Council of the European Union
General Secretariat

Interinstitutional files:
2023/0109 (COD)

Brussels, 28 September 2023

WK 12298/2023 INIT

LIMITE

CYBER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Horizontal Working Party on Cyber Issues
Subject:	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 - Delegations' comments

Delegations will find in the Annex comments from the BE, CZ, DK, IE, DE, FR, HR, IT, HU, NL, AT, PL, PT, SK, FI and SE Delegation.

Table of Contents

BELGIUM

The amendments suggested below aim at improving the current text of the Cyber Solidarity Act (CSoA) proposal in two main ways:

- by adjusting the terminology currently used to avoid misperceptions and to improve legal certainty,
- by encouraging cross-border cooperation within the scope of existing structures as much as possible and by avoiding a legally binding approach where it is not necessary and could even be counterproductive.

	Amendment suggestions (in bold)	**Comments**
I. "Cyber Shield" & "SOCs"		
Recitals 12 to 15	(12) […] A large-scale Union infrastructure of ~~**SOCs should be deployed ('the European Cyber Shield'), comprising of**~~ ~~**several**~~ interoperating cross-border **cyber threat intelligence-sharing** platforms **(CTIPs)**, each grouping together several national **TIPS**~~**SOCs**~~ **("European Cyber Early Warning System")**. 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 **with the objective of preventing attacks and limiting the damage caused by**	First, Belgium supports **replacing the term "Cyber Shield" by another term such as "European Cyber (Early) Warning System".** The word "shield" has a military connotation which creates confusion. Furthermore, it does not accurately reflect the objective pursued here, i.e. the detection and analysis of cyber threats through intelligence-sharing in order to issue alerts. Second, in the same line of thought, we think that the current text does not sufficiently clearly explain the purpose of the information-exchange within the "Cyber Shield"/"European Cyber Early Warning System". We believe **the purpose of the**

	cyberattacks, notably through the rapid, automated and targeted issuance of early warnings to relevant organisations and individuals. The European Cyber Early Warning System would ~~and~~ thus **support the CSIRTs Network and** complement **~~and support~~** Union entities and networks responsible for **preventing and mitigating cybersecurity crises ~~crisis management~~** in the Union, notably the EU Cyber Crises Liaison Organisation Network ('EU-CyCLONe'), as defined in Directive (EU) 2022/2555 of the European Parliament and of the Council 24 . (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 **CTIPs~~SOCs~~** should act as a reference point and gateway at national level for participation in the European Cyber **Early Warning System~~Shield~~** and should ensure that cyber threat information from public and private entities is shared and collected at national level in an effective and	**first pillar of the CSoA is to prevent cyber incidents**. **We thus suggest making the preventive – i.e. early warning - objective much more explicit** in the wording of the text. For instance, we could specify, through amendments to Recital 12, Article 1(2)(a) and Article 3, that the "European Cyber Early Warning System" aims to enable the rapid, automated and targeted issuance of early warnings to relevant organisations and individuals in order to prevent cyberattacks, or at least to limit the damage caused by cyberattacks.[1] Third, we think the use of the term "Security Operation Centre" (SOC) is confusing and should be avoided. Taking into account the outcome of the very useful discussions during the SOC workshop of 12 September 2023, we suggest: • As first choice, to **replace the term "SOC" by "Cyber Threat Intelligence-sharing Platforms (CTIPs)"** or "Cyber Threat Intelligence hubs (CTIHs)",

[1] Example of an early warning preventing an attack: A spear warning alert will inform an organisation that they are particularly vulnerable to a given attack (e.g. because of an outdated system or because they are part of the target group).

Example of an early warning limiting the damage caused by an attack: A pre-ransomware alert informs an organisation that its system has already been compromised (e.g. the attacker has gained access to some parts of the network) but that it may still be possible to avoid the encryption of its data by taking appropriate measures.

	streamlined manner. **Some CTIPs already exist, such as the Malware Information Sharing Platform - a tool used by several CSIRTs to exchange technical threat information quickly and directly with each other and with relevant entities.** **[Recitals 14 to 15 would also have to be rephrased accordingly to replace "Cyber Shield" by "Cyber Early Warning system" and "SOC" by "cyber threat intelligence-sharing platform"]**	• As second choice, if the term "SOC" is maintained, to amend the definition to make it clear that it refers to **a set of functions and not an entity,** consistent with the Commission statement made during the 18 September HWPCI meeting. The CSoA should <u>not</u> require the creation of a new "SOC" entity, where an entity (such as a national CSIRT) already performs the tasks described at national level.
Art. 1 – Subject matter & objectives	[…] 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 **to enable the rapid, automated and targeted issuance of early warnings to relevant organisations and individuals in order to prevent cyberattacks, or at least to limit the damage caused by cyberattacks. Such capabilities will also ~~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; […]	The fact that the European Commission and the ECCC have already used the term "SOC" in the context of DEP projects does not create any obligation to use such a term in EU legislation. On the opposite, we believe that the DEP can adapt its terminology for future tenders and calls for proposals to align itself with new EU legislation.

	[…] 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.	
Art. 2 - Definitions	[…] 1. 'Cross-border **threat intelligence-sharing platform** ~~**Security Operations Centre**~~' ("Cross-border ~~**SOC**~~**TIP**") means a multi-country platform, that brings together in a coordinated network structure national **bodies tasked with detecting, monitoring and analysing cyber threats** ~~**SOCs**~~ from at least three Member States who form a Hosting Consortium, and that is designed to prevent cyber threats and incidents and to support the production of high-quality intelligence, notably through the exchange of data from various sources, public and private, as well as through the sharing of state-of-the-art tools and jointly developing cyber detection, analysis, and prevention and protection capabilities in a trusted environment; […]	
Art. 3 – "Cyber Shield"	Establishment of the European Cyber ~~**Shield**~~**Early Warning System** 1. An interconnected pan-European infrastructure of **Cyber**	

	Threat Intelligence-Sharing Platforms~~Security Operations Centres~~ (‘European Cyber **~~Shield~~Early Warning System**’) shall be established to develop advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union. It shall consist of all National **Cyber Threat Intelligence-Sharing Platforms~~Security Operations Centres~~** (‘National C**TIPs~~SOCs~~**’) and Cross-border **Cyber Threat Intelligence-Sharing Platforms~~Security Operations Centres~~** (‘Cross-border C**TIPs~~SOCs~~**’). Actions implementing the European Cyber **~~Shield~~Early Warning System** 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~~Early Warning System** shall: (a) pool and share data on cyber threats and incidents from various sources through cross-border C**TIPs~~SOCs~~**; (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 thanks to the issuance by National CTIPs of early warnings to relevant entities and individuals**; (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 advanced artificial intelligence and data analytics tools. […]	
Art. 4 – "National SOCs"	National **Cyber Threat Intelligence-sharing Platforms~~Security Operations Centres~~** 1. In order to participate in the European Cyber **~~Shield~~Early Warning System**, each Member State shall designate **at least one national public body acting as CTIP~~SOC. The National SOC shall be a public body.~~** 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 **CTIP~~SOC~~**. It shall be equipped with state-of-the-art technologies capable of detecting,	**Obtaining EU funding for the reinforcement of cyber intelligence capabilities should not be made legally conditional on membership in a cross-border threat Intelligence-sharing consortium**. We thus suggest deleting Art. 4(3). In several cases, sharing information at the level of the EU as a whole makes more sense than sharing it with a limited number of States within a consortium. In terms of intelligence-sharing among CSIRTs, we are thus not convinced that there is great value in imposing an intermediate level (consortium-level) between the national and European

	aggregating, and analysing data relevant to cybersecurity threats and incidents. 2. Following a call for expression of interest, National **CTIPs~~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 **CTIP~~SOC~~**s 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 **CTIP~~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~~**	levels. Moreover, given the still very recent formation of consortia in the context of cross-border "SOC" projects supported by the ECCC, it would be wise to leave as much flexibility as possible in the CSoA's wording of legal requirements, in order to be able to take into account as many lessons learned as possible that will emerge from these projects in future months and years. Belgium would also like to stress that the CSIRTs Network is already doing a great deal of work exchanging cyber threat intelligence across borders. This work should not be hindered or unnecessarily duplicated by the establishment of cross-border cyber threat intelligence-sharing platforms. We thus suggest the introduction of Art.5(5) to **give an explicit role to the CSIRTs network as the umbrella structure charged with monitoring the operation of cross-border CTIPs.** We also note that achieving the objectives of a European Cyber Early Warning System may involve a higher level of automation or strengthened efficiency of cross-border intelligence-sharing within the CSIRTs network.

	~~**additional Union support under this Regulation.**~~	
Art. 5 – "Cross-border SOCs"	Cross-border **Cyber Threat Intelligence-sharing Platforms**~~**Security Operations Centres**~~ 1. A Hosting Consortium consisting of at least three Member States, represented by National C**TIP**~~**SOC**~~s, 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 **CTIP**~~**SOC**~~. […] […]4. A Cross-border **CTIP**~~**SOC**~~ shall be represented for legal purposes by a National **CTIP**~~SOC~~ acting as coordinating **CTIP**~~**SOC**~~, or by the Hosing Consortium if it has legal personality. The co-ordinating **CTIP**~~**SOC**~~ shall be responsible for compliance with the requirements of the hosting and usage agreement and of this Regulation. **5. The CSIRTs Network shall monitor the operation of Cross-border CTIPs.**	
Recital 16 - Sensors	[…]. The information exchanged among participants in a Cross-border SOC could include, **for instance** ~~**data from networks and sensors**~~, threat intelligence feeds, indicators of compromise, and	Recital 16 suggests that national "SOCs"/CTIPs may place **sensors on critical infrastructures, which may be a very sensitive at national level**. It is important that such a possibility

	contextualised information about incidents, threats and vulnerabilities. In addition, cross-border **cyber threat intelligence-sharing platforms (CTIPs)**~~**SOCs may should**~~ also enter into cooperation agreements with other cross-border **CTIPs**~~**SOCs**~~.	be left to the discretion of the national CSIRTs. If network flows originating from critical infrastructures were to be subject to compulsory listening, this could undermine the trusted role of national CSIRTs. We therefore recommend removing the reference to "data from networks and sensors" in the Recital and clarifying that the list is not limitative, leaving it up to each cross-border "SOC"/TIP to determine what type of information they wish to share, and to what level of granularity.
Art. 6 - Info-sharing	Cooperation and information sharing within and between cross-border **CTIPs**~~**SOCs**~~ **["SOC" would need to be replaced by "CTIP" throughout the whole article]**	
Art. 7 - Coop. with EU bodies	1. Where the Cross-border **CTIPs**~~**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. **1a. CERT-EU shall be designated as CTIP for EU institutions and bodies and participate in the European Cyber Early Warning System.** 2. The Commission may, by means of implementing acts, determine the procedural arrangements for the information sharing	Belgium recommends that the **CSIRTs network should be the first and primary structure through which relevant information flows from the cross-border TIPs are channelled**. Further transmission of relevant information to EU-CyCLONe and the European Commission can be ensured by the CSIRTs Network via existing channels and procedures. Furthermore, provisions should be included to allow EU bodies such as **CERT-EU to participate** in and contribute to the European Cyber Early Warning System next to national CSIRTs.

	provided for in paragraphs 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation.	
II. Cyber Emergency Mechanism & the European Cybersecurity Reserve		
Recitals 30 & 37 – Preparedness & support to third countries	(30) In addition, the Cyber 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 **such as penetration tests, the organisation of simulation exercises, and the provision of technical advice on compliance with cybersecurity legislation (such as NIS2) and other best practice standards.** (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	The main objective of the Cyber Reserve is to provide assistance to European entities dealing with cyber incidents. A secondary objective is to help (associated) third countries deal with cybersecurity attacks. Likewise, **the Reserve could be used to help strengthen the preventive capabilities of entities in the EU**, as well as of those in third countries. Services such as penetration tests could be used to test and boost the cyber resilience of eligible entities**.** We thus suggest an amendment to Recital 30 aimed at stressing the importance of preventive actions, beyond coordinated testing. That said, **the programs and funding for these support actions should not mix the different objectives.** EU and non-EU entities should never be put in competition with each other for the same resources. Clear demarcations in the available funds should be set out by the ECCC to allocate different funds to EU and non-EU entities. Likewise, funding programs should clearly distinguish preventive from

	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. **Any risk of competition between the support provided to third countries and the support provided to EU Member States should be avoided.** 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.	reactive capabilities of the Reserve. We suggest including this principle in Recital 37.
Art. 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 **and other preventive and preparedness actions such as penetration tests and simulation exercises. Such preparedness actions may in some cases be provided by trusted providers**	

	participating in the EU Cybersecurity Reserve established under Article 12; (b)response actions, supporting response to and immediate recovery from significant and large-scale cybersecurity incidents, to be provided by trusted 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.	
Art. 11 – Coordinated tests	1. For the purpose of supporting the coordinated preparedness testing of entities referred to in Article 10(1), point (a), across the Union, the Commission, after consulting the NIS Cooperation Group and ENISA, shall identify the sectors, or sub-sectors, concerned, from the Sectors of High Criticality listed in Annex I to Directive (EU) 2022/2555 from which entities may be subject to the coordinated preparedness testing, taking into account existing and planned coordinated risk assessments and resilience testing at Union level. **The selection of entities to take part in the coordinated tests**	The wording of the article could be more precise and clarify that **national authorities are responsible for applying for the grants and will thus be tasked with selecting the relevant entities to take part in the coordinated tests**, on a voluntary basis, based on the critical sectors identified by the European Commission (intention confirmed by the European Commission during the 18 September HWPCI meeting).

	will be made by each participating Member State on a voluntary basis. […]	
Art. 12 – Cybersecurity Reserve	1. An EU Cybersecurity Reserve shall be established, in order to assist users referred to in paragraph 3 **in preventive and preparedness actions, as well as** in responding or providing support for responding to significant or large-scale cybersecurity incidents, and immediate recovery from such incidents. […] […] 6. The Commission ~~**may**~~**shall** entrust the operation and administration of the EU Cybersecurity Reserve~~**, in full or in part,**~~ to ENISA, by means of contribution agreements. […]	As stressed in our comments on Recital 30, Belgium believes that the "preparedness" dimension of the Cyber Emergency Mechanism should be strengthened and that **it should be possible to use the Cyber Reserve to support preparedness actions**, hence our suggested amendment to Art. 12(1). Moreover, we suggest amending Art. 12(6) to **more clearly specify the role of ENISA in relation to the Cybersecurity Reserve**. This would remove the uncertainty created by the current text, which leaves a lot of discretion to the European Commission.
Art. 13 – Requests for support	[…] 5. Requests for incident response and immediate recovery support shall include: **(a) the choice of provider(s)** ~~**(a)**~~**(b)** appropriate information regarding […]	We understand that **users can choose which provider(s) they wish to obtain services from**, from among the list of Cyber Reserve MSSPs. If this is indeed the case, we recommend **making it more explicit** in Art. 13.
Art. 14 – Implementation	1. Requests for support from the EU Cybersecurity Reserve, shall be assessed by the Commission **based on transparent and**	As regards the filtering of requests by the European Commission as foreseen in Art. 14(1), we have some reservations, especially

of the Cybersecurity Reserve	**objective criteria**, 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) **as soon as possible so as not to compromise the effectiveness of the proposed support action~~without delay.~~**	since the selection criteria in Art. 14(2) leave some room for interpretation. Belgium believes that the CSoA should include guarantees that this filtering will be objective, transparent and carried out quickly so as not to compromise the effectiveness of the response service – when the Cyber Reserve is used of incident response services.
Art. 16 – Trusted providers	**3. Procured services will be limited in time, and be subject to regular evaluation by the Commission whether the provider still complies with the selection criteria in point 2.**	It is important that the provided services are offered to support response to and immediate recovery from significant or large-scale cybersecurity incident and not replace structural investments or infrastructures required. This will also contribute to tackle the risk of vendor buy-in, by making sure that the delivered service is targeted to the specific incident at hand.
III. Incident Review Mechanism		
Recital 36 - Incident Review Mechanism	(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 **may~~should be able to~~** ask ENISA to review and assess threats, vulnerabilities and mitigation actions	Belgium is **not convinced that the cybersecurity incident review mechanism provided for in Art. 18 is legally necessary, especially since** Art. 7(4) of the CSA already gives a mandate to ENISA in this respect. We would rather support a more flexible approach based on **voluntary cooperation**, without the creation of a binding legal provision.

	with respect to a specific significant or large-scale cybersecurity incident. After the completion of a review and assessment of an incident, ENISA **mays~~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. This is however without prejudice to the role of national CSIRTs vis-à-vis their national constituents, which implies that **any information shared by private entities with ENISA should be obtained via the relevant national CSIRT or shared simultaneously with the relevant national CSIRT, in order not to undermine the roles and responsibilities of national CSIRTs, as established under the NIS2 Directive EU 2022/2555.** 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	Moreover, if Art. 18 remains, we see a risk that the current drafting could result in **a disintermediation of national CSIRTs**, e.g. if private entities involved in a cyber incident or crisis are asked to share information directly with ENISA without having to share it with their national CSIRT. The Commission having indicated during the meeting of the HWPCI on 18 September 2023 that it is open to consider an amendment in this direction, we suggest making it explicit that **any information shared by private entities with ENISA should be also shared with their national CSIRT.**

	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.	
Art. 18	**[Deletion of Art. 18 is our preferred choice.** **If the article remains, we would recommend amending it as follows:]** […] 2. To prepare the incident review report referred to in paragraph 1, ENISA **may consult**~~**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. **When consulting other stakeholders and any individual entity established in a Member State, ENISA should ensure that information is primarily obtained from the**	

	relevant national CSIRT. Where it is not, ENISA shall ensure that any information shared by entities established in a Member State is also shared with the relevant national CSIRT(s). 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.[…]	

CZECH REPUBLIC

[…]

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

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[2]
Having regard to the opinion of the European Economic and Social Committee[3],
Having regard to the opinion of the Committee of the Regions[4],
Acting in accordance with the ordinary legislative procedure,
Whereas:

Commented [A1]: For the time being we focus on the articles and do not comment on recitals, as they may require further adjustments based on the final text of articles.

[…]

HAVE ADOPTED THIS REGULATION:

Chapter I

GENERAL OBJECTIVES, SUBJECT MATTER, AND DEFINITIONS

Article 1

Subject-matter and objectives

2 OJ C […], […], p. […].
3 OJ C , , p. .
4 OJ C , , p. .

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 infrastructure of Computer security incident response teams (CSIRTs) and Security Operations Centres ('European Cyber Shield') to build and enhance common detection and situational awareness capabilities falling within the scope of the CSIRTs Network;

(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;

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 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;

(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..~~

3. This Regulation is without prejudice to the Member States' ~~primary~~ sole responsibility for national security, public security, and the primary responsibility for prevention, investigation, detection and prosecution of criminal offences.

Commented [A2]: We do not see an added value in the cybersecurity incident review mechanism. Moreover, the relevant actions by ENISA may constitute an interventions to national matters of the affected Member State, and negatively affect national processes such as ongoing criminal proceedings, etc. For these reasons, we do not support this initiative.

Commented [A3]: Art. 4(2) TEU; national security is Member States' sole responsibility.

Article 2

Definitions

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

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

Commented [A4]: As it was shown during the SOC workshop the terminology and definition of SOC is problematic. We think that tasks of the Cross-border SOC would suit better the CSIRT network and its members. That is why we would like to change this chapter to be more focused ond CSIRTs network members, national SOCs and other CSIRTs (which are not designated as members of CSIRTs network). The main entity should be CSIRTs network as set up in accordance with the NIS 2.

~~(1)~~(2) **'National Security Operations Centre ("National SOC")'**

(2) **'public body'** means a body governed by public law as defined in Article 2((1), point (4),), of Directive 2014/24/EU of the European Parliament and the Council[5];

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

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

(5) '**entities operating in critical or highly critical sectors'** means type of entities listed in Annex I and Annex II of Directive (EU) 2022/2555;

(6) '**cyber threat'** means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881;

(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;~~

(11) **'trusted providers'** means managed security service providers as defined in Article 6, point (40), of Directive (EU) 2022/2555 selected in accordance with Article 16 of this Regulation.

Commented [A5]: We believe a different term should be found to replace 'SOC' in this context. It became clear that the terminology is problematic and would be beneficial to use different wording for the purpose of these entities. Nevertheless, the type of entites being consider 'SOCs' under this wording should be defined in this article

Commented [A6]: "major cybersecurity threats" is used in the regulation but not defined

Commented [A7]: We prefer not to define this generally used term.

Commented [A8]: We prefer not to define this generally used term.

Chapter II

THE EUROPEAN CYBER SHIELD

Article 3

Establishment of the European Cyber Shield

1. An interconnected pan-European infrastructure of Computer security incident reponse teams (CSIRTs) and Security Operations Centres ('European Cyber Shield') shall be established to develop advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union. It shall consist of all the members of the CSIRTs network (established in accordance with the directive- 2022/2555), CSIRTs and National Security Operations Centres ('National SOCs') voluntarily registered by the Member States, ~~and Cross-border Security Operations Centres ('Cross-border SOCs').~~

[5] 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).

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;

(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 the activities of the CSIRTs Network aimed at better protection and response to cyber threats;

(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 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 and Computer security incident reponse teams

Commented [A9]: To be changed once a new term is found (throughout the entire text).

1. In order to participate in the European Cyber Shield, each Member State ~~shall~~ may designate a ~~at least one~~ National SOC or CSIRT as per article 11 of the directive 2022/2555 . The National SOC shall be a public body.

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~~sharing those with the member of the CSIRTs Network ~~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.

2. Following a call for expression of interest, National SOCs or CSIRTs ~~shall~~ 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 or CSIRTs 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 or CSIRT shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

3. A National SOC or CSIRT selected pursuant to paragraph 2 shall commit to concluding an information and intelligence sharing agreement with the respective Member State´s representative in the CSIRTs Network ~~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 or CSIRT has ~~is~~ not concluded an information and intelligence sharing agreement with the respective Member State´s representative in the CSIRTs Network ~~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 Centre~~CSIRTs Network members joint procurement

1. Members of the CSIRTs Network cooperate in accordance with article 15 of the directive 2022/2555. ~~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.~~

2. Following a call for expression of interest, a Member of the CSIRTs network ~~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 Member of the CSIRTs Network ~~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~~selected Member of the CSIRTs Network. Before launching the procedure for the acquisition of the tools and infrastructures, the ECCC and the Member of the CSIRTs Network~~Hosting Consortium~~ shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

Commented [A10]: The acquisition of tools and infrastructures of particular CSIRTs within the CNW would be supported using the DEP programme on the condition that these tools and infrastructures would be made available to the entire CNW.

~~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 Members of the CSIRTs network, National SOCs and CSIRTs ~~**cross-border SOCs**~~

1. ~~Members of~~ National SOCs and CSIRTs from the same Member State ~~a Hosting Consortium~~ shall exchange relevant information among themselves and share relevant information with the respective Member State´s representative in the CSIRTs Network, ~~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) aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;

(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 information and intelligence sharing agreement ~~written consortium agreement~~ referred to in Article ~~5~~4(3) shall establish:

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

~~4. Cross-border SOCs shall conclude cooperation agreements with one another, specifying information sharing principles among the cross-border platforms.~~

Article 7

Cooperation and information sharing with Union entities

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

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

Article 8

Security

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.

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. 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.~~

Chapter III

CYBER EMERGENCY MECHANISM

Article 9

Establishment of the Cyber Emergency Mechanism

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

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.

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 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.

2. As a part of the Mechanism, an Emergency Fund shall be established to rapidly cover immediate costs of Member States necessary for their swift response to significant and large-scale cybersecurity incidents.

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~~ recommended to take part in the voluntary coordinated preparedness testing, taking into account existing and planned coordinated risk assessments and resilience testing at Union level.

1a. The definition of the process associated to the coordinated preparedness testing shall be the sole competence of the Member States.

Commented [A11]: A definition should be in place for what the Mechanism itself is in this article.

Commented [A12]: See comment to Art. 2(6)

Commented [A13]: Since there are other actions then there is no reason to highlight this particular one. Otherwise a concrete list of preparedness actions should be cretaed.

Commented [A14]: COM's elaboration this should be developed in a recital (will be done within ECCC's work programme, MS will receive grants within which costs also from before the publication of the tender can be retroactively covered and will be standard costs such as per diem in cases when a MS sends its experts abroad)

Commented [A15]: This fund would allow the COM to award direct grants to the affected MS, without a call for proposals, to over costs necessary to ensure response. In our point of view, this fund would complement the Mechanism and should allow MS to accordingly invest in the response to and/or recovery from the incident.

Commented [A16]: What is the process for the launch of this action? Who will provide the respective services and who will decide on providing them?

Commented [A17]: There should be a clear framework for how these sectors are going to be selected based on objective criteria and how are Member States going to be involved.

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.

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.

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~~ may be deployable upon request in all Member States.

Commented [A18]: What type of services will that be?

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;

(c) Third countries as set out in Article 17 (1) of this Regulation.

4. Users referred to in paragraph 3, point (a), ~~shall~~ may 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, if assessed as beneficial by the user.

Commented [A19]: It is necessary that the regulation clearly states that using the Reserve is voluntary. Considering the sole responsibility of MS when it comes to national security, each MS should be able to assess the effects of the incident by itself and only then decide whether or not it wants to use the Reserve.

5. The Commission shall have overall responsibility for the implementation of the EU Cybersecurity Reserve. The Commission, in close cooperation with the ECCC, shall determine the priorities and evolution of the EU Cybersecurity Reserve, in line with the requirements of the users referred to in paragraph 3, points (a) and (b), 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 may 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, after consulting Member States and Union institutions, bodies and agencies ~~and the Commission~~. ENISA shall prepare a similar mapping, after consulting

Commented [A20]: Since other EU-IBAs (not only the COM) are also eligible users of the Reserve, their needs should also be taken into account and considered within the mapping.

the Commission, to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve pursuant to Article 17. The Commission shall inform the Council about the needs of third countries and, where relevant, ~~shall~~ consult the High Representative.

8. The Commission may, by means of implementing acts, specify the types and the number of response services required for the EU Cybersecurity Reserve. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2).

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~~ exhaist all other 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 designatet Point of Contact in 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 on how the provisions of article 9 and 10 of NIS2 directive have been met as regard~~sing~~ 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) general 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 may, by means of implementing acts, specify further the detailed arrangements for allocating the EU Cybersecurity Reserve support services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2).~~

Commented [A21]: Where are the requests from the other users going to be transmitted to?

Commented [A22]: Overall, we do not think that the request should be conditioned by sharing this amount of sensitive information, as referred to in this para. The necessity of providing the information must be sufficiently justified and assessed in relation to each type of information. Only on that basis it should be reflected in the text of the regulation.

Commented [A23]: In line with COM's clarification to our questions.

Commented [A24]: Specific procedures, deadlines and timelines need to be clarified in the regulations priod to its adoption, not an implementing act.

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- the ECCC~~ENISA or as defined in contribution agreements under Article 12(6)~~, and a ~~response~~ decision shall be transmitted to the users referred to in Article 12(3) without delay and in any event within 72 hours from the submission of the request at the latest.

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 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).

2a. The decision to provide EU Cybersecurity Reserve services shall be taken by the Council.

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.

4. The agreements referred to in paragraph 3 may be based on templates prepared by ENISA, after consulting Member States.

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.

