosting Consortium a grant to fund the operation of the tools and infrastructures. The Union financial contribution shall cover up to 75% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Hosting Consortium. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the Hosting Consortium shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.	infrastructures with the ECCC. The ECCC may award to the Hosting Consortium a grant to fund the operation of the tools and infrastructures. The Union financial contribution shall cover up to 75% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Hosting Consortium. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the Hosting Consortium shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

Or. en

Justification

While this Regulation does not include explicit criteria, other applicable legislation might reduce the certainty that a/every applicant is successful.

Amendment 120
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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

Text proposed by the Commission	*Amendment*
	2a. Procurement from and participation of a private entity that is established in a like-minded third country should be allowed if it does not contravene the security and defence interests of the Union and the Member States as established in the framework of the common foreign and security policy pursuant to Title V of the TEU, or the objectives set out in this Regulation. Those private entities should not be controlled by a non-associated third country or they shall have been subject to screening within the meaning of Regulation (EU) 2019/452 of the European Parliament and of the Council.

Or. en

Amendment 121
Evžen Tošenovský

Proposal for a regulation
Article 5 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Members of the Hosting Consortium shall conclude a written consortium agreement which sets out their internal arrangements for implementing the hosting and usage Agreement.	***deleted***

Or. en

Amendment 122
Evžen Tošenovský

Proposal for a regulation
Article 5 – paragraph 4

Text proposed by the Commission	*Amendment*
4. A Cross-border SOC shall be represented for legal purposes by a National SOC acting as coordinating SOC, or by the Hosing Consortium if it has legal personality. The co-ordinating SOC shall be responsible for compliance with the requirements of the hosting and usage agreement and of this Regulation.	***deleted***

Or. en

Amendment 123
Evžen Tošenovský

Proposal for a regulation
Article 6 – title

Text proposed by the Commission	*Amendment*
Cooperation and information sharing ***within and between cross-border SOCs***	***Strenghtened*** cooperation and information sharing ***at EU level***

Or. en

Amendment 124
Johan Nissinen

Proposal for a regulation
Article 6 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. Members of a Hosting Consortium ***shall*** exchange relevant information among themselves within the Cross-border SOC including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding the configuration of cybersecurity tools to detect cyber attacks, where such information sharing:	1. Members of a Hosting Consortium ***may*** exchange relevant information among themselves within the Cross-border SOC including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding the configuration of cybersecurity tools to detect cyber attacks, where such information sharing:

Or. en

Amendment 125
Evžen Tošenovský

Proposal for a regulation
Article 6 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. ***Members of a Hosting Consortium*** shall exchange relevant information among themselves within the ***Cross-border SOC*** including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity	1. ***CSIRTs-ISACs and other CSIRTs*** shall exchange relevant information among themselves within the ***CSIRTs Network,*** including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity

alerts and recommendations regarding the configuration of cybersecurity tools to detect cyber attacks, where such information sharing:	alerts and recommendations regarding the configuration of cybersecurity tools to detect cyber attacks, where such information sharing:

Or. en

Amendment 126
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposal for a regulation
Article 6 – paragraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) ***aims*** to prevent, detect, ***respond to or recover from*** incidents ***or to mitigate their impact***;	(a) ***improves the exchange of cyber threat intelligence between SOCs and industry ISACs with the aim*** to prevent, detect, ***or mitigate*** incidents;

Or. en

Amendment 127
Evžen Tošenovský

Proposal for a regulation
Article 6 – paragraph 2 – introductory part

Text proposed by the Commission	*Amendment*
2. The ***written consortium*** agreement ***referred to in Article 5(3) shall*** establish:	2. The ***information and intelligence sharing*** agreement ***among CSIRTs-ISACs, or where relevant, other CSIRTs, may*** establish:

Or. en

Amendment 128
Johan Nissinen

Proposal for a regulation
Article 6 – paragraph 2 – point a

Text proposed by the Commission	*Amendment*
(a) a commitment to share ***a significant amount of*** data referred to in paragraph 1, and the conditions under which that information is to be exchanged;	(a) a commitment to ***voluntarily*** share data referred to in paragraph 1, and the conditions under which that information is to be exchanged;

Or. en

Amendment 129
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposal for a regulation
Article 6 – paragraph 2 – point a

Text proposed by the Commission	*Amendment*
(a) a commitment to share ***a*** significant ***amount of*** data referred to in paragraph 1, and the conditions under which that information is to be exchanged;	(a) a commitment to share significant data referred to in paragraph 1, and the conditions under which that information is to be exchanged;

Or. en

Amendment 130
Evžen Tošenovský

Proposal for a regulation
Article 6 – paragraph 3

Text proposed by the Commission	*Amendment*
3. To encourage exchange of information between Cross-border SOCs, Cross-border SOCs shall ensure a high level of interoperability between themselves. To facilitate the interoperability between the Cross-border SOCs, the Commission may, by means of implementing acts, after consulting the ECCC, specify the conditions for this interoperability. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation.	***deleted***

Or. en

Amendment 131
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposal for a regulation
Article 6 – paragraph 3

Text proposed by the Commission	*Amendment*
3. To encourage exchange of information ***between*** Cross-border SOCs, Cross-border SOCs shall ensure a high level of interoperability between themselves. To facilitate the interoperability between the Cross-border SOCs, the Commission ***may,*** by means of ***implementing acts, after consulting the ECCC, specify*** the conditions for this interoperability. Those ***implementing*** acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation.	3. To encourage exchange of information ***amongst*** Cross-border SOCs ***and with industry ISACs***, Cross-border SOCs shall ensure a high level of interoperability between themselves ***and, where possible with industry ISACs***. To facilitate the interoperability between the Cross-border SOCs ***and with industry ISACs***, ***information sharing standards and protocols should be harmonized with international standards and industry best practices. The ECCC may also request*** the Commission by means of ***delegated acts to propose*** the conditions for this interoperability ***in close coordination with the regional SOCs and on the basis of international standards and industry best practices***. Those ***delegated*** acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation.

