



Brussels, 6 December 2024
(OR. en)

16527/24

CYBER 360
TELECOM 369
COSI 231
COPEN 535
CSDP/PSDC 854
DATAPROTECT 347
RECH 534
HYBRID 146
IPCR 72
JAI 1814
RELEX 1549
POLMIL 420

OUTCOME OF PROCEEDINGS

From: General Secretariat of the Council
To: Delegations
Subject: Council conclusions on ENISA

Delegations will find in the annex the Council conclusions on ENISA, as approved by the Council at its meeting held on 6 December 2024.

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 serious as they are now, owing to the sophistication of emerging cyber threats, the constantly changing 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 challenges. EMPHASISES that the work towards an increased level of cyber resilience should be continued following a whole-of-society approach. STRESSES 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 in the cyber domain. WELCOMES the various legislative and non-legislative initiatives that have provided the EU and its Member States with a strong and robust framework in this area, increasing the overall cyber resilience of the Union. 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 Network of National Coordination Centres (NCC) 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) are part of the EU cybersecurity ecosystem, each performing their part in the implementation of the EU-wide cybersecurity framework.
3. 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 cooperation and in their promotion of cybersecurity awareness and certification.

GENERAL POLICY RECOMMENDATIONS

4. 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 ecosystem, 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. In this respect, INVITES the Commission to examine and further strengthen ENISA's 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 reinforce ENISA's advisory role in providing expert and evidence-based guidance and recommendations, with regard to the implementation of current and future EU legislative and non-legislative initiatives, while ensuring a coherent EU cybersecurity framework.

5. 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. UNDERLINES that ENISA's **responsibilities have been significantly broadened** by recent legislative initiatives, including NIS 2, the Cyber Resilience Act and the Cyber Solidarity Act, among others. While NOTING that ENISA received additional resources as a result of some of these initiatives, HIGHLIGHTS that the broadening of ENISA's responsibilities and the growing complexity of the cyber threats and challenges have led to a considerable increase in its tasks, which should be reflected in **adequate resources** – 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 actions and assign priority to tasks related to supporting Member States in enhancing their cyber resilience, their operational cooperation and the development and implementation of Union Law when preparing the draft general budget of the Union.

ENISA'S SUPPORT TO POLICY DEVELOPMENT AND IMPLEMENTATION

6. RECALLS that under the current cybersecurity legal framework, ENISA is entrusted with several key supporting 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 close cooperation with the NIS CG and the Commission, to continue to provide general insights and analysis on the current legal environment as regards cybersecurity. ENCOURAGES ENISA to share and actively promote technical guidance and best practices in a regular and structured manner assisting the Member States in implementing cybersecurity policy and legislations.

7. ACKNOWLEDGES ENISA's vital role in the development of **European cybersecurity certification schemes**, underpinning trust in ICT products, services and processes and, in addition, the managed security services in light of the forthcoming targeted amendment of the Cybersecurity Act. STRESSES that Member States and industry are concerned by the lengthy process of selection, elaboration and adoption of cybersecurity certification schemes; therefore, URGES the Commission to use the opportunity of the Cyber Security Act evaluation to find ways to have a leaner, risk-based as well as more transparent and faster approach to the development of EU cybersecurity certification schemes while STRESSING the important role of Member States in the process. In addition, HIGHLIGHTS the importance of explicitly attributing responsibility for the maintenance of each certification scheme. Furthermore, RECALLS that ENISA should consult all relevant stakeholders in a timely manner by means of a formal, open, transparent and inclusive process when preparing candidate schemes and that the Commission should consult in an open, transparent and inclusive way when assessing the efficiency and use of adopted schemes. ENCOURAGES ENISA to further strengthen the collaboration with the data protection community, particularly the European Data Protection Board, where relevant, and the national competent authorities, with special regard to fostering synergies in the context of the development of future European cybersecurity certification schemes.

8. To prevent the unnecessary administrative burden that could arise from a complex reporting framework, CALLS ON ENISA in cooperation with the Commission to continue to exchange with Member States on the practicalities, simplification and streamlining of the reporting procedure. 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. RECALLS that information exchange between ENISA and Member States is based on a relationship of trust, where security and confidentiality are guaranteed in accordance with the Cybersecurity Act and relevant rules and protocols and should be limited to which is relevant and proportionate to the purpose of the exchange. EMPHASISES the need for data and information to be treated with due care.
9. HIGHLIGHTS the fact that ENISA is responsible for establishing and maintaining **the single reporting platform under the Cyber Resilience Act** which will have a concrete operational added value, especially for actively exploited vulnerabilities and severe incidents affecting the security of products with digital elements. Given the broad scope of this horizontal legislation, the single reporting platform should be an effective and secure tool for facilitating information sharing between national CSIRTs and ENISA. Consequently, URGES ENISA, as well as allocating sufficient human resources, to speed up the establishment of the platform as a key priority in order to ensure its readiness by the deadline set in the Cyber Resilience Act.

10. ACKNOWLEDGES ENISA's role in establishing a **European vulnerability database**, which aims to provide improved transparency regarding the disclosure of vulnerabilities, while ensuring 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 to ensure the smooth functionality of this database. In parallel, INVITES the NIS CG with the assistance of ENISA, to further publicise guidance, policies and procedures on vulnerability disclosure.
11. 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. In this regard, HIGHLIGHTS that ENISA should have a central role in the administration and operation of the EU Cybersecurity Reserve. INVITES ENISA 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 EU Cybersecurity Reserve as useful and tailored to users' needs as possible in all Member States. INVITES ENISA, once entrusted, to involve Member States, in particular by gathering input on the required criteria and informing about upcoming tenders, early in the process of establishing the EU Cybersecurity Reserve. INVITES ENISA, once entrusted, to ensure that the selection process of trusted managed security services providers is transparent, open, fair, and allows for the participation of providers from all Member States, irrespective of size. Additionally, RECALLS that ENISA is required to issue the interoperability guidelines for the Cross-Border Cyber Hubs without undue delay.

