European Parliament
2019-2024

Committee on Industry, Research and Energy

2023/0109(COD)

4.9.2023

***I
DRAFT REPORT

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

Committee on Industry, Research and Energy

Rapporteur: Lina Gálvez Muñoz

Symbols for procedures

*	Consultation procedure
***	Consent procedure
***I	Ordinary legislative procedure (first reading)
***II	Ordinary legislative procedure (second reading)
***III	Ordinary legislative procedure (third reading)

(The type of procedure depends on the legal basis proposed by the draft act.)

Amendments to a draft act

Amendments by Parliament set out in two columns

Deletions are indicated in ***bold italics*** in the left-hand column. Replacements are indicated in ***bold italics*** in both columns. New text is indicated in ***bold italics*** in the right-hand column.

The first and second lines of the header of each amendment identify the relevant part of the draft act under consideration. If an amendment pertains to an existing act that the draft act is seeking to amend, the amendment heading includes a third line identifying the existing act and a fourth line identifying the provision in that act that Parliament wishes to amend.

Amendments by Parliament in the form of a consolidated text

New text is highlighted in ***bold italics***. Deletions are indicated using either the ▌ symbol or strikeout. Replacements are indicated by highlighting the new text in ***bold italics*** and by deleting or striking out the text that has been replaced.
By way of exception, purely technical changes made by the drafting departments in preparing the final text are not highlighted.

CONTENTS

Page

DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION

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

(Ordinary legislative procedure: first reading)

The European Parliament,

– having regard to the Commission proposal to Parliament and the Council (COM(2023)0209),

– having regard to Article 294(2) and Articles 173(3) and 322(1), point (a), of the Treaty on the Functioning of the European Union, pursuant to which the Commission submitted the proposal to Parliament (C9-0136/2023),

– having regard to Article 294(3) of the Treaty on the Functioning of the European Union,

– having regard to the opinion of the European Economic and Social Committee of 13 July 2023[1],

– having regard to the opinion of the Committee of the Regions of ...[2],

– having regard to Rule 59 of its Rules of Procedure,

– having regard to the opinions of the Committee on Foreign Affairs and the Committee on Transport and Tourism,

– having regard to the report of the Committee on Industry, Research and Energy (A9-0000/2023),

1. Adopts its position at first reading hereinafter set out;

2. Approves its statement annexed to this resolution;

3. Calls on the Commission to refer the matter to Parliament again if it replaces, substantially amends or intends to substantially amend its proposal;

4. Instructs its President to forward its position to the Council, the Commission and the national parliaments.

[1] OJ C ...
[2] OJ C ...

Amendment 1

Proposal for a regulation
Recital 1

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

Or. en

Amendment 2

Proposal for a regulation
Recital 2

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

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.

critical sectors, generate substantial financial losses, undermine user confidence, cause major damage to the ***economies and democracies*** 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, strong cooperation is needed between the public sector, the private sector, academia and the media. Moreover, the Union's response needs to be coordinated with the international institutions and like-minded international partners, in line with the international cooperation frameworks, and agreements.***

Or. en

Amendment 3

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	(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***, including the small and medium-sized enterprises (SMEs),*** and entities operating critical infrastructures against the growing cybersecurity threats, which can have devastating societal and economic impacts. Therefore, investment in infrastructures and services ***and building capabilities to***

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.	***develop skills and opportunities for the whole population*** 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.
[16] https://futureu.europa.eu/en/	[16] https://futureu.europa.eu/en/
	Or. en

Amendment 4

Proposal for a regulation
Recital 3 a (new)

Text proposed by the Commission	*Amendment*
	(3a) Cyberattacks are frequently targeted at local, regional or national public services and infrastructures. Local authorities are among the most vulnerable targets due to their lack of financial and human resources. It is therefore particularly important that leaders at local level are made aware of the need to increase digital resilience , increase their capacity to reduce the impact of cyberattacks and seize the opportunities provided for by this Regulation [1a].
	[1a] European Committee of the Regions, Digital Resilience, 2023. https://cor.europa.eu/en/engage/studies/Documents/Digital%20resilience.pdf
	Or. en