Or. en

Amendment 132
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 6 – paragraph 3

Text proposed by the Commission	*Amendment*
3. To encourage exchange of information between Cross-border SOCs, Cross-border SOCs shall ensure a high	3. To encourage exchange of information between Cross-border SOCs, Cross-border SOCs shall ensure a high

level of interoperability between themselves. ***To*** facilitate the interoperability between the Cross-border SOCs, the Commission may**,** by means of implementing acts, after consulting the ECCC, specify the conditions for this interoperability. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation.

level of interoperability between themselves. ***Joint procurement of cyber infrastructures, services and tools may*** facilitate the interoperability between the Cross-border SOCs***. To specify the conditions for interoperability of the Cross-border SOCs***, the Commission**,** may by means of implementing acts, after consulting the ECCC ***and ENISA***, specify the conditions for this interoperability. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation.

Or. en

Amendment 133
Evžen Tošenovský

Proposal for a regulation
Article 6 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Cross-border SOCs shall conclude cooperation agreements with one another, specifying information sharing principles among the cross-border platforms.	***deleted***

Or. en

Amendment 134
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 6 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Cross-border SOCs shall conclude cooperation agreements with one another, specifying information sharing principles among the cross-border platforms.	4. Cross-border SOCs shall conclude cooperation agreements with one another, specifying information sharing principles among the cross-border platforms***, taking into consideration already existing***

	relevant information sharing mechanisms under the Directive (EU) 2022/2555. In the context of a potential or ongoing large-scale cybersecurity incident, information sharing mechanisms shall comply with the relevant provisions under the Directive (EU) 2022/2555.

Or. en

Amendment 135
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposal for a regulation
Article 6 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Cross-border SOCs shall conclude cooperation agreements with one another, specifying information sharing principles among the cross-border platforms.	4. Cross-border SOCs shall conclude cooperation agreements with one another ***and with industry ISACs***, specifying information sharing ***and interoperability*** principles among the cross-border platforms.

Or. en

Amendment 136
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposal for a regulation
Article 7 – title

Text proposed by the Commission	*Amendment*
Cooperation and information sharing with ***Union entities***	Cooperation and information sharing with ***the CSIRT network***

Or. en

Amendment 137
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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 ***for the purpose of shared situation awareness, the coordinating SOC*** shall provide ***the*** relevant information to ***its CSIRT or competent authority, which will report this to the*** EU=CyCLONe, the CSIRTs network and the Commission, in view of their respective crisis management roles ***and procedures*** in accordance with Directive (EU) 2022/2555 without undue delay.

Or. en

Justification

Suggest to keep to the NIS2 procedure for large scale incidents.

Amendment 138
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 ***and ENISA, in line with*** their respective crisis management roles in accordance with Directive (EU) 2022/2555 without undue delay.

Or. en

Amendment 139

Evžen Tošenovský

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 ***CSIRTs-ISACs*** obtain information relating to a potential or ongoing large-scale cybersecurity incident, they shall provide relevant information to ***EU-CyCLONe and*** the CSIRTs network, in view of their respective crisis management roles in accordance with Directive (EU) 2022/2555 without undue delay.

Or. en

Amendment 140
Evžen Tošenovský

Proposal for a regulation
Article 7 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The Commission may, by means of implementing acts, determine the procedural arrangements for the information sharing provided for in paragraphs 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation.	***deleted***

Or. en

Amendment 141
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposal for a regulation
Article 7 – paragraph 2

Text proposed by the Commission	*Amendment*

2. The Commission may, by means of implementing acts, determine the procedural arrangements for the information sharing provided for in paragraphs 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation.	2. The Commission may***, after consulting the cross-border platforms and the CSIRT network***, by means of implementing acts, determine the procedural arrangements for the information sharing provided for in paragraphs 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation ***and in accordance with Directive (EU) 2022/2555***.

Or. en

Justification

Suggest to keep to the NIS2 procedure for large scale incidents and therefore to consult the CSIRT network first.

Amendment 142
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 7 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The Commission may, by means of implementing acts, determine the procedural arrangements for the information sharing provided for in paragraphs 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation.	2. The Commission may***, after consulting ENISA***, by means of implementing acts, determine the procedural arrangements for the information sharing provided for in paragraphs 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation.

Or. en

Amendment 143
Johan Nissinen

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 ***confidentiality,*** 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.

Or. en

Amendment 144
Evžen Tošenovský

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.	***deleted***

Or. en

Amendment 145
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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 ***and with Directive (EU) 2022/2555 and 2022/2557***. 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.

Or. en

Amendment 146
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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***, after consulting ENISA,*** 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.

Or. en

Amendment 147
Johan Nissinen

Proposal for a regulation
Article 9 – paragraph 1

Text proposed by the Commission	*Amendment*
1. A Cyber Emergency Mechanism is established to improve the Union's resilience to major cybersecurity threats and prepare for and mitigate, in a spirit of solidarity, the short-term impact of significant and large-scale cybersecurity incidents (the 'Mechanism').	1. A Cyber Emergency Mechanism is established to improve the Union's resilience to major cybersecurity threats and prepare for and mitigate, in a spirit of solidarity, the short-term impact of significant and large-scale cybersecurity incidents (the 'Mechanism')***, at the explicit request of the Member State(s) concerned***.

