Council of the European Union

Brussels, 26 September 2024
(OR. en)

13008/1/24
REV 1

LIMITE

CYBER 247
TELECOM 264
COSI 145
COPEN 388
CSDP/PSDC 635
DATAPROTECT 273
RECH 393
HYBRID 120
IPCR 57
JAI 1312
RELEX 1084
POLMIL 314

NOTE

From:	Presidency
To:	Delegations
Subject:	Draft Council conclusions on ENISA

Delegations will find in the annex the revised version of the draft Council conclusions on ENISA - which will be submitted for discussion to the Horizontal Working Party on Cyber Issues. New additions are indicated in **bold** and underlined, deletions are in ~~strikethrough~~.

ANNEX

Draft Council conclusions on ENISA

THE COUNCIL OF THE EUROPEAN UNION,

1. HIGHLIGHTS that challenges deriving from global cyberspace have never been as complex, **diverse and increasingly serious** ~~and numerous as they are now~~, owing to the sophistication of emerging cyber threats, the constantly changing ~~cyber~~ **security** environment and the current geopolitical tensions. Therefore, the EU and its Member States should continue with their efforts to become more resilient with a view to effectively **identifying and addressing current and emerging threats and** ~~addressing those~~ challenges. EMPHASISES that the work towards an increased level of cyber resilience should be continued following a whole-of-society approach. ENCOURAGES the EU to continue to promote our common values and joint efforts within global forums in order to safeguard a free, global, open and secure cyberspace. **STRESSES** ~~RECALLS~~ that, in the years ahead, the EU and its Member States should focus on the effective implementation of legislative and non-legislative initiatives underpinning and contributing to all actions that have been taken so far in this respect.

2. **RECALLING that national security remains the sole responsibility of each Member State,** ACKNOWLEDGES that the EU and its Member States have worked together tremendously in recent years on establishing the necessary institutional setup and forms of collaboration at both national and EU level. WELCOMES the various legislative and non-legislative initiatives that have provided the EU and its Member States with a strong and robust framework. This framework has evolved to cover several aspects of the cyber domain: security, diplomacy, law enforcement and defence. NOTES that a large number of actors, including **Member States' cybersecurity authorities, the NIS Cooperation Group (NIS CG), the CSIRTs Network, the European cyber crisis liaison organisation network (EU-CyCLONe), the National Coordination Centres (NCC) Network and the European Cybersecurity Certification Group (ECCG),** the Commission, the European External Action Service **(EEAS)**, the European Union Agency for Cybersecurity (ENISA), the European Cybersecurity Competence Centre (ECCC), **CERT-EU,** the European Defence Agency (EDA),**and** Europol's European Cybercrime Centre (EC3) ~~CERT-EU, the NIS Cooperation Group (NIS CG), the CSIRTs Network, the European cyber crisis liaison organisation network (EU-CyCLONe)~~ are **part of the EU cybersecurity ecosystem, each performing their part** ~~involved~~ in **the implementation of the** ~~this~~ EU-wide framework. ~~in performing their respective tasks.~~

2a. RECOGNISES that over the past two decades ENISA has proven to be an invaluable entity in the European cybersecurity ecosystem, playing a crucial role in actively supporting Member States and EU institutions, bodies, offices and agencies (EUIBAs) **in their implementation and development of cybersecurity policies, in their capacity-building and preparedness, in their mutual efficient cooperation and in their promotion of cybersecurity awareness and certification**.

GENERAL POLICY RECOMMENDATIONS

3. INVITES the Commission to use **the evaluation of the Cybersecurity Act** as an opportunity to examine how it can contribute to the simplification of the complex cyber landscape, thus enhancing the effectiveness and efficient use of resources. Therefore, CALLS ON the Commission to ensure that ENISA's mandate **to support Member States and EU institutions, bodies, offices and agencies (EUIBAs)** is **focused and** clearly defined, with **concrete strategic objectives and prioritised tasks**, **in addition to** a more precise division of tasks and competences with respect to other actors, including the ECCC. In this respect, INVITES the Commission to examine and further strengthen ENISA's ~~operational~~ role in supporting **operational cooperation at** the EU **level** and **among** Member States in enhancing cyber resilience, **taking into account Member States' competences in this field**. In addition, CALLS ON the Commission to strengthen ENISA's advisory role, including as regards **implementation of current and** future EU **legislative and non legislative** initiatives, by providing expert guidance and recommendations, **while ensuring coherence in cybersecurity framework**.