Amendment 5

Proposal for a regulation
Recital 7

Text proposed by the Commission	*Amendment*
(7) It is necessary to strengthen the detection and situational awareness of cyber threats and incidents throughout the Union and to strengthen solidarity by enhancing Member States' and the Union's preparedness and capabilities to respond to significant and large-scale cybersecurity incidents. Therefore a pan-European infrastructure of SOCs (European Cyber Shield) should be deployed to build and enhance common detection and situational awareness capabilities; a Cybersecurity Emergency Mechanism should be established to support Member States in preparing for, responding to, and immediately recovering from significant and large-scale cybersecurity incidents; a Cybersecurity Incident Review Mechanism should be established to review and assess specific significant or large-scale incidents. These actions shall be without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union ('TFEU').	(7) It is necessary to strengthen the detection and situational awareness of cyber threats and incidents throughout the Union and to strengthen solidarity by enhancing Member States' and the Union's preparedness and capabilities to respond to significant and large-scale cybersecurity incidents. Therefore a pan-European infrastructure of SOCs (European Cyber Shield) should be deployed to build and enhance common detection and situational awareness ***capabilities, reinforcing the Union's threat detection and information sharing*** capabilities; a Cybersecurity Emergency Mechanism should be established to support Member States in preparing for, responding to, and immediately recovering from significant and large-scale cybersecurity incidents; a Cybersecurity Incident Review Mechanism should be established to review and assess specific significant or large-scale incidents. These actions shall be without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union ('TFEU').

Or. en

Amendment 6

Proposal for a regulation
Recital 9 a (new)

Text proposed by the Commission	*Amendment*
	(9a) In order to ensure continuity with regard to activities provided for by this Regulation beyond 2027, it is necessary to ensure a specific budget line in the

multiannual financial framework for 2028 to 2034. Member States should also commit themselves to supporting all necessary measures to reduce cyber threats and incidents throughout the Union and strengthening solidarity.

Or. en

Amendment 7

Proposal for a regulation
Recital 14

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

Or. en

Amendment 8

Proposal for a regulation
Recital 15

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

Or. en

Amendment 9

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	(20) By collecting, sharing and exchanging data, the European Cyber Shield should enhance the Union's technological sovereignty ***and open strategic autonomy***. The pooling of high-quality curated data should also contribute to the development of advanced artificial intelligence and data analytics technologies. It should be facilitated

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).

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 10

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	(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***, while developing industrial capacities in the Union, including for SMEs, with investment in research and innovation (R&I) to develop state-of-the-art technologies, such as those relating to cloud and artificial intelligence***. 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

similar conditions.	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 11

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. ***In order to fulfil the additional tasks deriving from this provision, ENISA should receive adequate, additional funding.***

Or. en

Justification

A certification scheme would serve to build long standing and trusted partnerships with the private sector.

Amendment 12

Proposal for a regulation
Recital 37 a (new)

Text proposed by the Commission	*Amendment*
	(37a) Third countries can access resources and support from the EU Cyber

Solidarity Act, using the incident response support from the EU Cybersecurity Reserve, and as third-country actors from the private sector are needed for the cyber reserve. In order to safeguard the Union's strategic assets, interests, autonomy or security, specific conditions may limit the participation of legal entities established in non-associated third countries. The external dimension of this Regulation should be in line with the provisions established in the Association Agreement under the Digital Europe Programme. The participation of third countries should be subject to public scrutiny, with the participation of the legislative powers, to guarantee that citizens can participate in the process.

Or. en

Amendment 13

Proposal for a regulation
Recital 38 a (new)

Text proposed by the Commission	*Amendment*
	(38a) A central pillar of this Regulation is the development of skills and competences. Therefore, a strengthened link is needed with the EU Cybersecurity Skills Academy to close the cybersecurity talent gap by bringing together private and public initiatives and providing training and certification for citizens that need to be accompanied by investment in access for all citizens in all territories to be trained in these skills. The strengthened link requires safeguards to avoid a 'brain drain' and should not pose a risk to labour mobility.