6. Within one month from the end of the support action, the users shall provide Commission ~~and~~ , ENISA, CSIRTs Network and, where appropriate, EU-CyCLONe with a summary report about the service provided. This feedback shall be used to evaluate the effectiveness of the Cyber Emergency Mechanism.~~, 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.

6a. An annual report shall be prepared by the Commission, aggregating the feedback received. This report shall be shared with the European Parliament and the Council.

Commented [A25]: There should be a clear time frame for the decision on the use of the Reserve. In case its services are needed, the users requesting help are going to be in a time-sensitive situation and will be needing feedback and support as soon as possible. Incidents like that might lead to long-term consequences if not dealt with right away. The users need to know for how long they should wait to hear back about their request.

Commented [A26]: If all of this information is to be a part of the template mentioned in art. 13(6), we should consider re-structuralising the text and putting this under Art. 13(5).

Commented [A27]: The deployment of the Reserve should be decided by the Council, in particular CRP II given its role under IPCR, or else PSC, as per CFSP procedures

Commented [A28]: OK if deadline for COM's response to user is set and met.

Commented [A29]: Why one month? If it is last reserve tool, then the consequences will be probably hard and the victims would need longer period to assess the results.

Commented [A30]: Should be specified in a recital – the end of the support action marks the moment when the support is finished or when the user will request to end the support when the situation is back under control, or else can be managed by own mechanisms of the user.

~~7. The Commission shall report to the NIS Cooperation Group about the use and the results of the support, on a regular basis.~~

Commented [A31]: Not clear what role the NIS CG plays in regards to the Cyber Reserve.

Article 15

Coordination of the Cyber Emergency Mechanism with crisis management mechanisms

Commented [A32]: Should be clear that this is about the Mechanism as a whole, not only the Reserve.

Commented [A33]: It should also be moved to the end of the chapter since Art. 16 and 17 still talk about the Reserve.

1. In cases where significant or large-scale cybersecurity incidents originate from or result in disasters as defined in Decision 1313/2013/EU[6], the support under this Regulation for responding to such incidents shall complementactions 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 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.~~

Commented [A34]: CRRTs PESCO project will be over in 2025, this seems redundant taking into account the progress of the negotiations

Commented [A35]: Does not seem necessary in this para since this is an individual decision of each MS, and having Art. 222 TFEU mentioned in the next one.

4. Support under the Cyber Emergency Mechanism may form part of the joint response between the Union and Member States in situations referred to in Article 222 of the Treaty on the Functioning of the European Union.

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:

Commented [A36]: Who is the contracting authority?

(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.

(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.

Commented [A37]: It is not clear from the text whether or not the Reserve would be open to non-EU providers as well as the ones that are EU-based

[6] 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).

2. When procuring services for the EU Cybersecurity Reserve, the contracting authority shall include in the procurement documents the following selection criteria, to be defined in each procurement by the respective Member State, for which the contracting authority is procuring services:

[…]

(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) where it can deliver the service;

(j) once an EU certification scheme for managed security service Regulation (EU) 2019/881 is in place, the provider shall be certified in accordance with that scheme.

Article 17

Support to third countries

[…]

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 inform 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**~~

Commented [A38]: Needs specification

Commented [A39]: Depends on the decision who is picking the provider, if it is victim decision, is it necessary? The provider should made clear in which languages it can provide its services.

Commented [A40]: It needs to be taken into account that third countries do not have a unified definition of a "significant or large-scale cybersecurity incident"

Commented [A41]: This is important as the information might also be beneficial for MS regarding possible bilateral support.

Commented [A42]: We do not see an added value in the cybersecurity incident review mechanism. Moreover, the relevant actions by ENISA may constitute an intervention to national matters of the affected Member State, and negatively affect national processes such as ongoing criminal proceedings, etc. For these reasons, we do not support this initiative.

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

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

~~3. The report shall cover a review and analysis of the specific significant or large-scale cybersecurity incident, including the main causes, vulnerabilities and lessons learned. It shall protect confidential information, in accordance with Union or national law concerning the protection of sensitive or classified information.~~

~~4. Where appropriate, the report shall draw recommendations to improve the Union's cyber posture.~~

~~5. Where possible, a version of the report shall be made available publicly. This version shall only include public information.~~

[…]

DENMARK

[…]

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- **Legal basis**

The legal basis for this proposal is Article 173(3) and Article 322(1), point (a) of the Treaty on the Functioning of the European Union (TFEU). Article 173 TFEU provides that the Union and the Member States shall ensure that the conditions necessary for the competitiveness of the Union's industry exists. This Regulation aims at strengthening the competitive position of industry and service sectors in Europe across the digitised economy and supporting their digital transformation, by ~~rein~~enforcing the level of cybersecurity in the Digital Single Market. In particular, it aims at increasing the resilience of citizens, businesses and entities operating in critical and highly critical sectors against the growing cybersecurity threats, which can have devastating societal and economic impacts.

The proposal is based also on Article 322(1), point (a) TFEU because it contains specific carry-over rules derogating from the principle of annuality set out in Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council (the 'Financial Regulation')[7]. For the purpose of sound financial management and considering the unpredictable, exceptional and specific nature of the cybersecurity landscape and cyber-threats, the Cybersecurity Emergency Mechanism should benefit from a certain degree of flexibility in relation to budgetary management, and in particular by allowing unused commitment and payment appropriations for actions pursuing the objectives set out in the Regulation to be automatically carried over to the following financial year. As this new rule raises issues with the Financial Regulation, this matter could be addressed in the context of the current negotiations of the Financial Regulation recast.

- **Subsidiarity (for non-exclusive competence)**

The strong cross-border nature of cybersecurity threats and the growing number of risks and incidents, which have spill-over effects across borders, sectors, and products, mean that the objectives of the present intervention cannot effectively be achieved by Member States alone and require common action and solidarity at Union level.

The experience of countering cyber-threats stemming from the war against Ukraine, together with the lessons learned from a cybersecurity exercise conducted under the French Presidency (EU CyCLES), showed that concrete mutual support mechanisms, notably cooperation with the private sector, should be developed to achieve solidarity at EU level. Against this background, the Council Conclusions of 23 May 2022 on the development of the European Union's cyber posture calls upon the Commission to present a proposal on a new Emergency Response Fund for Cybersecurity.

---

[7] 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 (OJ L 193, 30.7.2018, p. 1).

Support and actions at Union level to better detect cybersecurity threats, and to increase preparedness and response capacities provide added value because it avoids duplication of efforts across the Union and Member States. It would lead to a better exploitation of existing assets and to greater coordination and exchange of information on lessons learned. The Cyber Emergency Mechanism also envisages providing support to third countries associated to DEP from the EU Cybersecurity Reserve.

The support provided through the various initiatives to be established and funded at Union level will complement and not duplicate national capabilities as regards detection, situational awareness, preparedness and response to cyber threats and incidents.

- **Proportionality**

The actions do not go beyond what is needed to achieve the general and specific objectives of the Regulation. The actions in this Regulation do not affect Member States' responsibilities for national security, public security, the prevention, investigation, detection, and prosecution of criminal offences. Nor do they affect the legal obligations of entities operating in critical and highly critical sectors to adopt cybersecurity measures, in accordance with the NIS 2 Directive.

The actions covered by this Regulation are complementary to such efforts and measures, by supporting the creation of infrastructures for better detection and analysis of threats and providing support for preparedness and response actions in case of significant or large-scale incidents.

- **Choice of the instrument**

The proposal takes the form of a Regulation of the European Parliament and of the Council. This is the most suitable legal instrument, as only a Regulation, with its directly applicable legal provisions, can provide the necessary degree of uniformity needed for the establishment and operation of a European Cyber Shield and Cyber Emergency Mechanism, by providing for support from DEP for their establishment as well as clear conditions for using and allocating this support. Further conditions found not to be provided for in the Regulation will be defined through the usual process for determining the conditions surrounding calls in the Digital Europe Programme.

Commented [A43]: Conditions are made in the following provisions, however we find it to be appropriate to clarify any greyzones through the normal DEP procedure.

[…]

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

The Commission will monitor the implementation, the application, and the compliance with these new provisions with a view to assessing their effectiveness. The Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council by four years after the date of its application.

- **Detailed explanation of the specific provisions of the proposal**

General Objectives, subject matter, and definitions (Chapter I)

Chapter I sets out the objectives of the Regulation to strengthen solidarity at Union level in order to better detect, prepare and respond to cybersecurity threats and incidents and in particular, to strengthen common Union detection and situational awareness of cyber threats and incidents, 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 and to enhance Union resilience by reviewing and assessing significant or large-scaleincidents. This Chapter also sets out the actions through which these objectives will be achieved: the deployment of a European Cyber Shield, the creation of a Cyber Emergency Mechanism and the establishment of a Cybersecurity Incident Review Mechanism. It also sets out the definitions used throughout the instrument.

The European Cyber Shield (Chapter II)

Chapter II establishes the European Cyber Shield and sets out its various elements and the conditions for participation. Firstly, it announces the overall objective of the European Cyber Shield, which is to develop advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union, as well as the specific operational objectives. It specifies that Union funding for the European Cyber Shield shall be implemented in accordance with the DEP Regulation.

Further, the chapter describes the type of entities that shall form the European Cyber Shield. The shield shall consist of designated National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs'). A National SOC shall be designated by each participating Member State. This shall 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. Following a Call for Expression of Interest, a National SOC may be selected by the ECCC to participate in a joint procurement of tools and infrastructures with the ECCC and to receive a grant for running the tools and infrastructures. If a National SOC benefits from Union support, it shall commit to apply participate in a Cross-border SOC within two years.

Commented [A44]: Following which particular procedure, reported to whom ? It must be clear which entity/ies are SOC's within the meaning of this regulation, and which are not.

Cross-border SOCs shall consist of a consortium of at least three Member States, represented by National SOCs, who are committed to work together to coordinate their cyber detection and threat monitoring activities. Following an initial 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 and to receive a grant for running the tools and infrastructures. Members of the Hosting Consortium shall conclude a written consortium agreement which sets out their internal arrangements. This chapter then details the requirements for sharing information among the participants in a Cross-border SOC, and for sharing information between a Cross-border SOC and other Cross-border SOCs, as well as with relevant EU entities. National SOCs participating in a Cross-border SOC shall share relevant cyber threat related information with one another, and the

Commented [A45]: It is crucial for the successful establishment of regional SOCs that trust can be built with incremental sharing of data between the participating partners.

details, including the commitment to share significant amount of data and the conditions thereof should be defined in a consortium agreement. Cross-border SOCs shall ensure a high-level of interoperability between themselves. Cross-border SOCs should also conclude cooperation agreements with other Cross-border SOCs, specifying information sharing principles. Where 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. Chapter II concludes by specifying the security conditions for participating in the European Cyber Shield.

[…]

[…]

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

Commented [A46]: The language gives the impression that the SOCs are forced to enter into cooperation agreements with other SOCs, which is innapropriate.

[…]

(24) In view of the increasing risks and number of cyber incidents affecting Member States, it is necessary to set up a crisis support instrument to improve the Union's resilience to significant and large-scale cybersecurity incidents and complement Member States' actions through emergency financial support for preparedness, response and immediate recovery of essential services. That instrument should enable the rapid deployment of assistance in defined circumstances and under clear conditions and allow for a careful monitoring and evaluation of how resources have been used. Whilst the ~~primary~~ sole responsibility for preventing, preparing for and responding to cybersecurity incidents and crises lies with the Member States, the Cyber Emergency Mechanism promotes solidarity between Member States in accordance with Article 3(3) of the Treaty on European Union ('TEU').

Commented [A47]: The realization of the Cyber Solidarity Act, and the efforts to strengthen the EU's capacity to react swiftly and effectively to cyber threats and malicious activity in cyberspace towards the Union and MS, must be done with respect for the distribution of competences set out by the EU Treaties.

We find that the CSOA is marked by a large degree of mandatory elements. In light of this and since national security is the sole responsibility of the MS, DK would like the voluntary nature of the CSOA-initiatives to be more clearly highlighted throughout the legal act.

(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[8] 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.

Commented [A48]: Would like for COM to elaborate on why reference is made to article 47 (2) of TEU? It seems innapropriate.

(26) This instrument is without prejudice to procedures and frameworks to coordinate crisis response at Union level, in particular the UCPM[9], IPCR[10], 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.

Commented [A49]: Would like for COM to elaborate on why reference is made to article 47 (2) of TEU? It seems innapropriate.

[…]

(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

---

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

9 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).

10 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.

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

Commented [A50]: If COM can task ENISA to do a report on a large-scale cybersecurity incident in a MS without MS being able to effectively manage the inputs provided to the report, it constitutes a possible infringment on national sovereignty.

There is a reasonable risk that information on causes, impacts and mitigations of a large-scale cybersecuirty incident in a highly critical sector in a MS involves sensitive or classified information.

Incident review reports should only be conducted on a voluntary basis and under the condition that relevant national authorities in the MS in question is consulted and have given their explicit approval prior hereto.

(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.

(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.

Commented [A51]: When initially submitting the Expression of Interest MS did not sign on to the Commission having a role in i.e. interoperability between cross-border platforms or the procedural arrangements for information sharing. It is our understanding that principles on information sharing will be determined by cooperation agreements between cross border SOCs.

We have concerns against specifying conditions for interoperability, and possibly data sharing, through implementation acts. It is crucial for the successful establishment of regional SOCs, that trust can be built with incremental sharing of data between the participating partners.

(39) The objective of this Regulation can be better achieved at Union level than by the Member States. Hence, the Union may adopt measures, in accordance with the principles of subsidiarity and proportionality as set out in Article 5 of the Treaty on European Union. This Regulation does not go beyond what is necessary in order to achieve that objective.

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 infrastructure 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 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;

(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..

3. This Regulation is without prejudice to the Member States' ~~primary~~ sole responsibility for national security, public security, and the prevention, investigation, detection and prosecution of criminal offences.

Commented [A52]: The realization of the Cyber Solidarity Act, and the efforts to strengthen the EU's capacity to react swiftly and effectively to cyber threats and malicious activity in cyberspace towards the Union and MS, must be done with respect for the distribution of competences set out by the EU Treaties.

We find that the CSOA is marked by a large degree of mandatory elements. In light of this and since national security is the sole responsibility of the MS, DK would like the voluntary nature of the CSOA-initiatives to be more clearly highlighted throughout the legal act.

The regulation or implementing acts adopted pursuant to this regulation should not entail any obligations for Member States to perform any act contrary to Member States' considerations relating to national security, public security, and the prevention, investigation, detection and prosecution of criminal offences, including obligations to share or dissiminate classified or sensitive information.

Article 2

Definitions

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

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

~~(1)~~(2) **[National Security Operations Centres]**

(32) **'public body'** means a body governed by public law as defined in Article 2((1), point (4),), of Directive 2014/24/EU of the European Parliament and the Council[11];

(43) '**Hosting Consortium'** means a consortium composed of ~~participating states, represented by~~ National SOCs in the pariticpating Member States, that have agreed to establish and contribute to the acquisition of tools and infrastructure for, and operation of, a Cross-border SOC ;

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

(65) '**entities operating in critical or highly critical sectors'** means type of entities listed in Annex I and Annex II of Directive (EU) 2022/2555;

(76) '**cyber threat'** means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881;

(87) '**significant cybersecurity incident'** means a cybersecurity incident fulfilling criteria set out in Article 23(3) of Directive (EU) 2022/2555;

(98) '**large-scale cybersecurity incident'** means an incident as defined in Article 6, point (7) of Directive (EU)2022/2555;

(109) **'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;

(110) **'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;

(121) **'trusted providers'** means managed security service providers as defined in Article 6, point (40), of Directive (EU) 2022/2555 selected in accordance with Article 16 of this Regulation.

Commented [A53]: How are the cross-border SOCs under this regulation deliminated from possible other cross-border SOCs which Member States may setup outside the scope of this regulation?

Should a designation process or funding requirement be set up for Cross-border SOCs to fall within the remit of this regulation ?

Commented [A54]: We see a need for clear definitions on: 1) what constitutes a National SOC, and 2) a coordinating SOC (a National SOC serving as coordinator for the establishment of a Cross-border SOC). Member States have their own national set-ups regarding cybersecurity and cyber crisis management and these national set-ups should be respected.

The current unclear definitions of a national SOC – art. 4(1) – risks encroaching on Member States' organization and operation of their sovereign SOC and CSIRT structures.

We find it crucial that there is a clear distinction between these two types of SOCs. Currently, there is room for potential misinterpretation with respect to which entities that are liable to the different obligations.

In light of the prominent role that the national SOCs play in the 'European Cyber Shield', and in order to avoid confusion, we find that a clear definition on the National SOCs ought to be included (under art 2).

Commented [A55]: MS' are replaced by 'national SOC's' as the main subject of this sentence, since it should be made clear that 'Members of a Hosting Consortium' is the national SOC's and not the MS themselves, seeing that the entity in question might be obligated to share data under art. 6.

[11] 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).

Chapter II

THE EUROPEAN CYBER SHIELD

Article 3

Establishment of the European Cyber Shield

1. An interconnected pan-European infrastructure of Security Operations Centres ('European Cyber Shield') shall be established to develop advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union. It shall consist of designated~~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;

(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;

(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 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 receive funding to participate in the European Cyber Shield, each Member State may~~shall~~ designate at least one National SOC. The National SOC ~~shall~~ may be a public body. It ~~shall~~ may 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

Commented [A56]: Denmark recommends that the articles of chapter 2 (art. 3-8) is to the furthest extend possible left out of the CSOA proposal and instead regulated in the establishing agreements made between consortia and the Commission.

By doing so, the CSOA will also avoid the risk of making the effect of the legislation dependent on SOCs and SOC operations, which are a subject to diverging interpretations among Member States. Due to the unclear definitions of a national SOC – art. 4(1) – the CYSOL proposal risks encroaching on Member States' organization and operation of their sovereign SOC and CSIRT structures: art. 5(1,3,4); art. 6(3); and art. 7(1).

Commented [A57]: See comment for art 2.

Commented [A58]: Need for a procedure for the identification of SOCs which fall inside and outside of the scope of this regulation.

Commented [A59]: Is the National SOC a « platform » like the cross-border SOC?

Commented [A60]: See comment for art 2.

Commented [A61]: DK would like 'receive funding' to be inserted in order highlight the voluntary nature of the European Cyber Shield and underline that the article does not create legal bindings for MS that chose not to apply for funding or even be a part of the European Cyber Shield.

It is of utmost importance that the proposal conserves the voluntary nature of the Cross-border SOC projects. Member states should have freedom of maneuver to exploit long-standing arrangements and practices with trusted partners for the benefit of advancing stronger common detection and situational awareness. This will also avoid crowding out sensitive, national, and regional arrangements that eventually can contribute to the common good of the cyber shield.

technologies capable of detecting, aggregating, and analysing data relevant to cybersecurity threats and incidents.

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.

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 from three different Member States, 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.

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

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

Commented [A62]: Unclear whether it is mandatory or if national SOC scan enter into the joint procurement voluntarily – it should be voluntary.

Commented [A63]: Will the national SOC also be bound by EU regulation, i.e. GDPR, and revision (as a member of a regional SOC), even if it in itself does not apply for and receive funding from the ECCC?

Commented [A64]: Data to be shared under art. 6 (1) include information on vulnerabilities, adversarial tactics, threat-actor-specific information and near misses. If Member States are obliged to share such information on ongoing attacks the actor will most likely realize they have been discovered and make any remediation of the effects of the attack and protecting critical services very difficult.

Commented [A65]: DK would appreciate clarification and a clear definition regarding which entity "Members of a Hosting Consortium" refers to, as the entity will be obligated under art. 6 to share data. Is it the Member State as such – there by any government entity subject to member State law – as indicated in art. 2 (1) and (3) or is it only the national 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 SOCs

1. Having established a Cross Border SOC, mMembers of a Hosting Consortium ~~shall~~ exchange relevant information among themselves within the Cross-border SOC, which may include~~ing~~ 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) aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;

(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 amount of~~ data ~~referred to in paragraph 1~~, and the conditions under which that data~~information~~ is to be exchanged;

(b) a governance framework incentivising the sharing of data reffered to in paragraph 1~~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 between Cross-border SOCs, Cross-border SOCs shall ensure a high level of interoperability between themselves. To facilitate the interoperability between the Cross-border SOCs, the Commission may, by means of implementing acts, after consulting the ECCC, specify the conditions for this interoperability. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation.

4. Cross-border SOCs shall conclude cooperation agreements with one another, specifying information sharing principles among the cross-border platforms.

Article 7

Cooperation and information sharing with Union entities

Commented [A66]: To further solidify transparency on the scope of the CYSOL, we see a need for defining more clearly that 'Members of a Hosting Consortium' as referred to in art. 6(1) only refers to the designated national SOC that participates in the consortium and not other entities in the SOC and CSIRT structure of the participating Member State.

Commented [A67]: In regard to the proposal's article 6, we note that the data to be shared include information on vulnerabilities, adversarial tactics, threat-actor-specific information and near misses. DK suggests that 'may include' replace 'including' as an obligation to share such data raises questions related to national security and protecting against active cyber-attacks from i.e. third states. The exchange of information should be voluntary or at least expressly subject to national security reservations.

If Member States are obliged to share information on ongoing attacks, the threat actor will most likely realize they have been discovered, which will make any remediation of the effects of the attack and protecting critical services very difficult.

Commented [A68]: It should be up to the hosting consortiums (in other words the participating national SOCs) themselves to decide, what types of data that they should/should not share.

Commented [A69]: It is stated that the Commission may specify the conditions for interoperability between Cross-border SOCs by the means of implementing acts. Can you clarify what kind of conditions this could include? Can you confirm that the possible implementing acts will be limited to interoperability between the cross-border platforms and the specific data to be shared will be specified solely by the Cross-border SOCs cooperation agreements.

The proposal contains a disproportionate use of implementing acts concerning the cross-border SOCs. As the interoperability between the Cross-border SOCs will be ensured through the terms of the Joint Procurement and the Hosting and Usage Agreement, we do not find it necessary to include any implementing acts for article 6 (3).

Commented [A70]: To conserve the voluntary nature of the establishment of the CTI-sharing platforms, we propose that that the operations of the platforms should be solely regulated by the establishing grant agreements formalized between the consortiums and the Commission. This approach grants Member States the flexibility to exploit long-standing arrangements and practices with trusted partners for the benefit of advancing stronger common detection and situational awareness.

Commented [A71]: It is important to avoid the duplication of the already established EU crisis management structures of the CSIRTs Network and CyCLONe. The obligations of art. 7(1) become redundant as it is an unnecessary duplication of the NIS2 Directive's article 23 (1,4) which ensure that essential and important entities notify its CSIRT or its competent authority of any incident that has a significant impact on the provision of their services and oblige the member state's designated CSIRT to determine any cross-border impact of the incident. Additionally, the current definition of the National SOC risks duplicating the role and actions of the CSIRT-network as defined in art. 25 of the NIS 2 Directive.

Accordingly, the current proposal risks diffusing the current approach to collaboration and information-sharing at the EU-level. We propose that the CYSOL initiative refrain from imposing crisis management procedures to not impede the further development of the CSIRTs network and CyCLONe.

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.

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

Commented [A72]: Will it be up to the Cross-border SOC to assess what classifies as 'relevant information'? And if not: what will constitute 'relevant information' in terms of this article?

Commented [A73]: It is stated that the Commission may determine procedural arrangements for the information sharing between the regional SOCs and the Commission/CyCLONe/ the CSIRT network, does this also include decisions on what kind of information that should be shared? Could you elaborate on what kind of procedural arrangements that could be determined at a later state?

Article 8

Security

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.

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.

Commented [A74]: How does a MS ensure that the sharing of information with entities, which are not MS 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. 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.

Commented [A75]: Reference is here made to the fact that this will be regulated in the Hosting and Usage agreements that the respective consortiums will sign bilaterally with ECCC/COM.

Chapter III

CYBER EMERGENCY MECHANISM

Article 9

Establishment of the Cyber Emergency Mechanism

Commented [A76]: Can the Commission confirm that the 'preparedness part' of the Cyber Emergency Mechanism only consist of a fund from which the MS can apply for financial support, and accordingly, does not impose any obligations on the MS that do not apply for said support?

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

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.

Article 10

Type of actions

1. The Mechanism shall support the following types of actions:

(a) preparedness actions, including detecting measures to quickly identify major cybersecurity incidents and 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 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.

Commented [A77]: What entities does the Commission have in mind here? We assume that, if the preparedness testing involves entities that operate in more than one member state, then all MS will have to agree here to, not only the one receiving the funding. Can you confirm this? Furthermore, are the activities voluntary?

Article 11

Coordinated preparedness testing of entities

1. For the purpose of supporting voluntary~~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, on a consentual basis be subject to the coordinated preparedness testing, taking into account existing and planned coordinated risk assessments and resilience testing at Union level.

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.

Commented [A78]: DK would appreciate clarification on whether the preparedness testing of critical sectors as stated in art. 11 would be subject to Member State consent? If third party entities providing such services are to be deployed in our Member State this could raise legal issues.

Commented [A79]: If preparedness testing involves entities, which operate in more than one member state, then all affected MS will have to agree hereto, not only the one receiving the funding. If this is not the case, then a reservation should be built into the article, in order for it to clearly state that any transnational preparedness testing requires the explicit approval from all MS directly and indirectly involved.

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 upon request for responding to significant or large-scale cybersecurity incidents, and immediate recovery from such incidents.

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 – when taken together - be deployable in all Member States.

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.

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.

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.

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

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.

8. The Commission may, by means of implementing acts, specify the types and the number of response services required for the EU Cybersecurity Reserve. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2).

Article 13

Requests for support from the EU Cybersecurity Reserve

Commented [A80]: The insertions of 'upon request' are made order to emphazise the voluntary nature of this initative, as confirmed by COM in the preliminary discussions on CYSOL, but which is, as it stands now (in the proposal) unclear.

Commented [A81]: Which authority does the trusted service providers of the reserve have when deployed and to whom does it refer?

Commented [A82]: In order to ensure that smaller service providers who cannot cover all Member States will be able to make there ressources available to the reserve, it could be necessary to limit deployability to a select number of MS, and then instead make the entirity of servies deployable in all MS.

Commented [A83]: Under what circumstances and how are such agreements governed?

Will ENISA get more ressources if entrusted with the operation and administration of the reserve? Will ENISA be responsible for the procurement process and establishment of the reserve?

Commented [A84]: We assume that if this mapping will involve the situation in specific MS then it will be conducted only on a voluntary basis and with an explicit prior approval form the MS in question? Can you confirm this assumption?

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) where relevant, available 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 may, by means of implementing acts, specify further the detailed arrangements for allocating the EU Cybersecurity Reserve support services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2).

Commented [A85]: If the EU Cyber Reserve is to become effective in practice, the information that MS must provide during an ongoing incident should be kept to a minimum. It is difficult to see how a MS can prioritise providing substantive information while trying to respond to an ongoing incident at the same time.

Commented [A86]: The amoount of information is potentially quite comprehensive relative to the situation one can expect the entity requesting support being in.

One solution could be to make the requesting entity provide relevant information after the request has been received and support has been given to the requesting entity.

Commented [A87]: What is meant by detailed arrangements for allocating 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 delay.
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 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).

Commented [A88]: Does the Commission and ENISA decide on this?

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.

4. The agreements referred to in paragraph 3 may be based on templates prepared by ENISA, after consulting with Member States.

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.