Or. en

Amendment 148
Evžen Tošenovský

Proposal for a regulation
Article 9 – paragraph 1

Text proposed by the Commission	*Amendment*
1. A Cyber Emergency Mechanism is established to improve the Union's resilience to ***major*** cybersecurity threats and prepare for and mitigate, in a spirit of solidarity, the short-term impact of significant and large-scale cybersecurity incidents (the 'Mechanism').	1. A Cyber Emergency Mechanism is established to improve the Union's resilience to ***significant*** cybersecurity threats and prepare for and mitigate, in a spirit of solidarity, the short-term impact of significant and large-scale cybersecurity incidents (the 'Mechanism').

Or. en

Amendment 149
Johan Nissinen

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

Text proposed by the Commission	*Amendment*
(b) response actions, supporting	(b) response actions, supporting

response to and immediate recovery from significant and large-scale cybersecurity incidents, to be provided by trusted providers participating in the EU Cybersecurity Reserve established under Article 12;	response to and immediate recovery from significant and large-scale cybersecurity incidents, to be provided by trusted providers participating in the EU Cybersecurity Reserve established under Article 12***, at the explicit request of the Member State(s) concerned***;

Or. en

Amendment 150
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
(b) response actions, supporting response to and immediate recovery from significant and large-scale cybersecurity incidents, to be provided by trusted providers participating in the EU Cybersecurity Reserve established under Article 12;	(b) response actions, supporting response to and immediate recovery from significant and large-scale cybersecurity incidents, to be provided by trusted ***managed security service*** providers participating in the EU Cybersecurity Reserve established under Article 12;

Or. en

Amendment 151
Ville Niinistö
on behalf of the Verts/ALE Group

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

Text proposed by the Commission	*Amendment*
	1a. Following the triggering of the cyber emergency mechanism, the Commission shall report each year the assessment of both positive and negative working of the mechanism, including whether further cooperation or training requirements are needed.

Or. en

Amendment 152
Evžen Tošenovský

Proposal for a regulation
Article 11 – paragraph 1

Text proposed by the Commission	*Amendment*
1. For the purpose of supporting the coordinated preparedness testing of entities referred to in Article 10(1), point (a), across the Union, the Commission, after consulting the NIS Cooperation Group and ENISA, shall identify the sectors, or sub-sectors, concerned, from the Sectors of High Criticality listed in Annex I to Directive (EU) 2022/2555 from which entities may be subject to the coordinated preparedness testing, taking into account existing and planned coordinated risk assessments and resilience testing at Union level.	1. For the purpose of supporting the coordinated preparedness testing of entities referred to in Article 10(1), point (a), across the Union, the Commission, after consulting the NIS Cooperation Group and ENISA, shall identify the sectors, or sub-sectors, concerned, from the Sectors of High Criticality listed in Annex I to Directive (EU) 2022/2555 from which entities may be subject to the ***voluntary*** coordinated preparedness testing, taking into account existing and planned coordinated risk assessments and resilience testing at Union level.

Or. en

Amendment 153
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposal for a regulation
Article 11 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The NIS Cooperation Group in cooperation with the Commission, ENISA, and the High Representative, shall develop common risk scenarios and methodologies for the coordinated testing ***exercises***.	2. The NIS Cooperation Group in cooperation with the Commission, ENISA, and the High Representative, shall develop common risk scenarios and methodologies for the coordinated ***preparedness testing. This will inform the identification of sectors, or -subsectors concerned from which entities may be subject to the coordinated prepareness*** testing ***as described in paragraph 1***.

Or. en

Amendment 154
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 11 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The NIS Cooperation Group in cooperation with the Commission, ENISA, ***and*** the High Representative, shall develop common risk scenarios and methodologies for the coordinated testing exercises.	2. The NIS Cooperation Group in cooperation with the Commission, ENISA, the High Representative***, and the entities that may be subject to the preparedness testing***, shall develop common risk scenarios and methodologies for the coordinated testing exercises.

Or. en

Amendment 155
Johan Nissinen

Proposal for a regulation
Article 12 – paragraph 1

Text proposed by the Commission	*Amendment*
1. An EU Cybersecurity Reserve shall be established, in order to assist users referred to in paragraph 3, in responding or providing support for responding to significant or large-scale cybersecurity incidents, and immediate recovery from such incidents.	1. An EU Cybersecurity Reserve shall be established, in order to assist users referred to in paragraph 3, in responding or providing support for responding to significant or large-scale cybersecurity incidents, and immediate recovery from such incidents***, at the explicit request of the Member State(s) concerned and without prejudice to the specific character of the security and defence policy of certain Member States***.

Or. en

Amendment 156
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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***, shall reinforce the Union's resilience and sovereignty, and improve the Union's competitiveness***. ***The names of the selected trusted providers and their services shall be kept confidential.***

Or. en

Amendment 157
Johan Nissinen

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. ***The EU Cybersecurity Reserve does not limit the need to allow countries to monitor and assess their own needs.***

Or. en

Amendment 158
Evžen Tošenovský

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 ***managed security service*** providers selected in accordance with the criteria laid down in Article 16. The Reserve shall include pre-committed services. The services ***may be, upon request,*** deployable in all Member States.

Or. en

Amendment 159
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
(b) ***Union institutions, bodies and agencies***.	(b) ***Third countries refferred to in Article 17 of this Regulation***.

