EUROPEAN COURT OF AUDITORS

EN

Opinion 02/2023

(pursuant to Article 322(1), TFEU)

concerning 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 [Interinstitutional File 2023/0109(COD) of 18 April 2023]

Contents

Introduction

01 On 18 April 2023, the Commission published a 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 "EU Cyber Solidarity Act").

02 The proposed EU Cyber Solidarity Act lays down measures to detect, prepare for and respond to cybersecurity threats and incidents, in particular through:

- the **European Cyber Shield** to build and enhance coordinated detection and situational awareness capabilities;
- the **Cyber Emergency Mechanism** to support member states in preparing for, responding to, and recovering from significant and large-scale cybersecurity incidents;
- the **Cybersecurity Incident Review Mechanism** to review and assess significant or large-scale incidents.

03 The legal basis of the Commission's proposal means that consultation with the European Court of Auditors is mandatory[1]. The European Parliament and the Council of the European Union wrote to us on 2 and 7 June 2023 respectively, asking for our views. This opinion fulfils the consultation requirement.

[1] Article 322(1) of the Treaty on the Functioning of the European Union.

General observations

04 Member states bear primary responsibility for preventing, preparing for, and responding to cybersecurity incidents and crises affecting them. In accordance with Article 4(2) of the Treaty on European Union, national security remains the sole responsibility of each member state. However, the potential impact of significant or large-scale cybersecurity incidents means that common action at EU level may be necessary.

05 The ECA welcomes the proposal's objectives to strengthen the EU's collective cyber resilience. In this opinion, we provide specific comments on the three components of the proposed EU Cyber Solidarity Act and highlight some risks that we have identified in relation to the lack of impact assessment, the financial aspects, and how the measures laid down in the proposal might be implemented. In particular, we highlight that the proposed Regulation risks making the whole EU cybersecurity galaxy more complex and suggest ways to mitigate this risk (see paragraphs ***13***-***20***).

Specific comments

Lack of an impact assessment

06 The Commission's better regulation guidelines suggest using impact assessments and stakeholder consultations as part of a comprehensive analysis of policy design and implementation options. We consider comprehensive impact assessments as an essential tool to consider whether EU action is needed and analyse the potential impacts of available solutions before any proposal is adopted.

07 This proposed Regulation was not subject to an impact assessment. In section 3 of the accompanying explanatory memorandum, the Commission explained that it had opted not to carry out such an assessment due to the "*urgent nature of the proposal*". It also said that the measures introduced by the proposed Regulation would be supported by the Digital Europe Programme (DEP), and were in line with the DEP Regulation, which had undergone a specific impact assessment in 2018. Additionally, the Commission explained that the proposed measures were built upon previous actions prepared in close coordination with the main stakeholders and member states, integrating lessons learned.

08 However, we note that the DEP impact assessment does not cover the new measures introduced by the proposed Regulation. There is thus limited information on available policy options and the costs related to the proposal.

Partial information on funding

Partial information on funding and human resource needs

09 Funding for the measures laid down in the EU Cyber Solidarity Act will come from the DEP. The Commission stated in section 4 of its explanatory memorandum that €115 million had already been allocated to the European Cyber Shield in the form of pilots during 2021-2022. It also stated that the proposal would increase the budget of €743 million allocated in 2023-2027 to the DEP's specific objective of cybersecurity and trust by €100 million, through an internal reallocation of funding.

10 After this reallocation, the EU funding available for cybersecurity will be €843 million for 2023-2027. We note that this amount covers not only actions laid

down in the proposed Regulation, but also other cybersecurity actions in the DEP (such as support for industry or for standardisation). The proposal does not provide an estimate of the total expected costs related to establishing and implementing the proposed measures (the European Cyber Shield, the Cyber Emergency Mechanism (including the EU Cybersecurity Reserve), and the Cybersecurity Incident Review Mechanism). As the proposal is not accompanied by an impact assessment, we suggest that the Commission makes these cost estimates available to enhance transparency.

Partial information on the financial set-up of the European Cyber Shield

11 Chapter II of the proposed Regulation establishes the "European Cyber Shield" composed of national security operations centres (SOCs) and cross-border security operations centres (cross-border SOCs). The proposed Regulation provides that eligible national SOCs may receive an EU financial contribution covering up to 50 % of the acquisition costs of their tools and infrastructures, and up to 50 % of their operating costs. For cross-border SOCs, the EU co-financing is to cover up to 75 % of the acquisition costs of tools and infrastructures, and up to 50 % of the operating costs. The proposed Regulation does not specify why additional tools and infrastructures, supported at a higher co-financing rate, are needed in cross-border SOCs compared to the tools available to national SOCs in a consortium.

