Council of the European Union
General Secretariat

Interinstitutional files:
2023/0109 (COD)

Brussels, 31 January 2024

WK 1491/2024 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 (attachés)
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 - Presentation

Delegations will find in the Annex a presentation by the Presidency to illustrate the results of the latest technical meetings, presented by the Presidency at the HWPCI meeting on 31 January 2024.

PUBLIC

Cyber Solidarity Act update HWPCI 31/01/24

1. Result of the third round of technical meetings

   Basis: 4 col document WK 1345/2024

2. Possible compromise proposals on pending issues

3. Topics for the trilogue on 13/02

1. Outcome of the latest technical meetings

Article 19 – Amendments to the DEP Regulation (2021/694)

Pending

- **Terminology** that is not approved yet: CAS and (Cross-Border) Cyber Hubs
- Council addition that underlines the deployment of the Reserve being **'upon request' + 'certain third countries'**
- Linguistic change of the EP: '**Cybersecurity' vs. 'Cyber'**

Trilogue

- **Budget issues:** too political for the EP to be discussed during the ITM's.
  - Main points of debate:
    - **budget cap** for the Reserve
    - **Funding from** SO2 (AI) and 4 (skills)
    - **Required amounts for an effective reserve**
    - **Quid limiting derogation to annuality principle?**
- **Procurement from third country providers**

belgium24.eu

1. Outcome of the latest technical meetings

Article 19a – Additional resources for ENISA

Pending
• EP addition of a specific article to receive additional funding. Council points towards its recital 37a to take into account this concern as well as the upcoming review of the CSA where this will be considered in a broader context.

1. Outcome of the latest technical meetings

Article 20 – Evaluation (and review)

Agreed

- In principle **agreement on more detailed provisions for the evaluation report than COM proposal**, but need to align this with the rest of the text and feasibility for the Commission

Pending

- **Timeframe** for reporting – currently on the table 2 year and every 4 years afterwards
- EP addition
  - mention of **ISACs** in the regulation
  - **a measure of effectiveness**
  - reference to **skills and contribution of regulation to skills**
  - broadening **scope** reserve
  - a **review clause**

1. Outcome of the latest technical meetings

Article 20a – Exercise of the delegation

Trilogue
• **Delegated acts** referred to in Article 6(3), Article 7(2), Article 12(8) and Article 13(7) • Plea of Parliament to be **more involved** in this legislation

1. Outcome of the latest technical meetings

Annex

Agreed	Pending
• Line 255, 256 and 258 **text from EC proposal**	• EP: importance of **gender balance** (broad impact in DEP) • Alignment of **"managed security service"** with **DEP** to be checked by the EC • EP addition of '**including Cybersecurity Shield** & Alignment with definitions to be agreed upon • EP **Clarifications** on "actions supporting preparedness and response to cybersecurity incidents"

1. Important updates from last week

Agreed

Article 1 – Subject-matter and objectives

- Art. 1 (3) - *Line 62* on national security – Council's position accepted

1. Important updates from last week

Agreed

Article 2 - Definitions

- Preparedness & response Art. 2 (9) & (10) - *Lines 73 & 74:* deleted

- **Definitions: new approach** – National Cyber Hub / Crossborder Cyber Hub / Hosting consortium to be defined in the relevant articles 4-6

1. Important updates from last week

Agreed

Article 3 - Establishment of the European Cybersecurity Alert System

Art.3(2), first subpara, point (a), Line 81
*pool **relevant data and** information on cyber threats and incidents from various sources within the Cross Border Cyber Hubs and share analysed or aggregated information Cross Border Cyber Hubs, where relevant with the CSIRTs Network.*

Art, 3(2)(b) - Line 82

*Collect **and support the production of** high-quality**, actionable** information and cyber threat intelligence, through the use of state-of-the art tools and advanced technologies , and share that information and cyber threat intelligence*

2. Presidency Compromise proposals – from last week

Voluntary nature - Small change on the proposal to streamline references to the "voluntary nature" of the Cyber Solidarity Act's three pillars:

Pillar II – Emergency Mechanism		
Art. 9(1a) *Line 116a*	In the case of Member States, the actions provided under the Mechanism **shall be provided upon request and** shall be complementary to Member States' efforts and actions to prepare for, respond to and recover from cybersecurity incidents	Unchanged. Must be maintained to clearly state the voluntary nature of all actions under the Emergency Mechanism.
~~**Art. 10 (-1)**~~ ~~*Line 118a*~~	~~**Member States may request to participate in the actions under the Mechanism (current Council mandate)**~~	Could be deleted as the voluntary nature of the actions under the Emergency Mechanism is already clearly stated under Art. 9(1a).

belgium24.eu

2. Presidency Compromise proposals – from last week

Art. 16(2)(l) – *line 180* **– Use of languages for services in the Cyber Reserve**

Modified proposal combining flexibility and requirements where necessary

"the provider shall , if required by the Member State, be able to provide the service ***in one or more official languages of the Member State, as required by that Member State.****"*

2. Presidency Compromise proposals

New Art. 4(1a) – *line 89a* - **National Cyber Hubs**

National cyber hubs shall seek to ***make full use of the information they collect from both private and public sector sources*** *for the purpose of detecting and preventing cyber threats and incidents by c****ooperating, where appropriate, with the private sector, including managed security service providers that provide services to entities operating in sectors of high criticality or other critical sectors as well as with sectoral and cross-sectoral communities***

Where appropriate and in accordance with national and European Union law, the information collected by national cyber hubs may include telemetry, sensor or logging data from national critical entities [or: entities operating in sectors of high criticality]*.*

2. Presidency Compromise proposals

Art. 6(3) & (4) – *lines 105 & 106* - **Info-sharing between Cross-Border Hubs**

3. To encourage the exchange of relevant and, where appropriate, anonymised information between Cross-border cyber hubs, Cross-border cyber hubs shall ensure a high level of interoperability between themselves.