Or. en

Amendment 160
Evžen Tošenovský

Proposal for a regulation
Article 12 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Users referred to in paragraph 3, point (a), ***shall*** use the services from the EU Cybersecurity Reserve in order to respond or support response to and immediate recovery from significant or large-scale incidents affecting entities operating in critical or highly critical sectors.	4. Users referred to in paragraph 3, point (a), ***may, upon request*** 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.

Or. en

Amendment 161
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposal for a regulation
Article 12 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The Commission shall have overall responsibility for the implementation of the EU Cybersecurity Reserve. The Commission shall determine the priorities and evolution of the EU Cybersecurity Reserve**,** in line with the requirements of the users referred to in paragraph 3, and shall supervise its implementation, and ensure complementarity, consistency, synergies and links with other support actions under this Regulation as well as other Union actions and programmes.	5. The Commission shall have overall responsibility for the implementation of the EU Cybersecurity Reserve. The Commission shall determine the priorities and evolution of the EU Cybersecurity Reserve ***in coordination with the NIS2 Coordination Group and*** in line with the requirements of the users referred to in paragraph 3, and shall supervise its implementation, and ensure complementarity, consistency, synergies and links with other support actions under this Regulation as well as other Union actions and programmes.

Or. en

Amendment 162
Evžen Tošenovský

Proposal for a regulation
Article 12 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The Commission shall have overall responsibility for the implementation of the EU Cybersecurity Reserve. The Commission shall determine the priorities and evolution of the EU Cybersecurity Reserve, in line with the requirements of the users referred to in paragraph 3, and shall supervise its implementation, and ensure complementarity, consistency, synergies and links with other support actions under this Regulation as well as other Union actions and programmes.	5. The Commission shall have overall responsibility for the implementation of the EU Cybersecurity Reserve. The Commission ***in cooperation with ENISA*** shall determine the priorities and evolution of the EU Cybersecurity Reserve, in line with the requirements of the users referred to in paragraph 3, and shall supervise its implementation, and ensure complementarity, consistency, synergies and links with other support actions under this Regulation as well as other Union actions and programmes.

Or. en

Amendment 163
Evžen Tošenovský

Proposal for a regulation
Article 12 – paragraph 6

Text proposed by the Commission	*Amendment*
6. The Commission may entrust the operation and administration of the EU Cybersecurity Reserve, in full or in part, to ENISA, by means of contribution agreements.	***deleted***

Or. en

Amendment 164
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 12 – paragraph 6

Text proposed by the Commission	*Amendment*
6. The Commission ***may*** entrust the operation and administration of the EU Cybersecurity Reserve, in full or in part, to ENISA, by means of contribution agreements.	6. The Commission ***shall*** entrust the operation and administration of the EU Cybersecurity Reserve, in full or in part, to ENISA, by means of contribution agreements.

Or. en

Amendment 165
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 12 – paragraph 7

Text proposed by the Commission	*Amendment*
7. In order to support the Commission	7. In order to support the Commission

in establishing the EU Cybersecurity Reserve, ENISA shall prepare a mapping of the services needed, after consulting Member States and the Commission. ENISA shall prepare a similar mapping, after consulting the Commission, to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve pursuant to Article 17. The Commission, where relevant, shall consult the High Representative.	in establishing the EU Cybersecurity Reserve, ENISA shall prepare a mapping of the services needed, ***including the needed skills and capacity of the cybersecurity workforce,*** after consulting Member States and the Commission. ENISA shall prepare a similar mapping, after consulting the Commission ***and in partnership with the private sector***, to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve pursuant to Article 17. The Commission, where relevant, shall consult the High Representative.

Or. en

Amendment 166
Evžen Tošenovský

Proposal for a regulation
Article 12 – paragraph 7

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

Or. en

Amendment 167
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposal for a regulation

Article 12 – paragraph 7

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

Or. en

Amendment 168
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 12 – paragraph 8

Text proposed by the Commission	*Amendment*
8. The Commission may***, by means of implementing acts,*** specify the types and the number of response services required for the EU Cybersecurity Reserve. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2).	8. The Commission may ***adopt a Delegated Act in accordance with Article 20a of this Regulation to*** specify the types and the number of response services required for the EU Cybersecurity Reserve. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2).

Or. en

Amendment 169
Evžen Tošenovský

Proposal for a regulation
Article 13 – paragraph 5 – point a

Text proposed by the Commission	*Amendment*
(a) ***appropriate information regarding the*** affected entity and potential impacts of the incident and the planned use of the requested support, including an indication of the estimated needs;	(a) ***type of*** affected entity and potential impacts of the incident and the planned use of the requested support, including an indication of the estimated needs;

Or. en

Amendment 170
Evžen Tošenovský

Proposal for a regulation
Article 13 – paragraph 5 – point b

Text proposed by the Commission	*Amendment*
(b) ***information*** about measures taken to mitigate the incident for which the support is requested, as referred to in paragraph 2;	(b) ***general*** about measures taken to mitigate the incident for which the support is requested, as referred to in paragraph 2;

Or. en

Amendment 171
Evžen Tošenovský

Proposal for a regulation
Article 13 – paragraph 5 – point c

Text proposed by the Commission	*Amendment*
(c) information about other forms of support available to the affected entity***, including contractual arrangements in place for incident response and immediate recovery services, as well as insurance contracts potentially covering such type of incident.***	(c) information about other forms of support available to the affected entity

Or. en

Amendment 172

Evžen Tošenovský

Proposal for a regulation
Article 13 – paragraph 7

Text proposed by the Commission	*Amendment*
7. The Commission may, by means of implementing acts, specify further the detailed arrangements for allocating the EU Cybersecurity Reserve support services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2).	***deleted***

Or. en

Amendment 173
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 13 – paragraph 7

Text proposed by the Commission	*Amendment*
7. The Commission may***, by means of implementing acts,*** specify further the detailed arrangements for allocating the EU Cybersecurity Reserve support services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2).	7. The Commission may ***adopt delegated acts in accordance with Article 20a of this Regulation to*** specify further the detailed arrangements for allocating the EU Cybersecurity Reserve support services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2).