12 The proposed Regulation also does not specify how long national and cross-border SOCs' operating costs will be co-financed by the EU. This creates a risk that the operation of the European Cyber Shield and its sustainability become dependent on EU financing.

Risks linked to the European Cyber Shield

Increased complexity and additional layers

13 We noted in our review 02/2019[2] that the EU cybersecurity landscape is complex and multi-layered. It involves numerous private and public actors at regional, national, and EU level in the civilian sphere, including law enforcement entities and financial intelligence units. Cybersecurity is also a key element of national security and defence. We present a map of the new cybersecurity galaxy in the EU in the ***Annex*** to this opinion, which includes, in a shaded box, all the mechanisms and components

[2] Review 02/2019: "Challenges to effective EU cybersecurity policy".

introduced by the proposal. It illustrates the additional complexity and layers introduced by the Regulation.

14 The aim of the European Cyber Shield established in Chapter II of the proposed Regulation is to develop advanced EU capabilities to detect, analyse and process data on cyber threats and incidents. It will be an interconnected, pan-European infrastructure of national security operations centres and cross-border security operations centres.

15 In order to participate in the European Cyber Shield, member state shall designate at least one national SOC, which must be a public body. In turn, national SOCs should create cross-border SOCs, which will be consortia made up of SOCs from at least three member states committed to work together and coordinate their cybersecurity incident detection and cyber threat monitoring activities.

16 In recent years, the EU has reinforced its cybersecurity regulatory framework. One of its key instruments is the 2016 Network and Information Security Directive (the "NIS Directive") and the 2022 revision (the "NIS 2 Directive"). Under the NIS 2 Directive, member states should establish at national level one or more computer security incident response teams (CSIRTs). At EU level, the NIS 2 Directive also establishes the NIS cooperation group, the CSIRTs network, and the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe).

17 In 2021, the EU established the European Cybersecurity Competence Centre. This centre, inaugurated in May 2023, will be supported by a network of 27 National Coordination Centres, one for each member state, some of which are also national SOCs. The Centre will be responsible for implementing the cybersecurity component of the DEP, except for the EU Cybersecurity Reserve. This will be implemented by the Commission, but ENISA may be given responsibility for its operation and administration.

18 The Commission has also launched a Joint Cyber Unit. This unit was announced in 2020 in the EU Cybersecurity Strategy and further defined in a 2021 Commission recommendation.

19 In April 2023, the Commission announced the launch of the Cybersecurity Skills Academy, a new initiative aimed at closing the cybersecurity talent gap and boosting the "EU cyber workforce".

20 Against this background, we consider that the proposed Regulation risks making the whole EU cybersecurity galaxy more complex. There is a potential for overlap between the existing CSIRTs network and the SOCs. While the Commission stated in section 1 of its explanatory memorandum that the cross-border SOCs platforms should constitute a new capability that was complementary to the CSIRTs network, we note that some of the tasks and objectives of national SOCs, cross-border SOCs, CSIRTs, and the CSIRTs network are similar. These include threat detection and response, cyber threat intelligence and situational awareness. In principle, this risk could be mitigated by a progressive consolidation of the structures involved, in particular the national SOCs and CSIRTs, and the cross-border SOCs. Moreover, the proposal should clarify how these structures should interact by laying down clear governance arrangements and responsibilities in order to ensure effective coordination and achieve synergies.

Information sharing

21 In our special report 05/2022[3], we found that EU institutions, bodies and agencies did not systematically share key relevant cybersecurity information with each other, even when they were required to do so. Effective information sharing was further undermined by interoperability issues hindering secure communication. While our finding related to that comparatively small and homogeneous group of EU actors, we consider that this challenge will be increasingly relevant in the more complex and diverse cybersecurity galaxy at member state level.

22 Article 4 of the proposed Regulation states that national SOCs should act as a "reference point and gateway" for other public and private organisations at national level for collecting and analysing information on cybersecurity threats and incidents. However, there are currently no reporting requirements at EU level for public and private organisations (including national CSIRTs, private SOCs, and what are termed "essential and important entities" under the NIS 2 Directive) towards national SOCs. There is therefore a risk that national SOCs do not receive adequate data or information for their needs.

23 In section 2.2.2 of the legislative financial statement accompanying the proposal, the Commission identifies the risk that member states might not share a "sufficient amount" of relevant cyber threat information, either within the cross-border SOC platforms, or between cross-border platforms and other relevant entities at EU level.

