



---

*Plenary sitting*

---

**A9-0426/2023**

8.12.2023

**\*\*\*I**  
**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

	<b>Page</b>
DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION .....	5
EXPLANATORY STATEMENT .....	44
ANNEX: ENTITIES OR PERSONS FROM WHOM THE RAPPORTEUR HAS RECEIVED INPUT.....	48
OPINION OF THE COMMITTEE ON FOREIGN AFFAIRS .....	49
OPINION OF THE COMMITTEE ON TRANSPORT AND TOURISM.....	90
PROCEDURE – COMMITTEE RESPONSIBLE .....	113
FINAL VOTE BY ROLL CALL IN COMMITTEE RESPONSIBLE .....	114



## 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<sup>1</sup>,
  - 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 (A9-0426/2023),
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.

---

<sup>1</sup> OJ C 349, 29.9.2023, p. 167.

## Amendment 1

### AMENDMENTS BY THE EUROPEAN PARLIAMENT\*

to the Commission proposal

-----  
2023/0109 (COD)

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 *and amending Regulation (EU) 2021/694***

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 173(3) and Article 322(1), point (a) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the Court of Auditors<sup>2</sup>

Having regard to the opinion of the European Economic and Social Committee<sup>3</sup>,

Having regard to the opinion of the Committee of the Regions<sup>4</sup>,

Acting in accordance with the ordinary legislative procedure,

Whereas:

- (1) The use of and dependence on information and communication technologies have become fundamental aspects, ***but have, simultaneously introduced possible vulnerabilities***, in all sectors of economic activity ***and democracy*** as our public administrations, companies and citizens are more interconnected and interdependent across sectors and borders than ever before.
- (2) The magnitude, frequency and impact of cybersecurity incidents are increasing ***at a Union-wide and global level in terms of their 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-

---

\* Amendments: new or amended text is highlighted in bold italics; deletions are indicated by the symbol **■**.

<sup>2</sup> OJ C [...], [...], p. [...].

<sup>3</sup> OJ C , , p. .

<sup>4</sup> OJ C , , p. .

evolving threat landscape, the threat of possible large-scale incidents causing significant disruption or damage *economies and democracies* 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, **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. ***Close and coordinated cooperation is therefore needed between the public sector, the private sector, academia, civil society and the media. Moreover, the Union's response needs to be coordinated with international institutions as well as trusted and like-minded international partners. Trusted and like-minded international partners are countries that share the Union's values of democracy, commitment to human rights, effective multilateralism, and rules-based order, in line with the international cooperation frameworks and agreements. To ensure cooperation with trusted and like-minded international partners and protection against systemic rivals, entities established in third countries that are not parties to the GPA should not be allowed to participate in procurement under this Regulation.***

- (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<sup>5</sup>, it is necessary to increase the resilience of citizens, businesses, ***in particular microenterprises, small and medium-sized enterprises (SMEs) including startups*** and entities operating critical infrastructures, ***including local and regional authorities*** against the growing cybersecurity threats, which can have devastating societal and economic impacts. Therefore, investment in infrastructures and services ***and building capabilities to develop cybersecurity 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. The Union should also increase its capacities in these areas, notably as regards the collection and analysis of data on cybersecurity threats and incidents.
- (3a) ***Cyberattacks are frequently targeted at local, regional or national public services and infrastructures. Local authorities are among the most vulnerable targets of cyberattacks due to their lack of financial and human resources. It is therefore particularly important that decision-makers 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.***
- (4) The Union has already taken a number of measures to reduce vulnerabilities and increase the resilience of critical infrastructures and entities against cybersecurity risks,

---

<sup>5</sup> <https://futureu.europa.eu/en/>

in particular Directive (EU) 2022/2555 of the European Parliament and of the Council<sup>6</sup>, Commission Recommendation (EU) 2017/1584<sup>7</sup>, Directive 2013/40/EU of the European Parliament and of the Council<sup>8</sup> and Regulation (EU) 2019/881 of the European Parliament and of the Council<sup>9</sup>. In addition, the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure invites Member States to take urgent and effective measures, and to cooperate loyally, efficiently, in solidarity and in a coordinated manner with each other, the Commission and other relevant public authorities as well as the entities concerned, to enhance the resilience of critical infrastructure used to provide essential services in the internal market.

- (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<sup>10</sup>.
- (6) The Joint Communication on the EU Policy on Cyber Defence<sup>11</sup> adopted on 10 November 2022 announced an EU Cyber Solidarity Initiative with the following objectives: strengthening of common EU detection, situational awareness and response capabilities by promoting the deployment of an EU **network** of Security Operations Centres ('SOCs'), supporting gradual building of an EU-level cybersecurity reserve with services from trusted private providers and testing of critical entities for potential vulnerabilities based on EU risk assessments.
- (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 **prevent and** respond to significant and large-scale cybersecurity incidents. Therefore a pan-European **network 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;

---

<sup>6</sup> Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022).

<sup>7</sup> Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

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

<sup>9</sup> Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

<sup>10</sup> 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)

<sup>11</sup> Join Communication to the European Parliament and the Council EU Policy on Cyber Defence JOIN/2022/49 final



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').

- (8) To achieve these objectives, it is also necessary to amend Regulation (EU) 2021/694 of the European Parliament and of the Council<sup>12</sup> in certain areas. In particular, this Regulation should amend Regulation (EU) 2021/694 as regards adding new operational objectives related to the European Cyber Shield and the **Cybersecurity** Emergency Mechanism under Specific Objective 3 of DEP, which aims at guaranteeing the resilience, integrity and trustworthiness of the Digital Single Market, at strengthening capacities to monitor cyber-attacks and threats and to respond to them, and at reinforcing cross-border cooperation on cybersecurity. This will be complemented by the specific conditions under which financial support may be granted for those actions should be established and the governance and coordination mechanisms necessary in order to achieve the intended objectives should be defined. Other amendments to Regulation (EU) 2021/694 should include descriptions of proposed actions under the new operational objectives, as well as measurable indicators to monitor the implementation of these new operational objectives.
- (9) The financing of actions under this Regulation should be provided for in Regulation (EU) 2021/694, which should remain the relevant basic act for these actions enshrined within the Specific Objective 3 of DEP. Specific conditions for participation concerning each action will be provided for in the relevant work programmes, in line with the applicable provision of Regulation (EU) 2021/694.
- (9a) *In light of geopolitical developments and the growing cyber threat landscape (EPP 52) and in order to ensure continuity and further development of the measures laid down in this Regulation beyond 2027, particularly the European Cyber Shield and the Cybersecurity Emergency Mechanism, it is necessary to ensure a specific budget line in the multiannual financial framework for the period 2028-2034. Member States should endeavour to commit themselves to supporting all necessary measures to reduce cyber threats and incidents throughout the Union and to strengthen solidarity.***
- (10) Horizontal financial rules adopted by the European Parliament and by the Council on the basis of Article 322 TFEU apply to this Regulation. Those rules are laid down in Regulation **(EU, Euratom) 2018/1046 of the European Parliament and of the Council<sup>13</sup>** and determine in particular the procedure for establishing and implementing the Union budget, and provide for checks on the responsibility of financial actors. Rules adopted on the basis of Article 322 TFEU also include a general regime of conditionality

---

<sup>12</sup> Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (OJ L 166, 11.5.2021, p. 1).

<sup>13</sup> **Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 (OJ L 193, 30.7.2018, p. 1, ELI: <http://data.europa.eu/eli/reg/2018/1046/oj>).**

for the protection of the Union budget as established in Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council<sup>14</sup>.

- (11) For the purpose of sound financial management, specific rules should be laid down for the carry-over of unused commitment and payment appropriations. While respecting the principle that the Union budget is set annually, this Regulation should, on account of the unpredictable, exceptional and specific nature of the cybersecurity landscape, provide for possibilities to carry over unused funds beyond those set out in **Regulation (EU, Euratom) 2018/1046**, thus maximising the Cybersecurity Emergency Mechanism's capacity to support Member States in countering effectively cyber threats.
- (11a) *The Cybersecurity Emergency Mechanism and the EU Cybersecurity Reserve established in this Regulation are new initiatives and were not envisaged in the establishment of the multiannual financial framework for 2021-2027, and funding for those initiatives is intended to limit the reduction of funding for other priorities in the Digital Europe Programme to the minimum extent possible. The amount of the financial resources dedicated to the EU Cyber Security Reserve should therefore be decreased and it should be primarily drawn from the unallocated margins under the multiannual financial framework ceilings or mobilised through the non-thematic multiannual financial framework special instruments. Any earmarking or reallocation of funds from existing programmes should be kept to an absolute minimum, in order to shield existing programmes, in particular Erasmus+, from negative impact and ensure that those programmes can achieve their set objectives.***
- (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. ***A proactive approach to identifying, mitigating, and preventing potential cyber threats includes an increased capacity of advanced detection capabilities necessary to stop advanced persistent threats. Threat intelligence is information collected, analysed, and interpreted to understand potential threats and risks. By analysing and correlating vast amounts of data, it uncovers patterns, trends, and indicators of compromise that can reveal malicious activities or vulnerabilities.*** A ***network*** 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. ***A National SOC refers to a centralised capacity responsible for continuously gathering threat intelligence information and improving the cybersecurity posture of entities under national jurisdiction by preventing, detecting, and analysing cybersecurity threats.*** 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

---

<sup>14</sup> *Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council of 16 December 2020 on a general regime of conditionality for the protection of the Union budget (OJ L 433I, 22.12.2020, p. 1, ELI: <http://data.europa.eu/eli/reg/2020/2092/oj>).*

Network ('EU-CyCLONe'), as defined in Directive (EU) 2022/2555 of the European Parliament and of the Council<sup>15</sup>.

- (13) ***In order to participate in the Cyber Shield, each Member State should designate a public body at national level tasked with coordinating cyber threat detection activities in that Member State. Member States are encouraged to incorporate the National SOC capacity into their existing cyber structure and governance in order to avoid creating additional governance layers and to align this Regulation with existing legislative act, including Directive (EU) 2022/2555.*** These National SOC's should act as a reference point and gateway at national level for participation ***of private and public entities, particularly their National SOC's,*** 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 SOC's should strengthen the cooperation and information sharing between public and private entities to break up currently existing communication silos. 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 to strengthening the Union's resilience in the cybersecurity sphere.***
- (14) As part of the European Cyber Shield, a number of Cross-border Cybersecurity Operations Centres ('Cross-border SOC's') should be established. These should bring together National SOC's 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 SOC's should be to strengthen capacities to analyse, prevent and detect cybersecurity threats and to support the production of high-quality intelligence ***including collecting and sharing data and information on possible malicious hacking, newly developed malicious threats and exploits that have not yet deployed in a cyber-incidents, and analysis efforts,*** 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 ***and secure*** environment ***with the support of ENISA, in matters related to operational cooperation among Member States. Cross-border SOC's should facilitate and encourage the sharing of information in a trusted and secure environment and*** should provide new additional capacity, building upon and complementing existing SOC's and computer incident response teams ('CSIRT's') and other relevant actors.
- (15) At national level, the monitoring, detection and analysis of cyber threats is typically ensured by SOC's of public and private entities, in combination with CSIRT's. In addition, CSIRT's exchange information in the context of the CSIRT network, in accordance with Directive (EU) 2022/2555. The Cross-border SOC's should constitute a new ***capacity that is incorporated into the existing cybersecurity infrastructure, particularly CSIRT's network,*** by pooling and sharing data on cybersecurity threats from public and private entities, ***in particular their SOC's,*** enhancing the value of such data through expert analysis and jointly acquired infrastructures and state of the art tools, and

---

<sup>15</sup> 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](#)).

contributing to *the Union’s technological sovereignty, its open strategic autonomy, competitiveness and resilience and to the development of a significant cybersecurity ecosystem, including in cooperation with trusted and like-minded international partners.* .

- (16) The Cross-border SOC 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) *with a view to facilitating the break-up of currently existing communication siloes. In doing so, Cross-border SOC 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, indicators of compromise, and contextualised information about incidents, threats and vulnerabilities *including collecting and sharing data and information on possible malicious hacking, newly developed malicious threats and exploits that have not yet deployed in a cyber-incidents, and analysis efforts.* In addition, Cross-border SOC should also enter into cooperation agreements with other Cross-border SOC.
- (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<sup>16</sup>, as well as for providing analytical reports for the Integrated Political Crisis Response Mechanism (‘IPCR’) arrangements under **Council** Implementing Decision (EU) 2018/1993<sup>17</sup>. Therefore, in situations where Cross-border SOC 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 *accordance with 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.
- (18) Entities participating in the European Cyber Shield should ensure a high-level of interoperability among themselves including, as appropriate, as regards data formats,

---

<sup>16</sup> *Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism Text with EEA relevance* (OJ L 347, 20.12.2013, p. 924, *ELI*: <http://data.europa.eu/eli/dec/2013/1313/oj>).

<sup>17</sup> *Council Implementing Decision (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements* (OJ L 320, 17.12.2018, p. 28, *ELI*: [http://data.europa.eu/eli/dec\\_impl/2018/1993/oj](http://data.europa.eu/eli/dec_impl/2018/1993/oj)).



taxonomy, data handling and data analysis tools, and secure communications channels, a minimum level of application layer security, situational awareness dashboard, and indicators. The adoption of a common taxonomy and the development of a template for situational reports to describe the technical cause and impacts of cybersecurity incidents should take into account the ongoing work on incident notification in the context of the implementation of Directive (EU) 2022/2555.

- (19) In order to enable the exchange of data on cybersecurity threats from various sources, on a large-scale basis, in a trusted **and secure** environment, entities participating in the European Cyber Shield should be equipped with state-of-the-art and highly-secure tools, equipment and infrastructures **and 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.
- (20) By collecting, sharing and exchanging data, the European Cyber Shield should enhance the Union's technological sovereignty, **its open strategic autonomy, competitiveness and resilience and an EU significant cybersecurity ecosystem**. The pooling of high-quality curated data should also contribute to the development of advanced artificial intelligence and data analytics technologies. **Artificial intelligence is the most effective when paired with human analysis. Therefore, a skilled labour force remains essential for pooling high-quality data.** 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<sup>18</sup>.
- (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 security conditions, **respecting the civilian character of institutions 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..**
- (22) Information sharing among participants of the European Cyber Shield should comply with existing legal requirements and in particular Union and national data protection law, as well as the Union rules on competition governing the exchange of information. The recipient of the information should implement, insofar as the processing of personal data is necessary, technical and organisational measures that safeguard the rights and freedoms of data subjects, and destroy the data as soon as they are no longer necessary for the stated purpose and inform the body making the data available that the data have been destroyed.

---

<sup>18</sup> 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, **ELI: <http://data.europa.eu/eli/reg/2021/1173/oj>**).

- (23) Without prejudice to Article 346 of TFEU, the exchange of information that is confidential pursuant to Union or national *law* should be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of such information should preserve the confidentiality of the information and protect the security and commercial interests of the entities concerned, in full respect of trade and business secrets.
- (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, preparing for and responding to cybersecurity incidents and crises lies with the Member States, the *Cybersecurity* Emergency Mechanism promotes solidarity between Member States in accordance with Article 3(3) of the Treaty on European Union ('TEU').
- (25) The *Cybersecurity* Emergency Mechanism should provide support to Member States complementing their own measures and resources, and other existing support options in case of response to and immediate recovery from significant and large-scale cybersecurity incidents, such as the services provided by the European Union Agency for Cybersecurity ('ENISA') in accordance with its mandate, the coordinated response and the assistance from the CSIRTs network, the mitigation support from the EU-CyCLONE, as well as mutual assistance between Member States including in the context of Article 42(7) of TEU, the PESCO Cyber Rapid Response Teams<sup>19</sup> and Hybrid Rapid Response Teams. It should address the need to ensure that specialised means are available to support preparedness and response to cybersecurity incidents across the Union and in third countries.
- (26) This instrument is without prejudice to procedures and frameworks to coordinate crisis response at Union level, in particular the UCPM<sup>20</sup>, IPCR<sup>21</sup>, and Directive (EU) 2022/2555. It may contribute to or complement actions implemented in the context of Article 42(7) of TEU or in situations defined in Article 222 of TFEU. The use of this instrument should also be coordinated with the implementation of Cyber Diplomacy Toolbox's measures, where appropriate.
- (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 *Cybersecurity* Emergency Mechanism, the Member State should provide relevant information justifying the need for support.