Or. en

Amendment 174
Evžen Tošenovský

Proposal for a regulation
Article 14 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Requests for support from the EU Cybersecurity Reserve, shall be assessed by the Commission, with the support of ENISA ***or as defined in contribution agreements under Article 12(6), and a response*** shall be transmitted to the users referred to in Article 12(3) without delay.	1. Requests for support from the EU Cybersecurity Reserve, shall be assessed by the Commission, with the support of ENISA ***and its decision*** shall be transmitted to the users referred to in Article 12(3) without ***undue*** delay ***and in any event within 24 hours***.

Or. en

Amendment 175
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposal for a regulation
Article 14 – paragraph 2 – point d

Text proposed by the Commission	*Amendment*
(d) the potential cross-border nature of the incident and the risk of spill over to other Member States or users;	(d) the ***scale and*** potential cross-border nature of the incident and the risk of spill over to other Member States or users;

Or. en

Amendment 176
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 14 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The EU Cybersecurity Reserve services shall be provided in accordance with specific agreements between the service provider and the user to which the support under the EU Cybersecurity Reserve is provided. Those agreements shall include liability conditions.	3. The EU Cybersecurity Reserve services shall be provided in accordance with specific agreements between the service provider and the user to which the support under the EU Cybersecurity Reserve is provided. Those agreements shall include liability conditions ***and any other provisions the parties to the agreement deem necessary for the provision of the respective service***.

Or. en

Amendment 177
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposal for a regulation
Article 14 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The EU Cybersecurity Reserve services shall be provided in accordance with specific agreements between the service provider and the user to which the support under the EU Cybersecurity Reserve is provided. Those agreements shall include liability conditions.	3. The EU Cybersecurity Reserve services shall be provided ***upon approval of the user and*** in accordance with specific agreements between the service provider and the user to which the support under the EU Cybersecurity Reserve is provided. Those agreements shall include liability conditions.

Or. en

Amendment 178
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 14 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The agreements referred to in paragraph 3 ***may*** be based on templates prepared by ENISA, after consulting Member States.	4. The agreements referred to in paragraph 3 ***shall*** be based on templates prepared by ENISA, after consulting Member States ***and other users of the reserve***.

Or. en

Amendment 179
Evžen Tošenovský

Proposal for a regulation
Article 14 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The Commission and ENISA shall bear no contractual liability for damages caused to third parties by the services provided in the framework of the implementation of the EU Cybersecurity Reserve.	***deleted***

Or. en

Amendment 180
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposal for a regulation
Article 14 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The Commission and ENISA shall bear no contractual liability for damages caused to third parties by the services provided in the framework of the implementation of the EU Cybersecurity Reserve.	5. The Commission and ENISA shall bear no contractual liability for damages caused to third parties by the services provided in the framework of the implementation of the EU Cybersecurity Reserve***, except in cases of negligence in the evaluation of the application of the service provider, or in cases where the Commission or ENISA are users and are found responsible for damages***.

Or. en

Amendment 181
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 14 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The Commission and ENISA shall bear no contractual liability for damages caused to third parties by the services provided in the framework of the implementation of the EU Cybersecurity	5. The Commission and ENISA shall bear no contractual liability for damages caused to third parties by the services provided in the framework of the implementation of the EU Cybersecurity

Reserve.	Reserve***, except for cases where the Commission or ENISA are users of the Reserve according to Article 14 (3)***.

Or. en

Amendment 182
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposal for a regulation
Article 14 – paragraph 6

Text proposed by the Commission	*Amendment*
6. Within one month from the end of the support action, the users shall provide Commission and ENISA with a summary report about the service provided, results achieved and the lessons learned. When the user is from a third country as set out in Article 17, such report shall be shared with the High Representative.	6. Within one month from the end of the support action, the users shall provide Commission and ENISA with a summary report about the service provided, results achieved and the lessons learned. When the user is from a third country as set out in Article 17, such report shall be shared with the High Representative. ***The report shall respect Union or national law concerning the protection of sensitive or classified information.***

Or. en

Amendment 183
Evžen Tošenovský

Proposal for a regulation
Article 14 – paragraph 6

Text proposed by the Commission	*Amendment*
6. Within one month from the end of the support action, the users shall provide Commission ***and*** ENISA with a summary report about the service provided, results achieved and the lessons learned. When the user is from a third country as set out in Article 17, such report shall be shared with the High Representative.	6. Within one month from the end of the support action, the users shall provide Commission***,*** ENISA***, CSIRTs Network and, where relevant, EU-CyCLONe*** with a summary report about the service provided, results achieved and the lessons learned. When the user is from a third country as set out in Article 17, such report shall be shared with the High Representative.