---

[3] Special report 05/2022: "Cybersecurity of EU institutions, bodies and agencies - Level of preparedness overall not commensurate with the threats".

Such a lack of information sharing could undermine the effectiveness and added value of the European Cyber Shield.

24 We therefore welcome the fact that the proposal contains specific provisions in Articles 4, 5, and 6 to mitigate the risks linked to the lack of information sharing. The proposal provides that EU funding will be available to national SOCs only if they commit to participate in a cross-border SOC. We note, however, that there is no reimbursement of the financial support received during the first two years if the national SOC does not join a cross-border SOC. The proposed Regulation also requires members of cross-border SOCs to commit to share a "significant amount of data" with each other and set up a governance framework in a written consortium agreement.

25 In addition, the proposal states in Article 7 that the cross-border SOCs must provide relevant information relating to a potential or ongoing large-scale cybersecurity incident to EU-CyCLONe, the CSIRTs network and the Commission "without undue delay". We stress the importance of ensuring adequate enforcement of this provision.

26 The proposed Regulation provides in Article 6 that the Commission may, by means of implementing acts, specify the conditions for interoperability between cross-border SOCs. Article 8 provides that the Commission may also adopt implementing acts laying down technical requirements for member states to ensure there is a high level of data and physical security of the infrastructure. These conditions and requirements should be agreed upon swiftly to avoid incompatible systems being developed alongside each other, and to reduce costs.

Risks linked to the Cyber Emergency Mechanism

Deployment of the EU Cybersecurity Reserve

27 We noted in our special report 05/2022 that CERT-EU, the EU's own computer emergency response team that provides response support to EU institutions, bodies and agencies, did not operate on a 24/7 basis at the time of the audit.

28 The proposed Regulation provides in Article 14 that requests for support from the EU Cybersecurity Reserve will be assessed by the Commission, supported by ENISA, and that a response will be sent "without delay". As there may be multiple and concurrent requests requiring prioritisation, the proposed Regulation establishes some decision-making criteria. Article 13 specifies that, the Commission may, by means of

implementing acts, specify further the detailed arrangements for allocating the Reserve.

29 We consider it vitally important that the timelapse between the request to receive support services from the EU Cybersecurity Reserve and the response by the Commission is not delayed by the timing of the request. However, the proposal does not specify a pre-defined deadline and does not request that organisational steps are taken to achieve this deadline.

Derogation from the principle of "annuality"

30 One of the basic principles of the EU budget is its annuality, meaning that appropriations entered in the budget are authorised for a financial year up to 31 December. Unused commitments and payment appropriations are not automatically carried over to the following financial year. This principle is set out in Chapter 2 of the Financial Regulation.

31 In Article 19, the proposed Regulation derogates from this principle for the funding of actions under the Cyber Emergency Mechanism. It lays down that unused commitment and payment appropriations for actions related to preparedness, response, and mutual assistance are to be automatically carried over and may be committed and paid up to 31 December of the following financial year. In section 2 of its explanatory memorandum, the Commission explained that this flexibility in budgetary management was needed because of the "*unpredictable, exceptional and specific nature of the cybersecurity landscape and cyber-threats*".

32 As far as preparedness is concerned, we consider that coordinated preparedness testing of entities should be planned activities and are therefore in general neither unpredictable nor exceptional. In our view, such planned activities do not require a derogation from the basic principle of annuality.

33 However, as the EU Cybersecurity Reserve and mutual assistance will only be used in response to unpredictable events, we consider that the rationale for this derogation can only be justified in this case.

34 For clarity, and in line with the drafting of other regulations such as on the Union Civil Protection Mechanism or the Neighbourhood, Development and International Cooperation Instrument – Global Europe, we also consider that the proposed

Regulation should specify that the automatic carry-over of unused commitments should be limited to the following year.

Risks linked to the Cybersecurity Incident Review Mechanism

35 Article 18 of the proposed Regulation states that, if requested by the Commission, EU-CyCLONe, or the CSIRTs network, ENISA is to review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. After collaborating with all relevant stakeholders, ENISA must deliver an incident review report covering the main causes, vulnerabilities and lessons learned.

36 We consider this to be an important feedback mechanism to continuously reinforce the EU's detection, preparedness and response capabilities in the face of cybersecurity threats and incidents. However, we suggest that the proposed Regulation should specify a maximum deadline for the delivery of ENISA's report after any incident, in order to ensure that feedback is provided in good time. Moreover, the proposal indicates that the report should draw recommendations to improve the Union's cyber posture where appropriate. However, the proposal does not specify how these recommendations should be followed-up.