6. Within one month from the end of the support action, the users shall provide Commission and ENISA with a summary report about the service provided, results achieved and the lessons learned. When the user is from a third country as set out in Article 17, such report shall be shared with the High Representative.

Commented [A89]: What are the specifications for this summary report?

7. The Commission shall report to the NIS Cooperation Group about the use and the results of the support, on a regular basis.

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[12], the support under this Regulation for responding to such incidents shall complementactions 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 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

[12] 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).

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.

4. Support under the Cyber Emergency Mechanism may form part of the joint response between the Union and Member States in situations referred to in Article 222 of the Treaty on the Functioning of the European Union.

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 – when taken together - includes services that may be deployed in all Member States, taking into account in particular national requirements, including compatibility 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.

(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.

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 the hardware and software technical equipment necessary to support the requested service;

(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;

Commented [A90]: In establishing the EU Cybersecurity Reserve, the services that will be provided may be deployed in all Member States, taking into account in particular national requirements for the provision of such services (a). Also, the Trusted Providers needs to provide the service in the local language of the Member States(s) (i). As we understand it, the trusted providers will in total be covering the requirements of all Member States, however, do these principles outline that there is one or more Trusted Providers in each Member State and if so, will there be a government involvement with this/these trusted provider(s)?

Commented [A91]: Cf. DK comments to article 12.

Commented [A92]: How is this to be done in practice?

Commented [A93]: Will a generic framework be established or is the point to make a case by case framework?

Commented [A94]: Issued by which authority, in accordance with which rules? How is appropriate defined – in general or case by case?

In practice this will be very difficult to comply with, as security clearences can take a long time to acquire.

(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) where it can deliver the service;

(j) once an EU certification scheme for managed security service Regulation (EU) 2019/881 is in place, the provider shall be certified in accordance with that scheme.

Commented [A95]: Should be clarified what timeframe is acceptable.

Commented [A96]: It appears that a provider does not have to cover all member states, - and this we find is a sound approach- but some of the requirements are depending on external factors, e.g. (h) "able to provide the service within a short timeframe". This depends on the situation, of how much else is happening and how many other assignments the provider has taken on already. Furthermore, this requirement may resort to a sheer demand for size, omitting relevant smaller providers in may circumstances, and eventually missing the objective of the reserve.

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 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. If the review or assesments include incidents in specific member states or private enteties operating in said states, relevant authorities shold be consulted and give their explicit approval prior hertho.

Following the completion of a review and assessment of an incident, ENISA shall deliver an incident review report to the CSIRTs network, the EU-CyCLONe and the Commission to support them in carrying out their tasks, in particular in view of those set out in Articles 15 and 16 of Directive (EU) 2022/2555. Where relevant, the Commission shall share the report with the High Representative.

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

3. The report shall cover a review and analysis of the specific significant or large-scale cybersecurity incident, including the main causes, vulnerabilities and lessons learned. It shall protect confidential information, in accordance with Union or national law concerning the protection of sensitive or classified information.

4. Where appropriate, the report shall draw recommendations to improve the Union's cyber posture.

5. Where possible, a version of the report shall be made available publicly. This version shall only include public information.

[…]

Formatted: English (United States)

Commented [A97]: DK assumes that, if this review and threat assessment includes the situation in specific MS (also if, it solely concerns private entities), it will only be conducted on a voluntary basis and under the condition that relevant national authorities in the MS in question is consulted and have given their explicit approval prior hereto.

Commented [A98]: If COM can task ENISA to do a report on a large-scale cybersecurity incident in a MS without MS being able to effectively manage the inputs provided to the report, it constitutes a possible infringment on national sovereignty.

There is a reasonable risk that information on causes, impacts and mitigations of a large-scale cybersecuirty incident in a highly critical sector in a MS involves sensitive or classified information.

Incident review reports should only be conducted on a voluntary basis and under the condition that relevant national authorities in the MS in question is consulted and have given their explicit approval prior hereto.

IRELAND

Ireland thanks the Spanish Presidency for the opportunity to provide further comments and textual suggestions on the draft Cyber Solidarity Act.

Ireland supports the comments made by several Member States on the importance of taking the time to ensure the proposal is legally sound and bring added value to the EU and its member states. We note that an impact assessment would greatly assist in this.

Ireland is also supportive of comments that have been made concerning possible duplication with existing initiatives. We would appreciate a considered gap analysis that would determine how the new structures and instruments proposed in the CSA will interact with existing structures, e.g. the CSIRTs and CyCLONe networks, and the European Cyber Security Competence Centre and Network. We look forward to engaging on amended text, or textual suggestions, when available.

Ireland supports the comments made by other Member States, and the Commission Legal Service, in relation to clarifying and strengthening the references to national security in the text. Equally, we look forward to seeing clarity on the voluntary nature of the proposal in the next iteration of the text.

Trusted Providers

To enable the Cyber Reserve to be used by and useful to Member States, Ireland believes that further clarity and certainty is required in terms of the selection of trusted providers. We are not convinced of the added value of the Cyber Reserve in the event of a strict application of article 12.5 DEP. The presence in the Single Market of suppliers of cutting edge security services and technologies owned and controlled by entities outside the Union cannot be disputed, nor can the important position they occupy within critical ICT supply chains. Ireland supports having an Emergency Mechanism that provides for a pragmatic and flexible approach, to ensure the effectiveness of this instrument. We will continue to reflect on the HWPCI discussions and consider how to ensure Article 16 can support the development of European cyber security capacity while ensuring the Cyber Reserve delivers services that are effective, state of the art, and achieve value for money.

Suggested amendment to Article 12(7):

12(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. Service providers that are established in the Union but are controlled from third countries shall not be excluded from participation where the mapping exercise shows Member States require these services to add value to the incident response. 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. Commission, where relevant, shall consult the High Representative.

Suggested amendment to Article 16(1)(a):

> (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, and the ability of services to quickly engage with and add value to Member State mechanisms;

In relation to Article 16.2, we propose deletion of point (d). Ireland does not have the legal structure to provide security clearance to personnel in this way, and we believe the risks are adequately addressed under (a) and (b).

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 the hardware and software technical equipment necessary to support the requested service;
(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) where it can deliver the service;
(j) once an EU certification scheme for managed security service Regulation (EU) 2019/881 is in place, the provider shall be certified in accordance with that scheme.

Support to Third Countries

We suggest some additional text in recital 37 and Article 17:

(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 spillover, 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. Recognising that support measures of this nature may encompass activities falling within the scope of CSDP Missions or the deployment of military or dual-use technologies, the Commission shall consult with the High Representative and the Council in assessing requests from third countries. In the event that this support is provided to cyber defence authorities or comprises measures falling within the scope of active cyber protection as set out in Directive EU 2022/2555, its deployment should based on a defensive strategy that excludes offensive measures. As the Union's principal cyber security incident response network, the CyCLONe Network established in Directive EU 2022/2555 shall advise the Commission in reviewing requests for support from the Cyber Reserve. 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.

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.

1. bis The Commission shall consult with the High Representative, the Council and the CyCLONe Network as established in Directive EU 2022/2555 in considering requests for support from third countries.

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 coordinate with the High Representative about the requests received and the implementation of the support granted to third countries from the EU Cybersecurity Reserve.

GERMANY

[…]

•Consistency with existing policy provisions in the policy area

The EU framework comprises several legislations already in place or proposed at Union level to reduce vulnerabilities, increase the resilience of critical entities against cybersecurity risks and support the coordinated management of large-scale cybersecurity incidents and crises, notably the Directive on measures for a high common level of security of network and information systems across the Union (NIS2)[5], the Cybersecurity Act[6], the Directive on attacks against information systems[7] the Commission Recommendation (EU) 2017/1584 on coordinated response to large-scale cybersecurity incidents and crises[8].

The actions proposed under the Cyber Solidarity Act cover situational awareness, information sharing, as well as support for preparedness and response to cyber incidents. These actions are consistent with and support the objectives of the regulatory framework in place at Union level, notably under Directive (EU) 2022/2555 ('the NIS2 Directive'). The Cyber Solidarity Act will especially build on and support the existing cybersecurity operational cooperation

Commented [A99]: We suggest a gap analysis to avoid duplication and to allocate our capacities, personal ones as well as financial ones.

[5] 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).

[6] 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).

[7] 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.

[8] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM/2022/454 final.

and crisis management frameworks, in particular European cyber crisis liaison organisation network (EU-CyCLONe) and the computer security incident response teams (CSIRTs) network.

The cross-border SOCs platforms 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 state of the art tools, and contributing to the development of Union capabilities and technological sovereignty.

Finally, this proposal is consistent with the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure[9] that 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.

[…]

2. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Stakeholder consultations**

The actions of this Regulation will be supported by DEP, which was subject to wide consultation. In addition, they will build on first steps that have been prepared in close cooperation with the main stakeholders. As regards SOCs, the Commission has developed a concept paper on the development of cross-border SOCs platforms and a Call for Expression of Interest in close cooperation with Member States in the framework of the European Cybersecurity Competence Centre (ECCC). In this context, a survey of national SOCs capacities was conducted and common approaches and technical requirements have been discussed within the technical working group of the ECCC that gathers representatives of

Member States. In addition, exchanges took place with industry, notably through the expert group on SOCs created by ENISA and the European Cyber Security Organisation (ECSO).

Secondly, as regards preparedness and incident response, the Commission has set up a short-term programme to support Member States, through additional funding allocated to ENISA from DEP, to immediately reinforce preparedness and capacities to respond to major cyber incidents. Member States' and industry's feedback gathered during the implementation of this short-term programme is already providing valuable insights that have fed into the preparation of the proposed Regulation to address identified shortcomings. This was a first step in line with the Council conclusions on the Cyber posture requesting the Commission to come forward with a proposal for a new Emergency Response Fund for Cybersecurity.

In addition, a workshop with Member States experts on the Cyber Emergency Mechanism was held on 16 February 2023, on the basis of a discussion paper. All Member States participated in this workshop and eleven Member States provided further contributions in writing.

- **Impact assessment**

Due to the urgent nature of the proposal, no impact assessment was carried out. The actions of this Regulation will be supported by the DEP and are in line with those set in the DEP Regulation, which was subject to a dedicated impact assessment. This Regulation will not entail any significant administrative or environmental impacts beyond those already assessed in the impact assessment of the DEP Regulation.

Furthermore, it builds on first actions developed in closed collaboration with the main stakeholders, as set out above, and follow up on Member States' call for the Commission to present a proposal on a new Emergency Response Fund for Cybersecurity by the end of Q3 2022.

Specifically, regarding situational awareness and detection under the European Cyber Shield, a Call for Expression of Interest to jointly procure tools and infrastructure to establish Cross-border SOCs, and a call for grants to enable capacity building of SOCs serving public and private organisations, were held under DEP cybersecurity work programme 2021-2022.

In the area of preparedness and incident response, as mentioned above the Commission has set up a short-term programme to support Member States from DEP, being implemented by ENISA. Services covered include preparedness actions, such as penetration testing of critical entities in order to identify vulnerabilities. It also strengthens possibilities to assist Member States in case of a major incident affecting critical entities. The implementation by ENISA of this short-term programme is under way and has already provided relevant insights that have been taken into account in the preparation of this Regulation.

Commented [A100]: It remains questionable why no impact assessment was drawn up in advance. The draft could have benefited from that, especially with respect to the interaction with other initiatives and for identifying the real requirements.

- **Fundamental rights**

By contributing to the security of digital information, this proposal will contribute to protecting the right to liberty and security in accordance with Article 6 of the EU Charter of Fundamental Rights, and the right to respect for private and family life in accordance with Article 7 of the EU Charter of Fundamental Rights. By protecting businesses from economically damaging cyberattacks, the proposal will also contribute to the freedom to conduct a business in accordance with Article 16 of the EU Charter of Fundamental Rights, and the right to property in accordance with Article 17 of the EU Charter of Fundamental Rights. Finally, by protecting the integrity of critical infrastructure in the face of cyberattacks, the proposal will contribute to the right to healthcare in accordance with Article 35 of the EU Charter of Fundamental Rights, and the right to access to services of general economic interest in accordance with Article 36 of the EU Charter of Fundamental Rights.

3. BUDGETARY IMPLICATIONS

The actions of this Regulation will be supported by funding under Strategic Objective 'Cybersecurity and Trust' of DEP.

Commented [A101]: Name of SO3 is "Cybersecurity and Trust"

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 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 WP from the period 2023-2027 which could bring 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.

An overview of the costs involved is included in the 'Legislative financial statement' accompanying this proposal.

4. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

The Commission will monitor the implementation, the application, and the compliance with these new provisions with a view to assessing their effectiveness. The Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council by four years after the date of its application.

- **Detailed explanation of the specific provisions of the proposal**

General Objectives, subject matter, and definitions (Chapter I)

Chapter I sets out the objectives of the Regulation to strengthen solidarity at Union level in order to better detect, prepare and respond to cybersecurity threats and incidents and in particular, to strengthen common Union detection and situational awareness of cyber threats and incidents, 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 and to enhance Union resilience by reviewing and assessing significant or large-scaleincidents. This Chapter also sets out the actions through which these objectives will be achieved: the deployment of a European Cyber Shield, the creation of a Cyber Emergency Mechanism and the establishment of a Cybersecurity Incident Review Mechanism. It also sets out the definitions used throughout the instrument.

The European Cyber Shield (Chapter II)

Chapter II establishes the European Cyber Shield and sets out its various elements and the conditions for participation. Firstly, it announces the overall objective of the European Cyber Shield, which is to develop advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union, as well as the specific operational objectives. It specifies that Union funding for the European Cyber Shield shall be implemented in accordance with the DEP Regulation.

Further, the chapter describes the type of entities that shall form the European Cyber Shield. The shield shall consist of National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs'). A National SOC shall be designated by each participating Member State. This shall 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. Following a Call for Expression of Interest, a National SOC may be selected by the ECCC to participate in a joint procurement of tools and infrastructures with the ECCC and to receive a grant for running the tools and infrastructures. If a National SOC benefits from Union support, it shall commit to apply participate in a Cross-border SOC within two years.

Cross-border SOCs shall consist of a consortium of at least three Member States, represented by National SOCs, who are committed to work together to coordinate their cyber detection and threat monitoring activities. Following an initial 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 and to receive a grant for running the tools and infrastructures. Members of the Hosting Consortium shall conclude a written consortium agreement which sets out their internal arrangements. This chapter then details the requirements for sharing information among the participants in a Cross-border SOC, and for sharing information

between a Cross-border SOC and other Cross-border SOCs, as well as with relevant EU entities. National SOCs participating in a Cross-border SOC shall share relevant cyber threat related information with one another, and the details, including the commitment to share significant amount of data and the conditions thereof should be defined in a consortium agreement. Cross-border SOCs shall ensure a high-level of interoperability between themselves. Cross-border SOCs should also conclude cooperation agreements with other Cross-border SOCs, specifying information sharing principles. Where 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. Chapter II concludes by specifying the security conditions for participating in the European Cyber Shield.

Cybersecurity Emergency Mechanism (Chapter III)

Chapter III establishes the Cyber Emergency Mechanism 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 or crises. Actions implementing the Cyber Emergency Mechanism shall be supported by funding from DEP. The Mechanism provides for actions to support preparedness, including coordinated testing of entities operating in highly critical sectors, response to and immediate recovery from significant or large-scale cybersecurity incidents or mitigate significant cyber threats and mutual assistance actions.

The Cyber Emergency Mechanism preparedness actions include the coordinated preparedness testing of entities operating in highly critical sectors. The Commission, after consulting ENISA and the NIS Cooperation Group, should regularly identify relevant sectors or subsectors from the Sectors of High Criticality listed in Annex I of Directive (EU) No 2022/2555, from which entities may be subject to the coordinated preparedness testing at EU level.

For the purpose of implementing the proposed incident response actions, this Regulation establishes an EU Cybersecurity Reserve, consisting of incident response services from trusted providers, selected in accordance with the criteria laid down in this Regulation. Users of the services from the EU Cybersecurity Reserve shall include Member States' cyber crisis management authorities and CSIRTs and Union institutions, bodies and agencies. The Commission shall have overall responsibility for the implementation of the EU Cybersecurity Reserve and may entrust, in full or in part, ENISA with the operation and administration of the EU Cybersecurity Reserve.

To receive support from the EU Cybersecurity Reserve, the users should take their own measures to mitigate the effects of the incident for which the support is requested. The requests for support from the EU Cybersecurity Reserve should include necessary relevant information about the incident and the measures already taken by the users. The Chapter

Commented [A102]: We wish a clarification of the conditions for such a coordinated testing

Commented [A103]: What does an "immediate recovery" mean in cases of cyber incidents?

Commented [A104]: There needs to be a clear procedure how this will be done. It is questionable whether this task should be assigned to the COM. See also comments under the relevant Article.

Commented [A105]: Are there funds foreseen for ENISA? And additional human resources? Otherwise, it would be inappropriate and not sustainable to put this on top of ENISA's list of tasks.

describes as well the implementation modalities, including assessment of requests to the EU Cybersecurity Reserve.

The Regulation provides as well for the procurement principles and selection criteria regarding trusted providers of the EU Cybersecurity Reserve.

Third countries may request support from the EU Cybersecurity Reserve where Association Agreements concluded regarding their participation in DEP provide for this. This Chapter describes further conditions and modalities of such participation.

Cybersecurity Incident Review Mechanism (Chapter IV)

At the request of the Commission, the EU-CyCLONe or the CSIRTs network, ENISA should review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. The review and assessment should be delivered by ENISA in the form of an incident review report to the CSIRTs network, the EU-CyCLONe and the Commission to support them in carrying out their tasks. When the incident relates to a third country, the report should be shared by the Commission with the High Representative. The report should include lessons learned and where appropriate, recommendations to improve the Union's cyber posture.

Final Provisions (Chapter V)

Chapter V contains amendments to the DEP Regulation, and an obligation for the Commission to prepare regular reports for the evaluation and review of the Regulation to the European Parliament and to the Council. The Commission is empowered to adopt implementing acts in accordance with the examination procedure referred to in Article 21 to: specify the conditions for this 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 a high level of data and physical security of the infrastructure and to protect the security interests of the Union when sharing information with entities that are not Member States public bodies; 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.

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

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[1]

Having regard to the opinion of the European Economic and Social Committee[2],

Having regard to the opinion of the Committee of the Regions[3],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(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.

(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 war against ~~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.

[1] OJ C […], […], p. […].

[2] OJ C , , p. .

[3] OJ C , , p. .

Formatted: Polish

(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[4], 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.

Commented [A106]: No logical connection → What comes first? The need or the investment?

(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[5], Commission Recommendation (EU) 2017/1584[6], Directive 2013/40/EU of the European Parliament and of the Council[7] and Regulation (EU) 2019/881 of the European Parliament and of the Council[8]. 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 and respond to cybersecurity threats and incidents. Member States have also invited the Commission to present a proposal on a new Emergency Response Fund for Cybersecurity in the Council Conclusions on an EU Cyber Posture[9].

---

4 https://futureu.europa.eu/en/

5 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).

6 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).

7 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).

8 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).

[9] 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)

(6) The Joint Communication on the EU Policy on Cyber Defence[10] 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.

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

(8) To achieve these objectives, it is also necessary to amend Regulation (EU) 2021/694 of the European Parliament and of the Council[11] 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 Cyber 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.

(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 the Financial Regulation 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

[10] Join Communication to the European Parliament and the Council EU Policy on Cyber Defence JOIN/2022/49 final

[11] 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).

general regime of conditionality for the protection of the Union budget as established in Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council.

(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.

(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 Parliament and of the Council[12].

(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.

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

Commented [A107]: From our perspective, there is no added value here with respect to existing structures. Please see below further details.

[12] 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).

(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.

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

(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.

(18) Entities participating in the European Cyber Shield should ensure a high-level of interoperability among themselves including, as appropriate, as regards data formats, 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 environment, entities participating in the European

Cyber Shield should be equipped with state-of-the-art and highly-secure tools, equipment and infrastructures. This should make it possible to improve collective detection capacities and timely warnings to authorities and relevant entities, notably by using the latest artificial intelligence and data analytics technologies.

(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[13].

(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.

(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.

(23) Without prejudice to Article 346 of TFEU, the exchange of information that is confidential pursuant to Union or national rules 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 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 Cyber Emergency

[13] 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).

Mechanism promotes solidarity between Member States in accordance with Article 3(3) of the Treaty on European Union ('TEU').

(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[14] 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[15], IPCR[16,] 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 and the affected Member State should be ensured. When requesting support under the Cyber Emergency Mechanism, the Member State should provide relevant information justifying the need for support.

(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.

---

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

15 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).

[16] 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.

(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[17]. 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.

(30) In addition, the Cyber 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 Cyber 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 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.

(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

[17] 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

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.

(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.

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

Commented [A108]: Similar to the discussion about CSA+, we have concerns about the scheme to certify the provider because no cybersecurity scheme has been adopted yet.
And ENISA needs an additional funding and workforce to fulfill all its tasks

(36) In order to support the objectives of this Regulation of promoting shared situational awareness, enhancing Union's resilience and enabling effective response to significant and large-scale cybersecurity incidents, the EU=CyCLONe, the CSIRTs network or the Commission should be able to ask ENISA to review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. After the completion of a review and assessment of an incident, ENISA should prepare an incident review report, in collaboration with relevant stakeholders, including representatives from the private sector, Member States, the Commission and other relevant EU institutions, bodies and agencies. As regards the private sector, ENISA is developing channels for exchanging information with specialised providers, including providers of managed security solutions and vendors, in order to contribute to ENISA's mission of achieving a high common level of cybersecurity across the Union. Building on the collaboration with stakeholders, including the private sector, the review report on specific incidents should aim at assessing the causes, impacts and mitigations of an incident, after it has occurred. Particular attention should be paid to the input and lessons shared by the managed security service providers that fulfil the conditions of highest professional integrity, impartiality and requisite technical expertise as required by this Regulation. The report should be delivered and feed into the work of the EU=CyCLONe, the CSIRTs network and the Commission. When the incident relates to a third country, it will also be shared by the Commission with the High Representative.

(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.

(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.

Commented [A109]: Does the Commission have the capacities and capability for this task?

(39) The objective of this Regulation can be better achieved at Union level than by the Member States. Hence, the Union may adopt measures, in accordance with the principles of subsidiarity and proportionality as set out in Article 5 of the Treaty on European Union. This Regulation does not go beyond what is necessary in order to achieve that objective.

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 infrastructure 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 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;

(b) to reinforce preparedness of entities operating in critical and highly critical sectors across the Union and strengthen solidarity by ~~developing~~ improving existing common response capacities against significant or large-scale cybersecurity incidents building upon those provisions established through DIRECTIVE (EU) 2022/2555, 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..

3. This Regulation is without prejudice to the Member States' ~~primary~~ sole 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:

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

(2) **'public body'** means a body governed by public law as defined in Article 2((1), point (4),), of Directive 2014/24/EU of the European Parliament and the Council[18];

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

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

(5) '**entities operating in critical or highly critical sectors'** means type of entities listed in Annex I and Annex II of Directive (EU) 2022/2555;

Commented [A110]: There is no need for new developments here since there are existing mechanisms within NIS2, see for example Art. 29 "Cybersecurity information-sharing arrangements" Para 1:

„Member States shall ensure that entities falling within the scope of this Directive and, where relevant, other entities not falling within the scope of this Directive are able to exchange on a voluntary basis **relevant cybersecurity information among themselves, 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 configuration of cybersecurity tools to detect cyberattacks,** where such information sharing"

Also, CyCLONe has already a relevant mandate, see for example Rec. 71 in NIS2:
„EU-CyCLONe should work as an intermediary between the technical and political level during large-scale cybersecurity incidents and crises and should enhance cooperation at operational level and support decision- making at political level. In cooperation with the Commission, having regard to the Commission's competence in the area of crisis management, **EU-CyCLONe should build on the CSIRTs network findings and use its own capabilities to create impact analysis of large-scale cybersecurity incidents and crises**.

Commented [A111]: Missing "national SOCs" definition. We refer to the understanding of so called SOCs as a platform for information sharing.

Commented [A112]: There should be no operational mandate of so called "Cross-border SOCs" which potentially duplicate tasks of the NIS2 CSIRTs NW.

For some examples of duplication please refer to Art. 15 (3):

CSIRTs NW shall have the following tasks:

(b)
to facilitate the sharing, transfer and exchange of technology and relevant measures, policies, tools, processes, best practices and frameworks among the CSIRTs;

(c)
to exchange relevant information about incidents, near misses, cyber threats, risks and vulnerabilities;

[18] 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).

(6) '**cyber threat'** means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881;

(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;

(11) **'trusted providers'** means managed security service providers as defined in Article 6, point (40), of Directive (EU) 2022/2555 selected in accordance with Article 16 of this Regulation.

Commented [A113]: Why limited to significant or large-scale incidents?

Chapter II

THE EUROPEAN CYBER SHIELD

Article 3

Establishment of the European Cyber Shield

1. An interconnected pan-European infrastructure of Security Operations Centres ('European Cyber Shield') shall be established ~~to develop advanced~~integrating existing capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union such as those structures implemented through DIRECTIVE (EU) 2022/2555. 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;

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

Commented [A114]: As other MS we agree on discussing the name, having less connotation to military terms, for instance that proposed by FRA or BEL.

Red line: Before establishing new structures, we need a thorough discussion among MS about remaining business cases for a SOC network apart from tasks covered by already existing networks established by NIS2 (CSIRTs NW, CyCLONe, Cooperation Group).

The role that SOCs can play in the context of better protection, detection and response and how this relates to the roles of CSIRTs is misleading in the current draft of the Act. In essence, SOCs and CSIRTs can be the same organisation in one MS and can mean in the end same people contributing to many networks with the same tasks.

Commented [A115]: As said before, we doubt the need for a new operational structure here. We want to refer to the CSIRTS / CyCLONe networks and the NIS cooperation group, because they can be seen as THE existing example for cross-border information sharing and might be a starting point for discussing potential improvements.

We recommend inviting the contribution of other actors and networks such as the CSIRTs Network, ECCC or CyCLONe members who are not necessarily participating in the negotiations of the CSoA, but whose practical view is needed in the further discussion.

Commented [A116]: This is almost exactly one of the tasks of the CSIRTs network (Art. 15 para 3 c, see above). Even before NIS2, many different tools (chat, share point, MISP) were established to enhance / enable this exchange. The decisive point is probably not a new infrastructure but the ability and willingness of Member States to share and to select the information that is worth sharing → Partly achieved by CSIRTs NW, members mainly share own findings about incidents and threats, not those of third parties, can be technically improved

Commented [A117]: There is no personnel to produce content

Commented [A118]: ENISA already tries to aggregate and share the information provided by the different teams (e. g. "heat map"). Regarding incidents, compared with NIS1, NIS2 provides for shorter reporting cycles towards the EU level and the respective numbers are regularly presented within the Cooperation Group.
→ Partly achieved by CSIRTs NW, collaboration with the aim that every Member State can produce the type of actionable information they need for their constituencies, could be technically improved, however AI probably is not what is needed here

(c) contribute to better protection and response to cyber threats;

Commented [A119]: A very generic task that probably every actor / committee / body within the complex EU cybersecurity ecosystem would claim → Achieved by **CSIRTs NW**, by sharing of assessments of vulnerabilities, and information about incidents that could have a cross border effect, (as specified in 23 (6) NIS2 / article 30 (2) NIS2)

(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 participate in the European Cyber Shield, each Member State shall designate at least one National SOC. The National SOC shall be a public body.

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.

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.