3a. In the same spirit, ENCOURAGES the Commission to consider streamlining ENISA's role in respect of tasks that are not at the core of its mission~~, for example skills~~. UNDERLINES that ENISA's **responsibilities have been significantly broadened** by recent legislative initiatives, including NIS 2 and the forthcoming Cyber Resilience Act and Cyber Solidarity Act, among others. **While NOTING that some of these initiatives provided for additional human resources,** HIGHLIGHTS that the broadening of ENISA's responsibilities **and the growing complexity of the cyber threats and challenges have** ~~has~~ led to a considerable increase in its tasks, which should be accompanied by **adequate resources** – ~~both~~ human, **financial** and technical – in order to fully enable the Agency to execute all the tasks under its competence, without pre-empting the negotiation of the Multiannual Financial Framework. To this end, CALLS ON the Commission to prioritise between actions **and assign priority to tasks related to supporting Member States and their operational cooperation, the development and implementation of Union Law** when preparing the draft general budget of the Union to enable the Agency to execute all its tasks effectively, thereby contributing to the overall level of cyber resilience of the EU and its Member States.

ENISA'S SUPPORT TO MEMBER STATES TO ENHANCE CYBER RESILIENCE AND OPERATIONAL COOPERATION

4. (old 9+10) ~~ACKNOWLEDGES~~ **STRESSES** that ENISA fulfils an important role **as secretariat of the two EU-level Member States driven cyber cooperation networks, the CSIRTs Network and EU-CyCLONe. EMPHASISES ENISA's valuable participation in the NIS CG, notably through its active involvement and technical contributions in the various work streams.** ENCOURAGES ENISA to continue to support the functioning and cooperation of these networks in the future, since they provide ~~important~~ **fundamental** channels for Member States to collaborate at different levels.

5. (old 12) REITERATES the need to enhance ~~shared~~ **common situational awareness** at EU level, which contributes to the EU's cyber posture, in connection with the detection of, prevention for, and response to cybersecurity incidents. **In this regard,** STRESSES the importance of **ENISA's** foresight activities**, regular reports and threat assessments, which, together with established international cooperation, contribute to improving situational awareness.** ~~performed by ENISA that assist with developing a common understanding of emerging and future cybersecurity challenges and opportunities~~ **HIGHLIGHTS that the Commission' Cyber Situation and Analysis Centre serves an internal function within the Commission and is supported by its collaboration with ENISA and CERT-EU. In order to create maximum potential for synergies and to reduce complexity within the EU cyber ecosystem**, INVITES the Commission **to take the results of** ~~use~~ the evaluation of the Cyber Security Act **into account in order to streamline the tasks of the Commission's Cyber Situation and Analysis Centre and ENISA's related tasks, whilst ensuring no duplication, at the same time, safeguarding ENISA's central role, with due respect to Member States national competences.**

~~CERT-EU and ENISA to continue enhancing their cooperation within the Commission's Cyber Situation and Analysis Centre~~.

6. (old 20) **STRESSES that developing** ~~shared~~ **common situational awareness is an essential starting point for successful crisis management.** UNDERLINES that, at EU level, a variety of key actors are involved in **responding to large-scale cybersecurity incidents**, and that, in the event of such incidents, the effective cooperation among Member States is mainly underpinned by the CSIRTs Network and EU-CyCLONe. ~~RECALLS that as the secretariat of these networks,~~ ENISA **plays an important role in cyber-** ~~contributes importantly to~~ crisis management **as the secretariat to the CSIRTs Network and EU-CyCLONe**. ~~STRESSES that developing shared situational awareness – to which ENISA meaningfully contributes through its activities – is an essential starting point for successful crisis management. In this regard, the frequently published reports and threat assessments compiled by ENISA, in addition to established international cooperation, are useful input for improving EU-level situational awareness.~~ **INVITES the Commission to use the revision of the Cyber Security Blueprint to properly reflect the additional tasks and responsibilities attributed to ENISA by the recent cybersecurity legislation.**