---

<sup>19</sup> COUNCIL DECISION (CFSP) 2017/ 2315 - of 11 December 2017 - establishing permanent structured cooperation (PESCO) and determining the list of participating Member States.

<sup>20</sup> Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924).

<sup>21</sup> Integrated Political Crisis Response arrangements (IPCR) and in accordance with Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises.

- (28) Directive (EU) 2022/2555 requires Member States to designate or establish one or more cyber crisis management authorities and ensure they have adequate resources to carry out their tasks in an effective and efficient manner. It also requires Member States to identify capabilities, assets and procedures that can be deployed in the case of a crisis as well as to adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. Member States are also required to establish one or more CSIRTs tasked with incident handling responsibilities in accordance with a well-defined process and covering at least the sectors, subsectors and types of entities under the scope of that Directive, and to ensure they have adequate resources to carry out effectively their tasks. This Regulation is without prejudice to the Commission's role in ensuring the compliance by Member States with the obligations of Directive (EU) 2022/2555. The **Cybersecurity** Emergency Mechanism should provide assistance for actions aimed at reinforcing preparedness as well as incident response actions to mitigate the impact of significant and large-scale cybersecurity incidents, to support immediate recovery and/or restore the functioning of essential services.
- (29) As part of the preparedness actions, to promote a consistent approach and strengthen security across the Union and its internal market, support should be provided for testing and assessing cybersecurity of entities operating in highly critical sectors identified pursuant to Directive (EU) 2022/2555 in a coordinated manner. For this purpose, the Commission, with the support of ENISA and in cooperation with the NIS Cooperation Group established by Directive (EU) 2022/2555, should regularly identify relevant sectors or subsectors, which should be eligible to receive financial support for coordinated testing at Union level. The sectors or subsectors should be selected from Annex I to Directive (EU) 2022/2555 ('Sectors of High Criticality'). The coordinated testing exercises should be based on common risk scenarios and methodologies. The selection of sectors and development of risk scenarios should take into account relevant Union-wide risk assessments and risk scenarios, including the need to avoid duplication, such as the risk evaluation and risk scenarios called for in the Council conclusions on the development of the European Union's cyber posture to be conducted by the Commission, the High Representative and the NIS Cooperation Group, in coordination with relevant civilian and military bodies and agencies and established networks, including the EU-CyCLONe, as well as the risk assessment of communications networks and infrastructures requested by the Joint Ministerial Call of Nevers and conducted by the NIS Cooperation Group, with the support of the Commission and ENISA, and in cooperation with the Body of European Regulators for Electronic Communications (BEREC), the coordinated risk assessments to be conducted under Article 22 of Directive (EU) 2022/2555 and digital operational resilience testing as provided for in Regulation (EU) 2022/2554 of the European Parliament and of the Council<sup>22</sup>. The selection of sectors should also take into account the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.

---

<sup>22</sup> Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

- (30) In addition, the **Cybersecurity** Emergency Mechanism should offer support for other preparedness actions and support preparedness in other sectors, not covered by the coordinated testing of entities operating in highly critical sectors. Those actions could include various types of national preparedness activities.
- (31) The **Cybersecurity** Emergency Mechanism should also provide support for incident response actions to mitigate the impact of significant and large-scale cybersecurity incidents, to support immediate recovery or restore the functioning of essential services. Where appropriate, it should complement the UCPM to ensure a comprehensive approach to respond to the impacts of cyber incidents on citizens.
- (32) The **Cybersecurity** Emergency Mechanism should support assistance provided by Member States to a Member State affected by a significant or large-scale cybersecurity incident, including by the CSIRTs network set out in Article 15 of Directive (EU) 2022/2555. Member States providing assistance should be allowed to submit requests to cover costs related to dispatching of expert teams in the framework of mutual assistance. The eligible costs could include travel, accommodation and daily allowance expenses of cybersecurity experts.
- (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 reinforcing the Union's resilience, including the participation of European managed security services providers that are SMEs and ensuring the creation of a cybersecurity ecosystem, in particular microenterprises, SMEs including startups, with investment in research and innovation (R&I) to develop state-of-the-art technologies, such as those relating to cloud and artificial intelligence. 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. **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, **offices** and agencies, under similar conditions. **The Commission should ensure the involvement of and extensive exchanges with the Member States aiming to avoid duplication with similar initiatives, including within the North Atlantic Treaty Organization (NATO).**
- (34) For the purpose of selecting private service providers to provide services in the context of the EU Cybersecurity Reserve, it is necessary to establish a set of minimum criteria that should be included in the call for tenders to select these providers, so as to ensure that the needs of Member States' authorities and entities operating in critical or highly critical sectors are met. **The participation of smaller providers, active at regional and local level should be encouraged.**



- (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 *Cybersecurity* Emergency Mechanism. ***In order to fulfil the additional tasks deriving from this provision, ENISA should receive adequate, additional funding.***
- (36) In order to support the objectives of this Regulation of promoting shared situational awareness, enhancing Union's resilience and enabling effective response to significant and large-scale cybersecurity incidents, the EU=CyCLONe, the CSIRTs network or the Commission should be able to ask ENISA to review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. After the completion of a review and assessment of an incident, ENISA should prepare an incident review report, in collaboration with relevant stakeholders, including representatives from the private sector, Member States, the Commission and other relevant EU institutions, bodies, *offices* and agencies. As regards the private sector, ENISA is developing channels for exchanging information with specialised providers, including providers of managed security solutions and vendors, in order to contribute to ENISA's mission of achieving a high common level of cybersecurity across the Union. Building on the collaboration with stakeholders, including the private sector, the review report on specific incidents should aim at assessing the causes, impacts and mitigations of an incident, after it has occurred. Particular attention should be paid to the input and lessons shared by the managed security service providers that fulfil the conditions of highest professional integrity, impartiality and requisite technical expertise as required by this Regulation. The report should be delivered and feed into the work of the EU=CyCLONe, the CSIRTs network and the Commission. When the incident relates to a third country, it will also be shared by the Commission with the High Representative.
- (37) Taking into account the unpredictable nature of cybersecurity attacks and the fact that they are often not contained in a specific geographical area and pose high risk of spill-over, the strengthening of resilience of neighbouring countries and their capacity to respond effectively to significant and large-scale cybersecurity incidents contributes to the protection of the Union as a whole. Therefore, third countries associated to the DEP may be supported from the EU Cybersecurity Reserve, where this is provided for in the respective association agreement to DEP. The funding for associated third countries should be supported by the Union in the framework of relevant partnerships and funding instruments for those countries. The support should cover services in the area of response to and immediate recovery from significant or large-scale cybersecurity incidents. The conditions set for the EU Cybersecurity Reserve and trusted providers in this Regulation should apply when providing support to the third countries associated to DEP.
- (37a) ***Third countries could access resources and support pursuant to this Regulation, using the incident response support from the EU Cybersecurity Reserve. Furthermore, incident response service providers from third countries, including third countries associated to the Digital Europe Programme or other international partner countries, and NATO members, may be needed for the provision of specific services in the EU Cybersecurity Reserve. By way of derogation from Regulation (EU, Euratom) 2018/1046, in order to strengthen the Union's technological sovereignty, its open strategic autonomy, competitiveness and resilience, and to safeguard the Union's strategic assets, interests, or security, entities established in third countries that are***

*not party to the GPA and that have not been subject to screening within the meaning of Regulation (EU) 2019/452 of the European Parliament and of the Council<sup>23</sup> and, where necessary, to mitigation measures, taking into account the objectives set out in this Regulation, should not be allowed to participate. 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 ensure that citizens can participate in the process.*

- (38) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to specify the conditions for the interoperability between Cross-border SOCs; determine the procedural arrangements for the information sharing related to a potential or ongoing large-scale cybersecurity incident between Cross-border SOCs and Union entities; laying down technical requirements to ensure security of the European Cyber Shield; specify the types and the number of response services required for the EU Cybersecurity Reserve; and, specify further the detailed arrangements for allocating the EU Cybersecurity Reserve support services. Those powers should be exercised in accordance with Regulation (EU) 182/2011 of the European Parliament and of the Council\*.

---

\* *Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13, ELI: <http://data.europa.eu/eli/reg/2011/182/oj>).*

- (38a) *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 Cybersecurity Emergency Mechanism. It is therefore concerning that the Union is faced with a talent gap, characterised 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, in all territories, 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. All measures aiming to increase cybersecurity skills requires safeguards to avoid a 'brain drain' and a risk to labour mobility.*

---

<sup>23</sup> Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union (OJ L 79I , 21.3.2019, p. 1), ELI: <http://data.europa.eu/eli/reg/2019/452/oj>.

- (38b) *The 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. Women must be present and part of the design of the digital future and its governance.*
- (38c) *Strengthening research and innovation (R&I) in cybersecurity is intended to increase the resilience and the open strategic autonomy of the Union. Similarly, it is important to create synergies with R&I programmes and with existing instruments and institutions and to strengthen cooperation and coordination among the different stakeholders, including the private sector, civil society, academia, Member States, the Commission and ENISA;*
- (38d) *This Regulation should contribute to 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. The application of this Regulation should also contribute to improving the implementation of other legislation, for example on artificial intelligence, data privacy and data regulation in terms of cybersecurity and cyber resilience.*
- (38e) *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.*
- (38f) *In order to supplement certain non-essential elements of this Regulation, the power to adopt acts in accordance with Article 290 TFEU 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 Cybersecurity 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\*. 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.*

---

\*OJ L 123, 12.5.2016, p. 1, ELI: [http://data.europa.eu/eli/agree\\_interinstit/2016/512/oj](http://data.europa.eu/eli/agree_interinstit/2016/512/oj).

- (39) *Since the objectives of this Regulation, namely to reinforce the Union's cyber threat prevention, detection, response and recover capacities and to establish a general framework breaking up communication silo cannot be sufficiently achieved by the*

*Member States but can rather* be better achieved at Union level. 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. ***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,

HAVE ADOPTED THIS REGULATION:

## *Chapter I*

### **GENERAL OBJECTIVES, SUBJECT MATTER, AND DEFINITIONS**

#### *Article 1*

#### **Subject-matter and objectives**

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:

- (a) the deployment of a pan-European **network** of Security Operations Centres ('European Cyber Shield') to build and enhance common detection and situational awareness capabilities;
- (b) the creation of a Cybersecurity Emergency Mechanism to support Member States in preparing for, responding to, and immediate recovery from significant and large-scale cybersecurity incidents;
- (c) the establishment of a European Cybersecurity Incident Review Mechanism to review and assess significant or large-scale incidents.

2. This Regulation pursues the objective to strengthen solidarity at Union level through following specific objectives:

- (a) to strengthen common Union detection and situational awareness of cyber threats and incidents thus allowing ***support for the industrial capacity of the Union and the Member States in the cybersecurity sector, and to*** reinforce the competitive position of industry, ***in particular microenterprises, SMEs including startups,*** and services sectors in the Union across the digital economy and ***to*** contribute to the Union's technological sovereignty ***its open strategic autonomy, competitiveness and and resilience in that sector, strengthening the cybersecurity ecosystem with a view to ensuring strong Union capabilities, including in cooperation with international partners;***
- (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');

(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.

*(ca) to develop, in a coordinated manner, skills, knowhow abilities and competencies of the workforce, with a view to ensuring cybersecurity and creating synergies with the Cybersecurity Skills Academy.*

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.

## Article 2

### Definitions

For the purposes of this Regulation, the following definitions apply:

*(-1a) 'National Security Operations Centre' or 'National SOC' means a centralised national capacity continuously gathering and analysing cyber threat intelligence information and improving the cybersecurity posture in accordance with Article 4;*

(1) **'Cross-border Security Operations Centre' or 'Cross-border SOC'** means a multi-country platform, that brings together in a coordinated network structure national SOC's *in accordance with Article 5;*

(2) **'public body'** means *bodies* governed by public law as defined in Article 2(1), point (4), of Directive 2014/24/EU of the European Parliament and the Council<sup>24</sup>;

(3) **'Hosting Consortium'** means a consortium composed of participating states, represented by National SOC's, *in accordance with Article 5.;*

(4) **'entity'** means an entity as defined in Article 6, point (38), of Directive (EU) 2022/2555;

*(4a) 'critical entity' means critical entity as defined in Article 2, point (1), of Directive (EU) 2022/2557 of the European Parliament and of the Council<sup>25</sup>.*

(5) **'entities operating in critical or highly critical sectors'** means entities *in the sectors* listed in *Annexes I and II to Directive (EU) 2022/2555;*

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

*(5b) 'risk' means risk as defined in Article 6, point (9), of Directive (EU) 2022/2555;*

---

<sup>24</sup> 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).

<sup>25</sup> ***Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ L 333, 27.12.2022, p. 164, ELI: <http://data.europa.eu/eli/dir/2022/2557/oj>).***



- (6) ‘**cyber threat**’ means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881;
- (6a) ‘**significant cyber threat**’ means a significant cyber threat as defined in Article 6, point (11), of Directive (EU) 2022/2555;
- (7) ‘**significant cybersecurity incident**’ means a cybersecurity incident fulfilling criteria set out in Article 23(3) of Directive (EU) 2022/2555;
- (8) ‘**large-scale cybersecurity incident**’ means an incident as defined in Article 6, point (7), of Directive (EU) 2022/2555;
- (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;
- (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 and short-term adverse consequences;
- (10a) ‘**managed security service provider**’ means a managed service provider as defined in Article 6, point (40), of Directive (EU) 2022/2555;
- (11) ‘**trusted managed security service providers**’ means managed security service providers selected *to be included in the EU Cybersecurity Reserve* in accordance with Article 16 of this Regulation.

## *Chapter II*

### **THE EUROPEAN CYBER SHIELD**

#### *Article 3*

#### **Establishment of the European Cyber Shield**

1. A **network** 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’).

Actions implementing the European Cyber Shield shall be supported by funding from the Digital Europe Programme and implemented in accordance with Regulation (EU) 2021/694 and in particular Specific Objective 3 thereof.

2. The European Cyber Shield shall:

(a) pool and share data on cyber threats and incidents from various sources through Cross-border SOCs *and where relevant exchange of information with CSIRTs Network*;

(b) produce high-quality, actionable information and cyber threat intelligence, through the use of state-of-the-art tools, notably Artificial Intelligence and data analytics technologies;

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

(d) contribute to faster detection of cyber threats and situational awareness across the Union;

(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.

It shall be developed in cooperation with the pan-European High Performance Computing infrastructure established pursuant to Regulation (EU) 2021/1173.

#### Article 4

### National Security Operations Centres

1. 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 *centralised capacity in a public body. When possible, the National SOCs shall be incorporated into the CSIRTs or other existing cybersecurity infrastructures and governance.*

It shall have the capacity to act as a reference point and gateway to other public and private organisations at national level, *particularly their National SOCs*, for collecting and analysing information on cybersecurity threats and incidents, *and, where relevant, sharing those information with members of the CSIRTs network of that Member State*, and contributing to a Cross-border SOC. It shall be equipped with state-of-the-art technologies capable of *preventing*, detecting, aggregating, and analysing data relevant to cybersecurity threats and incidents.

*A National SOC or CSIRT may request telemetry, sensor or logging data of their national critical entities from managed security service providers that provide a service to the critical entity. That data shall be shared in accordance with Union data protection law and with the sole purpose of supporting the National SOC or CSIRT to the detect and prevent cybersecurity threats and incidents.*

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.

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.

## Article 5

### Cross-border Security Operations Centres

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. ***A Cross-border SOC shall be designed to detect and analyse cyber threats, prevent incidents and support the production of high-quality intelligence, in particular through the exchange of data from various sources, public and private, as well as through the sharing of state-of-the-art tools and by jointly developing cyber detection, analysis, prevention and protection capabilities in a trusted and secure environment.***

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.