~~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/CSIRTs, committed to working together to, for example coordinate their cyber-detection and threat monitoring activities shall be eligible to participate in actions to establish a Cross-border SOC.

Commented [A120]: This especially depends on the information that is shared and what is done with it afterwards. The CSIRTs Network is in principle already a suitable forum but also an example of shortcomings.--> Achieved by **CSIRTs NW**,but can technically been improved

Commented [A121]: See general comments above on tasks of the CSIRTs NW referring to Art. 15 of NIS2.

These tasks are already achieved by CSIRTs NW as THE exchange network for national CSIRTs of EU Member States on operational information. This
especially includes CTI and information about incidents and vulnerabilities.
Most of the member CSIRTs also incorporate SOC functions or act as proxies for their SOCs.

Commented [A122]: Overall, this task is assigned to ENISA in support of the Member States as well as the EUIBAs.
There are many services and activities provided by ENISA, e. g. in the area of certification, organisation of exercises and trainings as well as situational awareness via diverse reports. Regarding the development of advanced artificial intelligence and
data analytics tools, the **ECCC** i. a. has the task to "support Union technological capacities, capabilities and skills in relation to the resilience and reliability of the infrastructure of network and information systems, including critical infrastructure and commonly used hardware and software in the Union" (Art. 3 para 1 b). → Partly achieved by **CSIRTs NW**, CSIRTs NW is acting as proxy towards national contingencies for operational topics. Furthermore, part of the tasks are mains tasks achieved by **ENISA** and/or **ECCC**.

Commented [A123]: Is there an obligation to apply?

Commented [A124]: This step sounds like a huge bureaucratic task and might interfere with national and operational decisions.

Commented [A125]: Deletion

Justification: In some MS like in Germany the National SOC is organizationally inseparable from the National Cyber Security Authority. An exclusion of the National SOC from the CSoA would thus result in an exclusion of the National Cyber Security Authority, which we feel is too much of a restriction.

Commented [A126]: Should be discussed: There should also be allowances for single or just two MS to apply for funding.

Commented [A127]: Is this a "must" when entering a hosting consortium? Are there considerations on alternative scenarios?

In general, funding opportunities as proposed by the CSoA are very welcomed and shall also be usable by CSIRTs/SOCs to build cooperation platforms on the basis of the needs of existing actors and networks,

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

Commented [A128]: Why should ECCC decide upon funding with operative effects? It is understandable that ECCC decides on funding but cross-border SOCs may also contribute to the "Cyber Shield" with operative implications. There should be a differentiation between funding and possible operational tasks as the ECCC has no mandate over these decisions.

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.

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.

Commented [A129]: This means the consortium needs to discuss the funding of the remaining resources individually?

Commented [A130]: Is this legally allowed? Can a MS be responsible for another one? Should be clarified by legal service.

Article 6

Cooperation and information sharing within and between cross-border SOCs

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) aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;

(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 amount of~~ 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)~~(b) targets for contribution to the development of advanced artificial intelligence and data analytics tools.

To encourage exchange of information between Cross-border SOCs, Cross-border SOCs shall ensure a high level of interoperability between themselves. ~~To facilitate the interoperability between the Cross-border SOCs, the Commission may, by means of implementing acts, after consulting the ECCC, specify the conditions for this~~

Commented [A131]: See general comments above on tasks of the CSIRTs NW referring to Art. 15 of NIS2 as well as Art. 29.

These tasks are already achieved by CSIRTs NW as THE exchange network for national CSIRTs of EU Member States on operational information and/or MS CSIRTs for their own constituency of public and private entities. This especially includes CTI and information about incidents and vulnerabilities.
Most of the member CSIRTs also incorporate SOC functions or act as proxies for their SOCs.

This whole article should be re-formulated based on a discussion of „business cases“ for cross-border SOCs or the „Shield“.

Commented [A132]: There should be – from a legal side – no obligation to share a significant amount of data.

Commented [A133]: Not clear what this implies. Either the legal basis, channels and benefit of sharing exist or they do not. To overcome this by thinking of incentives is naïve and does not reflect certain constraints.

~~interoperability.~~ ~~Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation.~~

Commented [A134]: There should be no top down decisions on interoperability questions from Com side.
Also, the ECCC is not a place for operative decisions. → deletion

3. Cross-border SOCs shall conclude cooperation agreements with one another, specifying information sharing principles among the cross-border platforms.

Article 7

~~**Cooperation and information sharing with Union entities**~~

~~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.~~

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

Article 8

Security

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.

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. 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.

Chapter III

Formatted: Justified, Indent: First line: 0 cm, Right: 2.18 cm, Space Before: 6 pt, After: 0 pt, Add space between paragraphs of the same style, Line spacing: single, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.4 cm + Indent at: 0.84 cm, No widow/orphan control, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Commented [A135]: Additional point: Would a consortium be free to decide which info is transmitted to other actors. Who has the „last" responsibility/what if one member of the cross-border SOC is not willing to share.

Commented [A136]: In our view there is no need for another "feed" from MS SOCs towards EU CyCLONe. Rather, it is of utmost importance to "feed in" information flows via the National CSIRTs/SPoC and the CSIRTs NW as the exchange network for operational exchange. Opening parallel communication lines are leading to confusion among national stakeholders. The cooperation and information sharing arrangements between CSIRTs NW and CyCLONe are already covered in NIS2 (see for example Art. 15 (6)) → should be deleted

Information that is used in SOCs for detection is very, very technical. Information that is shared on such a platform would be list of IPs or other indicators for detection. This can be considered a feed for the CSIRTs NW but not for the EU CyCLONe or the Commission (as a political entity). This would completely mix the specializations between technical and strategical level.
Potential Compromise: Delivering aggregated reports to the political level.

Commented [A137]: Scrutiny reservation: Requirements very vague. Why is an implementing act necessary instead of taking existing requirements being proposed by NIS2 or existing European/international standards?

CYBER EMERGENCY MECHANISM

Article 9

Establishment of the Cyber Emergency Mechanism

1. A Cyber Emergency Mechanism is established to improve the Union's resilience to ~~major cybersecurity~~ large scale cybersecurity incidents ~~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 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.

Commented [A138]: Terminology: A threat does not necessarily lead to an emergency. Why not use „large scale" as proposed in the Context of CyCLONe-NW (Art. 16 (1) NIS2)

Article 10

Type of actions

Commented [A139]: We need clarification about the actions of the mechanism and the role of the EU Commission (see comments in the paragraphs below)

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 providers participating in the EU Cybersecurity Reserve established under Article 12;

~~**1.1.** 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.~~

Commented [A140]: Isn't this already done through the EU-CyCLONe (Art. 16 (3)) EU Directive 2022/2555) and also the CSIRTs in Art. 10 (4), Art. 10 (7), Art. 11 (3), Art. 11(5), Art. 13 (5) EU Directive 2022/2555? A relevant cross-references to EU Directive 2022/2555 is also made in this draft Regulation in Art. 11.
What is the added value of the Mechanism?
How can double structures be avoided in this regulation, since these tasks are already clearly defined in EU Directive 2022/2555?

Commented [A141]: From our understanding, this is already laid down as a CSIRT task in Art. 11(5) EU Directive 2022/2555. Also relevant: Part of it is already an EU-CyCLONe task (see Art. 16 (3d-e) EU Directive 2022/2555)? Duplication and no added value.

Article 11

Coordinated preparedness testing of entities

Commented [A142]: We need clarification about the "coordinated preparedness testing" (art. 10) and the role of the Commission in this scenario.

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

~~• 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.~~

Commented [A143]: These are questions and responsibilities of member-states, e.g. according to NIS2. No task for the Commission.
Not clear what the added value is of the "coordinated preparedness testing of entities", since a clear cross-reference is made to a specific Article in Directive (EU) 2022/2555. Therefore, this seems to be a duplication, which can be deleted, as it is already regulated in a Directive.

Commented [A144]: Not clear what the added value is of this paragraph on the "coordinated preparedness testing of entities is", since the tasks of the NIS Cooperation Group are already laid down in Art. 14 of EU Directive 2022/2555. Therefore, this seems to be a duplication, which can be deleted, as it is already regulated in a Directive.

Article 12

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.

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.

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.

~~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.~~

~~5.~~4. The Commission shall have ~~overall~~ a shared responsibility with the MS for the implementation of the EU Cybersecurity Reserve. The Member States and 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.

~~6.~~5. The Commission may entrust the operation and administration of the EU Cybersecurity Reserve, in full or in part, to ENISA, by means of contribution agreements.

~~7.~~6. In order to support the Member States and 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 Member States and 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.

~~8.~~7. The Commission may, by means of implementing acts, specify the types and the number of response services required for the EU Cybersecurity Reserve. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2).

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

Commented [A145]: Are those services managed by MS themselves? What will be their respective tasks therein?

Commented [A146]: The use of services is mandatory („shall"). This is not a decision taken by the MS, but by the victim itself.

Commented [A147]: The German Federal Office for Information Security already offers support to entities in critical or highly critical sectors. In our view, this would lead to a duplication of support structures and undermine each Member States' national sovereignty in handling incidences as foreseen in Art. 10 (1) of the EU Directive 2022/2555.

What is the added value of "pre-committed services" (see paragraph 2)? What are these services? What would happen in the case that more than the "pre-committed services" are needed? How quickly can such services be accessed in the case of a major cyber incident, if the Commission needs to be contacted regarding the contact details from companies on the reserve list (see paragraph 5)? This could lead to an additional bureaucratic effort instead of each Member State being able to immediately react to a cyber incident with its own available means.

Commented [A148]: The COM has the whole responsibility and power. This is not a wishful situation from the perspective of a Member State. There should be a co-responsibility.

Maybe a task for the NIS Cooperation Group?

Commented [A149]: Needs to be discussed on the basis of the commentary above. There should always be a shared responsibility. While ENISA can act as a secretary there should be a clear description of decision opportunities by MS.

Please consider that funds/staff needs to be reserved for ENISA.

Commented [A150]: This should also be discussed in the context of Cyber Diplomacy.

Commented [A151]: From a practical point of view, a new instrument should be used and tested by MS first. Participation of third countries should not be a priority and should be postponed to a later stage.

Commented [A152]: To include third countries is a political decision that needs to be considered carefully, also from a geopolitical perspective. There should not be a scenario where COM decides on priorities and support alone.

Commented [A153]: What about long-term recovery? This often also poses a challenge and can be very cost intense.

Commented [A154]: In Art.12 there was an obligation to use services, but „may" is more appropriate.

Commented [A155]: Users are not necessarily the victims which have the responsibility in the first place.

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

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 delay.

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 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).

Commented [A156]: Why? Which information exactly. What about national sovereignty and victim's protection, if wished? Information can also be given in an abstract form without indicating details about the victim.

Commented [A157]: And maybe also other countries being officially requested as this avoids a situation with strange outcomes. For instance, a country like Moldavia asks Russia and the EU alike for help.

Commented [A158]: As already asked in our comment in Art. 12(4): How quickly can such services be accessed in the case of a major cyber incident, if the Commission needs to be contacted regarding the contact details from companies on the reserve list (see paragraph 5)? This could lead to an additional bureaucratic effort instead of each Member State being able to immediately react to a cyber incident with its own available means

Commented [A159]: What is the competence of the COM as a non-operational actor to assess the following criteria? It sounds ambitious and almost impossible: to assess the request (according to a) – e)) and to respond without delay. Will the COM have a 24x7 entity for this?

Commented [A160]: Can all these criteria be made transparent by the victim/user of the service in all cases?

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.

4. The agreements referred to in paragraph 3 may be based on templates prepared by ENISA, after consulting Member States.

5. Member States, ~~T~~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.

6. Within one month from the end of the support action, the users shall provide Commission and ENISA with a summary report about the service provided, results achieved and the lessons learned. When the user is from a third country as set out in Article 17, such report shall be shared with the High Representative.

7. The Commission shall report to the NIS Cooperation Group about the use and the results of the support, on a regular basis.

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[19], the support under this Regulation for responding to such incidents shall complementactions 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 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.

4. Support under the Cyber Emergency Mechanism may form part of the joint response between the Union and Member States in situations referred to in Article 222 of the Treaty on the Functioning of the European Union.

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:

Commented [A161]: When the user is a MS CSIRT → is it not necessary to make an agreement with the victim as well?

Commented [A162]: Depending on the incident, there might be more time needed.

Commented [A163]: Is there a competence for regulating this area within this legal act?

Commented [A164]: Who will this be? The user?

[19] 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).

(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.

(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.

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 the hardware and software technical equipment necessary to support the requested service;

(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) where it can deliver the service;

(j) once an EU certification scheme for managed security service Regulation (EU) 2019/881 is in place, the provider shall be certified in accordance with that scheme.

Commented [A165]: We agree to the selected criteria. More details should be discussed when drafting the scheme.

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 coordinate with the High Representative about the requests received and the implementation of the support granted to third countries from the EU Cybersecurity Reserve.

Commented [A166]: This should also be discussed in the context of Cyber Diplomacy

Commented [A167]: MS are not informed about this or have no legal possibility to acquire this information. Therefore, this needs to be changed.

Commented [A168]: MS should play a role in decision making here.

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. Participation in this review is voluntary for Member States. Following the completion of a review and assessment of an incident, ENISA shall deliver an incident review report to the CSIRTs network, the EU-CyCLONe and the Commission to support them in carrying out their tasks, in particular in view of those set out in Articles

15 and 16 of Directive (EU) 2022/2555. Where relevant, the Commission shall share the report with the High Representative.

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

3. The report shall cover a review and analysis of the specific significant or large-scale cybersecurity incident, including the main causes, vulnerabilities and lessons learned. It shall protect confidential information, in accordance with Union or national law concerning the protection of sensitive or classified information.

4. Where appropriate, the report shall draw recommendations to improve the Union's cyber posture.

5. Where possible, a version of the report shall be made available publicly. This version shall only include public information.

Commented [A169]: Is this obligatory?
There is a bureaucratic burden laid down on MS to read reports and comment on it.
Also, it can lead to strange situations when one of the responsible actors asks ENISA to provide a report on an incident when a certain MS is not willing to collaborate. ENISA shall not have a supervisory role towards MS. If information from MS is needed the existing channels and procedures should be used.

Commented [A170]: Red line: There shall be no direct collaboration of ENISA with entities affected. This mandate lies clearly within the MS authorities. Those requests should be channeled via the MS responsible authorities.

Commented [A171]: Classified information cannot be processed at the moment.

Commented [A172]: A "blaming and shaming" should be avoided. There needs to be mechanism for a victim/MS to agree on the report overall/ or make changes.

Commented [A173]: Many challenges: Who/what prevents ENISA from being overloaded with unnecessary requests.

What are the obligations by MS to participate in this activity? → There should be no obligation if a MS has fundamental reasons not to provide assistance to this. Maybe refer to the peer review mechanism in NIS2 here ("participation is voluntary"). There also other provisions that can be taken from Art. 19 NIS2.

What about legal requirements to contact all involved parties?

[…]

[47] As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 20 % for collection costs.

FRANCE

[…]

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

[…]

(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.

(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 operational, technical and political ~~all~~ levels of the Union's cybersecurity framework. Strengthening the EU resilience to cyber threat ~~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 for , 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.

(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[13] , 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 along with feed cybersecurity cooperation network such as the CSIRT network, 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.

[…]

Commented [A174]: FR supports the overall objective of the proposal aiming à structuring the european cyber ecosystem within the incident response realm, through the establishment of a cyber reserve supporting national competent authorities to prevent, face and response to cyber incidents

FR is still in the process of analyzing the text and will come back with other proposals.

Commented [A175]: FR suggests to precise the level involved.

Commented [A176]: FR suggests to include the fact that there is an overall objective of strengthening the EU resilience to prepare, face and response to cyber threat.

Commented [A177]: FR suggests to include the fact that there is an overall objective of strengthening the EU resilience to prepare, face and response to cyber threat.

Commented [A178]: FR suggests to put an emphasis on the articulation with the CSIRT network.

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

(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~~XXX) should be deployed to build and enhance common detection and situational awareness capabilities and should be monitored by the CSIRT network as a tool that would facilitate to conduct analysis ; a Cybersecurity Emergency Mechanism should be established to support Member States in anticipating, preparing for, responding to, mitigating the impacts of and ~~immediately~~ gradual 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 when requesting by member states cyber cooperation network or the EUIBAS and should keep updated them updated by providing a state of play of the work achieved with regards to the request. 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[14] 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~~ XXX and the Cyber 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.

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

(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.

Commented [A179]: FR suggests to specify that the SOC project should be monitored by the CSIRT network in order to avoid duplications of activities. If the CSIRT network monitors the cross border soc then it would be easier to distinguish the activities that relate to the CSIRT network and those that relate to the SOC project

Commented [A180]: FR suggests to delete the wording of immediate recovery as the recovery takes a long time and could be up to 1 year for some operation.

Commented [A181]: FR : it is difficult to immediately recover from large scale cyber incidents and it might take a long time (i.e. 6months or more). In order to keep it flexible, it might be relevant to refer to mitigate the impacts of the incidents and ensuring a smooth recovery.

Commented [A182]: FR suggests to specify the process that would be put in place.
ENISA should keep updated CyCLONe / CSIRT network of the work achieved by providing a report of state of play of the activities conducted.

Commented [A183]: FR would like to be provided with clarifications on this proposal.

[14] 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).

(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~~'XXX'), comprising of several interoperating cross-border platforms, each grouping together several National SOCs Coordinator. 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~~be monitored by the CSIRT network and used as a tool to increase detection of cybersecurity threats and incidents and thus complement and support Union entities and networks responsible for crisis management in the Union. For example, relevant information should be shared to , ~~notably~~ the EU Cyber Crises Liaison Organisation Network ('EU-CyCLONe') in order to support the network to conduct its activities, as defined in Directive (EU) 2022/2555 of the European Parliament and of the Council[15], on the basis of the Standards rules of procedures and Terms of reference established under within the CSIRT network.

(13) Pursuant to the Directive (EU) 2022/2555, article 10(1), each Member State shall designate or establish one or more CSIRTs~~Each Member State~~. As CSIRTs are in charge of coordinating alerts at national level, - ~~should~~National CSIRT could be ~~–~~designated as ~~a public body at national level tasked with~~ coordinating cyber threat detection activities at ~~in that Member State~~national level and then, being identified as the National SOC Coordinator.

(14) ~~–~~These National SOCs Coordinator should act as a reference point and gateway at national level for participation in the European Cyber ~~Shield~~ XXX 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.

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

(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~~ tool ~~that is complementary to~~at the disposal of the CSIRTs network, by pooling and sharing data on cybersecurity threats from public and private entities, enhancing the value of such data

Commented [A184]: FR suggests to deal with National SOC coordinator as it is technically incorrect to deal with national SOCs as a SOC has a limited perimeter and functions.

Commented [A185]: FR suggests to specify that the SOC platform is monitored by the CSIRT network to avoid duplications of activities between the two and if so, then, EU CyCLONe could be informed on the basis of the specific CSIRT network TORs/SOPs.

Commented [A186]: FR : CyCLONe has a key role to play to draw the situational awareness picture in the EU. Information should be shared to the network in order to support the network to conduct its activities.

Commented [A187]: FR suggests to designate the national CSIRT as the coordinating entity as it will be easier practically to coordinate alerts.

Commented [A188]: FR consider the SOC platform could provide a benefic tool to the CSIRT network in its activities.

[15] 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).

through expert analysis and jointly acquired infrastructures and state of the art tools, and contributing to the development of Union capabilities and technological sovereignty.

(16) The Cross-border SOCs should act as a central point allowing for a broad pooling of relevant data and cyber threat intelligence, enable the spreading of threat information among a large and diverse set of actors (e.g., Computer Emergency Response Teams ('CERTs'), CSIRTs, Information Sharing and Analysis Centers ('ISACs'), operators of critical infrastructures). The information exchanged among participants in a Cross-border SOC could include data ~~from networks and sensors, threat intelligence feeds, indicators of compromise, and contextualised information about incidents, threats and vulnerabilities~~that would be defined among the participating National SOC coordinators. In addition, Cross-border SOCs should also enter into cooperation agreements with other Cross-border SOCs.

Commented [A189]: FR suggests to keep it flexible as the listing could be interpreted in a prescriptive way. Each network SOC will have to determine the scope of their activities and what they consider to be relevant during the sharing process.

(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.

Commented [A190]: FR suggest to rephrase this paragraph by taking into account the fact that the SOC platform is understood as the CSIRT network tool and monitored by the CSIRT network.
FR will provide with wording at a later stage.

(18) Entities participating in the European Cyber ~~Shield~~ XXX should ensure a high-level of interoperability ~~among themselves including, as appropriate, as regards data formats, 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.

Commented [A191]: FR suggests to withdraw this part in order to keep it flexible and let the details defined by the parties of the consortium.

(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~~ XXX should be equipped with state-of-the-art and highly-secure tools, equipment and infrastructures. This should make it possible to improve collective detection capacities and timely warnings to authorities and relevant entities, notably by using the latest artificial intelligence and data analytics technologies.

(20) By collecting, sharing and exchanging data, the European Cyber ~~Shield~~ XXX 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~~ XXX with the pan-European High Performance Computing infrastructure established

by Council Regulation (EU) 2021/1173[16] and following orientations defined within the Stategic agenda of the European Cybersecurity Competence Centre.

(21) While the European Cyber ~~Shield~~ XXX 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. Interaction between t~~T~~he ~~development of the~~ European Cyber ~~Shield~~ XXX and ~~should~~ the cyber defense community should be foreseen once the European Cyber XXX is established~~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~~.

(22) Information sharing among participants of the European Cyber ~~Shield~~ XXX should be based on a voluntary basis and 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.

(23) Without prejudice to Article 346 of TFEU, the exchange of information that is confidential pursuant to Union or national rules 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 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 Cyber Emergency Mechanism promotes solidarity between Member States in accordance with Article 3(3) of the Treaty on European Union ('TEU').

(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~~as well as the crisis coordintaion provided ~~by~~through ~~from~~ the EU-CyCLONe.

(26) Coordination should be foreseen between the Emergency mechanism ~~, as well as~~and mutual assistance between Member States ~~including~~ in the context of Article 42(7) of TEU, the

[16] 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).

Commented [A192]: FR suggests to refer to the strategic agenda of the ECCC and the general orientations provided by the document when referring to fundings of innovation / industrial and research projects.

Commented [A193]: FR suggests to specify that interaction are possible but the Cyber XXX should be distingushed from the developments that could be done within the defense realm

Commented [A194]: FR would like to stress the importance of voluntary cooperation between member states when dealing with sharing information. It is on the same basis that what is done within CyCLONe and the CSIRT network.

Commented [A195]: FR : suggestion to recall the role of CyCLONe.

PESCO Cyber Rapid Response Teams[17] 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.

Commented [A196]: FR suggests to differentiate assistance that falls within the scope of the civilian realm and assistance within the security and defense realm (i.e. PESCO project)

(26) This instrument is without prejudice to procedures and frameworks to coordinate crisis response at Union level, in particular the UCPM[18], IPCR[19], 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 and the affected Member State should be ensured. When requesting support under the Cyber Emergency Mechanism, the Member State should provide relevant information justifying the need for support.

(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.

(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

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

[18] 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).

[19] 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.

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[20]. 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.

(30) In addition, the Cyber 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 Cyber 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 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.

(33) A Union-level Cybersecurity Reserve should gradually be set up, consisting of services from private providers of managed security services to support response, mitigate the impacts of and ~~immediate~~ ensure the gradual 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.

(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.

Commented [A197]: FR would like to get more insights on this proposal

Commented [A198]: FR suggests to withdraw immediate as it is difficult to define.
Also, it is difficult to immediately recover from large scale cyber incidents and it might take a long time (i.e. 6months or more). In order to keep it flexible, it might be relevant to refer to mitigate the impacts of the incidents and ensuring a smooth recovery.

[20] 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

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

(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. ENISA should keep informed member states cooperation network such as EU-CyCLONe, the CSIRT network and NIS cooperation group of the ongoing work achieved in order to avoid duplications of activities and ensure coordination between them. 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 with due respect of Member states competences, 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.

Commented [A199]: FR suggests that ENISA should informed member states cooperation network in order to avoid duplications of activities between them (CyCLONe, NIS CG)

Commented [A200]: FR suggests to define that if ENISA is in contact with the private sector it should be respectful of the competences of the national cybersecurity authorities.

(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, mitigate the impacts of -and enhance a gradual ~~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.

Commented [A201]: FR suggests to open up the reserve to third countries in the European political community as it would strengthen the EU resilience to face cyber threats.
This opening should be based on specific fundings.

(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.

(39) The objective of this Regulation can be better achieved at Union level than by the Member States. Hence, the Union may adopt measures, in accordance with the principles of subsidiarity and proportionality as set out in Article 5 of the Treaty on European Union. This Regulation does not go beyond what is necessary in order to achieve that objective.

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 infrastructure of Security Operations Centres ('European Cyber XXX~~Shield~~') to build and enhance common detection and situational awareness capabilities falling within the scope of the CSIRT network;

(b) the creation of a Cybersecurity Emergency Mechanism to support Member States in preparing for, responding to, mitigating the impacts of and gradualy ~~immediate~~ recovering~~y~~ from significant and large-scale cybersecurity incidents;

(c) the establishment of a European Cybersecurity Incident Review Mechanism to support Member states actions in the review and assessment of 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 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;

(b) to reinforce preparedness of entities operating in critical and highly critical sectors across the Union and strengthen solidarity by strengthening the EU capacities to ~~developing common~~ respond~~se capacities~~ ~~against~~ to 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 while ensuring close coordination cyber cooperation network such as NIS Cooperation Group, EU CyCLONe and the CSIRT network, including drawing lessons learned and, ~~where appropriate~~upon the request of Member states, non binding recommendations~~.~~.

Formatted: Highlight

Commented [A202]: FR suggests to include the European cyber XXX within the CSIRT in order to ease the identification of activities between the two.
The CSIRT network is **a network where members can cooperate, exchange information and build trust**. Members are able to improve the handling of cross-border incidents and discuss how to respond in a coordinated manner to specific incidents.
According to the NIS2 Directive, the CSIRT network aims to " (a) to exchange information about the CSIRTs' capabilities; (b) to facilitate the sharing, transfer and exchange of technology and relevant measures, policies, tools, processes, best practices and frameworks among the CSIRTs; (c) to exchange relevant information about incidents, near misses, cyber threats, risks and vulnerabilities; (d) to exchange information with regard to cybersecurity publications and recommendations; (e) to ensure interoperability with regard to information-sharing specifications and protocols; (f) at the request of a member of the CSIRTs network potentially affected by an incident, to exchange and discuss information in relation to that incident and associated cyber threats, risks and vulnerabilities; (g) at the request of a member of the CSIRTs network, to discuss and, where possible, a coordinated response to an incident that has been identified within the jurisdiction of that Member State;".

Then the activities foreseen for the SOC platform falls within the scope of the CSIRT network activities.

In order to improve the CSIRT network capabilities to monitor an incident, the outcomes from the Cross border SOC might provide solid ground to conduct analysis.

Thereof, it might be logical to link the CSIRT network and the cross border platform and consider the latter as a tool at the disposal of the CSIRT network to support it in fulfilling its mission.

Commented [A203]: FR : it is difficult to immediately recover from large scale cyber incidents and it might take a long time (i.e. 6months or more). In order to keep it flexible, it might be relevant to refer to mitigate the impacts of the incidents and ensuring a smooth recovery.

