C/2024/1049

9.2.2024

Opinion of the European Committee of the Regions — EU Cyber Solidarity Act and digital resilience

(C/2024/1049)

Rapporteur: Pehr GRANFALK (SE/EPP), Member of Solna Municipal Council

Reference document: 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

Proposal COM(2023) 209 final

I. RECOMMENDATIONS FOR AMENDMENTS

COM(2023) 209

Amendment 1

Recital 1

Text proposed by the European Commission	CoR amendment
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.	The use of and dependence on information and communication technologies have become fundamental aspects ***but have also exposed vulnerabilities*** 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.

Reason

Self-explanatory.

Amendment 2

Recital 3

Text proposed by the European Commission	CoR amendment
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, 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. […]	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, it is necessary to increase the resilience of citizens, businesses***, public administrations at national, regional and local level,*** and entities operating critical infrastructures against the growing cybersecurity threats, which can have devastating societal and economic impacts. […]

Reason

Local and regional administrations provide citizen-centred services that are critical for society, and are one of the key elements in a vibrant European market.

Amendment 3

Recital 29

Text proposed by the European Commission	CoR amendment
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 […]	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')***, along with public administration entities at local and regional level regardless of whether they are considered highly critical under national law.*** The coordinated testing exercises […]

Reason

As Member States are given the option of excluding local and regional authorities when implementing NIS 2 ([1]), it should be ensured that these authorities are also covered by the Cyber Solidarity Act.

Amendment 4

Recital 30

Text proposed by the European Commission	CoR amendment
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.	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 critical sectors, ***and in public administrations regardless of whether they are considered critical under national law***. Those actions could include various types of national preparedness activities.

([1]) 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).

Reason

Local and regional authorities should be given the opportunity to benefit from support under the Cyber Emergency Mechanism.

Amendment 5

Recital 33

Text proposed by the European Commission	CoR amendment
A Union-level Cybersecurity Reserve should gradually be set up, consisting of services from private providers of managed security services to support response and 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.	A Union-level Cybersecurity Reserve should gradually be set up, consisting of services from private providers of managed security services to support response and 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 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.

Reason

Support from the EU Cybersecurity Reserve should be provided not only to affected entities that are active in critical or highly critical sectors.

Amendment 6

Article 1(2), point (b)

Text proposed by the European Commission	CoR amendment
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');	to reinforce preparedness of entities operating in critical and highly critical sectors ***and in public administrations at national and subnational level*** 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');

Reason

Public authorities at subnational level should also be covered by this Regulation.

Amendment 7

Article 4(1), second paragraph

Text proposed by the European Commission	CoR amendment
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 have the capacity to act as a reference point and gateway to other public and private organisations at national ***and subnational*** level for collecting and analysing information on cybersecurity threats and incidents and contributing to a Cross-border SOC. […]

Reason

National security operations centres (SOCs) should also collect and analyse information from entities at regional and local level.

Amendment 8

Article 5(2)

Text proposed by the European Commission	CoR amendment
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.	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 ***from resources other than those included in Regulation (EU) 2021/1060 (the Common Provisions Regulation)***. 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.

Reason

Actions under the Cyber Solidarity Act should not be financed through cohesion policy programmes.

Amendment 9

Article 9(1)

Text proposed by the European Commission	CoR amendment
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').	A Cyber Emergency Mechanism is established to improve the Union's resilience to 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').

Reason

The Cyber Emergency Mechanism should prepare for and mitigate the short-term effects of all types of cybersecurity incidents.

Amendment 10

Article 10(2), (new)

Text proposed by the European Commission	CoR amendment
	2. The Commission shall draw up an annual report to assess how the Mechanism is working and any need for additional cooperation or training requirements.

Reason

The Commission should provide regular reports as the field of cybersecurity is constantly evolving and requirements need to keep up with the latest developments.

Amendment 11

Article 11(1)

Text proposed by the European Commission	CoR amendment
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.	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***, including local public administrations,*** 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.

Reason

Local and regional authorities should be able to benefit from the Cyber Emergency Mechanism. The amendment incorporates into the articles of the proposed Regulation the request made by the rapporteur in Amendment 3 (concerning Recital 30).

Amendment 12

Article 14(2), point (b)

Text proposed by the European Commission	CoR amendment
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;	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***, including public administration entities at local and regional level***;

Reason

Clarifying that the scope includes subnational entities.

Amendment 13

Article 18(1)

Text proposed by the European Commission	CoR amendment
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.	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 possible, the CSIRTs network shall share the report with public administrations at subnational level.*** Where relevant, the Commission shall share the report with the High Representative.

Reason

Clarifying that the scope includes subnational entities.

II. **POLICY RECOMMENDATIONS**

POSITION OF THE EUROPEAN COMMITTEE OF THE REGIONS

The European Committee of the Regions (CoR) welcomes the Commission's proposal for a Regulation to strengthen European cooperation on cybersecurity. Today, the EU's Member States are highly connected and digitally networked, and this will only increase in the years to come. The Committee therefore welcomes the Commission's initiative to jointly address the cyber threats posed by our increased digitalisation. The proposal addresses the increasing number of cyber incidents — not least in areas for which municipalities and regions are responsible — and the importance of ensuring that critical societal functions prepare for, handle and learn from incidents. In the CoR's view, the Commission's proposals can help to increase digital resilience within the EU.