***2a. By way of derogation from Article 176 of Regulation (EU, Euratom) 2018/1046, entities established in third countries that are not parties to the GPA shall not participate in the joint procurement of tools and infrastructures.***

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.

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.

## Article 6

### Cooperation and information sharing within and between *Cross-border* SOC<sup>s</sup>

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:

- (a) ***improves the exchange of cyber threat intelligence between National and Cross-border SOC<sup>s</sup> and industry ISAC<sup>s</sup> with the aim to prevent, detect, or mitigate threats;***
- (b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative threat research between public and private entities.

2. The written consortium agreement referred to in Article 5(3) shall establish:

- (a) a commitment to share a significant **■** .data referred to in paragraph 1, and the conditions under which that information is to be exchanged;
- (b) a governance framework incentivising the sharing of information by all participants;
- (c) targets for contribution to the development of advanced artificial intelligence and data analytics tools.

3. To encourage exchange of information ***among*** Cross-border SOC<sup>s</sup> ***and with industry ISAC<sup>s</sup>***, Cross-border SOC<sup>s</sup> shall ensure a high level of interoperability between themselves ***and, where possible, with industry ISAC<sup>s</sup>***. To facilitate the interoperability between the Cross-border SOC<sup>s</sup> ***and with industry ISAC<sup>s</sup>***, ***information sharing standards and protocols may be harmonised with international standards and industry best practices. The joint procurement of cyber infrastructures, services and tools shall also be encouraged. Moreover, after consulting the ECCC and ENISA, the Commission is empowered, by... [six months from the date of entry into force of this Regulation] to adopt delegated acts in accordance with Article 20a to supplement this Regulation, by specifying the conditions for this interoperability in close coordination with the Cross-border SOC<sup>s</sup> and on the basis of international standards and industry best practices.***

4. Cross-border SOC<sup>s</sup> shall conclude cooperation agreements with one another ***and with, where appropriate, industry ISAC<sup>s</sup>***, specifying information sharing ***and interoperability*** principles

among the cross-border platforms, ***taking into consideration existing relevant information sharing mechanisms provided for in Directive (EU) 2022/2555. Where appropriate, Cross-border SOC's shall conclude cooperation agreements with industry ISACs. In the context of a potential or ongoing large-scale cybersecurity incident, information sharing mechanisms shall comply with the relevant provisions of the Directive (EU) 2022/2555.***

#### Article 7

##### **Cooperation and information sharing with *the CSIRT network***

1. Where the Cross-border SOC's 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 and ENISA, in line with their respective crisis management roles and procedures in accordance with Directive (EU) 2022/2555 without undue delay. This paragraph shall not impose further obligations on public or private entities to communicate a potential or ongoing large-scale cybersecurity incident for the fulfilment of the obligations laid down in the Directive (EU) 2022/2555.***
2. The Commission ***is empowered to adopt delegated acts in accordance with Article 20a after consulting the CSIRT network to supplement this Regulation by determining the procedural arrangements for the information sharing provided for in paragraphs 1 of this Article and in accordance with Directive (EU) 2022/2555.***

#### Article 8

##### **Security**

1. Member States participating in the European Cyber Shield shall ensure a high level of ***confidentiality and*** 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.
2. Member States participating in the European Cyber Shield shall ensure that the sharing of information within the European Cyber Shield with entities which are not Member State public bodies does not negatively affect the security interests of the Union.
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. ***They shall comply with Directives (EU) 2022/2555 and (EU) 2022/2557.*** In ***its implementing acts***, the Commission, supported by the High Representative, shall take into account relevant defence-level security standards, in order to facilitate cooperation with military actors.

## *Chapter III*

### **CYBERSECURITY EMERGENCY MECHANISM**

#### *Article 9*

##### **Establishment of the *Cybersecurity* Emergency Mechanism**

1. A ***Cybersecurity*** 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').
2. Actions implementing the Mechanism shall be supported by funding from DEP and implemented in accordance with Regulation (EU) 2021/694 and in particular Specific Objective 3 thereof.

#### *Article 10*

##### **Type of actions**

1. The Mechanism shall support the following types of actions:
    - (a) preparedness actions, including the coordinated preparedness testing of entities operating in highly critical sectors across the Union;
    - (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;
    - (c) mutual assistance actions consisting of the provision of assistance from national authorities of one Member State to another Member State, in particular as provided for in Article 11(3), point (f), of Directive (EU) 2022/2555.
- 1a. Following the triggering of the Mechanism, the Commission shall, on an annual basis, assess and publish a report on both the positive and the negative working of the Mechanism, including whether further cooperation or training requirements are needed.***

#### *Article 11*

##### **Coordinated preparedness testing of entities**

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 *in accordance with the arrangements established for the entities in the Sectors of High Criticality listed in Annex I to Directive (EU) 2022/2555.*

2. The NIS Cooperation Group in cooperation with the Commission, ENISA, and the High Representative, *and the entities that are subject to coordinated preparedness testing pursuant to paragraph 1*, shall develop common risk scenarios and methodologies for the coordinated preparedness testing exercises, *culminating in a concerted workplan. Entities subject to coordinated preparedness testing shall develop and implement a remediation plan that carries out the recommendations resulting from preparedness tests.*

*The NIS Cooperation Group may inform the prioritisation of sectors, or sub-sectors for the coordinated preparedness testing exercises.*

## Article 12

### Establishment of the EU Cybersecurity Reserve

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.

*Where it is apparent that the procured services cannot be fully used for the purposes of providing support for responding to significant or large-scale incidents, those services can exceptionally be converted to exercises or trainings for dealing with incidents, and provided to the users upon request, by the contracting authority.*

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 *EU Cybersecurity reserve* shall include pre-committed services. The services shall be deployable in all Member States, *shall reinforce the Union's technological sovereignty, its open strategic autonomy, competitiveness and resilience in the cyber security sector including by boosting innovation in the Digital Single Market across the Union.*

3. Users of the services from the EU Cybersecurity Reserve shall include:

- (a) Member States' cyber crisis management authorities and CSIRTs as referred to in Article 9 (1) and (2) and Article 10 of Directive (EU) 2022/2555, respectively;
- (b) Union institutions, bodies and agencies *as referred to in Article 3 (1) of the Regulation (EU) .../2023 of the European Parliament and of the Council<sup>26</sup> and CERT-EU.*

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.

---

<sup>26</sup> *Regulation (EU) .../2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (OJ C , , p , , ELI: ...).*

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.
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.
7. In order to support the Commission 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, ***and where appropriate, managed security services providers, and other cybersecurity industry representatives***. ENISA shall prepare a similar mapping, after consulting the Commission, ***managed security services providers, and where appropriate, other cybersecurity industry representatives*** 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 ***and inform the Council about the needs of third countries***.
8. The Commission ***is empowered to 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. ■ ..

### *Article 13*

#### **Requests for support from the EU Cybersecurity Reserve**

1. The users referred to in Article 12(3) may request services from the EU Cybersecurity Reserve to support response to and immediate recovery from significant or large-scale cybersecurity incidents.
2. To receive support from the EU Cybersecurity Reserve, the users referred to in Article 12(3) shall take measures to mitigate the effects of the incident for which the support is requested, including the provision of direct technical assistance, and other resources to assist the response to the incident, and immediate recovery efforts.
3. Requests for support from users referred to in Article 12(3), point (a), of this Regulation shall be transmitted to the Commission and ENISA via the Single Point of Contact designated or established by the Member State in accordance with Article 8(3) of Directive (EU) 2022/2555.
4. Member States shall inform the CSIRTs network, and where appropriate EU-CyCLONe, about their requests for incident response and immediate recovery support pursuant to this Article.
5. Requests for incident response and immediate recovery support shall include:
  - (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;
  - (b) information about measures taken to mitigate the incident for which the support is requested, as referred to in paragraph 2;

- (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.
6. ENISA, in cooperation with the Commission and the NIS Cooperation Group, shall develop a template to facilitate the submission of requests for support from the EU Cybersecurity Reserve.
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. ■

#### Article 14

### Implementation of the support from the EU Cybersecurity Reserve

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 *undue* delay *and in any event within 24 hours*.
2. To prioritise requests, in the case of multiple concurrent requests, the following criteria shall be taken into account, where relevant:
- (a) the severity of the cybersecurity incident;
  - (b) the type of entity affected, with higher priority given to incidents affecting essential entities as defined in Article 3(1) of Directive (EU) 2022/2555;
  - (c) the potential impact on the affected Member State(s) 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;
  - (e) the measures taken by the user to assist the response, and immediate recovery efforts, as referred in Article 13(2) and Article 13(5), point (b).
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*.
4. The agreements referred to in paragraph 3 *shall* be based on templates prepared by ENISA, after consulting Member States *and, where appropriate, other users 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 gross negligence in the evaluation of the application of the service provider or in case where the Commission or ENISA are users of the EU Cybersecurity Reserve according to Article 14 (3)*.



6. Within one month from the end of the support action, the users shall provide Commission and 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. ***The report shall respect Union and national law concerning the protection of sensitive or classified information.***

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

#### *Article 15*

##### **Coordination with crisis management mechanisms**

1. In cases where significant or large-scale cybersecurity incidents originate from or result in disasters as defined in Decision 1313/2013/EU<sup>27</sup>, the support under this Regulation for responding to such incidents shall complement actions under and without prejudice to Decision 1313/2013/EU.

2. In the event of a large-scale, cross border cybersecurity incident where Integrated Political Crisis Response arrangements (IPCR) are triggered, the support under this Regulation for responding to such incident shall be handled in accordance with relevant protocols and procedures under the IPCR.

3. In consultation with the High Representative, support under the ***Cybersecurity*** 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) ***TFEU***.

4. Support under the ***Cybersecurity*** Emergency Mechanism may form part of the joint response between the Union and Member States in situations referred to in Article 222 ***TFEU***

#### *Article 16*

##### **Trusted providers**

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:

- (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;
- (b) ensure the protection of the essential security interests of the Union and its Member States.

---

<sup>27</sup> Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924).

- (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, **and the achievement of gender balance in the sector, and reinforcing the Union’s technological sovereignty, open strategic autonomy, competitiveness and resilience.**

2. When procuring services for the EU Cybersecurity Reserve, the contracting authority shall include in the procurement documents the following selection criteria:

- (a) the provider shall demonstrate that its personnel has the highest degree of professional integrity, independence, responsibility, and the requisite technical competence to perform the activities in their specific field, and ensures the permanence/continuity of expertise as well as the required technical resources;
- (b) the provider, its subsidiaries and subcontractors shall have in place a framework to protect sensitive information relating to the service, and in particular evidence, findings and reports, and is compliant with Union security rules on the protection of EU classified information;
- (c) the provider shall provide sufficient proof that its governing structure is transparent, not likely to compromise its impartiality and the quality of its services or to cause conflicts of interest;
- (d) the provider shall have appropriate security clearance, at least for personnel intended for service deployment;
- (e) the provider shall have the relevant level of security for its IT systems;
- (f) the provider shall be equipped with **up to date** the hardware and software technical equipment necessary to support the requested service **and shall, as applicable, comply with Regulation (EU) .../... of the European Parliament and of the Council<sup>28</sup> (2022/0272(COD))**;
- (g) the provider shall be able to demonstrate that it has experience in delivering similar services to relevant national authorities or entities operating in critical or highly critical sectors;
- (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;
- (i) the provider shall be able to provide the service in the local language of the Member State(s), **or in one of the working languages of the Union’s institutions**, where it can deliver the service;
- (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 **within a period of two years after the scheme has been adopted.**
- (ja) the provider shall be able to provide the service independently and not as part of a bundle, thus safeguarding the user possibility to switch to another service provider;**

---

<sup>28</sup> Regulation (EU) .../... of the European Parliament and of the Council of ... on ... (OJ L, ..., ELI: ...).



- (jb) *for the purposes of Article 12(1) the provider shall include in the tenders proposal the possibility for conversion of unused incident response services into exercises or trainings;*
- (jc) *the provider shall be established and shall have its executive management structures in the Union, in an associated country or in a third country that is part to the Government Procurement Agreement in the context of World Trade Organisation(GPA).*
- (jd) . *The provider shall not be subject to control by a non-associated third country or by a non-associated third-country entity that is not party to the GPA or, alternatively, such an entity shall have been subject to screening within the meaning of Regulation (EU) 2019/452 and, where necessary, to mitigation measures, taking into account the objectives set out in this Regulation.*

#### Article 17

### Support to third countries

1. Third countries may request support from the EU Cybersecurity Reserve where Association Agreements concluded regarding their participation in DEP provide for this.
2. Support from the EU Cybersecurity Reserve shall be in accordance with this Regulation, and shall comply with any specific conditions laid down in the Association Agreements referred to in paragraph 1.
3. Users from associated third countries eligible to receive services from the EU Cybersecurity Reserve shall include competent authorities such as CSIRTs and cyber crisis management authorities.
4. Each third country eligible for support from the EU Cybersecurity Reserve shall designate an authority to act as a single point of contact for the purpose of this Regulation.
5. Prior to receiving any support from the EU Cybersecurity Reserve, third countries shall provide to the Commission and the High Representative information about their cyber resilience and risk management capabilities, including at least information on national measures taken to prepare for significant or large-scale cybersecurity incidents, as well as information on responsible national entities, including CSIRTs or equivalent entities, their capabilities and the resources allocated to them. Where provisions of Articles 13 and 14 of this Regulation refer to Member States, they shall apply to third countries as set out in paragraph 1.
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.

## *Chapter IV*

### **CYBERSECURITY INCIDENT REVIEW MECHANISM**

#### *Article 18*

#### **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 ***with and gather feedback from*** all relevant stakeholders, including representatives of Member States, the Commission, other relevant EU institutions, bodies, ***offices*** and agencies, managed security services providers ***in the National and Cross-border 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 cybersecurity services 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.
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.***
- 3a. The report referred to in paragraph 1 of this Article shall set out lessons learned from the peer reviews carried out pursuant to Article 19 of Directive (EU) 2022/2555.***
4. Where appropriate, the report shall draw recommendations, ***including for all relevant stakeholders,*** 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.

## *Chapter V*

### **FINAL PROVISIONS**

#### *Article 19*

#### **Amendments to Regulation (EU) 2021/694**

Regulation (EU) 2021/694 is amended as follows:

(1) Article 6 is amended as follows:

(a) paragraph 1 is amended as follows:

(i) the following point (aa) is inserted:

‘(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’;

(ii) the following point (g) is added:

‘(g) establish and operate a **Cybersecurity** Emergency Mechanism to support Member States in preparing for and responding to significant cybersecurity incidents, complementary to national resources and capabilities and other forms of support available at Union level, including the establishment of an EU Cybersecurity Reserve’;

(b) Paragraph 2 is replaced by the following:

‘2. The actions under Specific Objective 3 shall be implemented primarily through the European Cybersecurity Industrial, technology and research Competence Centre and the Network of National Coordination Centres, in accordance with Regulation (EU) 2021/887 of the European Parliament and of the Council\*with the exception of actions implementing the EU Cybersecurity Reserve, which shall be implemented by the Commission and ENISA.

---

\* Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, (OJ L 202, 8.6.2021, p. 1, *ELI*: <http://data.europa.eu/eli/reg/2021/887/oj>).’;

(2) Article 9 is amended as follows:

(a) in paragraph 2, points (b), (c) and (d) are replaced by the following:

‘(b), EUR 1 776 956 000 for Specific Objective 2 – Artificial Intelligence;

(c), EUR **1 620 566 000** for Specific Objective 3 – Cybersecurity and Trust;

(d), EUR **500 347 000** for Specific Objective 4 – Advanced Digital Skills’;

***(aa) the following new paragraph 2a is inserted:***

*‘ (2a). The amount referred to in paragraph 2 point c shall primarily be used for achieving the operational objectives referred into art. 6 par. 1 (a-f) of the Programme.’;*

*(ab) the following new paragraph 2b is inserted:*

*‘ (2b). The amount for the establishment and implementation of the EU Cybersecurity Reserve shall not exceed EUR 27 million for the intended duration of the Regulation laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for, and respond to cybersecurity threats and incidents.’;*

(b) the following paragraph 8 is added:

*‘8. By way of 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.’;*

*The Commission shall inform the Parliament and the Council of appropriations carried over in accordance with art. 12(6) of Regulation (EU, Euratom) 2018/1046.*

(3) In Article 14, paragraph 2 is replaced by the following:

“2. The Programme may provide funding in any of the forms laid down in the Regulation **(EU, Euratom) 2018/1046**, including in particular through procurement as a primary form, or grants and prizes.