Commented [A204]: FR : member states cooperation network have a key role to play to review and assess significant or large scale incidents.
This mechnaism should be established to support their actions.

Commented [A205]: FR suggests to deal with the « strenghening of EU capacities to respond to large scale cyber incidents » as the EU SOC pilot project is more about pooling information and benefiting from the analysis.

Commented [A206]: FR proposes to open up the reserve to third countries in the european political community in order to boost the EU resilience to face / respond/ recover from cyber incidents.

Commented [A207]: FR : the review mechanisms should be done in coordination with Member states in order to avoid duplications of activities with cyber cooperation network (CyCLONe, CSIRT network and NIS CG).

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:

(1) **'~~Cross-border Security Operations Centre~~Cyber threat intelligence platform' ("~~Cross-border SOC~~CTI Plantform")** means a ~~a multi-country~~ platform~~,~~ that ~~brings~~ together in a coordinated network structure national SOCs coordinators ~~from at least three Member States~~ and representatives from the private sector who form a Hosting Consortium,~~-~~and that is designed to detect and analyse ~~prevent~~ cyber threats and incidents and that would ~~o~~ support the production of ~~high-quality intelligence~~ reports, notably through the voluntary exchange of data from open source, ~~various sources,~~ public and private sources, and based ~~s well as throughon~~ the sharing of state-of-the-art tools ~~and jointly developing cyber detection, analysis, and prevention and protection capabilities in a trusted environment~~**;**

(2) **'public body'** means a body governed by public law as defined in Article 2((1), point (4),), of Directive 2014/24/EU of the European Parliament and the Council[21];

(3) **'Hosting Consortium'** means a consortium composed of participating states, represented by National SOCs coordinators and representatives from the private sector, that have agreed to establish and contribute to the acquisition of tools and infrastructure for, and operation of, a Cross-border SOC ;

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

(5) '**entities operating in critical or highly critical sectors'** means type of entities listed in Annex I and Annex II of Directive (EU) 2022/2555;

(6) '**cyber threat'** means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881;

(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 mitigate the risk of significant or large scale cybersecurity incident along with ensure an effective ~~rapid~~ and timely response to a significant or large-scale cybersecurity incident, obtained as a result of risk assessment and anticipation scenario, training and monitoring actions taken in advance;

Commented [A208]: FR suggests to withdraw primary responsability as it is the sole competence of Member states to deal with national security and defense interests.

Commented [A209]: FR : suggestion to deal with CTI platform instead of cross border SOC, then it would not prevent the private sector to be associated to the platform.
As a platform, it is a tool that could be used by the CSIRT network.

Commented [A210]: See supra the rational supra regarding National soc coordinator

Commented [A211]: FR would like the PCY to provide with explanation regarding this number.

Commented [A212]: FR considers the role of a SOC is to detect and analyse incidents. We should specify it in the text to avoid any duplications with the CNW

Commented [A213]: FR considers that voluntary exchange of data should be key

Commented [A214]: FR underlines that detection capacities fall within the scope of national competence and can not be pooled with other EUMS.

Commented [A215]: FR : see comment above

Commented [A216]: FR considers that preparedness is also about how to avoid that the risk happens along with based on training and anticipation scenario. Our wording proposal take into account article 9 of directive EU 2022/2555.

[21] 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).

(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;

(11) **'trusted providers'** means managed security service providers as defined in Article 6, point (40), of Directive (EU) 2022/2555 selected in accordance with Article 16 of this Regulation.

Chapter II

THE EUROPEAN CYBER XXX

Article 3

Establishment of the European Cyber XXX

1. An interconnected pan-European infrastructure of Security Operations Centres ('European Cyber XXX') shall be established to develop advanced capabilities for the Union to detect, and analyse data on cyber threats and incidents in the Union. It shall be deployed by the CSIRT network and feed the CSIRT network analysis.
2. It shall consist of all National Security Operations Centres coordinator ('National SOCs coordinators') and Cross-border Security Operations Centres ('Cross-border SOCs').

Actions implementing the European Cyber XXX 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 XXX ~~Shield~~ shall:

(a) collect ~~pool and share~~ data on cyber threats and incidents from open source, and ~~various sources~~public and private sources through cross-border SOCs;

(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 support the CSIRT network in the activities better protection and response to cyber threats;

(d) contribute to ~~faster~~ enhance the EU detection capabilities 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 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 along with due respect of developments stated within the strategic agenda of the European cybersecurity competence center.

Commented [A217]: FR considers that the SOC has a role to detect incidents and provide an analysis based on the data collected.In our view, the analysis should be processes by the CSIRT network

Commented [A218]: FR : in order to avoid duplication of activities with the CSIRT network the cross border SOC should be deployed within the CSIRT network, like that it would be a tool at the disposal of the CSIRT and enable a smooth respond in case of crisis or large scale cyber incidents

Commented [A219]: See comment supra

Commented [A220]: FR considers this activity falls within the scope of the CSIRT network (art 11 3. Directive EU 2022/2555).

Commented [A221]: FR suggests to withdraw this part, as it is similar to the 3.b

Commented [A222]: FR would like to precise the type of sources involved.

Commented [A223]: FR considers the financing of innovation projects/new technologies falls within the scope of the ECCC. In order to ensure coherent developments, reference to the strategic agenda of the ECCC might help to guide the funding of projects.

Article 4

National Security Operations Centres Coordinators

1. In order to participate in the European Cyber Shield, each Member State shall designate at least one National SOC Coordinator. The National SOC Coordinator shall be a public body.

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.

Following the Directive (EU) 2022/2555, article 10(1) inviting each Member State to designate or establish one or more CSIRTs. National CSIRT could be designated to coordinate cyber threat detection activities at national level and then, being identified as the National SOC Coordinator.

2. Following a call for expression of interest, National SOCs Coordinator 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 Coordinator 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 Coordinator shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

3. A National SOC coordinator selected pursuant to paragraph 2 shall be encouraged to ~~commit~~ to voluntarily 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 Coordinators and representatives from the private sectors, committed to working together to

Commented [A224]: FR : as stated above, SOC have a limited perimeter and are specific to each entity. FR would prefer to use the terminology of National SOC, in order to be more targeted and specific.

Formatted: Indent: Left: 0 cm, First line: 0 cm

Commented [A225]: FR suggests to designate the national CSIRT as the coordinating entity as it will be easier practically to coordinate alerts.

Formatted: Font:

Formatted: Manual Considérant

Commented [A226]: FR would like the PCY to provide some explanation during the next HWPCI on this part.

Commented [A227]: FR : Member states should only be encouraged to participate in a Cross-boder SOC and it should not be compulsory.

Commented [A228]: FR : the Cross border SOC is also about pooling data from the private sector. A participation of private entities to the Cross border security operations centres should be envisionned.

coordinate their cyber-detection and threat monitoring activities shall be eligible to participate in actions to establish a Cross-border SOC.

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

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 Coordinator 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 SOCs

1. Members of a Hosting Consortium shall exchange ~~relevant~~ information on a voluntary basis among themselves within the Cross-border SOC, that would be defined between the parties of the consortium ~~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) aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;~~

The exchange of such information might support the CSIRT network activities through the enhancement of

~~(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

Commented [A229]: FR would like the PCY to provide clarifications on the budget aspect during the next HWPCI.

Commented [A230]: FR considers that :
1/ information should be shared on a voluntary basis. In order to guarantee trust between MS and the quality of the information they share we should give sufficient leaway to MS to share relevant information.
2/ information that can be shared should be defined betweeen the members of the hosting consortium under contractual provisions and not under the legislative proposal in order to keep it flexible. Also, information refered in the part 1 are in duplications with article 15 3 c and a of NIS2 concerning CSIRT network activities.

Commented [A231]: FR : suggestion to withdraw this part as it is in duplication of the activity of the CSIRT network (please refer to article 15 3 of NIS2)

Formatted: Normal

Commented [A232]: FR would like to withdraw, as it falls within the scope of national security and defense interest.

Commented [A233]: FR underlines that duplicate the CSIRT network activities (art. 11 3. b and g).

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

4. Cross-border SOCs shall conclude cooperation agreements with one another, specifying information sharing principles among the cross-border platforms.

Article 6 bis

Articulation between the CSIRT network and the European Cyber XXX

1. The Cross border platform shall be established without duplicating the activities of the CSIRT network, as defined by the article 15 (3) of the Directive (EU) 2022/2555.
2. The Cross border platform should be understood as a tool at the disposal of the CSIRT network to conduct the activities defined by the Directive (EU) 2022/2055 and be monitored by the CSIRT network.
3. The CSIRT network internal procedures should defined the articulation envisioned with the European Cyber XXX.

Article 7

Cooperation and information sharing with Union entities

1. ~~1.~~ Information collected by the CTI platform should be shared to the CSIRT network in order to support the network in the daily performance of their missions following the Directive (EU) 2022/2555.
2. The CSIRT network could afterwards share the information to EU-CyCLONe on the basis of their internal procedures.
3. The CSIRT network could also inform the Secretariat of the IICB in order to keep informed the EUIBAS.

Commented [A234]: FR : suggestion to withdraw as it is the role of the CSIRT network (article 15 3. g and 15. 3 j of NIS2)

Formatted: Font: Bold, Not Italic

Formatted: List Paragraph,Listaszerű bekezdés1,List Paragraph à moi,Colorful List - Accent 11,Medium Grid 1 - Accent 21,Listaszeru bekezdés1,Colorful List - Accent 111,Dot pt,F5 List Paragraph,List Paragraph1,No Spacing1,List Paragraph Char Char Char,Bullets,L,3,2, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.63 cm + Indent at: 1.27 cm

Commented [A235]: FR suggests to include a new article aiming to explain the articulation between the CSIRT network and the European cyber XXX.

Formatted: Check spelling and grammar

Formatted: Font:

Formatted: List Paragraph,Listaszerű bekezdés1,List Paragraph à moi,Colorful List - Accent 11,Medium Grid 1 - Accent 21,Listaszeru bekezdés1,Colorful List - Accent 111,Dot pt,F5 List Paragraph,List Paragraph1,No Spacing1,List Paragraph Char Char Char,Bullets,L,3,2, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.63 cm + Indent at: 1.27 cm

Formatted: List Paragraph,Listaszerű bekezdés1,List Paragraph à moi,Colorful List - Accent 11,Medium Grid 1 - Accent 21,Listaszeru bekezdés1,Colorful List - Accent 111,Dot pt,F5 List Paragraph,List Paragraph1,No Spacing1,List Paragraph Char Char Char,Bullets,L,3,2, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.63 cm + Indent at: 1.27 cm

Formatted: Font:

~~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.~~

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

Commented [A236]: FR : if the European cyber XXX is a tool at the disposal of the CSIRT network, then the interaction between the Cross border platform and EU CyCLONe would follow the TORs and SOPs of the CSIRT network.

Article 8

Security

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.
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. 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.

Chapter III

CYBER EMERGENCY MECHANISM

Article 9

Establishment of the Cyber Emergency Mechanism

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

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, mitigation of impact from -and smooth ~~immediate~~ recovery from significant and large-scale cybersecurity incidents, to be provided by trusted providers participating in the EU Cybersecurity Reserve established under Article 12;

(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.

Commented [A237]: FR : see comment supra

Commented [A238]: FR suggests to consult the CSIRT network on this last point in order to get enlightment about how it is implemented and works.

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 at Union level.

2. The definition of the process associated to the coordinated preparedness testing should be of the sole competence of the Member states.

Commented [A239]: FR : it should be the role of the Member states to develop conduct the presparedness test

3. The NIS Cooperation Group in coordination with EU ~~-~~CyCLONe as part of its preparedness role, ~~in cooperation with~~supported by the Commission, ENISA, and the High Representative, shall develop common risk scenarios and methodologies for the coordinated testing exercises.

4. The coordinated preparedness testing could be conducted by trusted managed security service providers once an EU certification scheme for managed security service under the Regulation (EU) 2019/881 is in place.

Member states could add up security criteria for the identification of the trusted managed security service providers when essential or important entities fall within the scope of national security and defense interests.

4.Within the transitional period of the adoption of certification scheme for managed security service providers, Member states shall define the process at national level that will be followed.

Commented [A240]: FR : the drafting of risk scenarios should lie within the competence of the member states and member states could be supported by the EC and ENISA.

Commented [A241]: FR : with the amendment of the CSA, coordinated response testing could be realised by managed security service providers.
For security concerns, Member states shall be entitled to define specific security criteria.

Commented [A242]: FR : transitory provisions should be established in order to anticipate the time between the adoption of the scheme and the entry of force of the text.

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.

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.

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.

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, mitigate the impact of and ~~immediate~~ ensure the smooth recovery from significant or large-scale incidents affecting entities operating in critical or highly critical sectors.

Commented [A243]: FR : see comments above

5. An ad hoc committee, composed of the Secretariat of the IICB ~~The~~, the Chair of the HWPCI , and cyber cooperation network at technical (CSIRT network) and operational (CyCLONe) level ~~Commission~~ shall have overall responsibility for the implementation of the EU Cybersecurity

Reserve. The ~~Commission~~ ad hoc committee 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.

6. The ad hoc committee~~Commission~~ may 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, 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.

8. The Commission may, by means of implementing acts, specify the types and the number of response services required for the EU Cybersecurity Reserve. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2).

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 ad hoc committee ~~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~~ smooth 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;

Commented [A244]: FR proposes to create an ad hoc committee that would be in charge of the implementation of the reserve / assessment of the requests. It will enable to keep the Member states informed of the process.

Formatted: Justified

Commented [A245]: FR considers that CyCLONe should be informed (on a voluntary basis) as the network has a role to play at operational level to draw the global situational awareness picture. This would aim to create a link between all cybersecurity regulations and different cooperation networks. This would create a coherent framework at the EU level.

Commented [A246]: Fr : see above

Commented [A247]: FR suggest to define a timeline. If we deal with an urgent situation, then processes shall run smoothly.

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

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~~ad committee, with the support of ENISA or as defined in contribution agreements under Article 12(6), and a response shall be transmitted to the users referred to in Article 12(3) without delay.

Commented [A248]: FR : please see comment above

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 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.

4. The agreements referred to in paragraph 3 may be based on templates prepared by ENISA, after consulting Member States.

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.

6. Within one month from the end of the support action, the users shall provide ~~Commission~~ ad hoc committee ~~and ENISA~~ with a summary report about the service provided, results achieved and the

lessons learned. The user is invited to share the report to EU-CyCLONe. When the user is from a third country as set out in Article 17, such report shall be shared with the High Representative.

7. The ~~Commission~~ ad hoc committee shall report to the NIS Cooperation Group about the use and the results of the support, on a regular basis.

Commented [A249]: FR : as CyCLONe draws the situational awareness picture, then, it is relevant for the network to be informed about the developments

Commented [A250]: Additionnaly, CyCLONe is expected to work and respond to potentioal cross-border incidents.

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[22], the support under this Regulation for responding to such incidents shall complementactions 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 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.

4. Support under the Cyber Emergency Mechanism may form part of the joint response between the Union and Member States in situations referred to in Article 222 of the Treaty on the Functioning of the European Union.

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.

[22] 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.

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 the hardware and software technical equipment necessary to support the requested service;

(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) where it can deliver the service;

(j) once an EU certification scheme for managed security service Regulation (EU) 2019/881 is in place, the provider shall be certified in accordance with that scheme.

Article 17

Support to third countries

Commented [A251]: FR proposes to extend the benefit of the cyber reserve to countries that are part of the european political community as it will strengthen the EU resilience to face cyber threats.

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~~ ad hoc committee 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~~ ad hoc committee shall coordinate with the High Representative about the requests received and the implementation of the support granted to third countries from the EU Cybersecurity Reserve.

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 all relevant stakeholders, including representatives of Member States from CyCLONe and the CSIRT network, the Commission, other relevant EU institutions, bodies and agencies, managed security services providers and users of cybersecurity services with due respect to the national cyber authorities competence as defined by the Directive (EU) 2022/2555. ~~Where appropriate, ENISA~~ [illegible] Consultations with relevant

Commented [A252]: FR would like this part to be aligned with the ongoing CRA negotiation. FR would recommend to align this part with the Council mandate of the CRA when it comes to the role of ENISA regarding vulnerabilities.
More, FR considers that vulnerabilities assessment falls within the scope of the CSIRT network

Commented [A253]: FR : suggestion to specify

Commented [A254]: FR : under NIS2, it falls within the national competence that national cyber competent authority are in contact with their constituents and this aspect should be respected.

Commented [A255]: FR : suggestion to withdraw this part, as it is the competence of the Member states.

Commented [A256]: FR : see comment above
This provision is too vague and might be concurrent to national cyber competent authority activities, then, suggestion to withdraw it

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. The report shall be reviewed by Member states cooperation network in order to ensure that there is duplication of work. It shall protect confidential information, in accordance with Union or national law concerning the protection of sensitive or classified information.

~~4. Where appropriate, the report shall draw recommendations to improve the Union's cyber posture.~~

5. Where possible, a version of the report shall be made available publicly after a review from the Member states cooperation network. This version shall only include public information.

[…]

Commented [A257]: FR : Cf. supra

Commented [A258]: FR considers is not the role of ENISA as foreseen within the CSA.

Commented [A259]: FR : EU CyCLONe / CSIRT network and the NIS Cooperation group shall be entitled to review the document to check if there are no TLP AMBER / RED / STRICT information before disclosing information to the public.

3.2.4. Compatibility with the current multiannual financial framework

The proposal/initiative:

– [X] can be fully financed through redeployment within the relevant heading of the Multiannual Financial Framework (MFF).

Explain what reprogramming is required, specifying the budget lines concerned and the corresponding amounts. Please provide an excel table in the case of major reprogramming.

	2023	2024	2025	2026	2027	total
SO1	16.232.897	20.528.765	17.406.899	16.223.464	10.022.366	80.414.391
SO2 initial	226.316.819	295.067.000	195.649.000	221.809.000	246.608.000	1.185.449.819
To CYBER initiative			18.000.000	28.000.000	19.000.000	65.000.000
NEW SO2	**226.316.819**	**295.067.000**	**177.649.000**	**193.809.000**	**227.608.000**	**1.120.449.819**
SO3 DB 24	24.361.553	35.596.172	3.638.000	3.638.000	11.175.000	78.408.725
Fom SO2-SO4			15.000.000	15.000.000	6.000.000	36.000.000
New SO3	**24.361.553**	**35.596.172**	**18.638.000**	**18.638.000**	**17.175.000**	**114.408.725**
ECCC initial	176.222.303	208.374.879	104.228.130	90.704.986	84.851.497	664.381.795
From SO2-SO4			13.000.000	23.000.000	28.000.000	64.000.000
New ECCC	**176.222.303**	**208.374.879**	**117.228.130**	**113.704.986**	**112.851.497**	**728.381.795**
SO4 initial	66.902.708	64.892.032	56.577.977	70.477.245	72.107.201	330.957.163
To CYBER initiative			10.000.000	10.000.000	15.000.000	35.000.000
NEW SO4	**66.902.708**	**64.892.032**	**46.577.977**	**60.477.245**	**57.107.201**	**295.957.163**

Commented [A260]: FR : what are the impacts for the projects under the SO2 and SO1 due to the reallocation ? and for the ECCC ?

– [ ] requires use of the unallocated margin under the relevant heading of the MFF and/or use of the special instruments as defined in the MFF Regulation.

Explain what is required, specifying the headings and budget lines concerned, the corresponding amounts, and the instruments proposed to be used.

– [ ] requires a revision of the MFF.

Explain what is required, specifying the headings and budget lines concerned and the corresponding amounts.

[…]

CROATIA

Recitals

For the time being, we do not comment on recitals, as they probably should require further adjustments based on the final text on articles.

General remarks

HR welcomes initiatives aiming to build stronger and more effective EU cooperation in the area of cyber security with the purpose of achieving a higher common level of cybersecurity in the EU.

In that manner, the Cyber Solidarity Act (CSoA) addresses very important, but also sensitive topics, especially when information sharing is in question.

The EK draft of the CSoA sets out provisions that needs to be clarified to a greater extent.

It is particularly necessary to clarify the information sharing and participation obligations of Member States under the Emergency Mechanism and the Cybersecurity Reserve in the Cyber Shield.

In that manner, HR recalls that all EU proposals for cooperation and information sharing with respect to cyber security incidents and threats must respect Member States' national competence in delivering essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security, as recognised in Article 4 of TFEU.

In addition, HR has serious concerns about the proposed SOCs network duplicating work already assigned to the CSIRTs and CyCLONe network in the NIS 2 Directive.

Especially taking into account the amount of delegation's comments on EK draft and questions raised, we call on the Presidency not to rush through the process and we strongly support PL proposal on reading through article-by-article of the EK draft in the HWP CI.

CHAPTER I

The terminology used in the draft regarding the SOCs causes a lot of confusion and it needs to be improved, including related definitions.

CHAPTER II

Chapter II establishes the European Cyber Shield and sets out its various elements and the conditions for participation. The chapter describes the type of entities that shall form the European Cyber Shield and says that the shield shall consist of National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs').

It is not clear what added value the designation of SOCs per Member State and the establishment of cross-border security operations centres would have in addition to the designation of national CSIRTs and the establishment of a CSIRT network under NIS 2.

The CSoA should not create any overlapping structures with the national CSIRT's roles and CSIRT-network structure. It is crucial to avoid the unnecessary duplications, especially as they going to increase the amount of information sharing, the time needed, the human and other capacities required, which could jeopardise the achievement of the intended impact of CSoA.

National CSIRT's appointed by NIS2 directive have specific national responsibilities for Member States and act as central point of contact for both national incidents as well for the other CSIRT in the EU.

The Article 4 of CSoA should introduce the possibility for Member States to identify the NIS2 designated national CSIRT as National SOC. In relation to that, having in mind the proposed CSoA definition of the term "*public body*", the next sentence in Article 4.1. should be deleted: "*The National SOC shall be a public body*." The definition of "*public body*" in Article 2 should be deleted accordingly.

CHAPTER III

HR supports the proposal for including the preparedness testing in the scope of the Emergency Mechanism, as the testing exercises may effectively prevent cyber threats.

From the EK draft, it is not clear are these services (testing) mandatory or voluntary. The use of services should be voluntary for Member States.

In addition, it is important to define clearly, what type of the entity may use this action (only entities from highly critical sectors, both entities from highly critical sectors and entities from critical sectors, other entities, if yes, need to be further specified).

HR supports establishment of the EU Cybersecurity Reserve. We believe that it is necessary that the CSoA clearly state that the use of the Reserve is voluntary.

When the trusted providers are in question, the text should give clear answer whether or not the Reserve is open for non-EU provider.

The selection criteria for trusted provider in Article 16 should be define as concrete as possible.

ITALY

These comments are without prejudice to further positions the Italian National Cybersecurity Agency or other national authorities may provide on this matter.

Methodological note: in this further round of comments and amendment proposals, we focus on the articles and do not comment on recitals and Annexes, as they may require further adjustments based on the final text of articles.

1 General objectives, subject matter and definition

According to article 4, paragraph 2 of the TFEU, national security, as well as maintaining law and order are essential State functions. In particular, national security remains the sole responsibility of each Member State.

See proposed amendment to articles 1 in Section 5.

2 European Cyber Shield

With regards to the provision to establish a European Cyber Shield (ECS) through a pan-European network of Security Operation Center (SOC), we welcome the proposal, in order to identify relevant early warning that may not be detectable at MS level, and are fully invested in identifying appropriate adjustment to ensure this novel mechanism fits and synergizes with the existing EU cyber incidents and cyber crises management mechanisms. Therefore, **we would welcome clarifications on**:

1. the role of the SOC network with respect to the CSIRT Network and CyCLONe, established by Directive 2022/2555, clearly defining the differences in order to address possible overlaps and duplications, and to ensure roles consistency as well. Indeed, the framework shall clearly define the roles of each actor involved (eg., National SOCs, Cross-Border SOCs, CSIRTs Network, CyCLONe, etc.) promoting effective synergies among them;
2. the information flow from the SOC Network toward other stakeholders, such as the CSIRT Network and CyCLONe. In this regard, the governance will have to provide technical guidance to ensure availability and harmonization of the technical collaboration means, more specifically the taxonomies, metrics and communication protocols;
3. the establishment and functioning of cross-border SOCs (article 5 and following), with particular regard to the management and reporting of EU funding that can be allocated by the ECCC, and the legal representation of the coordinating SOC. As far as the Regulation proposal makes reference to a written agreement among the consortium members, it would be interesting to know if there are any indications or guidelines on this new cooperation model;

4. the designation of national SOCs. Currently, article 4 suggests the possibility for the MS to indicate one or more national SOCs. In this regard, it should be clarified how the relationships and the exchange of information between Brussels and the Capitals would be structured in the presence of more national SOCs. In particular, we believe there should be a central, national SOC, coordinating the other national SOCs and participating to the cross-border SOCs. This does not prevent the other national SOCs, either public or private, to share information with the national SOCs of other Member States bilaterally.

See proposed amendment to articles 3-8 in Section 5.

3 Cyber Emergency Mechanism (CEM)

With regards to the provision concerning the Cyber Emergency Mechanism, we welcome the proposal to establish this mechanism with appropriate funding in order to strengthen and enhance MS and EU cyber resilience. In the meanwhile, we look forward to the negotiation in order to improve the governance and applicability of some of the provided instruments. Specifically, **we would see fit**:

1. an increased involvement of the CyCLONe with respect to exercise and stress testing, fully taking into consideration the crisis preparation and management role of the newly established network as outlined by the NIS2 Directive;
2. to provide supervision and control to MS (through CyCLONe and/or Council) on the support actions for MS;
3. an in-depth analysis of the lesson learned through the ENISA Cybersecurity Support Action pilot project. In this regard, it would be useful to understand how the Cybersecurity Support Action conducted by ENISA pursuant to articles 6 and 7 of the Cyber Security Act (CSA) is integrated with the trusted providers by the managed security service providers referred to in the amendments to the CSA, currently under negotiation;
4. an evaluation of the effectiveness of the proposed Cyber Reserve, considering the business model of such cybersecurity incident response providers. In this regard we believe that users enlisted in article 12, paragraph 2, can avail themselves of the services provided by trusted providers on voluntary basis and upon their request. Moreover, in article 13, paragraph 5, the request for incident response should contain only the information needed, taking into consideration the fact that it has to remain upon Member States the decision to share sensitive information. Further amendments are under consideration;
1. a comparison with similar mechanism put in place for other domains, such as Civil Protection, introducing more flexible financial support actions to encompass tools that are not being/cannot considered here, future proofing the regulation.

2. provided the Regulation proposal aims at structuring, also through relevant funds, cyber crisis management at EU level, we believe it should also address the current lack of appropriate resilient and secure communication, envisaging the establishment of a resilient and secure network(s) connecting, for instance, MS Cyber Crisis Management Authorities (within CyCLONe), MS CSIRT (within the CSIRT Network) and relevant EUIBAs. Amendment proposals in this regard are being drafted.

Moreover, the provision contained in article 11 appears to be sensitive, especially due to the role reserved to the NIS Cooperation group and ENISA, to be consulted by the EC for the purpose of identifying the sectors or subsectors involved, starting from the sectors of high criticality referred to in the Annex I of Directive (EU) 2022/2555, for the choice of entities to be subjected to coordinated preparedness testing.

See proposed amendment to articles 10-14 in Section 5.

4 Incindent Review Mechanism (IRM)

Provided cyber incident and crisis management falls within the scope of national security, which is the sole responsibility of MS, we have concerns with respect to the proposed mechanism.