Or. en

Amendment 14

Proposal for a regulation
Recital 38 b (new)

Text proposed by the Commission	*Amendment*
	(38b) Increased investment and active measures to develop skills in this sector are needed, taking into account that 2023 is the European Year of Skills, as well as increasing citizens' awareness, without prejudice to the need for geographical balance.

Or. en

Amendment 15

Proposal for a regulation
Recital 38 c (new)

Text proposed by the Commission	*Amendment*
	(38c) Reinforcement of specialised, interdisciplinary and general skills and competences across the Union is needed, with a special focus on women, as the gender gap persists in cybersecurity with women comprising 20 % of the average worldwide presence[1a]. Women must be present and part of the design of the digital future and its governance.
	[1a] European Parliament resolution of 10 June 2021 on promoting gender equality in science, technology, engineering and mathematics (STEM) education and careers (2019/2164(INI)) https://www.europarl.europa.eu/doceo/document/TA-9-2021-0296_EN.html#def_1_22

Or. en

Amendment 16

Proposal for a regulation
Recital 38 d (new)

Text proposed by the Commission	*Amendment*
	(38d) In order to develop skills and competences in cybersecurity, a reinforcement of the triangle between national competence centres, the European Cybersecurity Competence Centre (ECCC) and ENISA is needed. Including the participation of industry and creating partnerships with academia and civil society actors, counting with the regional experience, knowledge and specialisation in developing skills.

Or. en

Amendment 17

Proposal for a regulation
Recital 38 e (new)

Text proposed by the Commission	*Amendment*
	(38e) Strengthening R&I in cybersecurity will increase the resilience and the open strategic autonomy of the Union. Likewise, ensuring synergies with R&I programmes and with existing instruments and institutions and to reinforce the triangle of knowledge to bridge the skills gap across the Union by creating opportunities and investing in capacities will also help achieve the necessary resilience.

Or. en

Amendment 18

Proposal for a regulation
Recital 38 f (new)

Text proposed by the Commission	*Amendment*
	(38f) Moreover, this Regulation will increase the resilience of the Union, directly by means of cybersecurity and cyber resilience law and indirectly by means of the impact it can have for the exponential development of law with regard to artificial intelligence, data privacy and data regulation.

Or. en

Amendment 19

Proposal for a regulation
Recital 38 g (new)

Text proposed by the Commission	*Amendment*
	(38g) This Regulation is intended to achieve the commitment of the European Declaration on Digital Rights and Principles for the Digital Decade linked to protect the interests of our democracies, people, businesses and public institutions against cybersecurity risks and cybercrime including data breaches and identity theft or manipulation.

Or. en

Amendment 20

Proposal for a regulation
Recital 38 h (new)

Text proposed by the Commission	*Amendment*
	(38h) Increasing Cybersecurity Culture

which comprehends security, including that of the digital environment, as a public good will be key for the successful implementation of this Regulation. Therefore, developing measures to include and increase citizens' awareness should be another means of guaranteeing the safeguard of our democracies and fundamental values.

Or. en

Amendment 21

Proposal for a regulation
Recital 38 i (new)

Text proposed by the Commission	*Amendment*
	(38i) In order to supplement certain non-essential elements of this Regulation, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission to specify the conditions for interoperability between the Cross-border SOCs, establish the procedural arrangements for the information sharing between the Cross-border SOCs on the one hand and EU-CyCLONe, the CSIRTs network and the Commission on the other, specify the types and number of response services required for the EU Cybersecurity Reserve, and specify further the detailed arrangements for allocating the EU Cyersecurity Reserve support services. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[1]. In particular, to ensure equal participation in the preparation of delegated acts, the

European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

---

[1] OJ L 123, 12.5.2016, p. 1.