Where the achievement of the objective of an action requires the procurement of innovative goods and services, grants may be awarded only to beneficiaries that are contracting authorities or contracting entities as defined in Directives 2014/24/EU<sup>27</sup> and 2014/25/EU<sup>28</sup> of the European Parliament and of the Council.

Where the supply of innovative goods or services that are not yet available on a large-scale commercial basis is necessary to achieve the objectives of an action, the contracting authority or the contracting entity may authorise the award of multiple contracts within the same procurement procedure.

For duly justified reasons of public security, the contracting authority or the contracting entity may require that the place of performance of the contract be situated within the territory of the Union.

When implementing procurement procedures for the EU Cybersecurity Reserve established by Article 12 of Regulation (EU) 2023/..., the Commission and ENISA may act as a central purchasing body to procure on behalf of or in the name of third countries associated to the Programme in line with Article 10. The Commission and ENISA may also act as wholesaler, by buying, stocking and reselling or donating supplies and services, including rentals, to those third countries. By derogation from Article 169(3)

of Regulation (EU). .../..., the request from a single third country is sufficient to mandate the Commission or ENISA to act.

When implementing procurement procedures for the EU Cybersecurity Reserve established by Article 12 of Regulation (EU) 2023/...XX, the Commission and ENISA may act as a central purchasing body to procure on behalf of or in the name of Union institutions, bodies and agencies. The Commission and ENISA may also act as wholesaler, by buying, stocking and reselling or donating supplies and services, including rentals, to Union institutions, bodies and agencies. By derogation from Article 169(3) of Regulation (EU) .../..., the request from a single Union institution, body or agency is sufficient to mandate the Commission or ENISA to act.

The Programme may also provide financing in the form of financial instruments within blending operations. ’;

(4) The following article 16a is added:

**‘Article 16a**

In the case of actions implementing the European Cyber Shield established by Article 3 of Regulation (EU) 2023/XX, the applicable rules shall be those set out in Articles 4 and 5 of Regulation (EU) 2023/... In the case of conflict between the provisions of this Regulation and Articles 4 and 5 of Regulation (EU) 2023/..., the latter shall prevail and apply to those specific actions.’;

(5) Article 19 is replaced by the following:

‘Grants under the Programme shall be awarded and managed in accordance with Title VIII of **Regulation (EU, Euratom) 2018/1046** and may cover up to 100 % of the eligible costs, without prejudice to the co-financing principle as laid down in Article 190 of **Regulation (EU, Euratom) 2018/1046**. Such grants shall be awarded and managed as specified for each specific objective.

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 (EU) .../... and the Hosting Consortium referred to in Article 5 of Regulation (EU) .../..., in accordance with Article 195(1), point (d) of **Regulation (EU, Euratom) 2018/1046**.

Support in the form of grants for the **Cybersecurity** Emergency Mechanism as set out in Article 10 of Regulation (EU) .../... may be awarded directly by the ECCC to Member States without a call for proposals, in accordance with Article 195(1), point (d) of **Regulation (EU, Euratom) 2018/1046**.

For actions specified in Article 10(1), point (c) of Regulation (EU) .../..., the ECCC shall inform the Commission and ENISA about Member States’ requests for direct grants without a call for proposals.

For the support of mutual assistance for response to a significant or large-scale cybersecurity incident as defined in Article 10(c), of Regulation (EU) .../..., and in accordance with Article 193(2), second subparagraph, point (a), of **Regulation (EU, Euratom) 2018/1046**, in duly justified cases, the costs may be considered to be eligible even if they were incurred before the grant application was submitted.”;

(6) Annexes I and II to Regulation (EU) 2021/694 are amended in accordance with the Annex to this Regulation.

**Article 19a**  
**Additional resources for ENISA**

***ENISA shall receive additional resources to carry out its additional tasks conferred on it by this Regulation. That additional support, including funding, shall not jeopardise the achievement of the objectives of other Union’s Programmes, in particular the Digital Europe Programme.***

**Article 20**

**Evaluation and Review**

1. By [***two years from*** 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 shall submit a report*** to the European Parliament and to the Council.
2. ***The evaluation shall assess in particular:***
  - (a) ***the use and added value of the Cross-Border SOCs and the extent to which they contribute to fastening the detection of and response to cyber threats and situational awareness; the active participation of National SOCs in the European Cyber Shield, including the number of National SOCs and Cross-border SOCs established and the extent to which it has contributed to the production and exchange of high-quality actionable information and cyber threat intelligence; the number and costs of cybersecurity infrastructure, or tools, or both jointly procured; the number of cooperation agreements concluded between Cross-border SOCs and with industry ISACs; the number of incidents reported to the CSIRT network and the impact it has on the work of the CSIRT Network;***

- (b) both the positive and the negative working of the Cybersecurity Emergency Mechanism, including whether further cooperation or training requirements are needed;*
- (c) the contribution of this Regulation to reinforce the Union's resilience and open strategic autonomy, to improve the competitiveness of the relevant industry sectors, microenterprises, SMEs including start-ups, and the development of cybersecurity skills in the Union;*
- (d) the use and added value of the EU Cybersecurity Reserve, including the number of trusted security providers part of the EU Cybersecurity Reserve; the number, type, costs and impact of actions carried out supporting response to cybersecurity incidents, as well as its users and providers; the mean time for the Commission to acknowledge, the EU Cybersecurity Reserve to be deployed and to respond, and the user to recover from incidents; whether the scope of the EU Cybersecurity Reserve is to be broadened to incident preparedness services or common exercises with the trusted managed security service providers and potential users of the EU Cybersecurity Reserve to ensure efficient functioning of the EU Cybersecurity Reserve where necessary;*
- (e) 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;*
- (f) the contribution of this Regulation to the deployment and development of state-of-the-art technologies in the Union.*

*3. On the basis of the reports referred to in paragraph 1, the Commission shall, where appropriate, submit a legislative proposal to the European Parliament and to the Council to amend this Regulation.*

#### *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.*

#### *Article 21*

#### **Committee procedure**

1. The Commission shall be assisted by the Digital Europe Programme Coordination Committee established by Regulation (EU) 2021/694. That committee shall be a committee within the meaning of Regulation (EU) 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) 182/2011 shall apply.



*Article 22*

**Entry into force**

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Strasbourg,

*For the European Parliament*  
*The President*

*For the Council*  
*The President*

## ANNEX

Regulation (EU) 2021/694 is amended as follows:

(1) In Annex I, the section/ chapter ‘Specific Objective 3 – Cybersecurity and Trust’ is replaced by the following:

‘Specific Objective 3 – Cybersecurity and Trust

The Programme shall stimulate the reinforcement, building and acquisition of essential capacities to secure the Union’s digital economy, society and democracy by reinforcing the Union cybersecurity industrial potential and competitiveness, as well as by improving capabilities of both the private and public sectors to protect citizens and businesses from cyber threats, including by supporting the implementation of Directive (EU) 2016/1148.

Initial and, where appropriate, subsequent actions under this objective shall include:

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.
2. Scaling up existing technological capacities and networking the competence centres in Member States and making sure that those capacities respond to public sector and industry needs, including through products and services that reinforce cybersecurity and trust within the Digital Single Market.

3. Ensuring wide deployment of effective state-of-the-art cybersecurity and trust solutions across the Member States. Such deployment includes strengthening the security and safety of products, from their design to their commercialisation.

4. Support closing the cybersecurity skills gap, ***with a particular focus on achieving gender balance in the sector 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.***

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.’;

(2) In Annex II the section/chapter ‘Specific Objective 3 – Cybersecurity and Trust’ is replaced by the following:

‘Specific Objective 3 – Cybersecurity and Trust

3.1. The number of cybersecurity infrastructure, or tools, or both jointly procured ***as part of the Cybersecurity Shield.***

3.2. The number of users and user communities getting access to European cybersecurity facilities

3.3. The number, ***type, costs and impact*** of actions ***carried out*** supporting preparedness and response to cybersecurity incidents under the ***Cybersecurity*** Emergency Mechanism. ***The extent to which recommendations of preparedness tests have been implemented and carried out by the user as well as the mean time for the Commission to acknowledge, the EU Cybersecurity Reserve to respond, and the user to recover from incidents.***’

## 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.<sup>1</sup> 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<sup>2</sup>). 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<sup>3</sup>. 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 transition going further every day, digital resilience becomes more and more important for our

---

<sup>1</sup> ENISA Threat Landscape 2022, October 2022. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport>

<sup>2</sup> ENISA Threat Landscape: Health Sector, July 2023. <https://www.enisa.europa.eu/publications/health-threat-landscape/@@download/fullReport>

<sup>3</sup> European Committee of the Regions, Digital Resilience, 2023. <https://cor.europa.eu/en/engage/studies/Documents/Digital%20resilience.pdf>

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 resources, 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 persists in cybersecurity with women comprising 20% of the average worldwide presence.<sup>4</sup> Women must be present and part of the design of the digital future and its governance.

In addition, the Rapporteur proposes 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).

The Rapporteur proposes measures to include and increase citizen awareness without

---

<sup>4</sup> 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](https://www.europarl.europa.eu/doceo/document/TA-9-2021-0296_EN.html#def_1_22)



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.

**ANNEX: ENTITIES OR PERSONS  
FROM WHOM THE RAPPORTEUR HAS RECEIVED INPUT**

Pursuant to Article 8 of Annex I to the Rules of Procedure, the rapporteur declares that she has received input from the following entities or persons in the preparation of the report, until the adoption thereof in committee:

<b>Entity and/or person</b>
CorwdStrike
CyberPeace institute
Microsoft Corporation
Romanian National Cyber Security Directorate
ENISA
Centro Criptológico Nacional
Permanent Representation of Spain
Trellix
Palo Alto Networks Inc
Committee of the regions rapporteur

The list above is drawn up under the exclusive responsibility of the rapporteur.

27.10.2023

## OPINION OF THE COMMITTEE ON FOREIGN AFFAIRS

for the Committee on Industry, Research and Energy

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

Rapporteur for opinion: Dragoş Tudorache

### Amendment 1

#### Proposal for a regulation

##### Recital 1

*Text proposed by the Commission*

(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.

*Amendment*

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

### Amendment 2

#### Proposal for a regulation

##### Recital 2

*Text proposed by the Commission*

(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

*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.

the functioning of network and information systems. In view of the fast-evolving threat landscape, the threat of possible large-scale incidents causing significant disruption or damage to critical infrastructures demands heightened preparedness at all levels of the Union's cybersecurity framework. ***The gravity of these threats became even more relevant due to the return of war on our continent. These threats go*** beyond Russia's military aggression on Ukraine, and ***are*** likely to persist given the multiplicity of state-aligned, criminal and hacktivist actors involved in current geopolitical tensions. Such incidents can impede the provision of public services and the pursuit of economic activities, including in critical or highly critical sectors, generate substantial financial losses, undermine user confidence, cause major damage to the economy ***and security*** of the Union, and could even have health or life-threatening consequences ***by possibly undermining local or national security related installations***. Moreover, cybersecurity incidents are unpredictable, as they often emerge and evolve within very short periods of time, not contained within any specific geographical area, and occurring simultaneously or spreading instantly across many countries. ***Cybersecurity is important to protect our European values, and ensures the functioning of our democracies by shielding our election infrastructure and democratic procedures from any foreign interference.***

### Amendment 3

#### Proposal for a regulation

#### Recital 2 a (new)

*Text proposed by the Commission*

*Amendment*

***(2 a) Cybersecurity is crucial to keep our Union safe and prevent malicious actors, state and non-state, from***

*undermining our democracy, economy, and security. It is necessary to prevent a fragmented landscape as such a situation would not represent an adequate approach, in particular when faced with the challenge of future large scale cyber attack targetting several Member States at the same time or transnational critical infrastructure. Therefore, a Union body that would act as a coordination platform for all existing and future cyber security instruments, funds and mechanisms is needed.*

#### **Amendment 4**

##### **Proposal for a regulation**

##### **Recital 3**

*Text proposed by the Commission*

(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<sup>16</sup>, 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.

*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<sup>16</sup>, it is necessary to increase the resilience of citizens, businesses and entities operating critical infrastructures against the growing cybersecurity threats, which can have devastating societal and economic impacts. Therefore, investment in infrastructures and services that will support faster detection and response to cybersecurity threats and incidents is needed, and Member States need assistance in better preparing for, as well as responding to significant and large-scale cybersecurity incidents. The Union should also increase its capacities in these areas, notably as regards the collection and analysis of data on cybersecurity threats and incidents, *as well as its ability to act proactively and react decisively to*

---

<sup>16</sup> <https://futureu.europa.eu/en/>

---

<sup>16</sup> <https://futureu.europa.eu/en/>

## **Amendment 5**

### **Proposal for a regulation**

#### **Recital 4**

##### *Text proposed by the Commission*

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

##### *Amendment*

(4) The Union has already taken a number of measures to reduce vulnerabilities and increase the resilience of critical infrastructures and entities against cybersecurity risks, in particular Directive (EU) 2022/2555 of the European Parliament and of the Council<sup>17</sup>, Commission Recommendation (EU) 2017/1584<sup>18</sup>, Directive 2013/40/EU of the European Parliament and of the Council<sup>19</sup> and Regulation (EU) 2019/881 of the European Parliament and of the Council<sup>20</sup>. In addition, the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure invites Member States to take urgent and effective measures, and to cooperate loyally, efficiently, ***and proactively***, in solidarity and in a coordinated manner with each other, the Commission and other relevant public authorities as well as the entities concerned, to enhance the resilience of critical infrastructure used to provide essential services in the internal market. ***Furthermore, the Union approved and launched its Strategic Compass for Security and Defence on March 2022, which focuses inter alia on strengthening cyber security and enhancing international cooperation with like-minded allies and democratic partners especially in this matter. Moreover, cyber-security has been a focal point of the recent Third Joint Declaration on EU-NATO Cooperation of January 2023. In***



*particular, the final assessment report of the EU-NATO task force recommended making full use of synergies between EU and NATO[1], including the exchange of best practices between civilian and military actors on the implementation of relevant cyber-related policies and legislation.*

*[1]*

[https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736\\_en](https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_en)

---

<sup>17</sup> Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022).

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

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

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

---

<sup>17</sup> Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022).

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

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

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

## Amendment 6

### Proposal for a regulation Recital 6

*Text proposed by the Commission*

(6) The Joint Communication on the EU Policy on Cyber Defence<sup>22</sup> adopted on 10 November 2022 announced an EU Cyber Solidarity Initiative with the following objectives: strengthening of common EU detection, situational awareness and response capabilities by promoting the deployment of an EU infrastructure of Security Operations Centres ('SOCs'), supporting gradual building of an EU-level cybersecurity reserve with services from trusted private providers and testing of critical entities for potential vulnerabilities based on EU risk assessments.

---

<sup>22</sup> Joint Communication to the European Parliament and the Council EU Policy on Cyber Defence JOIN/2022/49 final

## Amendment 7

### Proposal for a regulation Recital 6 a (new)

*Text proposed by the Commission*

*Amendment*

(6) The Joint Communication on the EU Policy on Cyber Defence<sup>22</sup> adopted on 10 November 2022 announced an EU Cyber Solidarity Initiative with the following objectives: strengthening of common EU detection, situational awareness and response capabilities by promoting the deployment of an EU infrastructure of Security Operations Centres ('SOCs'), supporting gradual building of an EU-level cybersecurity reserve with services from trusted private providers and testing of critical entities for potential vulnerabilities based on EU risk assessments. ***In addition, the rapidly evolving cyber threat landscape and the fast pace of technological development also demonstrate the need for enhanced civil-military coordination and cooperation, as stressed by the Council in its Conclusions on the EU Policy on Cyber Defence[1].***

***[1] Council Conclusions on the EU Policy on Cyber Defence approved by the Council at its meeting on 22 May 2023, (9618/23)***

---

<sup>22</sup> Joint Communication to the European Parliament and the Council EU Policy on Cyber Defence JOIN/2022/49 final

*military matters and the dual-use nature of cyber tools and technologies, there is a need for a comprehensive and holistic approach to the digital domain. In the event of a large-scale cybersecurity incident and crisis involving more than one Member State, appropriate crisis management and governance should be established. Such structures should organise exchange of information, coordination and cooperation with the Union's external security and military crisis management structures and Member States' bodies in charge of security and defence (the cyber defence community). This should also apply to Common Security and Defence Policy operations and missions conducted by the Union to ensure peace and stability in its neighbourhood and beyond.*

## Amendment 8

### Proposal for a regulation

#### Recital 7

##### *Text proposed by the Commission*

(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.