Therefore, we propose to extend the mandate of CyCLONe to perform such activity, at the request of MS, which may also entail the support of ENISA as CyCLONe's Secretariat.

See proposed amendment to article 18 in Section 5.

5 Proposed amendments

For the time being, we limit our amendment proposals to the article and are not considering the recitals. Proposed deletion are ~~stricken red~~ and proposed addition are **bold green**.

Please find below the articles or paragraphs that were reviewed in this round of comments.

[…]

Article 1

Subject-matter and objectives

[…]

3. This Regulation is without prejudice to the Member States' **sole** ~~primary~~ responsibility for national security, public security, **and primary responsibility for** the prevention, investigation, detection and prosecution of criminal offences.

Article 2

Definitions

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

[…]

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

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

~~(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;~~

[…]

Article 3

Establishment of the European Network of Security Operations Centres ~~Cyber Shield~~

1. ~~An interconnected pan-European infrastructure~~ **A Network** of Security Operations Centres **('SOCs' Network')** ~~('European Cyber Shield')~~ shall be established to develop advanced capabilities for the Union to detect, analyse and process data on cyber **events** ~~threats and incidents~~ in the Union. It shall consist of all National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs'). **Cross-border SOCs are composed by a National SOC per Member State, acting as Coordinator and running the national platform node.**

Actions implementing the **('SOCs' Network')** ~~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 **SOCs' Network** ~~European Cyber Shield~~ shall:

(a) pool and share data on cyber **events** ~~threats and incidents~~ from various sources through cross-border SOCs;

(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 **an early identification of cyber incidents through the analysis of the cyber events detected** ~~better protection and response to cyber threats~~;

(d) contribute to ~~faster detection of~~ cyber threat~~s~~ **prevention and detection, as well as to** ~~and~~ **joint** situational awareness across the Union;

(e) correlate and enrich, through multiple sources, threat intelligence data with sighting information and evaluation of the overall impact of identified threats at EU level;

(f) provide support to strengthen incident response capabilities of the CSIRTs network;

(~~e~~**g**) provide services and activities for the cybersecurity community in the Union, including contributing to the development 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 participate in the **SOCs' Network** ~~European Cyber Shield~~, each Member State shall ~~designate~~ **identify a National SOC, acting as Coordinator and running the national platform node, connected with the others established in each Member State that, on voluntary basis, is willing to participate** ~~at least one National SOC.~~ The National **Coordinator** SOC shall be a public body.

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 **events that can lead to an early identification of cyber** threats and incidents**,** and contributing to a Cross-border SOC **platform**. It shall be equipped with state-of-the-art technologies capable of detecting, aggregating, and analysing data **potentially** relevant **for an early detetction of** ~~to~~ cybersecurity threats and incidents.

2. Following a call for expression of interest, National **Coordinator** 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 **Coordinator** 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 **Coordinator** SOC shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

3. A National **Coordinator** 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 **Coordinator** SOCs, committed to working together to coordinate their cyber-detection and **events** ~~threat~~ monitoring activities shall be eligible to participate in actions to establish a Cross-border SOC.

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

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 SOCs

1. Members of a Hosting Consortium ~~shall~~ exchange relevant information among themselves **on voluntary basis** within the Cross-border SOC including information relating to cyber **events** ~~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) aims to prevent~~,~~ **and** detect, ~~respond to or recover from~~ **cyber** incidents **and** ~~or~~ to mitigate their impact;

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

4. Cross-border SOCs shall conclude cooperation agreements with one another, specifying information sharing principles among the cross-border platforms.

Article 7

Cooperation and information sharing with Union entities

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.

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

Article 8

Security

1. Member States participating in the **SOCs' Network** ~~European Cyber Shield~~ shall ensure a high level of data security and physical security of the **SOCs' Network** ~~European Cyber Shield infrastructure~~ **platform nodes**, and shall ensure that the **underneath** 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 **network's platform nodes** ~~infrastructure~~.

2. Member States participating in the **SOCs' Network** ~~European Cyber Shield~~ shall ensure that the sharing of information within the **SOCs' Network** ~~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. 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.

Article 10

Type of actions

1. The Mechanism shall support the following types of actions:

(a) preparedness **and prevention** 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 providers participating in the EU Cybersecurity Reserve established under Article 12;

[…]

(d) establishment of an Emergency Fund to swiftly provide direct financial support to Member States necessary for their response to significant and large-scale cybersecurity incidents.

Article 10b

Cyber Emergency Mechanism Management Board

1. The Cyber Emergency Mechanism Management Board (CEMMB) is composed of representatives of the Council, as chair, the Commission and the EU-CyCLONe.

2. The CEMMB shall have overall responsibility for the implementation of the Cyber Emergency Mechanism.

3. ENISA shall provide the secretariat of the CEMMB.

4. The CEMMB can task the Commission, the EU-CyCLONe and ENISA to perform activities that are required to implement and enact the Cyber Emergency Mechanism.

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~~ **CEMMB**, after consulting the NIS Cooperation Group ~~and ENISA~~, shall identify the sectors, or sub-sectors, concerned, from the Sectors of High Criticality listed in Annex I to Directive (EU) 2022/2555 from which entities may be subject to the coordinated preparedness testing, taking into account existing and planned coordinated risk assessments and resilience testing at Union level.

2. The NIS Cooperation Group in cooperation with **the EU-CyCLONe,** the Commission, ENISA, and the High Representative, shall develop common risk scenarios and methodologies for the coordinated 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.

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~~ **can be deployed** in all Member States **upon their request**.

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.

4. Users referred to in paragraph 3, point (a), ~~shall use~~ **can avail themselves** of the services from the EU Cybersecurity Reserve **on voluntary basis** 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.

5. The **CEMMB** ~~Commission~~ shall have overall responsibility for the implementation of the EU Cybersecurity Reserve. The **CEMMB** ~~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.

5a. The CEMMB may entrust the operational supervision of the EU Cybersecurity Reserve, in full or in part, to the EU-CyCLONe.

6. The **CEMMB, with the support of the** Commission may**,** entrust the operation and administration of the EU Cybersecurity Reserve, in full or in part, to ENISA, by means of contribution agreements.

7. In order to support the **CEMMB** ~~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.

8. **At the request of the CEMMB,** the Commission may, by means of implementing acts, specify the types and the number of response services required for the EU Cybersecurity Reserve. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2).

Article 11b

Prepardness and prevention actions

[To be drafted]

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 **applicable** measures to mitigate the effects of the incident for which the support is requested, including**, if possibile,** 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 **CEMMB** ~~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~~ **and** 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 **type of** affected entity and potential impacts of the incident and the planned use of the requested support, including an indication of the estimated needs;

(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**, and under the supervision of the CEMMB,** shall develop a template to facilitate the submission of requests for support from the EU Cybersecurity Reserve.

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

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 **CEMMB** ~~Commission~~, with the support of ENISA or as defined in contribution agreements under Article 12(6), and a response shall be transmitted to the users referred to in Article 12(3) without delay.

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 potential cross-border nature of the incident and the risk of spill over to other Member States or users;

(e) the measures taken**, if applicable,** 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.

4. The agreements referred to in paragraph 3 may be based on templates prepared by ENISA, after consulting Member States.

5. The **CEEMB,** 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.

6. Within one month from the end of the support action, the users shall provide **CEMMB** ~~Commission~~ and **EU-CyCLONe** ~~ENISA~~ with a summary report about the service provided, results

achieved and the lessons learned. When the user is from a third country as set out in Article 17, such report shall be shared with the High Representative.

7. The **CEMMB** ~~Commission~~ shall report to the NIS Cooperation Group about the use and the results of the support, on a regular basis.

Article 14b

Emergnecy Fund

[To be drafted]

[…]

Article 18

Cybersecurity Incident Review Mechanism

1. **The EU-CyCLONe, with the support of** ~~At the request of 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~~ **EU-CyCLONe** shall deliver an incident review report to **its members and** 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 **EU-CyCLONe** ~~Commission~~ shall share the report with **the Council**, the High Representative **and/or the Commission**.

1b. The EU-CyCLONe shall update its rules of procedures to define the process to prepare and draft the incident review report.

2. To prepare the incident review report referred to in paragraph 1, **EU-CyCLONe** ~~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, **EU-CYCLONe** ~~ENISA~~ shall also collaborate with entities affected by significant or large-scale cybersecurity incidents. To support the review, **EU-CyCLONe** ~~ENISA~~ may also consult other types of stakeholders. Consulted representatives shall disclose any potential conflict of interest.

2b. If the consultation and collaboration mentioned in paragraph 2 involves national entities, the EU-CyCLONe should carry out such actions in full collaboration or through the relevant Member States' cyber crisis management authorities.

3. The report shall cover a review and analysis of the specific significant or large-scale cybersecurity incident, including the main causes, vulnerabilities and lessons learned. It shall

protect confidential information, in accordance with Union or national law concerning the protection of sensitive or classified information.

4. Where appropriate, the report shall draw recommendations to improve the Union's cyber posture.

5. Where possible, a version of the report shall be made available publicly. This version shall only include public information.

[…]

HUNGARY

Article 1

3. This Regulation is without prejudice to the Member States' sole~~primary~~ responsibility for national security, public security, and the prevention, investigation, detection and prosecution of criminal offences.

We suggest to have a general provision on sharing national security etc. information (the suggestion based on the text of NIS 2):

4. No Member State should be required to supply information the disclosure of which would be contrary to the essential interests of its national security, public security or defence.

Article 2

General comment to the notion of 'Hosting Consortium':

As it was proposed by other Member States, we are also in favour of establishing an information sharing technical platform.

Article 3

An additional sentence should be inserted in para 1.:

'The participation in the European Cyber Shield remains voluntary.'

We suggest the deletion of AI and data analytics technologies references in order to make the Regulation technology-independent and time-tested.

2. The European Cyber Shield shall:

(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~~;

Article 6

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

(a) a commitment to share ~~a significant amount of~~of the relevant data referred to in paragraph 1, and the conditions under which that information is to be exchanged;

Article 10

The Mechanism shall support the following types of actions:

(a) preparedness actions,

The regulation refers to 'preparedness actions' without further elaborating what actually is meant by and how Member States could use them.

The Mechanism shall support the following types of actions:

response actions, supporting response to and ~~immediate~~ smooth recovery from significant and large-scale cybersecurity incidents, to be provided by trusted providers participating in the EU Cybersecurity Reserve established under Article 12;

We suggest to change 'immediate recovery' to 'smooth recovery' throughout the whole text. We acknowledged the aim of the Reserve, namely to provide services which could contribute to recovering as fast as possible from large-scale incidents or crises, at the same time we find it bit misleading to use the word 'immediate' before recovery. It suggests something that might not be possible.

Article 13

Generally we have a preference to simplify the application procedure.

Article 14

We are still reluctant regarding the fact that the request for support from the Reserve will be assessed by the Commission since the Reserve is also going to be financed through DEP and the implementation of the cyber related part of DEP falls in the mandate of ECCC.

In the case if there are no concurrent requests, based on which criteria the Commission (with the support of the ENISA) will assess the request?

The text lacks the grounds for refusal of requests, the same goes for procedure to be followed in case of refusal. What actions can be taken if the Member State concerned does not agree with the negative outcome of the assessment made by the Commission on the request for support?

6. Within one month ~~from the end of the support action~~after the user regained full control over the situation, the users shall provide Commission and ENISA with a summary report about the service provided, results achieved and the lessons learned. When the user is from a third country as set out in Article 17, such report shall be shared with the High Representative.

7. The Commission shall report to the NIS Cooperation Group and the Governing Board of the ECCC about the use and the results of the support, on a regular basis.

Article 18

4. Where appropriate, the report shall draw non-binding~~–~~ recommendations to improve the Union's cyber posture.

5. Where possible, a version of the report shall be made available publicly, in case the concerned Member States give their consent . This version shall only include public information.

Article 20

By [four years after the date of ~~application~~ entry into force 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.

NETHERLANDS

NL would like to thank the Spanish Presidency for the opportunity to provide written comments on all relevant provisions in the CySOL. As NL is still in the process of scrutinising the proposal, please note that the written comments below on the CySOL are preliminary and may evolve or change over time. NL looks forward to the upcoming discussions, as well as further opportunities to provide more written comments.

Chapter II – The European Cyber Shield

With regards to chapter 2, the Netherlands would like to reiterate its support to the purpose of this initiative. We recognize the need for shared situational awareness within the Union. With regards to this chapter, and building on the exchange of practices during the SOC-workshop, the Netherlands takes note of the following points:

- That the purpose of the inclusion of this initiative within the Cyber Solidarity Act is to preserve the setup of cross-border networks as previously set in motion through the Cross-Border Call for Expression of Interest, and;
- That the primary purpose of the establishment of cross-border networks is the pooling and sharing of aggregated/analysed information and cyber threat intelligence.

The Netherlands believes that the text of the proposal should not only reflect those elements clearly but also that the text should not go beyond these elements so that no confusion will be created about the functions of cross-border networks.

Chapter III - Cyber Emergency Mechanism

With regards to article 11:

NL sees a potential overlap of the preparedness actions with responsibilities set out in the NIS2 Directive.

We suggest that the range (and types) of preparedness testing proposed in article 11 is further defined by the Commission to have a common understanding of the proposed actions set out in this article. The NL furthermore proposes that it should be further clarified within the article that the testing is up to the sole responsibility of Member States.

With regards to articles 12-17:

First and foremost, NL supports the objectives of the proposed Cyber Reserve and recognizes the value of deploying the private sector in addressing large-scale incidents. NL is therefore taking a constructive approach towards establishing an effective initiative, emphasizing the importance of ensuring it's functionality.

Nevertheless, aligned with the earlier request to the Commission in March 2022 in Nevers for the creation of a Cybersecurity Emergency Fund, NL supports the exploration of possibilities for establishing an Emergency Fund that can assist Member States in covering the expenses associated with incident response actions following large-scale cybersecurity incidents. NL contends that such a fund would offer greater practical efficiency and ease of operation compared to a Reserve.
If the establishment of such a fund is not among the (legal) options, NL would strongly welcome an (interactive) **scenario workshop** to better understand what the governance will look like and allow for the Council to gain a congruent understanding of the proposal. In such a workshop we will be able to walk step by step through the different phases of the proposal, while also considering the different roles, responsibilities (including those of the Member States) and processes.
Moreover, NL emphasizes the importance of having Member States involved in the process of establishing clear conditions and thresholds for deployment of the Cyber Reserve. We therefore stress the need for further clarification in the legal text regarding the deployment, and the (explicit) roles and responsibilities of the Member States, the Commission, ENISA, and Trusted Providers therein.

Preliminary Proposed Changes to Chapter I and Chapter II of the Cyber Solidarity Act

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 infrastructure of ~~Security Operations Centres (‘European Cyber Shield’)~~cross-border platforms 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 the processes of responding to significant or large-scale incidents.

Commented [A261]: The Netherlands proposes to steer away from the terms ‘SOC’, taking into account the purpose of this initiative, and instead focus on the functionalities of the cross-border networks. We would like to suggest using terms that more aptly reflect the objectives of the initiative, such as the term “cross-border platform” as used in the Call for Expression of Interest.

[…]

Article 2

Definitions

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

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

(2) **'public body'** means a body governed by public law as defined in Article 2((1), point (4),), of Directive 2014/24/EU of the European Parliament and the Council[18];

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

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

[…]

Chapter II

THE EUROPEAN CYBER SHIELD

Article 3

Establishment of the ~~European Cyber Shield~~XXXX

~~1. An interconnected pan-European infrastructure of Security Operations Centres ('European Cyber Shield') shall be established to develop advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union.~~ Cross-border platforms for pooling analysed/aggregated data and cyber threat intelligence on cybersecurity threats ~~between several Member States shall be~~ may be set up between Member States. ~~I~~They~~t~~ shall consist of ~~all designated~~ National ~~Security Operations Centres ('National SOCs')Participants~~CISRTs designated by Member States. ~~and Cross-border Security Operations Centres ('Cross-border SOCs'). platforms .~~

~~2. Actions implementing the European Cyber Shield~~Cross-border platforms ~~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.~~

~~3.~~1. ~~The European Cyber Shield~~These cross-border platforms shall:

(a) pool and share analysed/aggregated data on cyber threats and incidents from various sources through cross-border platforms~~SOC~~s;

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

Commented [A262]: The definition of what is referred to in the text as "national SOC" is missing from the definition list. As mentioned above, the Netherlands would propose to remove the term "SOC" from the CySOL text, and instead welcomes the use of 'national CSIRT' as used in the NIS2 directive.

The NL would propose to add the definition of such a participant as defined in the Call for Expression of Interest for the cross-border platforms or article 4.2 of this act where this is defined as an entity that has 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 platform."

Commented [A263]: The Netherlands welcomes alternative names for this initiative, such as "Early Warning System".

Commented [A264]: The Netherlands proposes to use the term "analysed" or "aggregated" throughout articles 3 to 8 of this act when referencing to "information" or "data". The added value of information sharing in this regard would lie in processed data. This would furthermore clearly establish that appropriate measures can be taken with regards to national security, when necessary, since this remains a matter of national competence.

Commented [A265]: As aforementioned, the Netherlands proposes to remove the term "national SOC" from the CySOL text, and instead welcomes the use "national CSIRT".

Commented [A266]: Is pool niet een beter woord? De informatie wordt verzameld door de nationale entiteiten en samengebracht in de cross-border versie

In order to:

~~(b)~~(c) contribute to better protection and response to cyber threats by relevant entities such as national competent authorities and the CSIRT-network; and

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

~~4. provide services and activities for the cybersecurity community in the Union, including contributing to the development advanced artificial intelligence and data analytics tools.~~

2. Actions implementing the Cross-border platforms 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.

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~~ Role of National CSIRTs

1. In order to participate in ~~the European Cyber Shield~~Cross-border platforms, each Member State ~~shall will~~may designate ~~at least one National SOC. The National SOC shall be~~ a public body mandated to coordinate prevention and detection of cyberthreats and incidents, such as a national CSIRT.

It shall have the capacity to act as a single 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~~platform. It shall be equipped with state- of-the-art technologies capable of detecting, aggregating, and analysing data relevant to cybersecurity threats and incidents.

2. Following a call for expression of interest, the designated National ~~SOCs~~ CSIRTs shall be ~~selected~~ recognised 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 Participants~~CSIRT 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 Participants~~CSIRT shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

Commented [A267]: NL prefers to move this part to a recital.

3. A National ~~SOC Participant~~CSIRT selected pursuant to paragraph 2 ~~shall~~ may commit to apply to participate in a Cross-border ~~SOC~~platform 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~~ platform by that time, it shall not be eligible for additional Union support under this Regulation.

Article 5

Cross-border ~~Security Operations Centres~~platforms

1. A Hosting Consortium consisting of at least three Member States, represented by designated National ~~SOCsParticipants~~CSIRT, 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~~ platform~~.~~

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

Commented [A268]: NL prefers to move this part to a recital.

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~~ platform shall be represented for legal purposes by the ~~a~~ National CSIRT acting as coordinating National CSIRT ~~SOC~~, or by the Hosing Consortium if it has legal personality. The co-ordinating ~~SOC~~ National CSIRT shall be responsible for compliance with the requirements of the hosting and usage agreement and of this Regulation.

~~4.~~5. Designated ~~N~~national ~~SOCsParticipants~~CSIRTs can apply to be eligible to join a cross-border ~~SOC~~ platform as a new member. The already joined cross-border ~~SOC~~platform members shall reserve the right to unanimously decide on the participation of a new member.

Article 6

Cooperation and information sharing within and between cross-border ~~SOCs~~platforms

1. Members of a Hosting Consortium shall exchange relevant information among themselves within the Cross-border platform~~SOC~~ for the purpose of generating shared situational awareness as further worked out by each cross-border ~~SOC~~platform in their written consortium agreement ~~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) aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;

(b) enhances the level of cybersecurity of the Union, 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 amount of~~ analysed/aggregated data on a voluntary ~~data~~ basis as 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.

~~To encourage exchange of information between Cross-border SOCs~~platforms, Cross-border ~~SOCs~~ platforms shall ensure a high level of interoperability between themselves. To facilitate the interoperability between the Cross-border ~~SOCs~~ platforms at a Union level, the Commission may, ~~by means of implementing acts,~~ after consulting the ECCC and the cross-border ~~SOC~~platforms, specify the conditions for ~~this~~ Union-wide interoperability. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2) of this Regulation. Cross-border ~~SOCs~~platforms reserve the right to define specific interoperability within their own
Cross-border ~~SOC~~platform.

~~Cross-border SOCs shall conclude cooperation agreements with one another, specifying information sharing principles among the cross-border platforms.~~

Article 7

Cooperation ~~and information sharing with Union entities~~with the CSIRTs Network

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

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

2. Cross-border platforms shall, where appropriate, ensure that (experiences with) state of the art tools, notably Artificial Intelligence and data analytics technology, used within the cross-border platforms is shared with the CSIRT Network.

Commented [A269]: The Netherlands would like to point out that analysed data is primarily relevant for the CSIRTs Network, where CERT-EU participates on behalf of EUIBAs. Relevant information can be shared through the CSIRT Network with CyCLONe (and nationally through nat CSIRT to cyclone member). CIE will also receive relevant information through CyCLONe

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.39 cm + Indent at: 0.84 cm

Article 8

Security

1. Member States participating in Cross-border networks~~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.

~~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.~~

~~• 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.~~

Chapter III

CYBER EMERGENCY MECHANISM

[…]

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 providers participating in the EU Cybersecurity Incident Response Mechanism~~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.

~~(a)~~2. As a part of the Mechanism, an Emergency Fund shall be established to rapidly cover immediate costs of Member States necessary for their swift response to significant and large-scale cybersecurity incidents.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0.42 cm

Article 11

Coordinated preparedness testing of entities

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

~~1.~~2. The definition of the coordinated preparedness testing and the associated process should be of the sole competence of the Member States.

~~2.~~3. The NIS Cooperation Group in coordination with EU-CyCLONe, ~~in cooperation with~~supported by the Commission, ENISA, and the High Representative, shall develop common risk scenarios and methodologies for the coordinated testing exercises.

[…]

AUSTRIA

GENERAL REMARKS

- We would kindly ask presidency to make full day meetings for the negotiations of the Cyber Solidarity Act. This is a very technical legislative proposal where the presence of experts is needed. It would be more efficient to have experts participate in full day meetings!
- Terminologie
  - National SOC → National SOC Platform
  - Cross-border SOC → Cross-border SOC platform
  - Hosting Consortium → Consortium
    - Not every participating National SOC Platform is bound the host tools / infrastructure. Whether a National SOC Platform is actually hosting something is up to agreement in the consortium. The term "hosting consortium" is thus misleading.
- Non consistent use of legal definition
  - Either cyber threat or cybersecurity threat
- The line between CSIRTs and National SOC Platforms / CSIRT-NW and Cross-border SOC Platforms needs to be clear
  - Refrain from referring to incidents; SOC Platforms should focus on events and threats

Legal Basis:

- We would like to see the legal basis (Art 173 (3)) TFEU for the proposed CSoA checked by CLS.

GENERAL OBJECTIVES, SUBJECT MATTER, AND DEFINITIONS

Definitions (Art 2):

- Def of National SOC Platform should be included
  - Workshop on 12 September has shown that there is room for various understandings of what a national SOC Platform is /what the tasks of National SOC Platforms are/could be. In order to enable cooperation between the National SOC Platforms of MS in a Cross-border SOC Platform a unified understanding is necessary.
  - Definition of 1) what a National SOC is, 2) which tasks does it have and 3) what abilities National SOC Platforms have should be added. 4) which are tasks of the national CSIRT and which are tasks of the National SOC Platform (especially regarding wording in Art 11 para 3 NIS 2 Directive)
- Def of Cross-border SOC Platform should be improved
  - No use of "incidents" – instead events + threats; incidents should be the sole competence of CSIRTS
  - Detection as the main function of Cross-border SOC Platform should be emphasized
  - Abilities should be elaborated: Machine to machine integration, sharing & collection in near-real time
  - Art 5 para 1 does not fully align with the current version of the definition on Art 2
- Need for a clear definition of Cyber Shield
- Ad para 2 - Public body (same as NIS 2):
  - 2014/24/EU referred to "'bodies governed by public law' - why change the wording?
- Ad para 3 – Hosting Consortium:
  - It should be added that a Hosting Consortium is represented by one coordinator + def of role of the coordinator
- Ad para 5: - entities operating in critical or highly critical sectors:

- Why isn't the legal definition and wording of NIS2 used?
- Ad para 9 – preparedness:
  - This def should be improved.
- Def of cybersecurity community
  - Used in Art 3 para 3 lit e

THE EUROPEAN CYBER SHIELD

Establishment of the European Cyber Shield (Art 3)

- Ad para 1 – Cyber Shield:
  - The aim of the Cyber Shield incl. the abilities are not clear and do not fully align with National SOC Platform / Cross-border SOC Platform.
  - There needs to be a common understanding of the tasks and aims and abilities of National SOC Platforms in order to be able to find a uniform understanding of the Cyber Shield.
- Ad para 1 – Composition of the Cyber Shield:
  - Wouldn't it be better if just Cross-border SOC Platforms participate and only those National SOC Platforms which are not part of a Cross border SOC Platform yet?
  - More participants make it hard to operate and built trust.
  - Def. of National SOC Platform and Cross border SOC Platform must ensure that only SOC Platforms from MS can participate.
- Ad para 2 – AI:
  - Refence to AI should be deleted.
  - Otherwise: Check if this aligns with AI-Act. What is the relationship between CSoA and AI-Act going to be? Check with Council Legal Service.

National Security Operations Centres (Art 4)

- Ad para 1 sub para 2 – contributing to National SOC Platforms:
  - "Other public and private organizations" needs to be further defined; What are other public and private organizations?
  - Who can contribute? Academia as well?
- Ad para 2 – call for expression of interest
  - There should be a maximum amount of how many National SOC Platforms per MS can be selected
  - A minimum threshold of how much is going to be covered by ECCC should be introduced.
- Ad para 3 – Union funding:
  - How long are Cross-border SOC Platforms not eligible to apply for further funding?
  - There needs to be some sort of time frame.

Cross-border Security Operations Centres (Art 5)

- Ad para 1:
  - Definition of a Cross-border SOC Platform in Art 5 does not fully align with the current version of the def in Art 2.
  - What does "shall be eligible to participate in actions" exactly mean? Which acions exactly?
- Ad para 2 – call for expression of interest
  - A time frame on the frequency on calls for expression of interested should be provided
  - A minimum threshold of how much is going to be covered by ECCC should be introduced.
- Ad para 2 – Hosting and Usage Agreement between ECCC and Hosting Consortium:
  - Either the definition of Hosting Consortium should be adapted to signal that the Hosting Consortium is acting through their coordinator.

- Alternatively, the clause in para 2 should be changed, stipulating that the H & U can also be concluded between the ECCC and the coordinator acting on behalf the Hosting Consortium.
- Ad para 4:
  - Representation of the Hosting Consortium should already be covered in the definitions. Maybe by adding a definition for coordinator.