7. (old 24) UNDERLINES ~~that~~ **the importance of** ~~by~~ organising regular **cybersecurity exercises** – which greatly increase the EU's preparedness in responding to incidents and crises. **ACKNOWLEDGES that** ENISA has gathered valuable and extensive experience in this field **supporting Member States**. ACKNOWLEDGES ENISA's important role in the planning, preparation, execution and evaluation phases of cybersecurity exercises, and EMPHASISES that it should continue to remain one of the central actors at EU level, keeping in mind that such exercises should be carried out based on structured frameworks and common terminologies. **INVITES ENISA, the CSIRTs Network and EU-CyCLONe to make most efficient use of existing regular exercises to test and improve the EU-crisis response framework, and to assure maximum uptake of the lessons learned.**

ENISA'S SUPPORT TO POLICY DEVELOPMENT AND IMPLEMENTATION

8. (old 25) RECALLS that under the current cybersecurity legal framework, ENISA is **entrusted** ~~charged~~ with several key supportive and advisory responsibilities across the EU. WELCOMES ENISA's role in that respect in providing **assistance to Member States** on the effective implementation of legislative and non-legislative initiatives. CALLS ON ENISA, in cooperation with the Commission, to continue to provide general insights and analysis on the current legal environment as regards cybersecurity~~, and in particular to develop more sector-specific guidelines, focusing on new sectors covered under the NIS 2 Directive~~. ENCOURAGES ENISA to share technical guidance and best practices in a regular and structured manner assisting the Member States in implementing cybersecurity policy and legislations. ~~In addition, INVITES ENISA to support the creation of a platform for sharing non-binding materials~~.

9. (old 16) In general, recent cybersecurity legislation will likely lead to a **complex reporting framework**, which could cause additional administrative burden, both for the entities obliged to make these reports and for their recipients. Therefore, CALLS ON ENISA in cooperation with the Commission to continue to exchange with Member States on the practicalities, ~~and~~ simplification **and streamlining** of the reporting procedure~~, ensuring an appropriate division of tasks~~. Further, RECALLS its invitation for the Commission to prepare, with the support of ENISA and other relevant EU entities, a mapping of relevant reporting obligations set out in the respective EU legislative acts in cyber and digital matters in order to identify opportunities to reduce the administrative burden. INVITES the Commission to consider ~~in this context~~ the potential of multipurpose reporting platforms **designed** ~~in order~~ to facilitate the compliance of **multiple** entities with ~~multiple~~ **various** reporting obligations.

10. (old 15) HIGHLIGHTS the fact that ENISA is responsible for establishing **the single reporting platform under the upcoming Cyber Resilience Act**, greatly contributing to the cybersecurity of products with digital elements. Given the broad scope of this horizontal legislation, the single reporting platform should be **an effective** ~~a~~ key tool for **facilitating secure information sharing between national CSIRTs and ENISA** ~~monitoring the cybersecurity of products, facilitating the risk mitigation of the national CSIRTs and thus contributing to overall cyber resilience in the EU, while ensuring the proper functioning of the single market~~. Consequently, URGES ENISA, while allocating sufficient human resources, to speed up the establishment of the platform in order to ensure its readiness by the deadline set in the Cyber Resilience Act.

11. (old 13) UNDERLINES that **monitoring trends regarding emerging technologies** in a fast-evolving domain such as cyber is of key importance for maintaining and further strengthening our cyber posture. RECOGNISES the work done by ENISA to draw the public's attention to the risks and possibilities of technologies such as artificial intelligence and quantum computing, thus facilitating a better understanding of the current challenges. **ENCOURAGES ENISA to continue this work and to actively advocate the implementation of its recommendations and to collaborate, where relevant, with the ECCC.**

12. (old 18) ACKNOWLEDGES ENISA's vital role in the development of **European cybersecurity certification schemes**, underpinning trust in ICT products, services and processes. Nevertheless, the lengthy process of elaboration and adoption of cybersecurity certification schemes concerns Member States and industry; therefore, URGES the Commission to find ways to have a leaner**, more transparent** and faster approach to the development of EU cybersecurity certification schemes **while STRESSING the important role of Member States in the process.** ~~which safeguards a strong European dimension in its implementation~~. **Furthermore, CALLS ON ENISA to consult all relevant stakeholders in a timely manner by means of a formal, open, transparent and inclusive process when preparing candidate schemes**.