##### *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, ***including the incidents involving more than one Member State. When feasible and necessary, a Cybersecurity***

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

***Emergency Mechanism should organise information-sharing and cooperation with Member States' defence authorities and supported by EU institutions, bodies and agencies (the EU cyber defence community);*** a Cybersecurity Incident Review Mechanism should be established to review and assess specific significant or large-scale incidents. ***Such new structures should also support EU CSDP operations and missions.*** These actions shall be without prejudice to Articles 107 and 108 of the Treaty on the Functioning of the European Union ('TFEU').

## Amendment 9

### Proposal for a regulation

#### Recital 11

##### *Text proposed by the Commission*

(11) For the purpose of sound financial management, specific rules should be laid down for the carry-over of unused commitment and payment appropriations. While respecting the principle that the Union budget is set annually, this Regulation should, on account of the unpredictable, exceptional and specific nature of the cybersecurity landscape, provide for possibilities to carry over unused funds beyond those set out in the Financial Regulation, thus maximising the Cybersecurity Emergency Mechanism's capacity to support Member States in countering effectively cyber threats.

##### *Amendment*

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

## Amendment 10

### Proposal for a regulation Recital 13

*Text proposed by the Commission*

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

*Amendment*

(13) Each Member State should designate a public body at national level tasked with coordinating cyber threat detection activities in that Member State. These National SOCs should act as a reference point and gateway at national level for participation in the European Cyber Shield and should ensure that cyber threat information from public and private entities is shared and collected at national level in an effective and streamlined manner. ***When feasible and necessary, SOCs should also allow for the participation of defence entities, establishing a 'defence pillar' in terms of governance and type of information shared, as set out in the Joint Communication on the EU Policy on Cyber Defence[1] and supported by the High Representative.***

***[1] Joint Communication to the European Parliament and the Council EU Policy on Cyber Defence JOIN/2022/49 final***

## Amendment 11

### Proposal for a regulation Recital 14

*Text proposed by the Commission*

(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

*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, ***including a 'defence pillar'***, so that the benefits of cross-border threat detection and information sharing and management

objective of Cross-border SOC's 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 SOC's and computer incident response teams ('CSIRT's') and other relevant actors.

can be fully achieved. The general objective of Cross-border SOC's should be to strengthen capacities to analyse, prevent and detect cybersecurity threats and to support the production of high-quality intelligence on cybersecurity threats, notably through the sharing of data from various sources, public or private **and, when necessary and feasible military with sufficient guidance for information sharing**, as well as through the sharing and joint use of state-of-the-art tools, and jointly developing detection, analysis and prevention capabilities in a trusted environment. They should provide new additional capacity, building upon and complementing existing SOC's and computer incident response teams ('CSIRT's') and other relevant actors.

## Amendment 12

### Proposal for a regulation

#### Recital 15

##### *Text proposed by the Commission*

(15) At national level, the monitoring, detection and analysis of cyber threats is typically ensured by SOC's of public and private entities, in combination with CSIRT's. In addition, CSIRT's exchange information in the context of the CSIRT network, in accordance with Directive (EU) 2022/2555. The Cross-border SOC's should constitute a new capability that is complementary to the CSIRT's 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**.

##### *Amendment*

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



## Amendment 13

### Proposal for a regulation

#### Recital 16

##### *Text proposed by the Commission*

(16) The Cross-border SOC 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 SOC should also enter into cooperation agreements with other Cross-border SOC.

##### *Amendment*

(16) The Cross-border SOC should act as a central point allowing for a broad pooling of relevant data and cyber threat intelligence, enable the spreading of threat information among a large and diverse set of actors (e.g., Computer Emergency Response Teams ('CERTs'), CSIRTs, Information Sharing and Analysis Centers ('ISACs'), operators of critical infrastructures, ***as well as the cyber defence community***). The information exchanged among participants in a Cross-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 SOC should also enter into cooperation agreements with other Cross-border SOC ***and operational network for milCERTs (MICNET) when established***.

## Amendment 14

### Proposal for a regulation

#### Recital 17

##### *Text proposed by the Commission*

(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,

##### *Amendment*

(17) Shared situational awareness among relevant authorities is an indispensable prerequisite for Union-wide preparedness and coordination with regards to significant and large-scale cybersecurity incidents. Directive (EU) 2022/2555 establishes the EU-CyCLONe to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions,

bodies and agencies. Recommendation (EU) 2017/1584 on coordinated response to large-scale cybersecurity incidents and crises addresses the role of all relevant actors. Directive (EU) 2022/2555 also recalls the Commission’s responsibilities in the Union Civil Protection Mechanism (‘UCPM’) established by Decision 1313/2013/EU of the European Parliament and of the Council, as well as for providing analytical reports for the Integrated Political Crisis Response Mechanism (‘IPCR’) arrangements under Implementing Decision (EU) 2018/1993. Therefore, in situations where Cross-border SOCs obtain information related to a potential or ongoing large-scale cybersecurity incident, they should provide relevant information to EU-CyCLONe, the 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.

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

## Amendment 15

### Proposal for a regulation

#### Recital 19

##### *Text proposed by the Commission*

(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

##### *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, ***excluding high-risk suppliers of critical***

collective detection capacities and timely warnings to authorities and relevant entities, notably by using the latest artificial intelligence and data analytics technologies.

***products with digital elements.*** This should make it possible to improve collective detection capacities and timely warnings to authorities and relevant entities, notably by using the latest artificial intelligence and data analytics technologies. ***Human oversight should be provided for when using AI, and sufficient level of AI literacy, necessary support and authority to exercise that function should be ensured.***

## Amendment 16

### Proposal for a regulation Recital 19 a (new)

*Text proposed by the Commission*

*Amendment*

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

## Amendment 17

### Proposal for a regulation Recital 20

#### *Text proposed by the Commission*

(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<sup>25</sup>.

---

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

#### *Amendment*

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

---

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

## Amendment 18

### Proposal for a regulation Recital 25

#### *Text proposed by the Commission*

(25) The Cyber Emergency Mechanism should provide support to Member States complementing their own measures and resources, and other existing support options in case of response to and immediate recovery from significant and large-scale cybersecurity incidents, such as the services provided by the European Union Agency for Cybersecurity ('ENISA') in accordance with its mandate, the coordinated response and the assistance

#### *Amendment*

(25) The Cyber Emergency Mechanism should provide support to Member States complementing their own measures and resources, and other existing support options in case of response to and immediate recovery from significant and large-scale cybersecurity incidents, such as the services provided by the European Union Agency for Cybersecurity ('ENISA') in accordance with its mandate, the coordinated response and the assistance

from the CSIRTs network, the mitigation support from the EU-CyCLONe, as well as mutual assistance between Member States including in the context of Article 42(7) of TEU, the PESCO Cyber Rapid Response Teams<sup>26</sup> and Hybrid Rapid Response Teams. It should address the need to ensure that specialised means are available to support preparedness and response to cybersecurity incidents across the Union and in third countries.

from the CSIRTs network, the mitigation support from the EU-CyCLONe, as well as mutual assistance between Member States including in the context of Article 42(7) of TEU, the PESCO Cyber Rapid Response Teams[1], ***the new PESCO-project Cyber Information Domain Coordination Centre (CIDCC) and its proposed successor the EU Cyber Defence Coordination Centre (EUCDCC)***, and Hybrid Rapid Response Teams. It should address the need to ensure that specialised means are available to support preparedness and response to cybersecurity incidents across the Union and in third countries, ***especially those EU candidate countries aligned with the EU Common Foreign and Security Policy and Common Security and Defence Policy, supporting them in building up their cyber capabilities and enhancing cross-border and regional cooperation among those candidate countries in the field of cyber.***

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

---

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

---

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

## **Amendment 19**

### **Proposal for a regulation Recital 26**

*Text proposed by the Commission*

(26) This instrument is without prejudice to procedures and frameworks to coordinate crisis response at Union level, in particular the UCPM<sup>27</sup>, IPCR<sup>28</sup>, and

*Amendment*

(26) This instrument is without prejudice to procedures and frameworks to coordinate crisis response at Union level, in particular the UCPM<sup>27</sup>, IPCR<sup>28</sup>, and

Directive (EU) 2022/2555. It may contribute to or complement actions implemented in the context of Article 42(7) of TEU or in situations defined in Article 222 of TFEU. The use of this instrument should also be coordinated with the implementation of Cyber Diplomacy Toolbox's measures, *where appropriate*.

Directive (EU) 2022/2555. It may contribute to or complement actions implemented in the context of Article 42(7) of TEU or in situations defined in Article 222 of TFEU. The use of this instrument should also be coordinated with the implementation of Cyber Diplomacy Toolbox's measures, ***enhancing cooperation at the strategic, operational and technical level between cyber defence and other cyber communities, particularly in order to strengthen capabilities against cybersecurity threats from outside the Union, including restrictive measures, that can be used to prevent and respond to malicious cyber activities.***

---

<sup>27</sup> Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924).

---

<sup>27</sup> Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924).

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

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

## Amendment 20

### Proposal for a regulation Recital 28

#### *Text proposed by the Commission*

(28) Directive (EU) 2022/2555 requires Member States to designate or establish one or more cyber crisis management authorities and ensure they have adequate resources to carry out their tasks in an effective and efficient manner. It also requires Member States to identify capabilities, assets and procedures that can be deployed in the case of a crisis as well as to adopt a national large-scale

#### *Amendment*

(28) Directive (EU) 2022/2555 requires Member States to designate or establish one or more cyber crisis management authorities and ensure they have adequate resources to carry out their tasks in an effective and efficient manner. It also requires Member States to identify capabilities, assets and procedures that can be deployed in the case of a crisis as well as to adopt a national large-scale



cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. Member States are also required to establish one or more CSIRTs tasked with incident handling responsibilities in accordance with a well-defined process and covering at least the sectors, subsectors and types of entities under the scope of that Directive, and to ensure they have adequate resources to carry out effectively their tasks. This Regulation is without prejudice to the Commission's role in ensuring the compliance by Member States with the obligations of Directive (EU) 2022/2555. The Cyber Emergency Mechanism should provide assistance for actions aimed at reinforcing preparedness as well as incident response actions to mitigate the impact of significant and large-scale cybersecurity incidents, to support immediate recovery and/or restore the functioning of essential services.

cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. Member States are also required to establish one or more CSIRTs tasked with incident handling responsibilities in accordance with a well-defined process and covering at least the sectors, subsectors and types of entities under the scope of that Directive, and to ensure they have adequate resources to carry out effectively their tasks. This Regulation is without prejudice to the Commission's role in ensuring the compliance by Member States with the obligations of Directive (EU) 2022/2555. The Cyber Emergency Mechanism should provide assistance for actions aimed at reinforcing preparedness as well as incident response actions to mitigate the impact of significant and large-scale cybersecurity incidents, to support immediate recovery and/or restore the functioning of essential services, ***making appropriate use of the whole range of defensive options available to the civilian and military communities.***

## Amendment 21

### Proposal for a regulation Recital 29

#### *Text proposed by the Commission*

(29) As part of the preparedness actions, to promote a consistent approach and strengthen security across the Union and its internal market, support should be provided for testing and assessing cybersecurity of entities operating in highly critical sectors identified pursuant to Directive (EU) 2022/2555 in a coordinated manner. For this purpose, the Commission, with the support of ENISA and in cooperation with the NIS Cooperation Group established by Directive (EU) 2022/2555, should regularly identify

#### *Amendment*

(29) As part of the preparedness actions, to promote a consistent approach and strengthen security across the Union and its internal market, support should be provided for testing and assessing cybersecurity of entities operating in highly critical sectors identified pursuant to Directive (EU) 2022/2555 in a coordinated manner. For this purpose, the Commission, with the support of ENISA and in cooperation with the NIS Cooperation Group established by Directive (EU) 2022/2555, should regularly identify

relevant sectors or subsectors, which should be eligible to receive financial support for coordinated testing at Union level. **The** sectors or subsectors should be selected from Annex I to Directive (EU) 2022/2555 ('Sectors of High Criticality'). The coordinated testing exercises should be based on common risk scenarios and methodologies. The selection of sectors and development of risk scenarios should take into account relevant Union-wide risk assessments and risk scenarios, including the need to avoid duplication, such as the risk evaluation and risk scenarios called for in the Council conclusions on the development of the European Union's cyber posture to be conducted by the Commission, the High Representative and the NIS Cooperation Group, in coordination with relevant civilian and military bodies and agencies and established networks, including the EU CyCLONe, as well as the risk assessment of communications networks and infrastructures requested by the Joint Ministerial Call of Nevers and conducted by the NIS Cooperation Group, with the support of the Commission and ENISA, and in cooperation with the Body of European Regulators for Electronic Communications (BEREC), the coordinated risk assessments to be conducted under Article 22 of Directive (EU) 2022/2555 and digital operational resilience testing as provided for in Regulation (EU) 2022/2554 of the European Parliament and of the Council<sup>29</sup>. The selection of sectors should also take into account the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.

relevant sectors or subsectors, which should be eligible to receive financial support for coordinated testing at Union level. **When appropriate, the European External Action Service (EEAS), in particular through the EU Intelligence Centre (INTCEN) and its Hybrid Fusion Cell, with the support of the Intelligence Directorate of the European Union Military Staff (EUMS) under the Single Intelligence Analysis Capability (SIAC), should also be associated to provide up-to-date assessments and thus contribute to the identification of the** sectors or subsectors **that** should be selected from Annex I to Directive (EU) 2022/2555 ('Sectors of High Criticality'). The coordinated testing exercises should be based on common risk scenarios and methodologies. **These exercises should also play an important role in improving cooperation between civilian and military entities. When organising exercises, the Commission, the EEAS and ENISA should therefore systematically consider including participants from other cyber communities, as such the European Defence Agency (EDA) and other relevant entities.** The selection of sectors and development of risk scenarios should take into account relevant Union-wide risk assessments and risk scenarios, including the need to avoid duplication, such as the risk evaluation and risk scenarios called for in the Council conclusions on the development of the European Union's cyber posture to be conducted by the Commission, the High Representative and the NIS Cooperation Group, in coordination with relevant civilian and military bodies and agencies and established networks, including the EU CyCLONe, as well as the risk assessment of communications networks and infrastructures requested by the Joint Ministerial Call of Nevers and conducted by the NIS Cooperation Group, with the support of the Commission and ENISA, and in cooperation with the Body of

European Regulators for Electronic Communications (BEREC), the coordinated risk assessments to be conducted under Article 22 of Directive (EU) 2022/2555 and digital operational resilience testing as provided for in Regulation (EU) 2022/2554 of the European Parliament and of the Council<sup>[1]</sup>. The selection of sectors should also take into account the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.

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

---

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

---

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

## **Amendment 22**

### **Proposal for a regulation Recital 32**

#### *Text proposed by the Commission*

(32) The Cyber Emergency Mechanism should support assistance provided by Member States to a Member State affected by a significant or large-scale cybersecurity incident, including by the CSIRTs network set out in Article 15 of Directive (EU) 2022/2555. Member States providing assistance should be allowed to submit requests to cover costs related to

#### *Amendment*

(32) The Cyber Emergency Mechanism should support assistance provided by Member States to a Member State affected by a significant or large-scale cybersecurity incident, including by the CSIRTs network set out in Article 15 of Directive (EU) 2022/2555. Member States providing assistance should be allowed to submit requests to cover costs related to

dispatching of expert teams in the framework of mutual assistance. The eligible costs could include travel, accommodation and daily allowance expenses of cybersecurity experts.

dispatching of expert teams in the framework of mutual assistance, ***ensuring efficient coordination among the EU's relevant programmes and instruments, including the European Peace Facility (EPF), CFSP and NDICI, when providing assistance to third countries, particularly Ukraine and Moldova.*** The eligible costs could include travel, accommodation and daily allowance expenses of cybersecurity experts.