Performance monitoring and policy evaluation

37 Article 19 of the proposed Regulation amends Annex II to the DEP Regulation by introducing a new measurable indicator, namely "*the number of actions supporting preparedness and response to cybersecurity incidents under the Cyber Emergency Mechanism*". This indicator complements two existing ones intended to monitor and report on progress towards the achievement of DEP's specific objective on cybersecurity and trust, i.e., "*the number of cybersecurity infrastructure[s], or tools, or both, jointly procured*", and "*the number of users and user communities getting access to European cybersecurity facilities*".

38 In our view, the proposed new indicator only measures output and will provide little insight into the use and results of the European Cyber Shield and Cyber Emergency Mechanism.

39 Article 20 of the proposal requires the Commission to submit a report on the evaluation and review of the Regulation to the European Parliament and the Council four years after its date of application.

40 While we consider that the evaluation should be based on sufficient and reliable data, the fast-changing threat landscape requires constant adaptation and innovation on the part of the EU and its member states. We therefore consider that the timing of the evaluation, as currently proposed, may be too late for the new programming period. Furthermore, the entire budgeted amount for the DEP specific objective on cybersecurity and trust will have been committed by the end of 2027.

Concluding remarks

41 4The proposed EU Cyber Solidarity Act lays down measures to detect, prepare for and respond to cybersecurity threats and incidents. The ECA welcomes the proposal's objectives to strengthen the EU's collective cyber resilience.

42 Our opinion highlights some risks that we have identified and how the measures laid down in the proposal might be implemented. In particular, we highlight the risks that the operation of the European Cyber Shield and its sustainability become dependent on EU financing; that its functioning is impeded by a lack of information sharing; and that the measures introduced by the proposal make the whole EU cybersecurity galaxy more complex.

43 As a result of our review of the legislative proposal, we suggest that the **Commission and legislators should consider**:

— making the cost estimates related to establishing and implementing the proposed measures available to enhance transparency (see paragraph ***10***);

— clarifying how national SOCs, cross-border SOCs, CSIRTs, and the CSIRTs network should interact by laying down clear governance arrangements and responsibilities in order to ensure effective coordination and achieve synergies (paragraph ***20***);

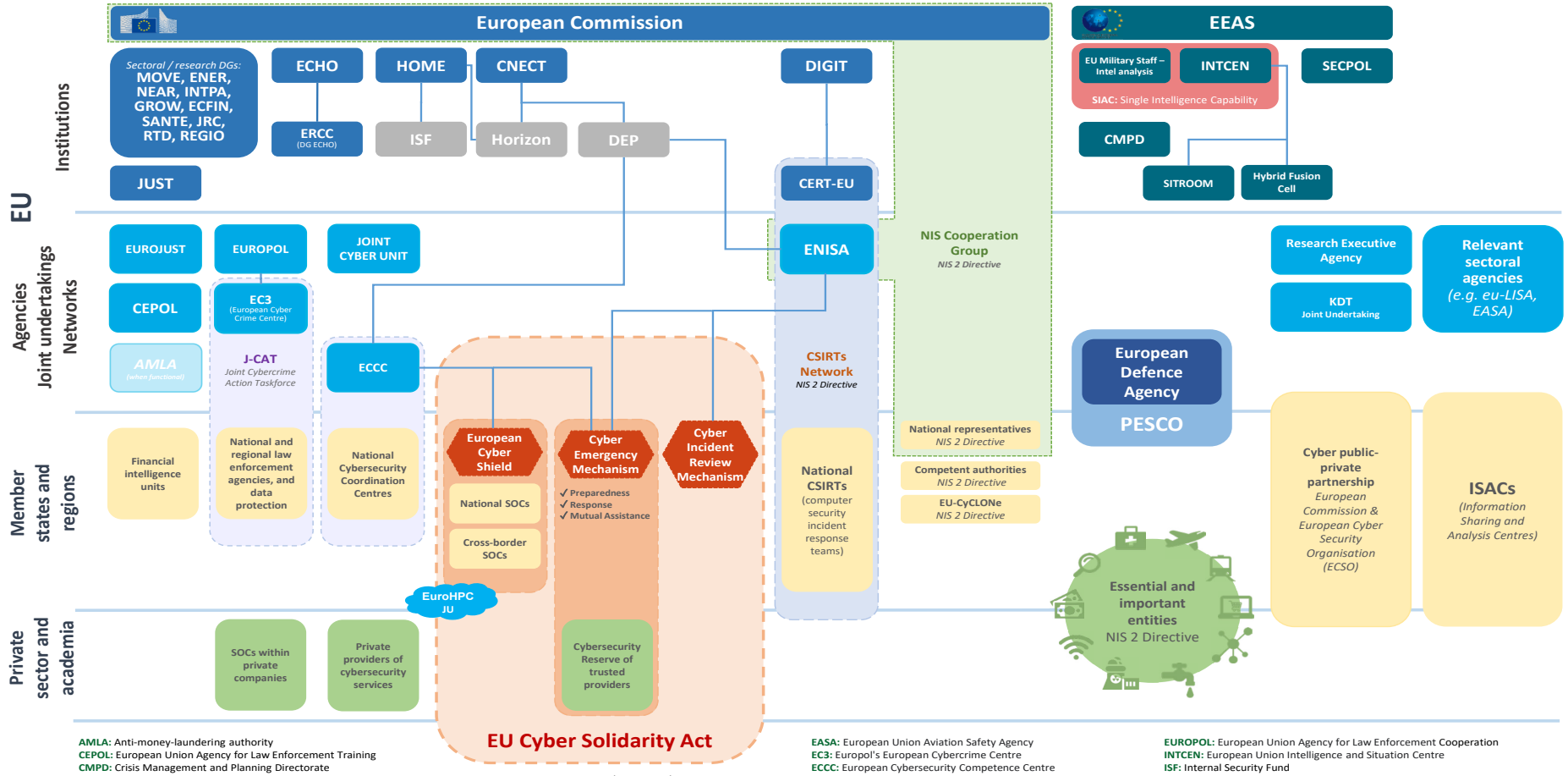
— ensuring that that the timelapse between the request to receive support services from the EU Cybersecurity Reserve and the response by the Commission is not delayed by the timing of the request (paragraph ***29***);