Or. en

Amendment 184
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposal for a regulation
Article 14 – paragraph 7

Text proposed by the Commission	*Amendment*
7. The Commission shall report to the NIS Cooperation Group about the use and the results of the support, on a regular basis.	7. The Commission shall report to the NIS Cooperation Group about the use and the results of the support, on a regular basis. ***It shall protect confidential information, in accordance with Union or national law concerning the protection of sensitive or classified information.***

Or. en

Amendment 185
Evžen Tošenovský

Proposal for a regulation
Article 14 – paragraph 7

Text proposed by the Commission	*Amendment*
7. The Commission shall report to the NIS Cooperation Group about the use and the results of the support***, on a regular basis***.	7. The Commission shall report ***at least twice a year*** to the NIS Cooperation Group about the use and the results of the support.

Or. en

Amendment 186
Evžen Tošenovský

Proposal for a regulation
Article 15 – title

Text proposed by the Commission	*Amendment*
Coordination with crisis management	Coordination ***of the Cyber Emergency Mechanism*** with crisis management

mechanisms	mechanisms

Or. en

Amendment 187
Evžen Tošenovský

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.

Or. en

Amendment 188
Evžen Tošenovský

Proposal for a regulation
Article 16 – title

Text proposed by the Commission	*Amendment*
Trusted providers	Trusted ***managed security service*** providers

Or. en

Amendment 189
Johan Nissinen

Proposal for a regulation

Article 16 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. In procurement procedures for the purpose of establishing the EU Cybersecurity Reserve, the contracting authority shall act in accordance with the principles laid down in the Regulation (EU, Euratom) 2018/1046 and in accordance with the following principles:	1. In procurement procedures for the purpose of establishing the EU Cybersecurity Reserve, the contracting authority shall act in accordance with the principles laid down in the Regulation (EU, Euratom) 2018/1046***, without prejudice to the Member States' primary responsibility for national security,*** and in accordance with the following principles:

Or. en

Amendment 190
Evžen Tošenovský

Proposal for a regulation
Article 16 – paragraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) ensure the EU Cybersecurity Reserve includes services that may be deployed in all Member States, taking into account in particular national requirements for the provision of such services, including certification or accreditation;	(a) ensure the EU Cybersecurity Reserve includes services that may be deployed in all Member States ***and third countries in accordance with Article 17 of this Regulation***, taking into account in particular national requirements for the provision of such services, including certification or accreditation;

Or. en

Amendment 191
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 16 – paragraph 1 – point c

Text proposed by the Commission	*Amendment*
(c) ensure that the EU Cybersecurity Reserve brings EU added value, by	(c) ensure that the EU Cybersecurity Reserve brings EU added value, by

contributing to the objectives set out in Article 3 of Regulation (EU) 2021/694, including promoting the development of cybersecurity skills in the EU.	contributing to the objectives set out in Article 3 of Regulation (EU) 2021/694, including promoting the development of cybersecurity skills in the EU***, reinforcing the Union's resilience and sovereignty, and improving the Union's competitiveness***.

Or. en

Amendment 192
Evžen Tošenovský

Proposal for a regulation
Article 16 – paragraph 1 – point c

Text proposed by the Commission	*Amendment*
(c) ensure that the EU Cybersecurity Reserve ***brings EU added value, by contributing*** to the objectives set out in Article 3 of Regulation (EU) 2021/694, including promoting the development of cybersecurity skills in the EU.	(c) ensure that the EU Cybersecurity Reserve ***contributes*** to the objectives set out in Article 3 of Regulation (EU) 2021/694, including promoting the development of cybersecurity skills in the EU.

Or. en

Amendment 193
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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

Text proposed by the Commission	*Amendment*
(f) the provider shall be equipped with the hardware and software technical equipment necessary to support the requested service;	(f) the provider shall be equipped with the ***up-to-date*** hardware and software technical equipment necessary to support the requested service ***and shall meet the requirements set out in Regulation XX/XXXX (Cyber Resilience Act), where applicable***;

Or. en

Amendment 194
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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

Text proposed by the Commission	*Amendment*
	(fa) the provider shall demonstrate that its decision and management structures are free from any undue influence by governments of states classified as systemic rivals of the Union;

Or. en

Amendment 195
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
(h) the provider shall be able to provide the service within a short timeframe in the Member State(s) where it can deliver the service;	(h) the provider shall be able to provide the service within a short timeframe in the Member State(s) ***or third countries*** where it can deliver the service;

Or. en

Amendment 196
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
(i) the provider shall be able to provide the service in the local language of the Member State(s) where it can deliver the service;	(i) the provider shall be able to provide the service in the local language of the Member State(s) ***or third countries*** where it can deliver the service ***or in one of the***

working languages of the EU institutions;

Or. en

Amendment 197
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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

Text proposed by the Commission	*Amendment*
(j) once an EU certification scheme for managed security service Regulation (EU) 2019/881 is in place, the provider shall be certified in accordance with that scheme.	(j) once an EU certification scheme for managed security service Regulation (EU) 2019/881 is in place, the provider shall be certified in accordance with that scheme***, within a period of two years after the scheme has been adopted***.

Or. en

Amendment 198
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
(j) once an ***EU*** certification scheme for managed security service Regulation (EU) 2019/881 is in place, the provider shall be certified in accordance with that scheme.	(j) once an ***European cybersecurity*** certification scheme for managed security service ***pursuant to*** Regulation (EU) 2019/881 is in place, the provider shall be certified in accordance with that scheme.

Or. en

Amendment 199
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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

Text proposed by the Commission	*Amendment*
(j) once an EU certification scheme for managed security service Regulation (EU) 2019/881 is in place, the provider shall be certified in accordance with that scheme.	(j) once an EU certification scheme for managed security service Regulation (EU) 2019/881 is in place, the provider shall be certified in accordance with that scheme ***within two years***.