## Amendment 23

### Proposal for a regulation Recital 33

#### *Text proposed by the Commission*

(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.

#### *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, ***including CSDP missions*** under similar conditions.

## Amendment 24

### Proposal for a regulation Recital 34

*Text proposed by the Commission*

(34) For the purpose of selecting private service providers to provide services in the context of the EU Cybersecurity Reserve, it is necessary to establish a set of minimum criteria that should be included in the call for tenders to select these providers, so as to ensure that the needs of Member States' authorities and entities operating in critical or highly critical sectors are met.

*Amendment*

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

## Amendment 25

### Proposal for a regulation Recital 36

*Text proposed by the Commission*

(36) In order to support the objectives of this Regulation of promoting shared situational awareness, enhancing Union's resilience and enabling effective response to significant and large-scale cybersecurity incidents, the EU=CyCLONe, the CSIRTs network or the Commission should be able to ask ENISA to review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. After the completion of a review and assessment of an incident, ENISA should prepare an incident review report, in collaboration with relevant stakeholders, including representatives from the private sector, Member States, the Commission and other relevant EU institutions, bodies and

*Amendment*

(36) In order to support the objectives of this Regulation of promoting shared situational awareness, enhancing Union's resilience and enabling effective response to significant and large-scale cybersecurity incidents, the EU=CyCLONe, the CSIRTs network or the Commission should be able to ask ENISA to review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. ***In view of the development of a secure connectivity system, building on the European quantum communication infrastructure (EuroQCI) and the European Union Governmental Satellite Communication (GOVSATCOM), in particular the implementation of GALILEO GNSS for***

agencies. As regards the private sector, ENISA is developing channels for exchanging information with specialised providers, including providers of managed security solutions and vendors, in order to contribute to ENISA's mission of achieving a high common level of cybersecurity across the Union. Building on the collaboration with stakeholders, including the private sector, the review report on specific incidents should aim at assessing the causes, impacts and mitigations of an incident, after it has occurred. Particular attention should be paid to the input and lessons shared by the managed security service providers that fulfil the conditions of highest professional integrity, impartiality and requisite technical expertise as required by this Regulation. The report should be delivered and feed into the work of the EU=CyCLONe, the CSIRTs network and the Commission. When the incident relates to a third country, it will also be shared by the Commission with the High Representative.

*defence users, any future possible development should take into account the advent of 'hyperwar' which merges the speed and sophistication of quantum computing with highly autonomous military systems* After the completion of a review and assessment of an incident, ENISA should prepare an incident review report, in collaboration with relevant stakeholders, including representatives from the private sector, Member States, the Commission and other relevant EU institutions, bodies and agencies. As regards the private sector, ENISA is developing channels for exchanging information with specialised providers, including providers of managed security solutions and vendors, in order to contribute to ENISA's mission of achieving a high common level of cybersecurity across the Union. Building on the collaboration with stakeholders, including the private sector, the review report on specific incidents should aim at assessing the causes, impacts and mitigations of an incident, after it has occurred. Particular attention should be paid to the input and lessons shared by the managed security service providers that fulfil the conditions of highest professional integrity, impartiality and requisite technical expertise as required by this Regulation. The report should be delivered and feed into the work of the EU=CyCLONe, the CSIRTs network and the Commission. When the incident relates to a third country, it will also be shared by the Commission with the High Representative, *the EEAS and any CSDP Mission in the country affected by the incident through their headquarters.*

## Amendment 26

### Proposal for a regulation Recital 37



*Text proposed by the Commission*

(37) Taking into account the unpredictable nature of cybersecurity attacks and the fact that they are often not contained in a specific geographical area and pose high risk of spill-over, the strengthening of resilience of neighbouring countries and their capacity to respond effectively to significant and large-scale cybersecurity incidents contributes to the protection of the Union as a whole. Therefore, third countries associated to the DEP *may* be supported from the EU Cybersecurity Reserve, where *this is provided for in the respective association agreement to DEP*. The funding for associated third countries should be supported by the Union in the framework of relevant partnerships and funding instruments for those countries. The support should cover services in the area of response to and immediate recovery from significant or large-scale cybersecurity incidents. The conditions set for the EU Cybersecurity Reserve and trusted providers in this Regulation should apply when providing support to the third countries associated to DEP.

**Amendment 27**

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

*Text proposed by the Commission*

(c) the establishment of a European Cybersecurity Incident Review Mechanism to review and assess significant or large-

*Amendment*

(37) Taking into account the unpredictable nature of cybersecurity attacks and the fact that they are often not contained in a specific geographical area and pose high risk of spill-over, the strengthening of resilience of neighbouring countries, *particularly Ukraine and Moldova*, and their capacity to respond effectively to significant and large-scale cybersecurity incidents contributes to the protection of the Union as a whole. Therefore, third countries associated to the DEP *should* be supported from the EU Cybersecurity Reserve. *The support should also apply to those third countries where a CSDP Mission is deployed with a specific mandate to strengthen the resilience to hybrid threats including cyber or where an EPF Assistance Measure has been adopted to strengthen the cyber resilience of the country*. The funding for associated third countries should be supported by the Union in the framework of relevant partnerships and funding instruments for those countries. The support should cover services in the area of response to and immediate recovery from significant or large-scale cybersecurity incidents. The conditions set for the EU Cybersecurity Reserve and trusted providers in this Regulation should apply when providing support to the third countries associated to DEP.

*Amendment*

(c) the establishment of a European Cybersecurity Incident Review Mechanism to review and assess significant or large-



scale incidents.

scale incidents *or threats*.

## Amendment 28

### Proposal for a regulation

#### Article 1 – paragraph 2 – point a

*Text proposed by the Commission*

(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;

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

## Amendment 29

### Proposal for a regulation

#### Article 1 – paragraph 2 – point b

*Text proposed by the Commission*

(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’);

*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’) ***or those third countries which are candidates for accession and do not contravene the security and defence interests of the Union and its Member States as established in the framework of the CFSP pursuant to Title V of the TEU; Member States should consider an active cyber defence programme to be part of their national cybersecurity strategy that incorporates regular joint training exercises between Member States and across international organisations. Such a***

*programme should provide a synchronised, real-time capability to discover, detect, analyse, and mitigate threats;*

### **Amendment 30**

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

*Text proposed by the Commission*

*Amendment*

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

### **Amendment 31**

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

*Text proposed by the Commission*

*Amendment*

**‘cyber defence community’ means Member States’ defence authorities and supported by EU institutions, bodies and agencies as sets out in the Joint Communication on EU Policy on Cyber Defence[1]**

**[1] Joint Communication to the European Parliament and the Council EU Policy on Cyber Defence JOIN/2022/49 final**

### **Amendment 32**

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

*Text proposed by the Commission*

*Amendment*

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

## Amendment 33

### Proposal for a regulation

#### Article 3 – paragraph 2 – subparagraph 1 – point d a (new)

*Text proposed by the Commission*

*Amendment*

*(d a) review and evaluate critical cybersecurity technologies and equipment deployed by SOCs in responding to cybersecurity incidents for systemic risks from control over high-risk providers by countries which would contravene the security and defence interests of the Union and its Member States as established in the framework of the CFSP pursuant to Title V of the TEU.*

## Amendment 34

### Proposal for a regulation

#### Article 4 – paragraph 1 – subparagraph 2

*Text proposed by the Commission*

*Amendment*

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

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

## Amendment 35

### Proposal for a regulation Article 4 – paragraph 2

#### *Text proposed by the Commission*

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.

#### *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, ***under the strict condition that such tools and infrastructure are provided by trusted providers in accordance with Art. 16.*** The Union financial contribution shall cover up to 50% of the acquisition costs of the tools and infrastructures, and up to 50% of the operation costs, with the remaining costs to be covered by the Member State. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the National SOC shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

## Amendment 36

### Proposal for a regulation Article 5 – paragraph 2

#### *Text proposed by the Commission*

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

#### *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, ***under the strict condition that such tools and infrastructure are provided by trusted providers in accordance with Art. 16.*** The Union

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.

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

### Amendment 37

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

*Text proposed by the Commission*

*Amendment*

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

### Amendment 38

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

*Text proposed by the Commission*

*Amendment*

**(b a) directly supports strengthening the military and defence capabilities of the participating members or prevents a direct and imminent threat to their security. While the exploitation of vulnerabilities in defence sector may cause significant disruption and harm, cyber security of defence industry requires special measures to ensure the security of the supply chains, particularly entities lower in supply chains, which do not require access to classified information, but that could carry serious risks to the entire sector. Special consideration should be given to the impact any breach could have and the threat of any potential manipulation of network data that could**

*render critical defence assets useless or even override their operating systems making them vulnerable to hijacking.*

## Amendment 39

### Proposal for a regulation

#### Article 6 – paragraph 1 – point b a (new)

*Text proposed by the Commission*

*Amendment*

*(b b) supports strengthening the defence capabilities of the participating members or prevents a direct and imminent threat to their security, ensuring the security of the supply chains, in particular those entities lower in supply chains, which do not require access to classified information, but that could carry serious risks to the entire sector.*

## Amendment 40

### Proposal for a regulation

#### Article 7 – paragraph 1

*Text proposed by the Commission*

*Amendment*

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

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

## Amendment 41

### Proposal for a regulation

#### Article 8 – paragraph 1

*Text proposed by the Commission*

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.

*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, ***de-risking and promoting EU's technological edge in critical sectors, including measures to restrict or exclude high-risk suppliers, as well as protect the security*** of data exchanged through the infrastructure.

**Amendment 42**

**Proposal for a regulation  
Article 8 – paragraph 2**

*Text proposed by the Commission*

2. Member States participating in the European Cyber Shield shall ensure that the sharing of information within the European Cyber Shield with entities which are not Member State public bodies does not negatively affect the security interests of the Union.

*Amendment*

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

**Amendment 43**

**Proposal for a regulation  
Article 8 – paragraph 3**

*Text proposed by the Commission*

3. The Commission may adopt implementing acts laying down technical requirements for Member States to comply

*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.

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

#### **Amendment 44**

##### **Proposal for a regulation Article 9 – paragraph 2**

*Text proposed by the Commission*

2. Actions implementing the Cyber Emergency Mechanism shall be supported by funding from DEP and implemented in accordance with Regulation (EU) 2021/694 and in particular Specific Objective 3 thereof.

*Amendment*

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

#### **Amendment 45**

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

*Text proposed by the Commission*

(a) preparedness actions, including the coordinated preparedness testing of entities operating in highly critical sectors across the Union;

*Amendment*

(a) preparedness actions, including the coordinated preparedness testing of entities operating in highly critical sectors, ***such as public infrastructure, election infrastructure, transport, healthcare financial, telecommunication, food supply***

*and security* across the Union;

#### **Amendment 46**

##### **Proposal for a regulation**

##### **Article 10 – paragraph 1 – point c**

*Text proposed by the Commission*

(c) mutual assistance actions consisting of the provision of assistance from national authorities of one Member State to another Member State, in particular as provided for in Article 11(3), point (f), of Directive (EU) 2022/2555.

*Amendment*

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

#### **Amendment 47**

##### **Proposal for a regulation**

##### **Article 10 – paragraph 1 – point c a (new)**

*Text proposed by the Commission*

*Amendment*

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

#### **Amendment 48**

##### **Proposal for a regulation**

##### **Article 11 – paragraph 2**

*Text proposed by the Commission*

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.

*Amendment*

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

## Amendment 49

### Proposal for a regulation Article 12 – paragraph 2

*Text proposed by the Commission*

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.

*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 ***and third countries, which satisfy the applicable requirements of this Regulation.***

## Amendment 50

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

*Text proposed by the Commission*

(b) Union institutions, bodies and agencies.

*Amendment*

(b) Union institutions, bodies and agencies, ***including CSDP missions.***

## Amendment 51

### Proposal for a regulation Article 12 – paragraph 4

*Text proposed by the Commission*

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.

*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, ***such as public infrastructure, election infrastructure, transport, healthcare financial, telecommunication, food supply and security.***

## Amendment 52

### Proposal for a regulation Article 12 – paragraph 5

*Text proposed by the Commission*

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.

*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 ***and objectives, in particular the strategic objective of reducing dependencies on high-risk suppliers, which would contravene the security and defence interests of the Union and its Member States as established in the framework of the CFSP pursuant to Title V of the TEU.***

## Amendment 53

### Proposal for a regulation Article 12 – paragraph 7

*Text proposed by the Commission*

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.

*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, ***supported by the EEAS.*** The Commission, where relevant, shall consult

the High Representative.

## Amendment 54

### Proposal for a regulation

#### Article 14 – paragraph 2 – point a a (new)

*Text proposed by the Commission*

*Amendment*

**(aa) the impact of the incident on the security and defence of the Union;**

## Amendment 55

### Proposal for a regulation

#### Article 15 – paragraph 3

*Text proposed by the Commission*

*Amendment*

3. In consultation with the High Representative, support under the Cyber Emergency Mechanism may complement assistance provided in the context of the Common Foreign and Security Policy and Common Security and Defence Policy, including through the Cyber Rapid Response Teams. It may also complement or contribute to assistance provided by one Member State to another Member State in the context of Article 42(7) of the Treaty on the European Union.

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

## Amendment 56

### Proposal for a regulation

#### Article 16 – paragraph 2 – point b a (new)

*Text proposed by the Commission*

*Amendment*

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

## **Amendment 57**

### **Proposal for a regulation**

#### **Article 16 – paragraph 2 – point f**

*Text proposed by the Commission*

(f) the provider shall be equipped with the hardware and software technical equipment necessary to support the requested service;

*Amendment*

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

## **Amendment 58**

### **Proposal for a regulation**

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

*Text proposed by the Commission*

*Amendment*

**(j a) No provider originating in a high-risk third country shall be admissible.**

## **Amendment 59**

### **Proposal for a regulation**

#### **Article 16 – paragraph 2 – point j b (new)**

*Text proposed by the Commission*

*Amendment*

**(j b) the provider shall be in close cooperation with relevant SMEs, where possible;**

## Amendment 60

### Proposal for a regulation Article 17 – paragraph 1

*Text proposed by the Commission*

1. Third countries may request support from the EU Cybersecurity Reserve where Association Agreements concluded regarding their participation in DEP provide for this.

*Amendment*

1. Third countries may request support from the EU Cybersecurity Reserve where:

*a) Association Agreements concluded regarding their participation in DEP provide for this;*

*b) those third countries where a CSDP Mission is deployed with a specific mandate to strengthen the resilience to hybrid threats including cyber or where an EPF Assistance Measure has been adopted to strengthen the cyber resilience of the country.*

## Amendment 61

### Proposal for a regulation Article 17 – paragraph 2

*Text proposed by the Commission*

2. Support from the EU Cybersecurity Reserve shall be in accordance with this Regulation, and shall comply with any specific conditions laid down in the Association Agreements referred to in paragraph 1.

*Amendment*

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

## Amendment 62

### Proposal for a regulation Article 18 – paragraph 1



*Text proposed by the Commission*

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.

*Amendment*

1. At the request of the Commission, the EU-CyCLONE or the CSIRTs network, ENISA shall review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. Following the completion of a review and assessment of an incident, ENISA shall deliver an incident review report to the CSIRTs network, the EU-CyCLONE and the Commission to support them in carrying out their tasks, in particular in view of those set out in Articles 15 and 16 of Directive (EU) 2022/2555. Where relevant, ***especially when the incident relates to a third country*** the Commission shall share the report with the High Representative ***and the EEAS***.