Or. en

Amendment 22

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) ***Since*** the objective of this Regulation***, namely to establish a general framework to avoid silos because cyber space has no borders, cannot be sufficiently achieved by the Member States but*** can ***rather*** be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. ***In accordance with the principle of proportionality, as set out in that Article,*** this Regulation does not go beyond what is necessary in order to achieve that objective.

Or. en

Amendment 23

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	(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;	cyber threats and incidents thus allowing to reinforce the competitive position of industry and services sectors in the Union across the digital economy***, grow industrial capacity of the Union and its Member States*** and contribute to the Union's technological sovereignty in the area of cybersecurity;

Or. en

Amendment 24

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

Text proposed by the Commission	*Amendment*
	(ca) to develop, in a coordinated manner, skills and capabilities to ensure cybersecurity, in close cooperation with the Cybersecurity Skills Academy, to provide real opportunities to all and reduce regional disparities, close the talent gap, including closing the gender gap within the cybersecurity sector, and to boost the Union cyber workforce.

Or. en

Amendment 25

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

Text proposed by the Commission	*Amendment*
	This Regulation shall enhance the operational cooperation between Member States, with the support of ENISA pursuant to Article 7 of Regulation (EU) 2019/881.

Or. en

Amendment 26

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 be able*** 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.

Or. en

Amendment 27

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 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 joint procurement of cyber infrastructures, services and tools shall be encouraged. Moreover,*** after consulting the ECCC ***and ENISA,*** the Commission ***is empowered to adopt delegated*** acts ***in accordance with Article 20a to supplement this Regulation***, ***byspecifying*** the conditions for this interoperability.

Or. en

Amendment 28

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. ***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 29

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, in view of their respective crisis management roles in accordance with Directive (EU) 2022/2555 without undue delay. ***This paragraph shall not impose any additional obligations on public or private entities to communicate a potential or ongoing large-scale cybersecurity incident.***

Or. en

Amendment 30

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 ***is empowered to adopt delegated*** acts ***in accordance with Article 20a to supplement this Regulation by determining*** the procedural arrangements for the information sharing provided for in paragraphs 1.

Or. en

Amendment 31

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 coordinated preparedness testing, ***in accordance with the arrangements established for the types of entity in the Sectors of High Criticality listed in Annex I to Directive (EU) 2022/2555***.

Or. en

Justification

In order to harmonise it with the NIS2 Directive.

Amendment 32

Proposal for a regulation
Article 12 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The EU Cybersecurity Reserve shall consist of incident response services from trusted providers selected in accordance with the criteria laid down in Article 16. The Reserve shall include pre-committed services. The services shall be deployable in all Member States.	2. The EU Cybersecurity Reserve shall consist of incident response services from trusted providers selected in accordance with the criteria laid down in Article 16. The Reserve shall include pre-committed services. The services shall be deployable in all Member States ***and shall contribute to boosting innovation in the Digital Single Market across the Union, bridging the innovation divide and generating the capabilities to make that possible***.

Or. en

Amendment 33

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 34

Proposal for a regulation
Article 12 – paragraph 8

Text proposed by the Commission	*Amendment*
8. The Commission ***may, by means of***	8. The Commission ***is empowered to***

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).***	***adopt delegated*** acts ***in accordance with Article 20a to supplement this Regulation by specifying*** the types and the number of response services required for the EU Cybersecurity Reserve.

Or. en

Amendment 35

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 ***is empowered to adopt delegated*** acts ***in accordance with Article 20a to supplement this Regulation by specifying*** further the detailed arrangements for allocating the EU Cybersecurity Reserve support services.

Or. en

Amendment 36

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

Text proposed by the Commission	*Amendment*
	(ea) the potential impact of human error that has produced the cybersecurity incident and has increased the risks of data breaches;

Or. en

Justification

e.g. The potential impact of a ransomware attack to a particular infrastructure from the health sector.

Amendment 37

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.

Or. en

Amendment 38

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 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***, with a particular focus on achieving gender balance***.