— limiting the derogation to the annuality principle to response actions and mutual assistance and clarifying that the automatic carry-over of unused commitments should be limited to the following year (paragraphs ***32***-***34***);

— specifying a maximum deadline for the delivery of ENISA’s report after any incident, in order to ensure that feedback is provided in good time (paragraph ***36***);

— advancing the timing for submission by the Commission of a report on the evaluation and review of the Regulation (paragraph ***40***).

Annex – The European cybersecurity galaxy



AMLA: Anti-money-laundering authority
CEPOL: European Union Agency for Law Enforcement Training
CMPD: Crisis Management and Planning Directorate
DG CONNECT: Communications Networks, Content and Technology
DG ECFIN: Directorate-General for Economic and Financial Affairs
DG ECHO: DG for European Civil Protection and Humanitarian Aid Operations
DG ENER: Directorate-General for Energy
DG GROW: DG for Internal Market, Industry, Entrepreneurship and SMEs
DG HOME: Directorate-General Migration and Home Affairs
DG INTPA: Directorate-General for International Partnerships
DG JUST: Directorate-General Justice and Consumers
DG MOVE: Directorate-General for Mobility and Transport
DG NEAR: DG for Neighbourhood and Enlargement Negotiations
DG REGIO: Directorate-General for Regional and Urban Policy
DG RTD: Directorate-General for Research and Innovation
DG SANTE: Directorate-General for Health and Food Safety
DIGIT: Directorate-General for Informatics
EASA: European Union Aviation Safety Agency
EC3: Europol's European Cybercrime Centre
ECCC: European Cybersecurity Competence Centre
ECSO: European Cyber Security Organisation
EDA: European Defence Agency
EEAS: European External Action Service
ERCC: Emergency Response Coordination Centre
EU-CyCLONe: European Cyber Crisis Liaison Organisation Network
EuroHPC: European High-Performance Computing
EUROJUST: European Union Agency for Criminal Justice Cooperation
EUROPOL: European Union Agency for Law Enforcement Cooperation
INTCEN: European Union Intelligence and Situation Centre
ISF: Internal Security Fund
JRC: Joint Research Centre
KDT: Key Digital Technologies
NIS Directive: Network and Information Security Directive
PESCO: Permanent Structured Cooperation Framework
SECPOL: Security Policy and Conflict Prevention
SITROOM: Situation Room
SOC: Security operations centre

Source: ECA.

This opinion was adopted by Chamber III headed by Ms Bettina Jakobsen, Member of the Court of Auditors, in Luxembourg at its meeting of 26 September 2023.

For the Court of Auditors

Tony Murphy
President

COPYRIGHT