Cooperation and information sharing within and between Cross-border SOC Platforms (Art 6)

- Ad para 1 - Information sharing:
  - What kind of information and with what aim will be shared should be looked at further.
  - At does not support sharing of raw-data through the Cross-border SOC Platforms.
- Ad para 2 - content of consortium agreement:
  - share and collect data in near-real-time through machine-to-machine integration should be added
    - This allows to better distingish National SOC Platforms / Cross-border SOC Platforms from CSIRTs / CSIRT-NW
    - However, check if the type of data / information is eligible for that
- Ad para 2 – a governance framework incentivising the sharing of information by all participants
  - What are ideas for that? What is meant by that?
- Ad para 2 - targets for contribution to the development of advanced artificial intelligence and data analytics tools
  - What are examples? How would this play out in practice?

Cooperation and information sharing with Union entities (Art 7)

- Ad para 1 – EU-CyCLONe, CSIRT-NW, EC:
  - Information sharing with EU entities should be more precise and relating to the need of each actor:
    - EU-CyCLONe: Information on large-scale incidents
    - CSIRT NW: not just information (and not only on large-scale incidents) but working together with CSIRT-NW → two-way street (IoC coming from CSIRT-NW); SOC Platforms providing support with information when it comes to incidents, information on vulnerabilities, retro hunting etc
    - EC: no information in general, but only when appropriate
- Ad para 2 – implementing act:
  - What are the procedural arrangements that are going to be subject to the implementing acts? Exempels!
  - Wouldn't it be useful if the information sharing is as burdenless as possible? Isn't there a risk that the implementing act introduces barriers for it? What about a recommendation by EC instead of an implementing act?

Security (Art 8)

- Ad para 1 - high level of data security and physical security:
  - This should be specified.
  - A reference to NIS2 and CER is necessary
- Ad para 2 – sharing with MS public bodies:
  - This needs to be mentioned at some point specifically that this is one of the business cases of a cross border SOC Platform. It's not clear from simply reading the act that cross-border

SOC Platform e.g. produce CTI Feeds which then again can be shared with other actors as well.
    - Sanctions should be introduced (e.g. cut of funds). Otherwise: what is the consequence if data is shared with non-trusted sources?
- Ad para 3 – implementing acts:
    - What are examples for technical requirements? What is going to be governed by those implementing acts?
    - Why not just refer to the standards set out in already existing provisions?
    - If we should proceed with implementing acts: Further clarification on the term "technical requirements" necessary.

CYBER EMERGENCY MECHANISM

General questions:

- Who decides which provider is going to assist?
- Who contacts the provider?
- Who pays the provider?
- Are the conditions for the service pre-set or would the user start negotiating with the provider when conducting the agreement?

Establishment of the Cyber Emergency Mechanism (Art 9)

- Ad para 1 - major cybersecurity threat:
    - Def missing- cf Definitions in NIS 2 Directive
- Ad para 1 - prepare for and mitigate, in a spirit of solidarity, the short-term impact of significant and large-scale cybersecurity incidents
    - How is this going to work?
- Ad para 2 - highly critical sectors:
    - Def missing
- Ad para 2 – actions implementing the CEM:
    - How does it work with other preparedness actions and mutual assistance?
    - A call for mutual assistance actions wouldn't make any sense. Can entities providing mutual assistance just reimburse themselves?

Type of actions (Art 10)

- Ad para 1:
    - I don't fully see how these actions cover the full spectrum of the aim for the Emergency Mechanism
    - Aim on Mechanism inter alia: improve resilience to major CS threats; type of actions only includes preparedness in highly critical sectors, response to significant and large-scale incidents & mutual assistance actions
    - Type of actions should be improved to cover the whole spectrum of the aim of the Mechanism
- Ad para 1 lit a - preparedness actions:
    - According to the slide the EC provided, there are 2 kind of preparedness actions – this should be made clear here as well.
    - How does this play out in practice? Can entities just apply for funding for their actions? Who is eligible for funding under DEP?
    - Further criteria for other preparedness actions? Why isn't there an article on that?
    - How does this correlate to mandatory preparedness actions stipulated by other Acts?

- Ad para 1 lit c:
  - Added value compared to EU-CyCLONe?
  - Relation to CSIRT should be defined
  - Who requests the funding? Is there going to be a « standing » call? Otherwise, how can one receive funding in the event of an incident? What criteria do need to be followed in order to receive money?

Coordinated preparedness testing of entities (Art 11)

- Ad para 1:
  - Why specifically reference to Annex 1 of NIS2 and not also to Annex 2?
  - Who applies for funding? Is it the entities participating in the testing? Are only the sectors identified eligible for funding under the Mechanism?

Establishment of the EU Cybersecurity Reserve (Art 12)

- Who pays the trusted providers (contract is between MS and trusted provider)? If MS are the ones paying – can the MS receive funding from DEP? Or is the sole purpose of the CEM to have providers on hold?
- Ad para 2 – pre-committed services:
  - what does that mean? What are pre-committed services? What can be deployed from the Reserve? Hours of service? Need for legal definition!
  - Maybe a def would be helpful.
  - "deployable in all MS" - This excludes small providers
- Ad para 3:
  - Reference to Art 17 para 3 should be made.
- Ad para 5 – EC shall determine the priorities
  - after consulting *the MS through some already established forum*
- Ad para 6:
  - not practical. Clear competences necessary.
- Ad para 8:
  - How will the implementing acts play out in practice?
  - Are implementing acts the right tool for that?

Requests for support from the EU Cybersecurity Reserve (Art 13)

- Text doesn't clearly state between which body the contract is concluded.
- Ad para 3: clear competences – either EC or ENISA
- Ad para 6:
  - A lot of actors for a template - What about NIS CG based on draft of EC? This way ENISA would not be tasked additionally
- Ad para 7 – implementing acts:
  - What are the details that would be specified?

Implementation of the support from the EU Cybersecurity Reserve (Art 14)

- Ad para 1 – Response time:
  - Exact timeframe should be stimulated: within XXX h
- Ad para 1 – competence:
  - clear competences – fast reaction in going to necessary
- Ad para 2:
  - Fallback provision if one incident is not clearly more important than the other

- Ad para 3:
  - Contract with the specific cyber crisis management authority and the provider?
  - Re specific agreements: only concluded after an incident occurs and EC / ENISA asses that the user is eligible?
  - Is the trusted provider going to be obliged to conclude that agreement to said conditions beforehand?
- Ad para 5 – Liability:
  - Limitation of liability should include MS as well
  - If MS CERT is aiding private company and asks the CER for support – they shouldn't be liable
- Ad para 6:
  - Report should go to CSIRT-NW or EU-CyCLONe!
- Ad para 6 + 7:
  - No regular information sharing - MS shall send aggregated report 1x p.a. incl lessons learned

Coordination with crisis management mechanisms (Art 15)

- Cybercrisis under NIS2 not taken into consideration.
- Why are some provisions "may" and others "shall"?
- Ad para 1 – complement actions under UCPM:
  - How is this supposed to work? Are the competent authorities under the UCPM also then eligible as users?

Trusted providers (Art 16)

- From the current def it is not clear that these should be private companies etc and not national CSIRTs. Could national CSIRTs apply as well? How would mutual assistance and the Reserve play together then?
- Who is the contracting authority?
- Ad para 1 – trusted providers:
  - Can trusted providers be a nat. person as well? Does it need to be an entity?
- Ad para 1 – principles:
  - For what are these principles used exactly?
- Ad para 1 lit a - deployed in all Member States:
  - What about small providers – How can we ensure that also small providers can participate?
- Ad para 1 lit a – incl certification or accreditation:
  - What does this exactly mean?
  - Wouldn't a reference to certifying authorities and the CSA be useful?
- Ad para 1 lit c:
  - This is very vague. What is the added value?
- Ad para 2:
  - Only EU-providers? Foreign providers eligible?
- Ad para 2 lit e – relevant level:
  - More concrete

Support to third countries (Art 17)

- Which countries may currently request support?

CYBERSECURITY INCIDENT REVIEW MECHANISM

Cybersecurity Incident Review Mechanism (Art 18)

- Legal basis should be looked at
- Ad para 1:
  - delete Commission as possible requestor
  - delete last sentence – sharing with High Representative
- Ad para 2:
  - National SOC Platforms / Cross-border SOC Platforms could be relevant stakeholder as well
  - ENISA shouldn't collaborate with entities affected – should be done through EU-CYCLONe / NIS authorities

POLAND

26.09.2023

PL comments to chapter II and definitions

Article 2

Definitions

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

(1) **'Cross-border ~~Security Operations Centre~~Collaboration Platform' ~~("Cross-border SOC")~~** means a multi-country platform, that brings together in a coordinated network structure CSIRTs~~SOCs~~ (as defined in art. 10 NIS2) from at least three Member States who form a Hosting Consortium, and that is designed to prevent cyber threats and incidents and to support the production of high-quality intelligence, notably through the exchange of data from various sources, public and private, as well as through the sharing of state-of-the-art tools and jointly developing cyber detection, analysis, and prevention and protection capabilities in a trusted environment**;**

Commented [A270]: Some terms have been adjusted to better align CSA with NIS2 and to reflect conclusions from discussions in the CSIRTs Network.

(2) **'public body'** means a body governed by public law as defined in Article 2((1), point (4),), of Directive 2014/24/EU of the European Parliament and the Council[23];

(3) **'Hosting Consortium'** means a consortium composed of participating states, represented by ~~SOCs~~CSIRTs, that have agreed to establish and contribute to the acquisition of tools, services and infrastructure for, and operation of, a Cross-border Collaboration Platform~~SOC~~;

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

(5) '**entities operating in critical or highly critical sectors'** means type of entities listed in Annex I and Annex II of Directive (EU) 2022/2555;

(6) '**cyber threat'** means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881;

(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;~~

Commented [A271]: Definitions in (9) and (10) are not necessary, as these are concepts that are well established and understood in cybersecurity and incident response, thus do not require clarification. Especially as the proposed definitions do not introduce any other new meaning to these terms.

23 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).

(~~11~~9) **'trusted providers'** means managed security service providers as defined in Article 6, point (40), of Directive (EU) 2022/2555 selected in accordance with Article 16 of this Regulation.

Chapter II

Enhanced cooperation on cyber threats detection ~~THE EUROPEAN CYBER SHIELD~~

Article 3

~~Establishment of the European Cyber Shield~~

1. An interconnected pan-European infrastructure of cross-border platforms for information sharing and coordination of preventive actions and incident response ('Cross-border Collaboration Platforms') ~~Security Operations Centres ('European Cyber Shield')~~ shall be established to develop advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union. ~~It shall consist of all National Security Operations Centres ('National SOCs') and Cross-border Security Operations Centres ('Cross-border SOCs').~~ The cross-border collaboration platforms ~~It~~ shall facilitate the cooperation between CSIRTs as defined in the NIS2.

Actions implementing Cross-border Collaboration Platforms' ~~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 Cross-border Collaboration Platforms' ~~European Cyber Shield~~ shall:

(a) support pool and share data on cyber threats and incidents from various sources ~~through eCross-border Collaboration PlatformsSOCs~~;

(b) support producing~~e~~ 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;

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

(e) support provision of ~~provide~~ services and activities for the cybersecurity community in the Union, including contributing to the development ~~advanced artificial intelligence and data analytics~~ analytical tools.

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

Commented [A272]: It should be made clear that it will not be another body or organization/network but rather *collaboration platform for information sharing and coordination of preventive actions and incident response between Computer Security Incident Response Teams*

Commented [A273]: Link between SOCs/CSIRTs and HPC is not clear to us. It should be explained or the reference removed.

Article 4

Role of CSIRTs~~National Security Operations Centres~~

~~1. In order to participate in the European Cyber Shield, each Member State shall designate at least one National SOC. The National SOC shall be a public body.~~

~~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.~~

2. Following a call for expression of interest, ~~SOCs~~CSIRTs designated in line with art. 10 NIS2, shall be selected by the European Cybersecurity Competence Centre ('ECCC') to participate in a joint procurement of tools, services and infrastructures and services with the ECCC to establish Cross-border Collaboration Platforms' ~~Collaboration Platforms~~. The ECCC may award grants to the selected ~~National~~ CSIRTs~~SOCs~~ to fund the operation of ~~those tools and infrastructures~~Cross-border Collaboration Platforms. The Union financial contribution shall cover up to 75~~50~~% of the acquisition costs of the tools, services 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 ~~SOC~~CSIRT shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

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

Commented [A274]: We propose to remove this point and refer to CSIRTs instead of National Security Operations Centres throughout the text. This will keep the proposed regulation aligned with NIS2 and reflect the practice, as the entities participating in the cross-border platforms (as of September 2023) funded by ECCC are all, in fact, CSIRTs.

Article 5

Cross-border ~~Security Operations Centres~~Collaboration Platforms

1. A Hosting Consortium consisting of at least three Member States, represented by CSIRTs~~SOCs~~, committed to working together to coordinate their ~~cyber detection and~~ threat detection, monitoring and analysis activities shall be eligible to participate in actions to establish a Cross-border Collaboration Platform~~SOC~~.

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, services 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, services 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.

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~~Collaboration Platform shall be represented for legal purposes by a CSIRT ~~SOC~~ acting as the coordinator~~ing SOC~~, or by the Hosing Consortium if it has legal personality. The coordinator~~co-ordinating SOC~~ shall be responsible for compliance with the requirements of the hosting and usage agreement and of this Regulation.

5. Relevant entities responsible for cybersecurity in Member States – especially Security Operations Centres in public or private sectors – may use Cross Border Collaboration Platforms to share high quality information and coordinate response to threats. In each case the rules of participation of such entities shall be governed by the hosting and usage agreement.

Commented [A275]: We propose to increase the flexibility of the regulation by adding an option for entities outside of the Hosting Consortium to participate in information sharing, as it can be beneficial for all users of such platforms.

Article 6

Cooperation and information sharing within and between C~~c~~ross-border Collaboration Platforms~~SOCs~~

1. Members of a Hosting Consortium shall voluntarily exchange relevant information among themselves within the Cross-border Collaboration Platforms~~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) aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;

(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 amount of~~ 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~~ analytical tools.

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

4. Cross-border ~~SOCs~~Collaboration Platforms shall conclude cooperation agreements with one another, specifying information sharing principles among the cross-border platforms.

Commented [A276]: We propose that it should be left for the Cross-border Collaboration Platform members to specify the conditions of cooperation and what technical and organisational measures they will implement to ensure the high level of interoperability due to CSIRTs and SOCs expertise, experience and capabilities in information sharing and incident response.

~~*Article 7*~~

~~**Cooperation and information sharing with Union entities**~~

~~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.~~

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

Commented [A277]: To avoid duplication of information sharing, reporting and crisis coordination mechanisms in NIS2, we propose to remove this article entirely.

Article 8

Security

1. Member States participating in the Cross-border Collaboration Platforms'~~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.

2. Member States participating in the Cross-border Collaboration Platforms' ~~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. 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.

PORTUGAL

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

Centro Nacional de Cibersegurança

27 September 2023

Portugal welcomes 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.

In Portugal's view, it is vital that the EU gives concrete steps towards coordinated approaches on detection and situational awareness of cyber threats and cybersecurity incidents, as well on preparedness of entities performing essential and important services to society in the EU.

Although the proposal is seen as a good starting point for discussion, Portugal sees room for improvement to accommodate aspects responding to the Member States' needs.

Bearing in mind this constructive position, considering

1. That no consensual concept on SOC's definition and a clear distinction between SOCs and a CSIRT/CERT exists amongst academic and expert communities – assuming that is the reason why the Proposal does not attempt a definition for "National SOC" in article 2 – the Proposal in its Chapter II should seek to have its dispositions focused on duties and functions rather than structures;

2. The need for a coordinated approach on cybersecurity, both at national and European levels, Portugal welcomes the references to structures and functions under the dispositions of Directive (EU) 2022/2555. However, we identify a missing link between the organisational provisions of Directive (EU) 2022/2555 and the designation of a public body to act as National SOC, which should be made through a Recital acknowledging the need to avoid overlaps between this Proposal and the Directive (EU) 2022/2555 regarding the designations of new structures or functions assignments;

Portugal proposes the following text amendments:

(13)	**Without prejudice to the competent authorities and single points of contact's role and obligations layed down by Directive (EU) 2022/2555,**

~~E~~each Member State should designate a public body at national level tasked with coordinating cyber threat detection activities **and cybersecurity situational awareness development responsabilities** in that Member State. These **public bodies acting as** 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.

Article 4

National Security Operations Centres

1. In order to participate in the European Cyber Shield, each Member State shall designate at least **one public body to act as** National SOC **ensuring that they have the means and capacities to develop and feed into national and European cybersecurity situational awareness**. ~~The National SOC shall be a public body.~~

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 **building and enhancing situational awareness**. **This entity acting as National SOC should be able to contribute to** ~~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.

2. Following a call for expression of interest, **entities acting as** 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 **entities acting as** 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 **entity acting as** National SOC shall conclude a hosting and usage agreement regulating the usage of the tools and infrastructures.

3. A**n entity acting as** 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.

Finally, a few requests for clarification:

- On Article 6, implementing acts are requested to the Commission on a basis of "specify the conditions" for interoperability between the Cross-border SOCs.
    - What type of "conditions" are envisaged here? Technical, financial legal?
    - Why only "after consulting the ECCC" and not also the Cross-border SOCs given they are the ones that know technical aspects of their platforms?

- On Article 12 (5) it is stated that "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."
    - Further on Article 16 a designation of "contracting authority" emerges. Who are or can be these "contracting authorities"?
    - Clarifications on the procurement procedures for the purpose of establishing the EU Cybersecurity Reserve are very welcomed.

Currently, Portugal still has a scrutiny reservation on the dispositions of the Proposal regarding the implementing acts given that the reading of such dispositions is still ongoing.

SLOVAKIA

The preliminary comments of Slovakia to the draft Cyber Solidarity Act

(doc. 8512/23 from 20 April 2023)

General comments:

SK supports an idea and a spirit of solidarity, which is the main cornerstone of the proposal, also within the cybersecurity domain. We think for the time being it is more practical to focus particularly on its normative part, while the preamble should be adjusted accordingly afterwards.

SK regrets that the proposal was published without any accompanying impact assessment or at least a relevant gap analysis focusing on possible duplications which may arise on the top of the already existing processes set by the valid cybersecurity legislative framework as well as on the already introduced reviewing cybersecurity mechanism and/or on overall financing from the DEP instrument including its sustainability and predictability, etc.

SK strongly believes that the main features of the proposed Cyber Solidarity Act should be implemented solely on voluntary basis respecting the principles of trust and confidence between partners, notably when sharing or exchanging data or information on relevant cybersecurity incidents. The current proposal, however, contains to a large extent many mandatory elements which may water down the whole approach on combatting the cybersecurity threats and minimizing the cybersecurity risks.

SK insists that national security is a sole responsibility of Member States. The Commission should not be proposing any legislation to amend this firm principle. Even when exchanging information through the envisaged SOCs, Member States should have a right to exclude information where and to the extent that such exclusion is necessary for their national security.

SK also sees a gap in the used terminology (e.g. SOC) which may be widely understood by practitioners. Our aim should be conversely to narrow the notion for a better certainty and clarity. A focus should not be therefore laid more on its institution character rather than on a service or a function it should provide. It should be made clear that SOC is mainly a service and can be offered by any recognized entity by a Member State, e.g. by CSIRT/CERT.

Apart from the functional elements of the proposal SK cannot agree with unjust financing of CB SOC infrastructure. The proposal says that if a national SOC is not a participating in a CB SOC Consortium, it shall not be eligible for DEP funding. We find this conditioning as discriminatory and disproportionate. The DEP is an EU community funding programme which is directly managed by the Commission and financed from the Member States´ budgets. It is based on mutual competition of projects, their excellence and voluntary participation of Member States. The proposed conditioning of a potential national SOC for participation in CB SOC goes therefore beyond the community character and spirit of the DEP programme. The DEP should also allow National SOC which will not form a part of CB SOC Consortia for proper funding. Moreover, a stronger role of ECCC has been deeply overlooked for the purposes of SOC calls.

Comments on the articles:

Art 1(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 infrastructure of Security Operations Centres ~~('European Cyber Shield')~~ to build and enhance common detection and situational awareness capabilities;

Komentár od [R1]: For the purposes of legislative clarity, it is not important to use any abbraviated set of new „buzz words "which may create controversies. It should be just deleted.

Art. 1(2)c

To be deleted ~~(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~~

Komentár od [R2]: As we miss any well substantiated reasoning why a new reviewing and assessment mechanism on cyber incidents should be introduced which could interfere with the internal competencies of Member States, we opt for deleting the whole part.

Art. 1(3)

This Regulation is without prejudice to the Member States' ~~primary~~ sole responsibility for national security, public security, and the prevention, investigation, detection and prosecution of criminal offences.

Komentár od [R3]: To be aligned with article 4(2) TFEU „In particular, national security remains the sole responsibility of each Member State".

Art. 2 (1)

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

Komentár od [R4]: Simplification

Art. 2

There is a missing definition on what is a **National SOC** besides already introduced definition on a Cross-border SOC. A National SOC should be notified to the Commission. If there is more than one SOC performing in a Member State, that Member State should decide which one should be designed as a National SOC and then notified to the Commission. A National SOC should also remain responsible for any internal coordination and exchange of information between the SOCs in a Member States, should there is more than one. A National SOC should be also regarded on the first place as a service or a function rather than an organisation or an institution. As such a National SOC should be well performing in the established CSIRT.

Komentár od [R5]: New definiton on a National SOC should be added.

Art. 3(1)

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

Respecting the principles of non-discrimination, proportionality and voluntariness, Aactions implementing the ~~European Cyber Shield~~ **interconnected pan-European infrastructure of Security Operations Centres** shall be supported by **EU funding, in particular** from the Digital Europe Programme and implemented in accordance with Regulation (EU) 2021/694 and in particular Specific Objective 3 thereof.

Art. 3(2)

The~~-~~ **interconnected pan-European infrastructure of Security Operations Centres** ~~European Cyber Shield~~ shall:

(a) pool and share **agreed and when necessary anonymised and aggregated** data on cyber threats and incidents from various sources through cross-border SOCs **using the established means of the CSIRT's network**;

Art. 4

(1) ~~In order to participate in~~ **For the purposes of** the **interconnected pan-European infrastructure of Security Operations Centres**, each Member State shall designate ~~at least~~ one National SOC. The National SOC **can**~~shall~~ **be established within the existing CSIRT or as a separate** ~~-~~public body~~.~~

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**, if applicable, voluntarily** ~~-~~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.

(3) to be fully deleted.

~~. 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.~~

Art 6

(1) **With regard to Art. 3(2)** Members of a Hosting Consortium ~~shall~~ **may** exchange relevant information among themselves within the Cross-border SOC including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding the configuration of cybersecurity tools to detect cyber attacks, where such information sharing:

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

(a) a commitment to share ~~a significant amount of~~**relevant** 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,

Komentár od [R6]: In case a National SOC decides not to join any Cross-border SOC, but still would be performing within the interconnected pan-European infrastructure of SOCs, a respective funding should be also made available to support such a SOC. Our reading is that this is missing from the current proposal.

Komentár od [R7]: Why to lock ourselves only in the DEP programme which is already quite constrained? There are plenty of other instruments, e.g. European Investment and Structural Funds and/or Recovery and/or Resilience Facility and/or other directly managed funds...

Komentár od [R8]: We find important to specify that not all data on cyber threats and incidents should be shared. Only the agreed data fulfilling the purpose, sometimes anonymised or aggregated, can be exchanged following a commercial agreement between the parties. For example, we may be reluctant to share data on a victim, but rather on an attacker...

Komentár od [R9]: We support the idea of National SOCs and Cross-border SOCs exchanging and sharing the agreed data via the CSIRTs network infrastructure. We are not in favour of creating a new dubious communication infrastructure.

Komentár od [R10]: See our comments for Art 2 – a National SOC

Komentár od [R11]: It is important to focus on the main function of a SOC rather than on its legal personality. Member States should have a liberty specifying which body will perform a task/function of a SOC.

Komentár od [R12]: There may be cases when a National SOC may not want to be part of a Cross-border SOC.

Komentár od [R13]: Paragraph 3 should be deleted in its entirety as it goes directly against the uttered principle of voluntariness, proportionality and it is discriminatory. When an envisaged Cross-border SOCs call from DEP is announced, participation of national SOCs from MS should be purely voluntary. Those not joining cross-border SOCs calls, should not be deprived of funding. It is specified in art 3(1) that the interconnected pan-European infrastructure of Security Operations Centres (so called european cyber shield) consists of all National Security Operations Centres and Cross-border Security Operations Centres.

(c) targets for contribution to the development of advanced artificial intelligence and data analytics tools.

(3) to be deleted.

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

(4)~~.~~ Cross-border SOCs shall conclude cooperation agreements with one another, specifying information sharing principles among the cross-border platforms.

New Paragraph) Member States can exclude exchange of information where and to the extent that such exclusion is necessary for their national security.

Art. 7

(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 **and**~~,~~ the CSIRTs network ~~and the Commission~~, in view of their respective crisis management roles in accordance with Directive (EU) 2022/2555 without undue delay.

Art. 8

The wording „**the interconnected pan-European infrastructure of Security Operations Centres**" instead of „European Cyber Shield" to be applied.

Art. 9

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

Art. 12

(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~~ **that may** ~~shall~~ be deployable in all Member States.

(3) Users of the services from the EU Cybersecurity Reserve ~~shall~~ **may** 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.
(c) Third countries pursuant to Article 17

Komentár od [R14]: There is no added value in the paragraph. Once we agree that data is exchanged via the CSIRT's network, there is tangible benefit for a dubious infrastructure and implementing acts procedures.

Formátované: Písmo: 12 b, Tučné, Podčiarknutie

Komentár od [R15]: A similar provision is enshrined in NIS2 Directive.

Formátované: Písmo: 12 b, Tučné, Podčiarknutie

Formátované: Písmo: 12 b, Tučné, Podčiarknutie

Komentár od [R16]: The role of the Commission here is without any added value. As the similar procedure is already established in EU crisis management structures (NIS2), the whole article 7 seems dubious and repetitive. We have to strive to get utmost from the already existing infrastructure under NIS2.

Komentár od [R17]: Our initial understanding is that we describe a funding mechanism here. If yes, the wording should be adapted in the whole proposal.

Komentár od [R18]: Just to broaden the possible scope for funding.

(4) Users referred to in paragraph 3, point (a), may~~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.

Art. 18

To be deleted in its entirety

Komentár od [R19]: The same comment as in art. 1(2) c we miss any well substantiated reasoning why a new reviewing and assessment mechanism on cyber incidents should be introduced which could interfere with the internal competencies of Member States, we opt for deleting the whole part.

FINLAND

[…]

HAVE ADOPTED THIS REGULATION:

Commented [A278]: Finland still holds a scrutiny reservation to the proposal.

Commented [A279]: Commision has indicated in the HWP CI that all the actions proposed in this regulation are voluntary. The voluntarity of the actions should be more clearly indicated in the text in all relevant chapters.

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 infrastructure 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 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;

(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..

3. This Regulation is without prejudice to the Member States' ~~primary~~ sole responsibility for national security, public security, and the prevention, investigation, detection and prosecution of criminal offences. This Regulation cannot be interpreted in a way leading to any harmonisation of the laws and regulations of the Member States.

Commented [A280]: National security is in the sole competence of the MS.

Commented [A281]: This comes from the legal basis, but for clarity it could be repeated here.