12. 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 contribute further to these tasks, to actively advocate for the implementation of its recommendations, and to advise and collaborate with, where relevant, the ECCC.

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

13. 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 fundamental channels for Member States to collaborate at different levels.
14. REITERATES the need to enhance **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, all of which contribute to improving situational awareness. ENCOURAGES ENISA to work in close co-operation with the Member States, in contributing to the development of EU-level situational awareness. In this context, RECOGNISES the important role of ENISA together with CERT-EU and Europol, in supporting the Council with situational briefings within the context of Cyber Diplomacy Toolbox complementing the situational awareness provided by Single Intelligence Analysis Capacity (SIAC) and STRESSES the need to build a comprehensive threat picture from various sources, including the private sector. ENCOURAGES in this regard the further development of ENISA's cooperation with the EEAS, and in particular with INTCEN in full respect of their respective mandates.

15. HIGHLIGHTS that the Cyber Situation and Analysis Centre of the Commission 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 the evaluation of the Cybersecurity Act as well as the discussions on the evaluation of the Cyber Blueprint into account in order to streamline the tasks of the Cyber Situation and Analysis Centre of the Commission and ENISA's related tasks. ENCOURAGES the Commission to avoid unnecessary duplication of tasks, while safeguarding ENISA's central role in contributing to developing common situational awareness at Union level in support of the Member States, with due respect to their national competences.
16. STRESSES that developing common situational awareness is a prerequisite for timely and effective crisis management of the Union as a whole. 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. ENISA plays an important role in cyber crisis management as the secretariat to the CSIRTs Network and EU-CyCLONe. INVITES the Commission to use the evaluation of the Cyber Blueprint to properly reflect the additional tasks and responsibilities for contributing to developing a cooperative response to large-scale cross-border cyber incidents or crises, as well the role attributed to ENISA as the secretariat of CSIRT Network and EU-CyCLONe and by the recent cybersecurity legislation.

17. UNDERLINES the importance of 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 COOPERATION WITH OTHER ACTORS IN THE CYBER ECOSYSTEM

18. REITERATES that, owing to the horizontal nature of cybersecurity, **collaboration among 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 other relevant entities in the cyber field.
19. 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 ENISA and ENCOURAGES them to continue their close cooperation in the future.

20. 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 and the ECCC to continue their close cooperation, especially in relation to research and innovation needs and priorities, as well as cyber skills, to increase the competitiveness of the Union's cybersecurity industry. INVITES the Commission to examine how synergies in the working of ENISA and the ECCC can be further optimised and how to better streamline activities according to their respective mandates.
21. UNDERLINES that providing regular updates on the threat landscape contributes to better identifying which measures and tools are needed in order to effectively fight cybercrime. HIGHLIGHTS the added value of the EU-Joint Cyber Assessment (J-CAR) reports, which are the outcome of the joint collaboration between ENISA, Europol's EC3 and CERT-EU, and have already provided valuable input in addressing the different challenges including the fight against cybercrime. INVITES ENISA and Europol to continue collaborating in a structured manner in the future.
22. 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 and the Commission, in those cases where ENISA has a role in supporting the implementation of the EU Policy on Cyber Defence, in close cooperation with the EDA, the ECCC and the cyber defence community. EMPHASISES ENISA's role as a civilian agency. UNDERLINES the importance of deepening and streamlining civil-military cooperation in the field of cyber within the EU including clear divisions of roles and responsibilities between the two communities and between the EU and NATO in full respect of the principles of inclusiveness, reciprocity, mutual openness and transparency, as well as the decision-making autonomy of both organisations. ENCOURAGES ENISA to continue to pursue working arrangement with NATO Communications and Information Agency.

23. 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**. NOTES that ENISA's international involvement should focus on strategic partners and EU candidate countries, in line with the EU's Common Foreign and Security Policy. STRESSES that in its international involvement, ENISA should act in accordance with its mandate and the respective provisions of the Cybersecurity Act. ACKNOWLEDGES the necessity of clarifying, in accordance with relevant procedures, ENISA's international involvement, ensuring in particular that its Management Board is duly and timely informed of the related activities. ENCOURAGES ENISA's involvement in relevant international cybersecurity cooperation frameworks, including organisations such as NATO and the OSCE.
24. REITERATES that the EU and its Member States have frequently highlighted gaps in **cybersecurity skills**. RECALLS 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 and ENCOURAGES the Commission and ENISA to build on these initiatives with special regard to the ongoing discussion on the European Digital Infrastructure Consortium (EDIC). To this end, INVITES the Commission to liaise with Member States interested in setting up a EDIC. ACKNOWLEDGES that both ENISA and the ECCC are mandated to promote skills across the Union. INVITES ENISA to prioritise supporting Member States' skills and education efforts, strengthening general public awareness and collaborate with the ECCC where appropriate.

25. ACKNOWLEDGES that ENISA has developed **cooperation with the private sector** in recent years. RECALLS that because the private sector continuously monitors the cyber threat landscape, the information gathered by the industry could help to improve common situational awareness. Therefore, ENCOURAGES ENISA, in close cooperation with the Member States and across EU entities to bolster cooperation with the private sector.
26. 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 and participating in standardisation activities, among other things.
27. 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.
-