Or. en

Amendment 39

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)***, connecting their participation to a national or local company,*** where it can deliver the service***,***

to enhance the trust of their participation;

Or. en

Amendment 40

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 all relevant stakeholders, including representatives of Member States, the Commission, other relevant EU institutions, bodies and agencies, managed security services providers ***in the SOCs*** and users of cybersecurity services***, complemented with guarantees and monitoring that is adequate to ensure that lessons learned and best practices identified are backed by the actors in the industry***. 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 41

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

Text proposed by the Commission	*Amendment*
	3a. The report shall include lessons learned from the peer reviews carried out pursuant to Article 19 of Directive (EU) 2022/2555.

Or. en

Amendment 42

Proposal for a regulation
Article 19 – paragraph 1 – point 2 – point b
Regulation (EU) 2021/694
Article 9 – paragraph 8

Text proposed by the Commission	*Amendment*
8. By derogation ***to*** Article 12(4) of Regulation (EU, Euratom) 2018/1046, unused commitment and payment appropriations for actions pursuing the objectives set out in Article 6(1), point (g) of this Regulation, shall be automatically carried over and may be committed and paid up to 31 December of the following financial year.;	8. By derogation ***from*** Article 12(4) of Regulation (EU, Euratom) 2018/1046, unused commitment and payment appropriations for actions ***in the context of the implementation of the EU Cybersecurity Reserve,*** pursuing the objectives set out in Article 6(1), point (g) of this Regulation, shall be automatically carried over and may be committed and paid up to 31 December of the following financial year.;

Or. en

Amendment 43

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

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. ***In the context of the Programme, additional resources shall be provided to ENISA in order to carry out its tasks, including funding for research and development and coordinating with national cybersecurity agencies and industry stakeholders. That additional***

funding shall not jeopardise the achievement of the objectives of the Programme.

Or. en

Amendment 44

Proposal for a regulation
Article 20 a (new)

Text proposed by the Commission	*Amendment*
	Article 20a
	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 6(3), Article 7(2), Article 12(8) and Article 13(7) shall be conferred on the Commission for a period of … 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 … 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 6(3), Article 7(2), 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 6(3), Article 7(2), 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 45

Proposal for a regulation
Annex I – paragraph 1 – point 1
Regulation (EU) 2021/694
Annex I – Specific Objective 3 – point 4

Text proposed by the Commission	*Amendment*
4. Support closing the cybersecurity skills gap by, for example, aligning cybersecurity skills programmes, adapting them to specific sectorial needs and facilitating access to targeted specialised training.	4. Support closing the cybersecurity skills gap***, with a particular focus on achieving gender balance*** by, for example, aligning cybersecurity skills programmes, adapting them to specific sectorial needs***, including an interdisciplinary and general focus*** and facilitating access to targeted

specialised training ***to enable all persons and territories, without prejudice to the possibility of benefiting from the opportunities provided by this Regulation***.

Or. en

EXPLANATORY STATEMENT

CONTEXT

Cybersecurity is and should be at the core of our democracies. Threats to cybersecurity are linked to the spread of insecurity among the population and companies, as well as to the rise of disinformation, which challenges democratic principles that preserve respect for human rights. To prevent this, a secure digital environment subject to public scrutiny is crucial for our democracies.

Cyberattacks in the EU are increasing in terms of methods and impact. In addition, the Russian attack to Ukraine has created deep changes, even before the invasion, and has opened a new era for **cyberware** according to the ENISA's Threat Landscape 2022 report.[3] The priorities identified from this conflict in cyber are the need to **build capabilities** in **multilateral programs** and projects and the need to **develop skills** fast. In order to be more resilient, a common European response is urgently needed, based on stronger cooperation at the European level beyond the national one.

Increasing Cybersecurity Culture which comprehends security, including that of the digital environment, as a public good will be key for the successful implementation of this regulation.