1. In order to achieve the goal of a digitally resilient Europe, it is essential for politicians and the public alike to recognise the importance of pooling efforts on cybersecurity. The CoR therefore urges the Member States, the Commission and all local authorities to join together to raise awareness of the need for action, including the need to increase investments in digital resilience, particularly on local and regional levels, and to consider developing protective policy instruments targeting financial ransomware attacks. This will require appropriate financial, technical and upskilling efforts.

2. The Committee notes that in many respects the proposal refers to and is based on the NIS 2 Directive. In the national implementation of NIS 2, it is up to each Member State to decide whether local authorities should fall within its scope ([2]). As each Member State can choose whether municipalities are to be defined as essential or important entities when implementing NIS 2, any differences between countries will be reflected in how the countries approach the Cyber Solidarity Act as currently proposed. In order to avoid a situation where local authorities responsible for essential operations in some Member States fall outside the scope of the Cyber Solidarity Act, it should be made clear in the legal text that such authorities are considered to be included whether or not they are covered by NIS 2.

3. Recognising that cybersecurity is a cornerstone of digital interoperability, it is imperative that efforts to enhance interoperability across regions are supported by robust cybersecurity measures, to ensure that cyber threats do not hinder the interoperability of regions across Europe.

4. Municipalities and regions need practical support from the structures that are to be established, not just reporting obligations to them. The Committee therefore calls for greater clarity on how this support will be provided to the regions, not least in order to raise cybersecurity levels in small municipalities.

Positions regarding the proposal's areas of action

The European Cyber Shield

Development of a pan-European infrastructure of Security Operations Centres (SOCs) to build and improve common capabilities to detect, analyse and process data on cyber threats and incidents.

5. In order obtain a comprehensive picture of the current state of cybersecurity in the EU, information, risk scenarios, threats and incidents also need to be aggregated from local and national system providers. In the CoR's view, the lack of clear incentives and processes for municipalities and regions to be active partners in strengthening digital resilience presents a risk. Including the local and regional level is key, as they are often the ones that own the digital solutions that are attacked. It is therefore important to create an environment in which municipalities and regions can, and should, be integrated and active partners in increasing the EU's cybersecurity.

6. The Committee's analyses have revealed considerable variations in countries' degree of maturity regarding protection and the security measures taken. Even within countries, there are significant differences between, for example, national authorities and smaller local authorities in terms of both their capabilities and their ambition in the field of cybersecurity. The Committee therefore considers it important for the Regulation to aim to reduce these differences and to ensure that all players involved have relatively equal abilities and ambitions.

7. The Committee notes that the new network of national and cross-border SOCs is liable to overlap with the tasks assigned to the computer security incident response teams (CSIRTs) network ([3]). Where national SOCs are established alongside CSIRTs, it is important to make it clear how cooperation will work and what the responsibilities of the national SOC and the CSIRT are in the event of an incident.

([2]) Article 2(5) of the NIS 2 Directive: 'Member States may provide for this Directive to apply to: (a) public administration entities at local level'.

([3]) Under Article 11(3) of the NIS 2 Directive, CSIRTs shall have the following tasks:
(a) monitoring and analysing cyber threats, vulnerabilities and incidents at national level and, upon request, providing assistance to essential and important entities concerned regarding real-time or near real-time monitoring of their network and information systems;
(b) providing early warnings, alerts, announcements and dissemination of information to essential and important entities concerned as well as to the competent authorities and other relevant stakeholders on cyber threats, vulnerabilities and incidents, if possible in near real-time;
(c) responding to incidents and providing assistance to the essential and important entities concerned, where applicable;
(d) collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;
(e) providing, upon the request of an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact;
(f) participating in the CSIRTs network and providing mutual assistance in accordance with their capacities and competencies to other members of the CSIRTs network upon their request;
(g) where applicable, acting as a coordinator for the purposes of the coordinated vulnerability disclosure under Article 12(1);
(h) contributing to the deployment of secure information-sharing tools pursuant to Article 10(3).

8. The Committee welcomes the specific objectives of the draft Regulation and the measures proposed therein. It finds it regrettable, however, that despite increasing cyber-attacks, local and regional authorities are not sufficiently covered by the current proposal and therefore proposes a number of legislative changes to address these shortcomings.

9. There is currently a lack of data and clear measurement points for incidents, threats and risks for municipalities and regions. Within the framework of the European Cyber Shield, indicators should be developed to determine how development and maturity are increasing in connection with the introduction of the Regulation. In the long term, the indicators can feed into a data-based risk-map, demonstrating where the greatest need for action is.

Cyber Emergency Mechanism

Aims to strengthen preparedness, to test preparedness in sectors regarded as critical, to improve the ability to recover from incidents, and to set up a cybersecurity reserve.

10. Large-scale incidents can arise from local events, and the proposal needs to demonstrate how both SOCs and the Cybersecurity Reserve can cover serious local disruptions, not just significant and large-scale incidents that have already occurred. Information sharing should not be limited to large-scale incidents, but also include potential risks.