Or. en

Justification

The Commission proposal is that a certification scheme will replace the technical requirements listed in this Regulation. This amendment allow companies, especially SMEs, more time to transition to that scheme, encouraging a more equal playing field across the Union. Until that time, they will have to adhere to the technical requirements of this Regulation.

Amendment 200
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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

Text proposed by the Commission	*Amendment*
	(ja) the provider shall be able to unbundle their services from the wider contract so the user can switch to another service provider;

Or. en

Amendment 201
Evžen Tošenovský

Proposal for a regulation
Article 17 – paragraph 6

Text proposed by the Commission	*Amendment*
6. The Commission shall coordinate with the High Representative about the requests received and the implementation of the support granted to third countries from the EU Cybersecurity Reserve.	6. The Commission shall ***without undue delay notify the Council and*** coordinate with the High Representative about the requests received and the implementation of the support granted to third countries from the EU Cybersecurity

Reserve.

Or. en

Amendment 202
Evžen Tošenovský

Proposal for a regulation
Article 18

Text proposed by the Commission	*Amendment*
Article 18	***deleted***
Cybersecurity Incident Review Mechanism	
1. At the request of the Commission, the EU-CyCLONe or the CSIRTs network, ENISA shall review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. Following the completion of a review and assessment of an incident, ENISA shall deliver an incident review report to the CSIRTs network, the EU-CyCLONe and the Commission to support them in carrying out their tasks, in particular in view of those set out in Articles 15 and 16 of Directive (EU) 2022/2555. Where relevant, the Commission shall share the report with the High Representative.	
2. To prepare the incident review report referred to in paragraph 1, ENISA shall collaborate all relevant stakeholders, including representatives of Member States, the Commission, other relevant EU institutions, bodies and agencies, managed security services providers and users of cybersecurity services. Where appropriate, ENISA shall also collaborate with entities affected by significant or large-scale cybersecurity incidents. To support the review, ENISA may also consult other types of stakeholders. Consulted representatives shall disclose any potential conflict of interest.	

3. The report shall cover a review and analysis of the specific significant or large-scale cybersecurity incident, including the main causes, vulnerabilities and lessons learned. It shall protect confidential information, in accordance with Union or national law concerning the protection of sensitive or classified information.	
4. Where appropriate, the report shall draw recommendations to improve the Union's cyber posture.	
5. Where possible, a version of the report shall be made available publicly. This version shall only include public information.	

Or. en

Amendment 203
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 18 – paragraph 2

Text proposed by the Commission	*Amendment*
2. To prepare the incident review report referred to in paragraph 1, ENISA shall collaborate all relevant stakeholders, including representatives of Member States, the Commission, other relevant EU institutions, bodies and agencies, managed security services providers and users of cybersecurity services. Where appropriate, ENISA shall also collaborate with entities affected by significant or large-scale cybersecurity incidents. To support the review, ENISA may also consult other types of stakeholders. Consulted representatives shall disclose any potential conflict of interest.	2. To prepare the incident review report referred to in paragraph 1, ENISA shall collaborate ***with and gather feedback from*** all relevant stakeholders, including representatives of Member States, the Commission, other relevant EU institutions, bodies and agencies, managed security services providers and users of cybersecurity services. Where appropriate, ENISA shall also collaborate with entities affected by significant or large-scale cybersecurity incidents. To support the review, ENISA may also consult other types of stakeholders. Consulted representatives shall disclose any potential conflict of interest.

Or. en

Amendment 204
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposal for a regulation
Article 18 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The report shall cover a review and analysis of the specific significant or large-scale cybersecurity incident, including the main causes, vulnerabilities and lessons learned. It shall protect confidential information, in accordance with Union or national law concerning the protection of sensitive or classified information.	3. The report shall cover a review and analysis of the specific significant or large-scale cybersecurity incident, including the main causes, vulnerabilities and lessons learned. It shall protect confidential information, in accordance with Union or national law concerning the protection of sensitive or classified information. ***It shall not include any details about actively exploited vulnerabilities that remain unpatched.***

Or. en

Amendment 205
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 18 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Where appropriate, the report shall draw recommendations to improve the Union's cyber posture**.**	4. Where appropriate, the report shall draw ***concrete*** recommendations**,** ***including for all relevant stakeholders,*** to improve the Union's cyber posture***;***

Or. en

Amendment 206
Johan Nissinen

Proposal for a regulation
Article 18 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Where appropriate, the report shall draw recommendations to improve the Union's cyber posture.	4. Where appropriate, the report shall draw ***non-legally binding voluntary*** recommendations to improve the Union's cyber posture.

Or. en

Amendment 207
Evžen Tošenovský

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

Text proposed by the Commission	*Amendment*
(aa) support the development of an EU Cyber Shield, including the development, deployment and operation of ***National and Cross-border SOCs platforms*** that contribute to situational awareness in the Union and to enhancing the cyber threat intelligence capacities of the Union;	(aa) support the development of an EU Cyber Shield, including the development, deployment and operation of ***CSIRTs-ISACs and SOCs*** that contribute to situational awareness in the Union and to enhancing the cyber threat intelligence capacities of the Union;

Or. en

Amendment 208
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 19 – paragraph 1 – point 3
Regulation (EU) 2021/694
Article 14 (2)

Text proposed by the Commission	*Amendment*
The Programme may provide funding in any of the forms laid down in the Financial Regulation, including in particular through procurement as a primary form, or grants and prizes.	The Programme may provide funding in any of the forms laid down in the Financial Regulation, including in particular through procurement as a primary form, or grants and prizes. ***ENISA shall receive additional resources to carry out its additional tasks***

laid down in Regulation XX/XXX (Cyber Solidarity Act). That additional funding shall not jeopardise the achievements of the objectives of the Programme.