**Amendment 63**

**Proposal for a regulation**

**Article 18 – paragraph 3 a (new)**

*Text proposed by the Commission*

*Amendment*

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

**Amendment 64**

**Proposal for a regulation**

**Article 19 – paragraph 1 – point 1 – point a – point 1**

Regulation (EU) 2021/694

Article 6, paragraph 1

*Text proposed by the Commission*

*Amendment*

(aa) support the development of an EU Cyber Shield, including the development, deployment and operation of National and Cross-border SOCs platforms that

(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;

contribute to situational awareness in the Union and to enhancing the cyber threat intelligence capacities of the Union ***and reducing the Union's dependency on high-risk providers of critical cybersecurity equipment or components, which would contravene the security and defence interests of the Union and its Member States as established in the framework of the CFSP pursuant to Title V of the TEU;***

## Amendment 65

### Proposal for a regulation Article 20 – paragraph 1

*Text proposed by the Commission*

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.

*Amendment*

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

## PROCEDURE – COMMITTEE ASKED FOR OPINION

<b>Title</b>	Laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents
<b>References</b>	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
<b>Committee responsible</b> Date announced in plenary	ITRE 1.6.2023
<b>Opinion by</b> Date announced in plenary	AFET 1.6.2023
<b>Rapporteur for the opinion</b> Date appointed	Dragoş Tudorache 16.6.2023
<b>Discussed in committee</b>	18.9.2023
<b>Date adopted</b>	24.10.2023
<b>Result of final vote</b>	+: 39 –: 4 0: 0
<b>Members present for the final vote</b>	Alexander Alexandrov Yordanov, Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Włodzimierz Cimoszewicz, Katalin Cseh, Michael Gahler, Giorgos Georgiou, Sunčana Glavak, Bernard Guetta, Sandra Kalniete, Dietmar Köster, Andrius Kubilius, David Lega, Leopoldo López Gil, Jaak Madison, Pedro Marques, David McAllister, Vangelis Meimarakis, Sven Mikser, Francisco José Millán Mon, Matjaž Nemeč, Demetris Papadakis, Kostas Papadakis, Tonino Picula, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Jordi Solé, Sergei Stanishev, Tineke Strik, Dominik Tarczyński, Dragoş Tudorache, Thomas Waitz, Bernhard Zimniok, Željana Zovko
<b>Substitutes present for the final vote</b>	Attila Ara-Kovács, Lars Patrick Berg, Andrey Kovatchev, Georgios Kyrtos, Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace

## FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

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

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

0	0

Key to symbols:

+ : in favour

- : against

0 : abstention

25.10.2023

## OPINION OF THE COMMITTEE ON TRANSPORT AND TOURISM

for the Committee on Industry, Research and Energy

on the proposal for a regulation of the European Parliament and of the Council on Measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents

(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Rapporteur for opinion: Gheorghe Falcă

### SHORT JUSTIFICATION

Organizations affected by cyberattacks, including in the transport sector, rarely report them, especially private sector companies, since they tend to see them as ‘bad publicity’. Most organizations prefer to deal with them internally and it is often the attackers who publicize them. In the EU, the good news is that the entry into force of Directive 2022/2555 on network security (known as the ‘NIS2 Directive’), which Member States have until October 2024 to transpose, harmonises the incident reporting obligations across the Member States. Therefore, a better understanding of the nature and scale of the problem is likely to emerge in coming years.

The European Union Agency for Cybersecurity (ENISA) published a recent report<sup>1</sup> that provides information on cybersecurity threats in the transport sector, where it emphasizes that cybercriminals were responsible for more than half of the incidents observed in the 2022 reporting period (55%) and that the leading motivation behind these attacks was financial gain. It also notes that most cyber-attacks in the transport sector target IT systems, causing operational disruptions.

As regards preparedness and response to cybersecurity incidents, there is currently limited support at Union level and solidarity between Member States. The Council Conclusions of May 2022 highlighted the need to address these gaps, by calling for the Commission to present a proposal on a new **Emergency Response Fund for Cybersecurity**<sup>2</sup>.

This Regulation implements the **EU Cybersecurity Strategy** adopted in December 2020 that announced the creation of a **European Cyber Shield**, reinforcing the cyber threat detection and information sharing capabilities in the European Union through a federation of national and

---

<sup>1</sup> [“Understanding Cyber Threats in Transport”](#), ENISA, published March 21, 2023.

<sup>2</sup> Council conclusions on the development of the European Union's cyber posture of 23 May 2022, (9364/22).

cross-border Security Operations Centres (SOCs). The actions of this Regulation will be supported by **funding under ‘Cybersecurity’ Strategic Objective of DEP (Digital Europe Programme)**.

The total budget includes an increase of EUR 100 million that this Regulation proposes to re-allocate from other strategic objectives of DEP. This will bring the new total amount available for cybersecurity actions under DEP to EUR 842.8 million.

Part of the additional EUR 100 million will reinforce the budget managed by the European Cybersecurity Competence Centre (ECCC) to implement actions on SOCs and preparedness as part of their work programme(s). Moreover, the additional funding will serve to support the establishment of the EU Cybersecurity Reserve. It complements the budget already foreseen for similar actions in the main DEP and Cybersecurity DEP Work Programme for the 2023-2027 period which could boost the total amount to 551 million for 2023-2027, while 115 million were dedicated already in the form of pilots for 2021-2022. Including Member States contributions, the overall budget could amount up to 1.109 billion euros.

## Rapporteur's position

Your rapporteur welcomes the new proposal and believes that it will offer significant benefits to the various stakeholders. The rapporteur underlines the necessity for a deeper understanding of the cybersecurity needs and requirements of transportation, as well as for providing transport critical entities with access to proper funding for preparedness, response and solving incidents.

Your rapporteur endorses the 'transport cybersecurity toolkit', which aims at contributing to greater levels of cyber-awareness and cyber-hygiene, with a specific focus on the transport sector. It addresses transport organisations, regardless of their size and domain of activity, as well as taking into account transport critical infrastructure and military mobility, particularly having regards the war in Ukraine, especially but not limited to:

- Air carriers, airport managing bodies, core airports, air traffic management and air traffic control centres, the European Union Aviation Safety Agency and Eurocontrol;
- Infrastructure managers, railway undertakings and the European Rail Traffic Management System (ERTMS);
- Inland, sea and coastal passenger and freight water transport companies, managing bodies of ports, including their port facilities, entities operating works and equipment contained within ports, operators of vessel traffic services;
- Road authorities responsible for traffic management control, operators of Intelligent Transport Systems;
- Postal and courier services.

Your Rapporteur believes that the size of the budget for the functioning of the **Emergency Response Fund for Cybersecurity** (ERFC) will determine its success; therefore, it should be sufficiently large to support Member States in **preparing for, responding to and recovering from** significant and large-scale cybersecurity incidents. Support for incident response shall also be made available to institutions, bodies, offices and agencies of the Union.

The **European Cyber Shield** will improve the cyber threat detection capabilities of the Member States. The **Cyber Emergency Mechanism** will complement Member States' actions through emergency support for preparedness, response and immediate recovery/restoration of the functioning of essential services.



## AMENDMENT

The Committee on Transport and Tourism calls on the Committee on Industry, Research and Energy, as the committee responsible, to take the following into account:

### Amendment 1

#### Proposal for a regulation

##### Recital 2

###### *Text proposed by the Commission*

(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.

###### *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, ***as well as critical IT and physical infrastructure***. 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, ***of public and private transport***, 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 as well as to mobility within*** 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.

## Amendment 2

### Proposal for a regulation Recital 2 a (new)

*Text proposed by the Commission*

*Amendment*

***(2a) An increasingly serious cybersecurity threat is posed to the transport sector by state-sponsored actors, cybercriminals and hacktivists targeting authorities, operators, manufacturers, suppliers and service providers in aviation, maritime, railway and road transport. The European Union Agency for Cybersecurity (ENISA) has observed a 25% increase in the monthly average number of reported incidents affecting the transport sector in 2022, compared to 2021 levels. A majority of the attacks on the transport sector targets information technology (IT) systems, with possible operational disruptions occurring as a result<sup>14a</sup>.***

---

<sup>14b</sup> ENISA (2023), ENISA threat landscape: Transport sector, pages 7 and 17.

## Amendment 3

### Proposal for a regulation Recital 2 b (new)

*Text proposed by the Commission*

*Amendment*

***(2b) Russia's unprovoked invasion of Ukraine determined a significant increase of cybersecurity incidents, including distributed denial-of-service (DDoS) cyber attacks, targeting the transport sector in the EU and areas close to the EU, mainly airports, railways and transport authorities<sup>14b</sup>. This increase in attacks is highly likely to continue.***

<sup>14b</sup> ENISA (2023), ENISA threat landscape: Transport sector, page 9.

#### Amendment 4

##### Proposal for a regulation Recital 2 c (new)

*Text proposed by the Commission*

*Amendment*

**(2c) Cyberattacks target authorities and bodies in all transport subsectors, with railway undertakings and infrastructure managers as well as port operators being affected. As regards the road sector, original equipment manufacturers (OEMs), suppliers and service providers were targeted, along with public transport operators. In the aviation sector, the main targets were airlines and airport operators, followed by service providers, surface transport operators and the supply chain<sup>14c</sup>.**

---

<sup>14c</sup> ENISA (2023), ENISA threat landscape: Transport sector, page 17.

#### Amendment 5

##### 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<sup>16</sup>, it is necessary to increase the resilience of citizens, businesses and entities operating critical infrastructures against the growing cybersecurity threats,

(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<sup>16</sup>, it is necessary to increase the resilience of citizens, businesses, **transport operators** and entities operating critical infrastructures against the growing

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.

---

<sup>16</sup> <https://futureu.europa.eu/en/>

## Amendment 6

### Proposal for a regulation

#### Recital 4

##### *Text proposed by the Commission*

(4) The Union has already taken a number of measures to reduce vulnerabilities and increase the resilience of critical infrastructures and entities against cybersecurity risks, in particular Directive (EU) 2022/2555 of the European Parliament and of the Council<sup>17</sup>, Commission Recommendation (EU) 2017/1584<sup>18</sup>, Directive 2013/40/EU of the European Parliament and of the Council<sup>19</sup> and Regulation (EU) 2019/881 of the European Parliament and of the Council<sup>20</sup>. In addition, the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure invites Member States to take urgent and effective measures, and to cooperate loyally, efficiently, in solidarity and in a coordinated manner with each other, the Commission and other relevant

cybersecurity threats, which can have devastating societal and economic impacts. Therefore, investment in infrastructures and services that will support faster detection and response to cybersecurity threats and incidents is needed, and Member States need assistance in better preparing for, as well as responding to significant and large-scale cybersecurity incidents. The Union should also increase its capacities in these areas, notably as regards the collection and analysis of data on cybersecurity threats and incidents ***as well as on the state and the evolution of the cybersecurity labour market as it plays an instrumental role in providing the necessary detection and response services.***

---

<sup>16</sup> <https://futureu.europa.eu/en/>

##### *Amendment*

(4) The Union has already taken a number of measures to reduce vulnerabilities and increase the resilience of critical infrastructures and entities against cybersecurity risks, in particular Directive (EU) 2022/2555 of the European Parliament and of the Council<sup>17</sup>, Commission Recommendation (EU) 2017/1584<sup>18</sup>, Directive 2013/40/EU of the European Parliament and of the Council<sup>19</sup> and Regulation (EU) 2019/881 of the European Parliament and of the Council<sup>20</sup> ***as well as the proposal for a Regulation on guidelines for the development of the trans-European transport network, and the proposal for a regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act).*** In addition, the Council Recommendation on

public authorities as well as the entities concerned, to enhance the resilience of critical infrastructure used to provide essential services in the internal market.

a Union-wide coordinated approach to strengthen the resilience of critical infrastructure invites Member States to take urgent and effective measures, and to cooperate loyally, efficiently, in solidarity and in a coordinated manner with each other, the Commission and other relevant public authorities as well as the entities concerned, to enhance the resilience of critical infrastructure used to provide essential services in the internal market.

---

<sup>17</sup> Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022).

---

<sup>17</sup> Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022).

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

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

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

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

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

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

## **Amendment 7**

### **Proposal for a regulation Recital 4 a (new)**

**(4a) While welcoming the European Commission’s Transport Cybersecurity Toolkit<sup>2a</sup>, which contains basic information on threats that may affect transport organisations (malware diffusion, denial of service, unauthorised access and theft, and software manipulation) and lists good mitigating practices, transport operators should be provided with proper training on cybersecurity and with proper tools to prevent cyber threats. The Union budget should also cover the support, such as training, provided by ENISA to enable the effective implementation by transport operators of best mitigating practices included in the Toolkit.**

---

<sup>1a</sup> *ENISA threat landscape: transport sector / ENISA, March 2023*

<sup>2a</sup> *European Commission, (2021). Transport Cybersecurity Toolkit, available at [https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity\\_en](https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_en)*

## **Amendment 8**

### **Proposal for a regulation Recital 4 a (new)**

**(4a) A Union-wide coordinated approach to strengthen the preparedness and resilience of critical infrastructure, such as transport infrastructure, is based on the Member States’ capacity building. As acknowledged in the recent Communication from the Commission to the European Parliament and the Council on Closing the cybersecurity talent gap to boost the EU’s competitiveness, growth and resilience<sup>19a</sup>, the security of the EU**

*cannot be guaranteed without the EU's most valuable asset: its people.*

---

*<sup>19a</sup> Communication from the Commission to the European Parliament and the Council on Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience ('The Cybersecurity Skills Academy') COM(2023) 207 final*

## Amendment 9

### Proposal for a regulation

#### Recital 12

*Text proposed by the Commission*

(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 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

*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. ***These critical assets and infrastructures include Intelligent Transport Systems, which, whilst essential for automated and multimodal mobility, operate on the basis of crucial exchanges of sensitive data.*** 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 incidents and thus complement and support



Parliament and of the Council<sup>24</sup> .

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<sup>24</sup> .

---

<sup>24</sup> 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).

---

<sup>24</sup> 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).

## Amendment 10

### Proposal for a regulation Recital 14 a (new)

*Text proposed by the Commission*

*Amendment*

***(14a) The transport sector is increasingly becoming one of the most lucrative businesses for cybercriminals, with customer data considered a highly valuable commodity and with the transport supply chain becoming more and more targeted. For this reason, transport infrastructure characterised by a cross-border nature or by data exchange through wireless technologies should be considered a pivotal object of analysis and monitoring for both national and, particularly, for Cross-border SOCs. For instance, the recent proposal revising the TEN-T Regulation requires greater solidarity and cooperation in sharing information on cross-border cyber threats that this transnational network might face. Similarly, Intelligent Transport Systems (ITS) are vital to make transport safer, more efficient and more sustainable, yet they make transport systems more vulnerable to cyber attacks***

*that can create accidents, traffic jams or cause economic losses to both private and public operators. In order to safeguard the safety of passengers, the protection of users' and providers' data and to avoid financial damages, it is essential that the implementation programme of the revised directive on Intelligent Transport Systems includes provisions and tools to strengthen the collaboration among Member States to detect, prepare for and respond to cybersecurity threats and incidents.*

## **Amendment 11**

### **Proposal for a regulation**

#### **Recital 15**

*Text proposed by the Commission*

(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.

*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. ***In this regard, in order to strengthen the Union's autonomy in the cyber field and with reference to Article 47 (4) of the proposal for a Regulation on guidelines for the development of the trans-European transport network (COM(2021)0812), it is also necessary to prevent access to data leading to cyber threats by enforcing a robust regulatory framework that governs foreign***

*ownership and investments in critical infrastructure, like in transport.*

## Amendment 12

### Proposal for a regulation Recital 21

*Text proposed by the Commission*

(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 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.