Article 2

Definitions

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

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

Commented [A282]: Either the definition of a Cross border SOC should be removed or also the definition of a SOC should be included in this article

Commented [A283]: If kept, the text should be clarified as this is rather a description than definition

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

Commented [A284]: Since this covers only bodies goverened by public law, then it would be better to change the definition to bodies governed by public law

(3) **'Hosting Consortium'** means ~~a consortium composed of participating states, represented by National SOCs, that have agreed to establish and contribute to the acquisition of tools and infrastructure for, and operation of,~~ a Cross-border SOC that applies to and participates in a joint procurement of tools and infrastructures with the ECCC;

Commented [A285]: This definition is clearer. The original defitions simply defined Hosting Consortiums as Cross-border SOCs.

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

(5) '**entities operating in critical or highly critical sectors'** means ~~type of~~ entities listed in Annex I and Annex II of Directive (EU) 2022/2555;

Commented [A286]: For legal certainty, the definition should not be open-ended

(6) '**cyber threat'** means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881;

(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;~~

Commented [A287]: These definitions are not absolutely necessary to be included here. However, if these are included it should be noted that preparedness and response actions are taken not only to prepare and respond for significant or large scale incidents but for cyber incidents of all volumes

[24] 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).

(11) **'trusted providers'** means managed security service providers as defined in Article 6, point (40), of Directive (EU) 2022/2555 selected in accordance with Article 16 of this Regulation.

Chapter II

THE EUROPEAN CYBER SHIELD

Article 3

Establishment of the European Cyber Shield

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

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 and produce high-quality, actionable information and cyber threat intelligence through cross-border SOCs;

(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;

(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 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

Commented [A288]: Finland welcomes the discussion of the name of the « Cyber Shield ». Finland sees that the current term « shield » misleading as the SOC's tasks mainly cover enhancing cyber threat detection and not blocking the cyber incidents.

Commented [A289]: This type of information is often provided most efficiently without the help of AI tools.

Commented [A290]: As disccused in HWP CI and in the workshop, the tasks and organization of a National SOC compared to CSIRTs should be indicated in the text. Finland sees that the cyber shield could complement the CSIRT's tasks or be perfomed by the CSIRT's to avoid duplication and confusion with the existing structures.

1. In order to participate in the European Cyber Shield, each Member State shall designate at least one National SOC. The National SOC shall be a public body or a competent authority.

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.

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.

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~~reimburse the awarded grant.

Article 5

Cross-border Security Operations Centres

1. ~~A Hosting Consortium consisting of a~~At least three Member States, represented by National SOCs, may form a Cross-border Security Operations Centre~~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~~.

It shall be a coordinated network structure that is designed to prevent cyber threats and incidents and to support the production of high-quality cyber threat intelligence, notably through the exchange of data from various sources, public and private, as well as through the sharing of state-of-the-art tools and jointly developing cyber detection, analysis, and prevention and protection capabilities in a trusted environment. A Cross-border Security Operations Centre may form a Hosting Consortium.

Commented [A291]: The voluntarity of this action should be more clearly stated in the text

Commented [A292]: As the definition of a public body is narrow (see the comment above), so there needs to be left more room for MS's to decide on how organise this nationally. In Finland, for constitutional reasons, the National SOC might have to be an authority.

Commented [A293]: This makes it unlcear whether the MS should give more rules in order to ensure this. And the legal base for this Regulations does not allow for harmonisation of MS laws.

Commented [A294]: In case para 3 is left in the text, we propose the reimbursement of the grants.

Commented [A295]: Now this is symmetrical with article 4 which makes the structure clearer.

Formatted: English (United States)

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

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.

The written consortium agreement shall also establish:

(a) a governance framework ;

(b) targets for contribution to the development of advanced artificial intelligence and data analytics tools.

Commented [A296]: Moved from article 6(2) with amendments (see the explanations there).

~~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.~~

Commented [A297]: We oppose this as it complicates the strucure for no real reason. There is no need for this as this can be best addressed in the agreements referred to in paras 2 and 3. Also, legal personhood is not compatible with the description of a Cross-border Security Operations being a network or a platform.

Article 6

Cooperation and information sharing within ~~and between~~ cross-border SOCs

1. Members of a Hosting Consortium shall exchange, in accordance with union and national law, ~~relevant~~ necessary information among themselves within the Cross-border SOC including information ~~relating to~~on 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 is necessary to:

Commented [A298]: The legal base does not allow for harmonisation, so the information to be shared need to be limited to what other EU law and national law allow.

Commented [A299]: It seems that the information exchange may include also confidential information, so there should be a threshold of necessity.

Commented [A300]: It seems that the information exchange may include also confidential information, so there should be a threshold of necessity.

(a) ~~aims to~~ prevent, detect, respond to or recover from incidents or to mitigate their impact;

(b) enhance~~s~~ 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:~~

Commented [A301]: Moved to article 5(3).

~~(a) a commitment to share a significant amount of data referred to in paragraph 1, and the conditions under which that information is to be exchanged;~~

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

~~4. Cross-border SOCs shall conclude cooperation agreements with one another, specifying information sharing principles among the cross-border platforms.~~

Article 7

Cooperation and information sharing with Union entities

1. Where the Cross-border SOCs obtain information ~~relating to~~on a potential or ongoing large-scale cybersecurity incident, they shall provide ~~relevant~~ necessary 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 and national law without undue delay.

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

Article 8

Security

1. Member States participating in the European Cyber Shield shall ensure on their part 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.

Commented [A302]: We have a constitutional issue with this – information exchange need to be based on law as it can include confidential information. Also, with para 1, this subpara is not needed.

Commented [A303]: This is not needed and interoperability is a a basic requirement and not a reason to exhancge information in itself.

Commented [A304]: This is not needed and interoperability is a a basic requirement and not a reason to exhancge information in itself.

Commented [A305]: Cross-border SOC's should be included here as the ECCC does not have such competence

Commented [A306]: We have a constitutional issue with this – information exchange need to be based on law as it can include confidential information. Information between the CBSOC's can only be shared in accordance with MS national legislation and EU legislation.

Commented [A307]: Too vague as the information exchanged can include confidential information

Commented [A308]: We must insist on taking into account also the national law as the legal bases does not allow for harmonisation of the Member State laws.

Commented [A309]: To be symmetrical with article 8(3) – this formulation is better in light of the fact that impelementing powers should adress only techincal questions.

Commented [A310]: Each MS is responsible for its own measures.

2. Member States participating in the European Cyber Shield shall ensure on their part 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. 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.

Commented [A311]: We would like to ask the Council legal service on whether this formulation is acceptable in the light of the legal basis not allowing harmonisation of MS laws.

Chapter III

CYBER EMERGENCY MECHANISM

Article 9

Establishment of the Cyber Emergency Mechanism

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

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.

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 providers participating in the EU Cybersecurity Reserve established under Article 12;

Commented [A312]: The types of these services should be clarified in the text and are these services also provided by trusted providers ?

(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.

Article 11

Commented [A313]: This article should be broadened and include more information of these services. Also the voluntarity of these services should be stated.

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 at Union level.
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.

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.
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.
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.
4. Users referred to in paragraph 3, point (a), may ~~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.

5. The Commission shall have overall responsibility for the implementation of the EU Cybersecurity Reserve. The Commission shall in cooperation with ENISA and Member States determine the priorities and evolution of the EU Cybersecurity Reserve, ~~in line with the requirements of the users referred to in paragraph 3,~~ The ~~and~~Commission 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 may 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, 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.

8. The Commission may, by means of implementing acts, specify the types and the number of response services required for the EU Cybersecurity Reserve. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2).

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 regularly 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:

Commented [A314]: Does the Commission have the technical and operational expertise needed to perform this task ?

Commented [A315]: Finland sees it necessary to state also in the text at least in some level of the types and forms of IR services

Commented [A316]: This should be aligned with the art 12(4) text

Commented [A317]: Does the Commission have the technical and operational expertise needed to perform this task ?

Commented [A318]: Should be noted that this information may be sensitive and in times of urgent incident response only necessary information exchange may be performed.

(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 CSIRT-network, NIS Cooperation Group and 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 may, by means of implementing acts, specify further the detailed arrangements for allocating the EU Cybersecurity Reserve support services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2).

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 delay.

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 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.

4. The agreements referred to in paragraph 3 may be based on templates prepared by ENISA, after consulting Member States.

Commented [A319]: This process should be designed agile and efficient to ensure that the help can be delivered in time. However, should be ensured that these services are not used to replace national IR actions and cababilities. Also the use of information should be clarified in the text.

Commented [A320]: Are these agreements made case by case basis ? If yes, see comment above.

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.

6. Within three months ~~one month~~ from the end of the support action, the users shall provide Commission and ENISA with a summary report about the service provided, results achieved and the lessons learned. When the user is from a third country as set out in Article 17, such report shall be shared with the High Representative.

7. The Commission shall report to the NIS Cooperation Group about the use and the results of the support, on a regular basis.

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[25], the support under this Regulation for responding to such incidents shall complementactions 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 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.

4. Support under the Cyber Emergency Mechanism may form part of the joint response between the Union and Member States in situations referred to in Article 222 of the Treaty on the Functioning of the European Union.

Article 16

Trusted providers

[25] 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).

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.

(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.

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;

Commented [A321]: MS have different requirements for security clearances so MS shall define the needed level of secuirty clearance

(e) the provider shall have the relevant level of security for its IT systems;

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

(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) where it can deliver the service if required by the Member State;

Commented [A322]: The market impact of this requirement should be analyzed. We prefer to have this requirement optional or deleted from the act.

(j) once an EU certification scheme for managed security service Regulation (EU) 2019/881 is in place, the provider shall be certified in accordance with that scheme.

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 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

Commented [A323]: The voluntarity of this mechanism should be more clearly indicated

1. At the request of ~~the Commission,~~ the EU-CyCLONe or the CSIRTs network, ENISA ~~shall~~ may 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.

Commented [A324]: If the request relates to an incident targeted or affected to a Member State, Member State shall give their consent to perform the review

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

3. The report shall cover a review and analysis of the specific significant or large-scale cybersecurity incident, including the main causes, vulnerabilities and lessons learned. It shall protect confidential information, in accordance with Union or national law concerning the protection of sensitive or classified information.

4. Where appropriate, the report shall draw recommendations to improve the Union's cyber posture.

5. Where possible, a version of the report shall be made available publicly. This version shall only include public information.

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:

(1) 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';

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

‘(g) establish and operate a Cyber 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’;

(a) 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[26] with the exception of actions implementing the EU Cybersecurity Reserve, which shall be implemented by the Commission and ENISA.**';**

(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 1 629 566 000 for Specific Objective 3 – Cybersecurity and Trust;

(d), EUR 482 347 000 for Specific Objective 4 – Advanced Digital Skills’;

(b) the following paragraph 8 is added:

‘8. By derogation to Article 12(4) of Regulation (EU, Euratom) 2018/1046, unused commitment and payment appropriations for actions pursuing the objectives set out in Article 6(1), point (g) of this Regulation, shall be ~~automatically~~ discretionally carried over and may be committed and paid up to 31 December of the following financial year.’;

Commented [A325]: This would be a very exceptional procedure, which is why Finland proposes a discretionary transfer of the funds instead of automatic transfer.

(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 Financial Regulation, including in particular through procurement as a primary form, or grants and prizes.

[26] 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. 1-31).

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 [27] and 2014/25/EU [28] 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/XX, 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). XXX/XXXX [FR Recast], 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) XXX/XXXX [FR Recast], 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:

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/XX. In the case of conflict between the provisions of this Regulation and Articles 4 and 5 of Regulation (EU) 2023/XX, 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 the Financial Regulation and may cover up to 100 % of the eligible costs, without prejudice to the co-financing principle as laid down in Article 190 of the Financial Regulation. 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 XXXX and the Hosting Consortium referred to in Article 5 of Regulation XXXX, in accordance with Article 195(1), point (d) of the Financial Regulation.~~

Support in the form of grants for the Cyber Emergency Mechanism as set out in Article 10 of Regulation XXXX may be awarded directly by the ECCC to Member States without a call for proposals, in accordance with Article 195(1), point (d) of the Financial Regulation.

For actions specified in Article 10(1), point (c) of Regulation 202X/XXXX, 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 XXXX, and in accordance with Article 193(2), second subparagraph, point (a), of the Financial Regulation, 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 are amended in accordance with the Annex to this Regulation.

[…]

SWEDEN

[…]

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 infrastructure 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.

Commented [A326]: SE supports BE :s suggestion to replace the term "SOC" with "Threat Intelligence-sharing (Platforms)". SE suggests that the term SOC is replaced throughout this Proposal.

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 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;

(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 MS, on a voluntary basis, reviewing and assessing significant or large-scale incidents, including drawing lessons learned and, where appropriate, recommendations..

3. This Regulation is without prejudice to the Member States' responsibility for safeguarding national security and their power to safeguard other essential State functions, including ensuring the

~~[illegible]~~ responsibility of each Member State.

Commented [A327]: SE suggest that text from art. 2.6 in the NIS 2 Directive is used here.

Commented [A328]: SE would like a reference to art. 4.2 (TEU) here.

Article 2

Definitions

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

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

Commented [A329]: SE supports the proposal by BE to replace "SOC" with "Threat Intelligence-sharing Platforms" throughout this Proposal. SE suggests that this term is included in the list of definitions.

(2) **'public body'** means a body governed by public law as defined in Article 2((1), point (4),), of Directive 2014/24/EU of the European Parliament and the Council[27];

Commented [A330]: SE would prefer the definition "public administration entity" from the NIS2-Directive.

(3) **'Hosting Consortium'** means a consortium composed of participating states, represented by National entity responsible for threat intelligence-sharing~~SOCs~~, that have agreed to establish and contribute to the acquisition of tools and infrastructure for, and operation of, a Cross-border ~~SOC~~;

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

(5) '**entities operating in critical or highly critical sectors'** means type of entities listed in Annex I and Annex II of Directive (EU) 2022/2555;

(6) '**cyber threat'** means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881;

(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;~~

Commented [A331]: SE does not find this definition necessary. It may also be limiting for the future.

(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;~~

Commented [A332]: SE does not find this definition necessary.

(11) **'trusted providers'** means managed security service providers as defined in Article 6, point (40), of Directive (EU) 2022/2555 selected in accordance with Article 16 of this Regulation.

---

[27] 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).

Chapter II

THE EUROPEAN CYBER WARNING SYSTEM ~~SHIELD~~

Article 3

Establishment of the European Cyber Warning System ~~Cyber Shield~~

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

Actions implementing the European Cyber ~~Shield~~ Warning System 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~~ Warning System shall, on a voluntary basis:

(a) ~~pool and share~~collect data on cyber threats and incidents from ~~various~~ sources through cross-border ~~SOCs~~;

(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) support the CSIRTs network by contribut~~e~~ing to better protection and response to cyber threats;

(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 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~~ Threat Intelligence-sharing Platforms

1. In order to participate in the European Cyber Warning System ~~Shield~~, each Member State shall designate at least one National ~~SOC~~. The National ~~SOC~~ shall be a public body.

Commented [A333]: SE notes that "shield" has military connotations. SE supports the suggestion from BE to rename it "Cyber Warning System".

Commented [A334]: SE would like to see a more descriptive term, eg. "Cyber Warning System" (as suggested by BE).

Commented [A335]: SE does not see the point with limiting this to certain technologies.

Commented [A336]: SE notes that the AI Act has not yet been finalized. Further, it is difficult to see how the Cyber Warning System would *contribute* to the *development* of AI.

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.

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.

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.

Commented [A337]: According to SE, it would be more logic to see that Enisa was responsible for procurements, not the ECCC.

Article 5

Cross-border ~~Security Operations Centres~~ Threat Intelligence-sharing Platforms

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~~. .

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

Commented [A338]: SE: What are the reason behind this threshold of union financing? Are there any parallels to other areas?

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.~~

Commented [A339]: SE : This text is too broad and may be potentially be incompatible with SE law.

Article 6

Cooperation and information sharing within and between cross-border Threat Intelligence-sharing Platforms~~SOCs~~

1. Members of a Hosting Consortium shall, on a voluntary basis, exchange relevant information among themselves within the Cross-border ~~SOC~~ which may includ~~ing~~ 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) aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;

(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 amount of~~ data on a voluntary basis ~~as referred to in paragraph 1~~, and the conditions under which that information is to be exchanged;

Commented [A340]: SE would welcome a deletion of this part, as it should be up to the participating MS in the different consortiums to decide the conditions of their sharingof data.

(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.

Commented [A341]: SE notes that the AI Act has not been finalized and SE wishes to avoid reference to AI in this regulation.

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

Commented [A342]: SE: Clarification needed. What kind of changes does the COM foresee? If not entirely clear, this should be deleted. This regulation should define the premises and conditions of the interoperatiblity and information sharing.

4. Cross-border ~~SOCs~~ shall, on a voluntary basis, conclude cooperation agreements with one another, specifying information sharing principles among the cross-border platforms.

Article 7

Cooperation and information sharing with Union entities

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, where relevant, the Commission, in view of their respective crisis management roles in accordance with Directive (EU) 2022/2555 without undue delay.

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

Commented [A343]: SE would like to ask for a comment from the COM or the PRES on how this article relates to the information sharing obligations laid down in the NIS2-directive. This to make sure there wont be any duplications of structures.

Commented [A344]: SE: Clarification needed. What kind of changes does the COM foresee? If not entirely clear, this should be deleted. This regulation should define the premises and conditions of the interoperatiblity and information sharing.

Article 8

Security

1. Member States participating in the European Cyber Warning System~~Shield~~ shall ensure a high level of data security and physical security of the European Cyber ~~Shield~~ Warning System 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 Warning System~~Shield~~ shall ensure that the sharing of information within the European Cyber ~~Shield~~ Warning System 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. 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.~~

Commented [A345]: SE suggests that this para is deleted, or otherwise clarified. What kind of changes does the COM foresee? If not entirely clear, this should be deleted. This regulation should define the premises and conditions of the interoperatiblity and information sharing.

Chapter III

CYBER EMERGENCY MECHANISM

Article 9

Establishment of the Cyber Emergency Mechanism

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

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.

Commented [A346]: SE : MS role needs to be clarified in this article. MS should have the opportunity to intervene regarding contracts and agreements.

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 providers participating in the EU Cybersecurity ~~Reserve~~ Support 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.

Commented [A347]: SE would like to ask for a comment from the COM on this "in particular". Does the COM foresee any other mutual assistance actions from one national authority of one MS to another MS than what is provided for in the NIS2-directive?

Article 11

Coordinated preparedness testing of entities

Commented [A348]: SE : MS role needs to be clarified in this article. MS should have the opportunity to intervene regarding contracts and agreements.

1. For the purpose of supporting ~~the~~ voluntary coordinated preparedness testing of entities referred to in Article 10(1), point (a), across the Union, the Commission, after consulting the NIS Cooperation Group and ENISA, shall identify the sectors, or sub-sectors, concerned, from the Sectors of High Criticality listed in Annex I to Directive (EU) 2022/2555 from which entities may

be subject to the coordinated preparedness testing, taking into account existing and planned coordinated risk assessments and resilience testing at Union level.

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.

Article 12

Establishment of the EU Cybersecurity ~~Reserve~~ Support

1. An EU Cybersecurity ~~Reserve~~ Support shall be established, in order to facilitate for voluntary assistance to users referred to in paragraph 3, in responding or providing support for responding to significant, ~~or~~ large-scale or major cybersecurity incidents, and immediate recovery from such incidents.

2. The EU Cybersecurity ~~Reserve~~ Support shall consist of incident response services from trusted providers selected in accordance with the criteria laid down in Article 16. The ~~Reserve~~ Support shall include pre-committed services. The services ~~shall~~ may be deployable upon request in all Member States and EUIBAs.

3. Users of the services from the EU Cybersecurity ~~Reserve~~ Support 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 ~~entities institutions, bodies and agencies~~,

c) Specified entities in eligible third countries

4. Users referred to in paragraph 3, point (a), ~~shall~~ may use the services from the EU Cybersecurity ~~Reserve~~ Support 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.

5. The Commission shall have overall responsibility for the implementation of the EU Cybersecurity ~~Reserve~~Support. The Commission, in close cooperation with ENISA, shall determine the priorities and evolution of the EU Cybersecurity ~~Reserve~~Support, 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 may entrust the operation and administration of the EU Cybersecurity ~~Reserve~~Support, in full or in part, to ENISA, by means of contribution agreements.

Commented [A349]: SE : Why not all NIS-entities? Also, who will finance these tests?

Commented [A350]: SE is wondering if these are the same risk-scenarios that are metionned in the Cyber Posture from 2022, and the Cyber Defence Policy from 2023, or if these are new ones?

Commented [A351]: SE: The term "reserve" has military connotations. SE suggestion: "Cybersecurity Support"

Commented [A352]: SE suggests that "*major* incidents" are included here so that also EUIBAs can request support.

Commented [A353]: SE would recommend to use "Union entities" and then refer to the definition in the regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (article 3.1).

Commented [A354]: SE would like to ask for a comment from ENISA on their possibility to realise such tasks, given their (limited) resources.

7. In order to support the Commission in establishing the EU Cybersecurity ~~Reserve~~Support, 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~~ Support pursuant to Article 17. The Commission, where relevant, shall consult the High Representative.

8. The Commission may, by means of implementing acts, specify the types and the number of response services required for the EU Cybersecurity ~~Reserve~~Support. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 21(2).

Article 13

Requests for support from the EU Cybersecurity ~~Reserve~~Support

1. The users referred to in Article 12(3) may request services from the EU Cybersecurity ~~Reserve~~ Support to support response to and immediate recovery from significant~~, or~~ large-scale or major cybersecurity incidents.

Commented [A355]: SE proposes this addition in order to include the wording related to EUIBAs.

2. To receive support from the EU Cybersecurity ~~Reserve~~Support, 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~~Support.

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

Commented [A356]: SE: These arrangements need to be more specified in this regulation.

Article 14

Implementation of the support from the EU Cybersecurity ~~Reserve~~Support

1. Requests for support from the EU Cybersecurity ~~Reserve~~Support, shall be assessed by the Commission, with the support of ENISA or as defined in contribution agreements under Article 12(6), and a response shall be transmitted to the users referred to in Article 12(3) without delay.

Commented [A357]: SE would like to see an inclusion of the concerned MS in the the requests.

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 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~~ Support 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~~ Support is provided. Those agreements shall include liability conditions.

Commented [A358]: SE welcomes a clarification of MS role in these agreements.

4. The agreements referred to in paragraph 3 may be based on templates prepared by ENISA, after consulting Member States.

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~~Support.

Commented [A359]: SE notes that service providers (art. 14 para 3) has contractual liabilities. What about the COM and ENISA?

6. Within one month from the end of the support action, the users shall provide Commission and ENISA with a summary report about the service provided, results achieved and the lessons learned. When the user is from a third country as set out in Article 17, such report shall be shared with the High Representative.

7. The Commission shall report to the NIS Cooperation Group about the use and the results of the support, on a regular basis.

Commented [A360]: SE: This should be specified.

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[28], the support under this Regulation for responding to such incidents shall complementactions 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 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.

4. Support under the Cyber Emergency Mechanism may form part of the joint response between the Union and Member States in situations referred to in Article 222 of the Treaty on the Functioning of the European Union.

Article 16

Trusted providers

1. In procurement procedures for the purpose of establishing the EU Cybersecurity ~~Reserve~~Support, 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~~ Support includes services that may be deployed in all Member States and eligible third countries, 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.

(c) ensure that the EU Cybersecurity ~~Reserve~~ Support 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.

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

[28] 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).

(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 an ~~framework~~ agreement 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 the hardware and software technical equipment necessary to support the requested service;

(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) where it can deliver the service;

(j) once an EU certification scheme for managed security service Regulation (EU) 2019/881 is in place, the provider shall be certified in accordance with that scheme.

Commented [A361]: SE: What counts as "sufficient" in this context? SE suggestion: delete.

Commented [A362]: SE: What counts as "appropriate" in this context? SE suggestion: delete.

Commented [A363]: SE question: Will the Cybersecurity Support ("reserve") only include European companies?

Article 17

Support to third countries

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

2. Support from the EU Cybersecurity ~~Reserve~~ Support 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~~ Support shall include competent authorities such as CSIRTs and cyber crisis management authorities.

4. Each third country eligible for support from the EU Cybersecurity ~~Reserve~~ Support 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~~Support, 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 inform 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~~Support.

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, and with the consent of Member States, 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 with anonymised analysed information, to the CSIRTs network, the EU-CyCLONe and the Commission to support them in carrying out their tasks, in particular in view of those set out in Articles 15 and 16 of Directive (EU) 2022/2555. Where relevant, the Commission shall share the report with the High Representative.

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

3. The report shall cover a review and analysis of the specific significant or large-scale cybersecurity incident, including the main causes, ~~vulnerabilities~~ and lessons learned. It shall protect confidential information, in accordance with Union or national law concerning the

Commented [A364]: SE notes that "vulnerabilities" could mean a number of different things for different MS. However, MS vulnerabilities may have implications for national security. SE suggestion: delete.

Commented [A365]: SE notes the importance that this review mechanism does not have negative impacts on actor's incentives to report incidents and thus suggests this clarification.

Commented [A366]: SE notes that "vulnerabilities" could mean a number of different things for different MS. However, MS vulnerabilities may have implications for national security. SE suggestion: delete.

protection of sensitive or classified information. Upon request from affected actors, the report shall only cover anonymised analysed information.

4. Where appropriate, the report shall draw recommendations to improve the Union's cyber posture.

5. Where possible, a version of the report shall be made available publicly. This version shall only include public information.

Commented [A367]: SE : what is intended with the reference to the Cyber posture here? Could this be clarified?

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:

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

'(aa) support the development of an EU Cyber ~~Shield~~Warning System, 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';

Commented [A368]: SE : Which threat intelligence capacities are referred to here? Institutions (SIAC? INTCEN?) capacities, or MS national capacitites?

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

'(g) establish and operate a Cyber 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~~'Support;

(a) 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[29] with the exception of actions implementing the EU Cybersecurity ~~Reserve~~Support, which shall be implemented by the Commission and ENISA.**';**

(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 1 629 566 000 for Specific Objective 3 – Cybersecurity and Trust;

(d), EUR 482 347 000 for Specific Objective 4 – Advanced Digital Skills';

(b) the following paragraph 8 is added:

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

(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 Financial Regulation, 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 [27] and 2014/25/EU [28] 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.

[29] 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. 1-31).

When implementing procurement procedures for the EU Cybersecurity ~~Reserve~~ Support 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 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). XXX/XXXX [FR Recast], 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~~ Support 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) XXX/XXXX [FR Recast], 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:

In the case of actions implementing the European Cyber ~~Shield~~ Warning System 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/XX. In the case of conflict between the provisions of this Regulation and Articles 4 and 5 of Regulation (EU) 2023/XX, 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 the Financial Regulation and may cover up to 100 % of the eligible costs, without prejudice to the co-financing principle as laid down in Article 190 of the Financial Regulation. 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 XXXX and the Hosting Consortium referred to in Article 5 of Regulation XXXX, in accordance with Article 195(1), point (d) of the Financial Regulation.

Support in the form of grants for the Cyber Emergency Mechanism as set out in Article 10 of Regulation XXXX may be awarded directly by the ECCC to Member States without a call for proposals, in accordance with Article 195(1), point (d) of the Financial Regulation.

For actions specified in Article 10(1), point (c) of Regulation 202X/XXXX, 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 XXXX, and in accordance with Article 193(2), second subparagraph, point (a), of the Financial Regulation, in duly justified cases, the costs may be considered to be eligible even if they were incurred before the grant application was submitted.";

[…]