Or. en

Amendment 209
Evžen Tošenovský

Proposal for a regulation
Article 19 – paragraph 1 – point 5
Regulation (EU) 2021/694
Article 19

Text proposed by the Commission	*Amendment*
Support in the form of grants may be awarded directly by the ECCC without a call for proposals to the ***National SOCs*** referred to in Article 4 of Regulation XXXX ***and the Hosting Consortium*** referred to in Article 5 of Regulation XXXX, in accordance with Article 195(1), point (d) of the Financial Regulation.	Support in the form of grants may be awarded directly by the ECCC without a call for proposals to the ***CSIRTs-ISACs*** referred to in Article 4 of Regulation XXXX referred to in Article 5 of Regulation XXXX, in accordance with Article 195(1), point (d) of the Financial Regulation.

Or. en

Amendment 210
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 20 – title

Text proposed by the Commission	*Amendment*
Evaluation	Evaluation ***and Review***

Or. en

Amendment 211
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 [***two*** years after the date of application of this Regulation] ***and every two years thereafter***, the Commission shall ***carry out an*** evaluation ***of the functioning of the measures laid down in*** this Regulation ***and submit a report*** to the European Parliament and the Council. ***The evaluation shall assess in particular:*** ***(a) the participation of Member States in the European Cyber Shield, including the number of National SOCs and cross-border SOCs established as part of the Regulation and the effectiveness of information exchange;*** ***(b) the contribution of this Regulation to reinforce the Union's resilience and sovereignty, to improve the competitiveness of the relevant industry sectors, including SMEs, and the development of cybersecurity skills in the EU;*** ***(c) the use of the Cybersecurity Reserve, including whether the scope of the reserve should be broadened to incident preparedness services or common exercises with the trusted providers and potential users of the Cybersecurity Reserve to ensure efficient functioning of the Reserve when needed;*** ***(d) the contribution of this Regulation to the development and improvement of the skills and competences of the workforce in the cybersecurity sector, needed to strengthen the Union's capacity to detect, prevent, respond to and recover from cybersecurity threats and incidents;*** ***(e) the contribution of this Regulation to the deployment and development of state-of-the-art technologies in the Union;*** ***On the basis of that report, the Commission shall, where appropriate,***

	submit a legislative proposal to the Parliament and the Council to amend this Regulation.

Or. en

Amendment 212
Evžen Tošenovský

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 [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. ***The report shall be accompanied, where necessary, by a legislative proposal.***

Or. en

Amendment 213
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen, Nicola Danti

Proposal for a regulation
Article 20 – paragraph 1 a (new)

Text proposed by the Commission	*Amendment*
	Every year when presenting the Draft Budget for the following year, the Commission shall submit a detailed assessment of ENISA's tasks under this Regulation as well as [the proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements] and other Union legislation and shall detail the financial and human resources needed to fulfil those tasks.

Or. en

Amendment 214
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposal for a regulation
Article 20 a (new)

Text proposed by the Commission	*Amendment*
	Article20a
	Exercise of the delegation
	1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
	2. The power to adopt delegated acts referred to in Article 12(8) and Article 13(7) shall be conferred on the Commission for a period of 5 years from … [date of entry into force of the basic legislative act or any other date set by the co-legislators]. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the 5 year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.
	3. The delegation of power referred to in Article 12(8) and Article 13(7) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force
	4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13

	April 2016 on Better Law-Making.
	5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
	6. A delegated act adopted pursuant to Article 12(8) or Article 13(7) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by [two months] at the initiative of the European Parliament or of the Council.

Or. en

Amendment 215
Evžen Tošenovský

Proposal for a regulation
Annex I – paragraph 1 – point 1
Regulation (EU) 2021/694
Annex I – chapter "Specific Objective 3 – Cybersercurity and Trust"

Text proposed by the Commission	*Amendment*
1. Co-investment with Member States in advanced cybersecurity equipment, infrastructures and knowhow that are essential to protect critical infrastructures and the Digital Single Market at large. Such co-investment could include investments in quantum facilities and data resources for cybersecurity, situational awareness in cyberspace including National ***SOCs and Cross-border*** SOCs forming the European Cyber Shield, as well as other tools to be made available to public and private sector across Europe.	1. Co-investment with Member States in advanced cybersecurity equipment, infrastructures and knowhow that are essential to protect critical infrastructures and the Digital Single Market at large. Such co-investment could include investments in quantum facilities and data resources for cybersecurity, situational awareness in cyberspace including national ***CSIRTs and*** SOCs forming the European Cyber Shield, as well as other tools to be made available to public and private sector across Europe.

Or. en

Amendment 216
Evžen Tošenovský

Proposal for a regulation
Annex I – paragraph 1 – point 1
Regulation (EU) 2021/694
Annex I – chapter "Specific Objective 3 – Cybersercurity and Trust"

Text proposed by the Commission	*Amendment*
5. Promoting solidarity among Member States in preparing for and responding to significant cybersecurity incidents through deployment of cybersecurity services across borders, including support for mutual assistance between public authorities and the establishment of a reserve of trusted ***cybersecurity*** providers at Union level.;	5. Promoting solidarity among Member States in preparing for and responding to significant cybersecurity incidents through deployment of cybersecurity services across borders, including support for mutual assistance between public authorities and the establishment of a reserve of trusted ***managed security service*** providers at Union level.;

Or. en