13. (old 14) ACKNOWLEDGES ENISA's role in establishing a **European vulnerability database**, which aims to provide improved transparency regarding the disclosure of vulnerabilities, ~~thus enhancing European technological sovereignty~~ **while emphasising the appropriate handling of sensitive data**. Considering the end of the transposition period of the NIS 2 Directive, URGES ENISA to step up all the necessary work ~~related to the establishment of the appropriate information systems, policies and procedures, and the adoption of the necessary technical and organisational measures~~ to ensure the smooth functionality of this database. **URGES the Commission to provide sufficient resources to ENISA for establishing and operating such database.** In parallel, INVITES **the NIS CG with the assistance of** ENISA, ~~with the assistance of the NIS CG~~, to further publicise policies and procedures on vulnerability disclosure.

14. (old 17) RECOGNISES the benefits of the **Cybersecurity Support Action** carried out by ENISA, which functions as a pool of cybersecurity services available for Member States to complement their endeavours, **as well as ENISA's experience gained from its implementation**. ~~REITERATES that ENISA has gained extensive experience throughout the implementation of the Cybersecurity Support Action on how to facilitate close cooperation between Member States and the private sector, which could serve as a source of expertise for the operation and administration of the EU **Cybersecurity Reserve** to be established under the forthcoming Cyber Solidarity Act. Regarding the forthcoming establishment of the EU Cybersecurity Reserve,~~ ~~STRESSES that~~ **INVITES** ENISA ~~should~~ **to** commence the mapping of the services needed **and their availability** immediately upon the entry into force of the Cyber Solidarity Act, in order to make the Reserve as useful and tailored to users' needs as possible **in all Member States**.

ENISA'S COOPERATION WITH OTHER ACTORS IN THE EU CYBER ECOSYSTEM

15. (old 4) REITERATES that, owing to the horizontal nature of cybersecurity, **collaboration among** ~~different communities~~ **all actors at Member States' and Union level** is vital, and therefore UNDERSCORES that increasing overall cyber resilience at European level also requires joint work between ENISA and the relevant entities in the cyber field~~, such as CERT-EU, the ECCC, the EC3 and the EDA~~.

16. (old 5) UNDERLINES that EUIBAs' ability to remain cyber-secure is of importance for overall EU-level cyber resilience, in which CERT-EU's role is invaluable. In this regard, WELCOMES the established structured cooperation between CERT-EU and ENISAand ENCOURAGES them to continue their close cooperation in the future~~, with special regard to the effective implementation of the Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union~~.

17. (old 6) [~~Once it has~~ **With the** achieved financial autonomy, the ECCC will contribute significantly to the development of a strong European cyber research, industrial and technological ecosystem, **encompassing skills for workforce development in line with its mandate**. ENCOURAGES ENISA to cooperate closely with the ECCC, especially in relation to research and innovation needs and priorities **as well as** cyber skills ~~and~~ **to increase the competitiveness of the Union's cybersecurity industry** ~~EU-level competitions~~. INVITES the Commission to examine how synergies in the workings of ENISA and the ECCC can be further optimised **and how to better streamline activities related to cyber skills to avoid any potential duplication of tasks, while increasing the effectiveness of ongoing and future efforts,** ~~thus contributing to stronger cybersecurity capabilities and preparedness of Member States and European businesses.~~

18. (old 7) ~~RECALLS that the ongoing activities of cyber criminals continue to pose substantial risks to the functioning of the single market.~~ UNDERLINES that providing regular updates on the threat landscape contributes to better identifying what measures and tools are needed in order to effectively fight cybercrime. ~~As a consequence,~~ ~~STRESSES~~ **HIGHLIGHTS** the ~~importance~~ **added value** of the EU-Joint Cyber Assessment (J-CAR) reports, which are the outcome of the joint collaboration between ENISA, the EC3 and CERT-EU, and have already provided valuable input in addressing the different challenges ~~regarding~~ **including** the fight against cybercrime. ~~With a view to further boosting cooperation with the law-enforcement community~~, INVITES ENISA and the EC3 to **continue** collaborate**ing** in a ~~more~~ structured ~~way~~ **manner** in the future.