11. Information on cybersecurity incidents is very often highly sensitive in nature and may need to contain technical details, or even personal data, that cannot currently be shared unless the parties have concluded contracts or agreements. Today, there are difficulties in sharing information at national level, so the question of how to transfer it across national borders is very complex. For the Cyber Emergency Mechanism to work, the Commission needs to ensure that all parties involved — public and private actors within the EU Cybersecurity Reserve — have the legal and technical conditions to share and receive information. In the Committee's view, the main need for information dissemination relates to incident resolution — i.e. how the entities under attack can in practice best deal with a major incident.

12. The CoR welcomes the fact that strict requirements will be imposed on private-sector service providers that will be involved in the proposed Cybersecurity Reserve. However, the wording of these requirements must not result in certain skills or system knowledge being excluded because only a few very large operators can meet the requirements imposed on providers of security services. The EU needs breadth in its security activities in order to be as resilient as possible.

13. Under the proposal, the Cybersecurity Reserve will consist of a list of trusted providers, which will be certified in accordance with the Cybersecurity Act ([4]). The European Union Agency for Cybersecurity (ENISA) is responsible for ensuring that products and services meet the stipulated cybersecurity requirements. The CoR highlights that it is important for ENISA to develop certification schemes quickly so that providers can be certified based on up-to-date technologies ([5]).

14. When establishing a Cybersecurity Reserve, it is also important to ensure that it does not impede competition or exclude providers that only operate in parts of the EU. The Cybersecurity Reserve and certifications need to be established on the basis of a quick and transparent process in order to find the most competent and relevant operators in this connection.

([4]) 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).

([5]) ENISA is currently developing three certifications, which are not yet complete — for ICT, 5G and cloud services. https://www.enisa.europa.eu/topics/standards/certification/eu-cybersecurity-certification-faq

15. The CoR considers it necessary to identify national technology and service providers of critical systems and to gather this information in a database. This information could be very valuable in the context of actions that require the mobilisation of local actors, and it could also be used in the work of the Cybersecurity Skills Academy.

16. When an incident occurs, the impact of the response depends on the speed with which it is deployed. The sharing of complex information on incidents and risks needs to reach the right target groups in a short time. As the proposal stands, a new organisation and structure will be put in place for sharing information, but the CoR would highlight the importance of using and refining existing information channels such as CyCLONe ([6]) and CSIRT when setting up national and cross-border SOCs.

Cybersecurity Incident Review Mechanism

A mechanism for reviewing cybersecurity incidents, specifically those that have had a major impact.

17. The need for cybersecurity skills, and for their funding, is following the same strong development trajectory as digitalisation. The CoR welcomes the Commission's establishment of a cybersecurity skills academy and calls for a clear strategy to specifically strengthen smaller municipalities and regions with fewer resources, given that there is a skills shortage in the EU.

18. The Committee underlines that strong digital resilience requires various stakeholders to work together, with public and private entities contributing through their expertise, experience and staff. It points out that local and regional authorities can play a role in building digital resilience, supporting each other by carrying out awareness-raising campaigns, sharing best practices and exchanging expertise. The more businesses invest in their digital resilience, the higher the cost of attacks for their adversaries, something which could also serve as a deterrent.

19. Today, Europe's municipalities and regions bear their own costs for maintaining a high level of cybersecurity, as well as the costs arising from incidents. The CoR sees a risk that the Regulation will create more work, stretching already tight resources. It is therefore important to ensure that the Regulation does not become a burden, but rather that it increases the capacity of each organisation by means of concrete tools, methods and support.

20. The CoR wonders why review reports cannot be shared within the network of national and cross-border SOCs — under the proposal, national SOCs can only access the public information. Learning from incidents is one of the most important tools in enabling actors to improve and develop their cybersecurity. The information should therefore be made accessible, with all the details, to all participants in the network.

21. The proposal presents funding at an overly general level. The CoR would like to see a much clearer description of how the funds are intended to be spent and what proportion is targeted directly at regions and municipalities.

([6]) Article 16(1) and (3) of the NIS 2 Directive.

European cyber crisis liaison organisation network (EU-CyCLONe)

1. EU-CyCLONe is established 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, offices and agencies.
3. EU-CyCLONe shall have the following tasks:
   (a) to increase the level of preparedness of the management of large-scale cybersecurity incidents and crises;
   (b) to develop a shared situational awareness for large-scale cybersecurity incidents and crises;
   (c) to assess the consequences and impact of relevant large-scale cybersecurity incidents and crises and propose possible mitigation measures;
   (d) to coordinate the management of large-scale cybersecurity incidents and crises and support decision-making at political level in relation to such incidents and crises;
   (e) to discuss, upon the request of a Member State concerned, national large-scale cybersecurity incident and crisis response plans referred to in Article 9(4).

22. Finally, the Committee points out that the proposal complies with the principles of subsidiarity and proportionality.

Brussels, 30 November 2023.

The President
of the European Committee of the Regions

Vasco ALVES CORDEIRO