Moreover, cyberattacks are frequently targeted at **local, regional or national public services** and infrastructures (e.g. the healthcare sector that remains a prime target for cyber-attacks[4]). Evidence also points out that **local authorities** are amongst the most vulnerable target due to the lack of financial and human resources, and it is particularly important the awareness among leaders at local level to increase digital resilience[5]. Attacks primarily and directly affect citizens and thus endanger our democracies, including through disinformation campaigns. The feeling of insecurity that these situations can create in the population can lead to political preferences that follow a radical commitment to security to the detriment of respect for fundamental rights. However, the opposite is true: security is an essential part of our democracies, compatible with and necessary for all other rights.

In addition, **companies and SMEs** in the EU are also experiencing cybercrime, and with the increasing use of the digital sphere to conduct businesses, there is a bigger concern in cybersecurity. SMEs are those less prepared, with fewer resources to protect themselves and even less aware that they can be subject of such attacks.

The expectation is that these attacks will continue and increase in the future. Especially in situations of political instability and more particularly in contexts of war. With the digital

[3] ENISA Threat Landscape 2022, October 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport

[4] ENISA Threat Landscape: Health Sector, July 2023. https://www.enisa.europa.eu/publications/health-threat-landscape/@@download/fullReport

[5] European Committee of the Regions, Digital Resilience, 2023. https://cor.europa.eu/en/engage/studies/Documents/Digital%20resilience.pdf

transition going further every day, digital resilience becomes more and more important for our daily lives and for the **open strategic autonomy of the EU.**

PROPOSAL OF THE RAPPORTEUR

The Rapporteur believes that the EU needs to be better prepared for the future and welcomes this urgent piece of legislation to pool recourses, information, and knowledge to ensure solidarity between Member States, to grow industrial capacity in the EU, to develop **co-ordinately skills and capabilities** that ensure cybersecurity, to be more resilient to future attacks and to protect our democracies against self-serving use of security needs. Moreover, it is important to protect the integrity of our electoral processes. This piece of legislation is an essential commitment to achieve the objective of **open strategic autonomy.**

For these reasons, the EU needs strong and **coordinated governance** in the EU and structured cooperation with the private sector to foster the development of the European cyber industry. In addition to collaboration with like-minded international partners, but also with other countries that do not have the same capabilities and may need to be assisted when they are victims of cyber-attacks. The EU Cyber Solidarity Act must define well its governance and not overlap already existing initiatives and legislation, such as the NIS2 Directive.

The proposal is based significantly on the exchange of information in a voluntary manner among Member States. For that reason, the Rapporteur proposes to enhance the guarantees to build trust among Member States to increase their participation and cooperation, for example regarding joint acquisitions of infrastructure as well as the involvement of the legislative powers, to ensure citizens trust and **democratic guarantees**.

Secondly, the Rapporteur proposes to **ensure the budget** from the upcoming MFFs for this initiative, also with commitment from the Member States, to guarantee continuity to the activities developed under the EU Cyber Solidarity Act beyond 2027.

Thirdly, the Rapporteur proposes to improve the **governance structure**, have a clear governance definition, and link it with existing legislation.

The Rapporteur also proposes a better **coordination** among Member States' different entities in charge of cyber security to offer a common cyber shield. Moreover, to increase ENISA's contribution on the coordination and interaction between the different actors of the national communities.

Regarding the **new cybersecurity reserve,** the Rapporteur believes it has the potential of developing industrial capacities in the EU, including for SMEs, with investments in research and innovation to develop state of the art technologies, such as cloud and artificial intelligence technologies. In addition, the Rapporteur proposes to maintain the participation of the industry, enhance the criteria and trust of their participation (i.e. connecting their participation to a national or local company) by clarifying the **criteria** and the definition of **technological sovereignty** and to guarantee a balance between non-EU and EU actors. In addition, the Rapporteur proposes for the **Cyber Emergency Mechanism** a **certification scheme** to be used for private providers to build a longstanding and trusted partnership.