Cross-Border Cyber Hubs shall conclude cooperation agreements with one another, specifying interoperability and information sharing principles among the Cross-Border Cyber Hubs, ***taking into account relevant international standards and industry best practices.*** *Cross-Border Cyber Hubs shall inform the Commission about the agreements concluded.*

2. Presidency Compromise proposals

Art. 6(1) – *lines 98, 99 & 100* – **Info-sharing within & between Cross-Border Hubs**

Members of a Hosting Consortium shall ensure that their National Cyber Hubs exchange, in accordance with the Consortium Agreement referred to in Article 5(3), relevant and where appropriate, anonymised information, ***such as 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****,* ***among themselves within the Cross-Border Cyber Hub,*** *where such information sharing:*
(a) fosters and enhances the detection of cyber threats and reinforces the capabilities of the CSIRTs network to prevent and respond to incidents or to mitigate their impact;
*(b) enhances the level of cybersecurity.****, in particular through raising awareness…***

belgium24.eu

2. Presidency Compromise proposals

Art. 7(1) – *line 108* - **Info-sharing with Union-level networks**

Early Warning to the **Commission** via EU-CyCLONE: **clarify the applicable principle, and also the interplay with Art. 16(2) of NIS2.**

Where the Cross-Border Cyber Hubs obtain information relating to a potential or ongoing large-scale cybersecurity incident they shall ensure, for the purpose of common situational awareness, that relevant information as well as early warnings are provided to the CSIRTs network, EU-CyCLONe, without undue delay, in view of their respective crisis management roles in accordance with Directive (EU) 2022/2555. ***[EU-CyCLONe shall share with the Commission all these early warnings received from the Cross-border Cyber Hubs.]***

Guiding Question 1: Should the Commission receive all the early warnings? (e.g. for IPCR purposes)

Guiding Question 2: does art. 16(2) of NIS2 guarantee the Commission to receive all early warnings through CyCLONe? (also as observer?)

NOTE: Following the discussion during the meeting, compromise will be sought in a clarifying recital underlining the functioning of existing crisis management structures.

belgium24.eu

2. Presidency Compromise proposals

Art. 11(2) – *line 125* – **Coordinated preparedness testing of entities**

The NIS Cooperation Group in cooperation with the Commission, the High Representative and ENISA, and, within the remit of its mandate, EU-CyCLONe, shall develop common risk scenarios and methodologies for the coordinated testing exercises under Article 10(1), point (a) (i) of this Regulation and, where appropriate, for other preparedness actions under Article 10(1)(a)(ii).

[Entities subject to coordinated preparedness testing shall develop and implement a remediation plan that carries out the recommendations resulting from preparedness tests.]

NOTE: Following the discussion during the meeting, compromise will be sought rather in a clarifying recital.

2. Presidency Compromise proposals

Assessing the activation of the Reserve

Art. 13(3) – *line 140*

Art. 14(1a) – *line. 149a*

Art. 14(2a) – *line 155b*

Guiding question. To whom should users send their requests:

(1) to ENISA first, who shares immediately everything with Commission? (for collaboration on prioritisation? -> if so, what about l.149a?

or

(2) to both at the same time?

2. Presidency Compromise proposals

Art. 14(2), point (ea) – *line 155a* - **Prioritisation for Member State users**

New 14(2) second subparagraph in stead of point (ea):

In case there is an equal assessment on the basis of the aforementioned criteria, the category of user under Article 12(3) of this Regulation **will also be taken into account,** with higher priority given to Member State users, then to Union institutions, bodies and agencies and finally to DEP-associated third countries.

Addition to recital 33: **When there is a need to prioritise requests in the case of multiple concurrent requests and an assessment of the relevant criteria indicates an equal importance or urgency, the category of the requesting user will be taken into account with higher priority given to Member State users, then to Union institutions, bodies and agencies and finally to DEP-associated third countries.**

belgium24.eu

3. Topics for the trilogue

- Budget: exchange of views
- Procurement from third country providers (art.16/19)
- External use of the reserve (art.17)
- Information sharing (art.6)
- Prioritization (art.14)
- Delegated acts / implementing acts

Preparation trilogue foreseen on Coreper 9/2

PUBLIC

FOLLOW US ON OUR SOCIAL MEDIA

@belgiumineu

@EU2024BE

Permanent Representation of Belgium to the EU

@EU2024BE

@EU2024BE

@EU2024BE

www.belgium24.eu

belgium24.eu

be EU

belgium24.eu