*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 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. ***It should also enable synergies with the Action Plan on Military Mobility 2.0. A well-functioning military mobility network needs to be resilient, including in the context of cyber and other hybrid threats that could affect critical nodes in the transport system that are dual-use. For instance, a cyber-attack on systems used in airports, harbours or railroads or a cyber-attack on military assets could have major consequences. Thus, digitalising processes and procedures, including for the necessary civilian and military cooperation, will require the strengthening of computer information systems (CIS) against cyber***

*threats.*

## Amendment 13

### Proposal for a regulation

#### Recital 21 a (new)

*Text proposed by the Commission*

*Amendment*

***(21a) In case of a cybersecurity crisis, an effective exchange of information is pivotal to ensure situational awareness among the military and civilian transport sectors. This exchange of information should also stimulate cooperation between relevant sectoral authorities responsible for transport, competent cybersecurity authorities, SOCs and CSIRTs.***

## Amendment 14

### Proposal for a regulation

#### Recital 29

*Text proposed by the Commission*

*Amendment*

(29) As part of the preparedness actions, to promote a consistent approach and strengthen security across the Union and its internal market, support should be provided for testing and assessing cybersecurity of entities operating in highly critical sectors identified pursuant to Directive (EU) 2022/2555 in a coordinated manner. For this purpose, the Commission, with the support of ENISA and in cooperation with the NIS Cooperation Group established by Directive (EU) 2022/2555, should regularly identify relevant sectors or subsectors, which should be eligible to receive financial support for coordinated testing at Union level. The sectors or subsectors should be selected from Annex I to Directive (EU) 2022/2555 ('Sectors of High Criticality'). The coordinated testing exercises should be based on common risk scenarios and

(29) As part of the preparedness actions, to promote a consistent approach and strengthen security across the Union and its internal market, support should be provided for testing and assessing cybersecurity of entities operating in highly critical sectors identified pursuant to Directive (EU) 2022/2555 in a coordinated manner. For this purpose, the Commission, with the support of ENISA and in cooperation with the NIS Cooperation Group established by Directive (EU) 2022/2555, should regularly identify relevant sectors or subsectors, which should be eligible to receive financial support for coordinated testing at Union level. The sectors or subsectors should be selected from Annex I to Directive (EU) 2022/2555 ('Sectors of High Criticality'). ***Specific attention should be given to the transport sector and its subsectors (air,***

methodologies. The selection of sectors and development of risk scenarios should take into account relevant Union-wide risk assessments and risk scenarios, including the need to avoid duplication, such as the risk evaluation and risk scenarios called for in the Council conclusions on the development of the European Union's cyber posture to be conducted by the Commission, the High Representative and the NIS Cooperation Group, in coordination with relevant civilian and military bodies and agencies and established networks, including the EU CyCLONe, as well as the risk assessment of communications networks and infrastructures requested by the Joint Ministerial Call of Nevers and conducted by the NIS Cooperation Group, with the support of the Commission and ENISA, and in cooperation with the Body of European Regulators for Electronic Communications (BEREC), the coordinated risk assessments to be conducted under Article 22 of Directive (EU) 2022/2555 and digital operational resilience testing as provided for in Regulation (EU) 2022/2554 of the European Parliament and of the Council<sup>29</sup>. The selection of sectors should also take into account the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.

---

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

*rail, water, road), as they incorporate critical infrastructure where cyber incidents and attacks could severely undermine the safety of passengers and operators.* The coordinated testing exercises should be based on common risk scenarios and methodologies. The selection of sectors and development of risk scenarios should take into account relevant Union-wide risk assessments and risk scenarios, including the need to avoid duplication, such as the risk evaluation and risk scenarios called for in the Council conclusions on the development of the European Union's cyber posture to be conducted by the Commission, the High Representative and the NIS Cooperation Group, in coordination with relevant civilian and military bodies and agencies and established networks, including the EU CyCLONe, as well as the risk assessment of communications networks and infrastructures requested by the Joint Ministerial Call of Nevers and conducted by the NIS Cooperation Group, with the support of the Commission and ENISA, and in cooperation with the Body of European Regulators for Electronic Communications (BEREC), the coordinated risk assessments to be conducted under Article 22 of Directive (EU) 2022/2555 and digital operational resilience testing as provided for in Regulation (EU) 2022/2554 of the European Parliament and of the Council<sup>29</sup>. The selection of sectors should also take into account the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.

---

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

## **Amendment 15**

### **Proposal for a regulation**

#### **Recital 30 a (new)**

*Text proposed by the Commission*

*Amendment*

***(30a) With a view to the criticality of the sector and to the implications of cyberthreats on mobility and, in consequence, on human lives of passengers and pedestrians, the transport sector should be prioritised with regards to the coordinated preparedness testing of entities.***

## **Amendment 16**

### **Proposal for a regulation**

#### **Recital 35 a (new)**

*Text proposed by the Commission*

*Amendment*

***(35a) In view of the increased tasks and responsibilities given to ENISA by this proposal as well as by the proposal on the on Cyber Resilience Act, the adoption of the ENISA Amending budget 1/2022 for the Pilot Implementation of a Cybersecurity Support Action is necessary. Moreover, in view of the Union interests at stake, additional financial and human resources should be allocated to ENISA.***

## **Amendment 17**

### **Proposal for a regulation**

#### **Recital 38 a (new)**

*Text proposed by the Commission*

*Amendment*

***(38a) The development of skills and competences should therefore receive***

*centre stage, across all sectors, not least to those that are vulnerable to cybersecurity threats, such as staff working on mass transit or critical infrastructures, including train control systems and digital transport planning tools for all modes of transport. The introduction and further development of the cybersecurity culture is therefore paramount to the success of implementing this regulation for both citizens' awareness and specialists' knowledge across all critical infrastructure sectors.*

## Amendment 18

### Proposal for a regulation

#### Article 1 – paragraph 2 – point a

*Text proposed by the Commission*

(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;

*Amendment*

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

## Amendment 19

### Proposal for a regulation

#### Article 1 – paragraph 2 – point b

*Text proposed by the Commission*

(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

*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, **with particular attention to critical IT and physical infrastructure**, including by making Union cybersecurity incident response support



Programme ('DEP');

available for third countries associated to the Digital Europe Programme ('DEP');

## Amendment 20

### Proposal for a regulation

#### Article 1 – paragraph 2 – point c a (new)

*Text proposed by the Commission*

*Amendment*

***(ca) to strengthen the Union's preparedness, cooperation and efficacy in protecting transport infrastructure and services in Member States from cybersecurity incidents, to ensure the transport sector's continuous functioning, the integrity of supply chains and Union-wide mobility.***

## Amendment 21

### 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 for transport infrastructure characterised by a cross-border nature, such as the TEN-T, or by data exchange through wireless technologies, like Intelligent Transport Systems.***

## Amendment 22

### Proposal for a regulation

#### Article 3 – paragraph 2 – subparagraph 2

*Text proposed by the Commission*

*Amendment*

It shall be developed in cooperation with the pan-European High Performance Computing infrastructure established pursuant to Regulation (EU) 2021/1173.

It shall be developed in cooperation with the pan-European High Performance Computing infrastructure established pursuant to Regulation (EU) 2021/1173. ***It shall enable collaboration, via dedicated***

*protocols and standards, with the cyber defence community, to ensure the development of stronger civilian detection and situational awareness capabilities for the protection of critical infrastructure. In this regard, synergies shall be developed also with the Action Plan on Military Mobility 2.0, and an effective exchange of information shall be ensured to provide situational awareness among the military and civilian transport sectors.*

## Amendment 23

### Proposal for a regulation Article 8 – paragraph 2 a (new)

*Text proposed by the Commission*

*Amendment*

**2a.** *The Commission shall involve the European Cyber Shield, in particular the cross-border SOCs, in its opinion to Member States in the framework of the proposal for a Regulation on the trans-European transport network (COM(2021)0812) whenever the participation of or contribution of any kind by a natural person of a third country or an undertaking of a third country is likely to affect the cybersecurity of cross-border critical infrastructure, such as the TEN-T.*

## Amendment 24

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

*Text proposed by the Commission*

*Amendment*

(a) preparedness actions, including the coordinated preparedness testing of entities operating in highly critical sectors across the Union;

(a) preparedness actions, including the coordinated preparedness testing of entities operating in highly critical sectors across the Union, ***with specific attention to transport infrastructure and its subsectors included in Annex I to Directive (EU)***

## Amendment 25

### Proposal for a regulation Article 18 – paragraph 2

*Text proposed by the Commission*

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.

*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, ***including transport operators***. To support the review, ENISA may also consult other types of stakeholders. Consulted representatives shall disclose any potential conflict of interest.

## Amendment 26

### Proposal for a regulation Article 19 – paragraph 1 – point 1 – point b Regulation (EU) 2021/694 Article 6 – Paragraph 2a (new)

*Text proposed by the Commission*

*Amendment*

***2a. In view of the Union interests at stake, in relation to its responsibilities for the preparation of candidate certification schemes pursuant to Regulation (EU) 2019/881, its responsibilities to review and assess cyber threats, vulnerabilities and mitigation, prepare an incident review report for Cybersecurity Incident Review Mechanism, as well as to provide training against cyber attacks and incidents to operators of critical infrastructure and in light of its newly assigned responsibilities***

*in the framework of the Proposal on the Cyber Resilience Act, ENISA shall be provided with the necessary resources under the Union budget in accordance with the applicable legislation.*

## **Amendment 27**

### **Proposal for a regulation**

**Article 19 – paragraph 1 – point 1 a (new)**

Regulation (EU) 2021/694

Article 7 – paragraph 1 – point ca (new)

*Text proposed by the Commission*

*Amendment*

*(1a) Article 7 is amended as follows:*

*(a) paragraph 1 is amended as follows:*

*(1) the following point (ca) is inserted:*

*(ca) support high-quality training to transport operators and transport critical infrastructure’s managers and workforce, also with the aim to effectively share and implement mitigating practices in face of cyber attacks or incidents to critical infrastructure, such as the ones provided by the Transport Cybersecurity Toolkit.*

## PROCEDURE – COMMITTEE ASKED FOR OPINION

<b>Title</b>	Laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents
<b>References</b>	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
<b>Committee responsible</b> Date announced in plenary	ITRE 1.6.2023
<b>Opinion by</b> Date announced in plenary	TRAN 1.6.2023
<b>Rapporteur for the opinion</b> Date appointed	Gheorghe Falcă 7.7.2023
<b>Date adopted</b>	25.10.2023
<b>Result of final vote</b>	+: 38 –: 0 0: 0
<b>Members present for the final vote</b>	Magdalena Adamowicz, Andris Ameriks, José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Karolin Braunsberger-Reinhold, Karima Delli, Anna Deparnay-Grunenberg, Gheorghe Falcă, Carlo Fidanza, Jens Gieseke, Elsi Katainen, Elena Kountoura, Bogusław Liberadzki, Peter Lundgren, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Tilly Metz, Cláudia Monteiro de Aguiar, Caroline Nagtegaal, Jan-Christoph Oetjen, Rovana Plumb, Thomas Rudner, Massimiliano Salini, Vera Tax, Barbara Thaler, István Ujhelyi, Achille Variati, Petar Vitanov, Elissavet Vozemberg-Vrionidi, Lucia Vuolo
<b>Substitutes present for the final vote</b>	Sara Cerdas, Josianne Cutajar, Roman Haider, Pär Holmgren, Pierre Karleskind, Colm Markey, Ljudmila Novak, Dorien Rookmaker

## FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

<b>38</b>	<b>+</b>
ECR	Carlo Fidanza, Peter Lundgren, Dorien Rookmaker
ID	Roman Haider
PPE	Magdalena Adamowicz, Karolin Braunsberger-Reinhold, Gheorghe Falcă, Jens Gieseke, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Colm Markey, Cláudia Monteiro de Aguiar, Ljudmila Novak, Massimiliano Salini, Barbara Thaler, Elissavet Vozemberg-Vrionidi, Lucia Vuolo
Renew	José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Pierre Karleskind, Elsi Katainen, Caroline Nagtegaal, Jan-Christoph Oetjen
S&D	Andris Ameriks, Sara Cerdas, Josianne Cutajar, Bogusław Liberadzki, Rovana Plumb, Thomas Rudner, Vera Tax, István Ujhelyi, Achille Variati, Petar Vitanov
The Left	Elena Kountoura
Verts/ALE	Karima Delli, Anna Deparnay-Grunenberg, Pär Holmgren, Tilly Metz

<b>0</b>	<b>-</b>

<b>0</b>	<b>0</b>

Key to symbols:

+ : in favour

- : against

0 : abstention

## PROCEDURE – COMMITTEE RESPONSIBLE

<b>Title</b>	Laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents			
<b>References</b>	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)			
<b>Date submitted to Parliament</b>	19.4.2023			
<b>Committee responsible</b> Date announced in plenary	ITRE 1.6.2023			
<b>Committees asked for opinions</b> Date announced in plenary	AFET 1.6.2023	BUDG 1.6.2023	CONT 1.6.2023	IMCO 1.6.2023
	TRAN 1.6.2023	LIBE 1.6.2023		
<b>Not delivering opinions</b> Date of decision	BUDG 26.4.2023	CONT 24.5.2023	IMCO 23.5.2023	LIBE 30.5.2023
<b>Rapporteurs</b> Date appointed	Lina Gálvez Muñoz 2.5.2023			
<b>Discussed in committee</b>	19.9.2023			
<b>Date adopted</b>	7.12.2023			
<b>Result of final vote</b>	+ : 43 - : 10 0 : 1			
<b>Members present for the final vote</b>	Nicola Beer, Hildegard Bentele, Vasile Blaga, Michael Bloss, Marc Botenga, Martin Buschmann, Jerzy Buzek, Maria da Graça Carvalho, Josianne Cutajar, Nicola Danti, Marie Dauchy, Pilar del Castillo Vera, Martina Dlabajová, Christian Ehler, Valter Flego, Niels Fuglsang, Nicolás González Casares, Henrike Hahn, Ivo Hristov, Ivars Ijabs, Romana Jerković, Seán Kelly, Izabela-Helena Kloc, Andrius Kubilius, Miapetra Kumpula-Natri, Iskra Mihaylova, Angelika Niebler, Niklas Nienaß, Johan Nissinen, Mikuláš Peksa, Tsvetelina Penkova, Morten Petersen, Markus Pieper, Manuela Ripa, Robert Roos, Sara Skytvedal, Riho Terras, Pernille Weiss, Carlos Zorrinho			
<b>Substitutes present for the final vote</b>	Andrus Ansip, Laura Ballarín Cereza, Cornelia Ernst, Alexis Georgoulis, Ladislav Ilčić, Elena Kountoura, Alin Mituța, Günther Sidl, Jordi Solé, Susana Solís Pérez			
<b>Substitutes under Rule 209(7) present for the final vote</b>	Alexander Alexandrov Yordanov, Jonás Fernández, Virginie Joron, Radan Kanev, Karin Karlsbro			
<b>Date tabled</b>	8.12.2023			



## FINAL VOTE BY ROLL CALL IN COMMITTEE RESPONSIBLE

43	+
ECR	Ladislav Ilčić, Izabela-Helena Kloc
ID	Marie Dauchy, Virginie Joron
NI	Alexis Georgoulis
PPE	Alexander Alexandrov Yordanov, Hildegard Bentele, Vasile Blaga, Jerzy Buzek, Maria da Graça Carvalho, Pilar del Castillo Vera, Christian Ehler, Radan Kanev, Seán Kelly, Andrius Kubilius, Angelika Niebler, Markus Pieper, Sara Skytvedal, Riho Terras, Pernille Weiss
Renew	Andrus Ansip, Nicola Beer, Nicola Danti, Martina Dlabajová, Valter Flego, Ivars Ijabs, Karin Karlsbro, Iskra Mihaylova, Alin Mituța, Morten Petersen, Susana Solís Pérez
S&D	Laura Ballarín Cereza, Josianne Cutajar, Jonás Fernández, Niels Fuglsang, Nicolás González Casares, Ivo Hristov, Romana Jerković, Miapetra Kumpula-Natri, Tsvetelina Penkova, Günther Sidl, Carlos Zorrinho
The Left	Elena Kountoura

10	-
ECR	Johan Nissinen, Robert Roos
The Left	Marc Botenga, Cornelia Ernst
Verts/ALE	Michael Bloss, Henrike Hahn, Niklas Nienaß, Mikuláš Peksa, Manuela Ripa, Jordi Solé

1	0
NI	Martin Buschmann

Key to symbols:

+ : in favour

- : against

0 : abstention