Regarding the **incident review mechanism**, the Rapporteur proposes to reinforce the role of ENISA and the private sector in the SOCs, with the right guarantees and monitoring, to validate if the lessons learned identified are also backed by the actors in the industry. Moreover, the Rapporteur proposes to include as lessons learned via the peer reviews as stated in the NIS2 Directive and to increase ENISA funding aiming at ensuring an effective application of legislation and adequate protection to face cybersecurity threats.

In addition, this proposal by definition has a very relevant **external dimension**, be it as third countries can access resources and support from the EU Cyber Solidarity Act, using the incident response support from the EU Cybersecurity Reserve, and as non-EU actors from private sector are still needed for the cyber reserve. The external dimension also has to be subject to public scrutiny, with the participation of the legislative powers to guarantee that citizens can participate in the process. Cybersecurity should be considered a public good.

Furthermore, a central pillar of this proposal is the development of skills and competences that should go beyond simply investing in knowledge development, but investing in access for all citizens to be able to train in these skills. The Rapporteur proposes to reinforce the link with the **EU Cybersecurity Skills Academy**, which intends to close the cybersecurity talent gap by bringing together private and public initiatives and providing training and certification for citizens. The strengthening will need safeguards to avoid brain drain and would not be detrimental to labour mobility.

Furthermore, the Rapporteur proposes to invest and include active measures to develop skills in this sector, considering that 2023 is the European Year of Skills, as well as increase citizens' awareness. The measures will be designed so that investments do not create imbalances between Member States, as the current high demand and high wages in this sector can lead to a certain type of brain drain towards the best-paid options.

For these reasons, the Rapporteur proposes a reinforcement of specialised, interdisciplinary, and general skills and competences across the EU, with a special focus on women, as the gender gap persist in cybersecurity with women comprising 20% of the average worldwide presence.[6] Women must be present and part of the design of the digital future and its governance.

In addition, the Rapporteur proses to reinforce the triangle between national competence centres, the European Cybersecurity Competence Centre (ECCC) and ENISA in developing skills and competences. Moreover, increasing the role of **industry** in **developing skills** and creating partnerships with **academia** and civil society actors, counting with the regional experience, knowledge, and specialisation and third country alliances, with like-minded partners in order to increase the exchanges and ensure a global approach to support citizens, businesses and institutions.

The rapporteur also proposes to share cooperation in talent and measure of human harm of the cyberattacks (e.g., the impact of a ransomware attack to the health sector).

[6] European Parliament resolution of 10 June 2021 on promoting gender equality in science, technology, engineering and mathematics (STEM) education and careers (2019/2164(INI)) https://www.europarl.europa.eu/doceo/document/TA-9-2021-0296_EN.html#def_1_22

The Rapporteur proposes measures to include and increase citizen awareness without alarmism, as another measure to guarantee the safeguard of our democracies and fundamental values. Increasing **Cybersecurity Culture** which comprehends security, including that of the digital environment, as a public good. This way we will be able to guarantee a model of digital democracy, as opposed to one of digital authoritarianism, with transparency, democracy, and the certainty that the development of an ex-ante legislation can bring.

Furthermore, the Rapporteur believes that to strengthening **R&I** in cybersecurity will increase the resilience and the open strategic autonomy of the EU. Likewise, ensuring synergies with research and innovation programs and with existing instruments and institutions and to reinforce the triangle of knowledge to bridge the skills gap across the EU.

Moreover, this legislation will increase the resilience of the EU and its Member States, not only directly via the cybersecurity and cyber resilience laws, but also with the impact it can have for the exponential development of artificial intelligence and the impact the regulation of data and data privacy can have on cybersecurity.

In addition, this legislation will help achieve the commitment of the **European Declaration on Digital Rights and Principles for the Digital Decade** linked to protect the interests of people, businesses and public institutions against cybersecurity risks and cybercrime including data breaches and identity theft or manipulation.

In this light, the Rapporteur believes this proposal should be operational as fast as possible, including the European Cybersecurity shield and the Cyber Emergency Mechanism, to have a general framework and avoid silos, as cyber space has no borders.