19. (old 8) STRESSES that cyber defence constitutes an important **and constantly developing** part of tackling threats arising from cyberspace. HIGHLIGHTS the need for ENISA to engage with the **EEAS** ~~European External Action Service~~ and the ~~European~~ Commission, in those cases where ENISA has a role in supporting the implementation of the **EU Policy on** Cyber Defence~~Policy~~, in close cooperation with the EDA, the ECCC and the cyber defence community. **UNDERLINES the importance of deepening and streamlining civil-military cooperation in the field of cyber within the EU and between the EU and NATO.**

20. (old 11) **ENCOURAGES the EU to continue to promote our common values and joint efforts within global forums in order to safeguard a free, global, open and secure cyberspace**. STRESSES that the cross-border nature of cyber threats and incidents requires strong and effective collaboration, not only at EU level, but also **with international organisations and partners.** ACKNOWLEDGES that ENISA has intensified ~~its actions in this respect and, as a result, the Agency's role has become more prominent, leading it to~~ **its international engagement** becoming recognised as a valuable partner on the global stage. NOTING ~~however~~ that ENISA's international involvement should focus on the most strategic partners and EU candidate countries, in line with **the** EU's ~~security policy priorities~~ **Common Foreign and Security Policy** ~~UNDERLINES the importance of actions taken by ENISA to strengthen its international cooperation., such as the Working Arrangements with the United States Cybersecurity and Infrastructure Security Agency (CISA), as well as the Ukrainian National Cybersecurity Coordination Centre (NCCC) and the Administration of the State Service of Special Communications and Information Protection of Ukraine (SSSCIP).~~

21. (old 21) REITERATES that ~~in recent years~~ the **EU** ~~European Union~~ and its Member States have frequently highlighted gaps in **cybersecurity skills**, ~~and have also provided recommendations and guidance for addressing them~~. STRESSES that the Commission and ENISA have introduced a broad and overarching framework to provide guidance to all stakeholders, such as the European Cybersecurity Skills Framework, the Communication on the Cybersecurity Skills Academy and the annually organised European Cyber Skills Conference.~~(old 22) HIGHLIGHTS that within its mandate, the ECCC supports the development of the EU's technological capacities, capabilities and skills throughout its activities. Therefore, INVITES the Commission to consider how to better streamline activities related to cyber skills carried out by ENISA and the ECCC to avoid any potential duplication of tasks, while increasing the effectiveness of ongoing and future efforts~~.

22. (old 23) ACKNOWLEDGES that ENISA has built the foundations for **cooperation with the private sector** in recent years. RECALLS that the private sector also continuously monitors the cyber threat landscape, thus the information gathered by the industry could help to improve ~~shared~~ **common** situational awareness. Therefore, ENCOURAGES ENISA **in cooperation with the Member States** to bolster cooperation with the private sector on exchanging information in this area **and to continue to work in the context of its Trusted Partnership programme**. ~~contributing to an enhanced shared situational awareness at the EU level~~.

23. (old 19) CALLS ON the Commission and ENISA to consider ways to enhance the collaboration between ENISA and European **standardisation** bodies. STRESSES the need for ENISA to increase its expertise for European cybersecurity standardisation by following up, participating in and influencing standardisation activities, among other things. ENCOURAGES ENISA to further strengthen the collaboration with the data protection community, particularly the European Data Protection Board **and the national competent authorities,** with special regard to fostering synergies in the context of the development of future European cybersecurity certification schemes.

24. (old 26) ~~RECOMMENDS~~ **URGES** the Commission and ENISA to examine how to further optimise the functioning of the EU cybersecurity framework, taking into account the recommendations and proposals made in these conclusions. Continuous cooperation, prioritisation of tasks and resources, as well as simplification of the complex cyber landscape will be key elements to cope with current and future challenges.