Opinion of the European Economic and Social Committee on 'Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services'

(COM(2023) 208 final) — 2023/0108 (COD)

and on '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'

(COM(2023) 209 final]) — 2023/0109 (COD)

(2023/C 349/25)

Rapporteur: **Dumitru FORNEA**

Co-rapporteur: **Alberto MAZZOLA**

Referral	European Parliament, 1.6.2023
	Council of the European Union, 7.6.2023
Legal basis	Article 114, 173(3) and 304 of the Treaty on the Functioning of the European Union
Section responsible	Consultative Commission on Industrial Change
Adopted at plenary	13.7.2023
Plenary session No	580
Outcome of vote	
(for/against/abstentions)	174/0/1

1. **Conclusions and recommendations**

1.1. The European Economic and Social Committee (EESC) welcomes the proposal for a Regulation ([1]) and considers that EU coordination is vital to address the current market fragmentation and enhance cooperation among EU private and public stakeholders with a view to improving cyber threat prevention, detection and response capacity. The EESC recommends that the proposal pay greater attention to upholding the principles of subsidiarity and proportionality, in accordance with Article 4(2) of the Treaty on European Union (TUE).

1.2. The Committee acknowledges the European Commission's efforts in the field of cybersecurity and emphasises that a comprehensive response to cyber incidents should encompass not only capabilities and processes, but also hardware and software elements. However, the EESC is against the numerous implementing powers proposed by the Regulation, especially since cybersecurity remains a Member State prerogative.

1.3. A medium-term strategy for achieving strategic autonomy in key technologies and critical sectors is needed, supporting EU-based companies as they establish research and production facilities. The EESC emphasises the crucial importance of procuring only EU technology to equip national security operations centres (SOCs) with cutting-edge technologies.

1.4. The EESC is concerned that no cybersecurity scheme has been adopted and no product has yet been cyber-certified four years after the adoption of the EU Cybersecurity Act ([2]). It recommends involving the EU's sectoral agencies ([3]) in the development of cybersecurity schemes, and adopting a minimum EU standard in collaboration with CEN, Cenelec and ETSI, including for 'Internet of People' (IoP) devices and the internet of Things (IoT).

([1]) Proposal for a Regulation laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents.

([2]) 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).

([3]) EASA, ERA, EMA, etc.

1.5. The EESC acknowledges the enhanced role proposed for ENISA and calls for designated personnel and adequate budget allocation for all additional activities to enable ENISA to fulfil its significant strategic role in line with the EU's cybersecurity ambitions.

1.6. Member States should reach a consensus on adopting a holistic cybersecurity approach that encompasses skilled personnel, consistently implemented processes and appropriate state-of-the-art technologies, with specific emphasis on enhancing cooperation with the private sector. Strong links and cooperation between the defence and private sectors are vital.

1.7. The technical specifications of the future IT infrastructure should enable seamless interoperability between national systems and the EU Cyber Shield. National SOCs must also be prepared to conduct national stress tests on critical infrastructure and share the results within the EU Cyber Shield.

1.8. The Committee proposes that each consortium's coordinating SOC should hold a one-year mandate within a common rotation system. EU funding for the Hosting Consortium should cover 100 % of the acquisition costs for tools and infrastructure, and 50 % of the operational costs (as opposed to the proposed 75 %–50 % ratio).

1.9. Since skills shortages in cybersecurity have increased in recent years, the Committee welcomes the Cybersecurity Skills Academy initiative and considers that indicators measuring progress on reducing cybersecurity skills gaps are needed.

1.10. The EESC notes that the European Commission has not provided a precise cost estimation for the required programs, data analytics technologies and infrastructure development projects. It deems the proposed funding sources at EU level to be inadequate and urges the exploration of additional sources, including the pooling of private funding resources.

1.11. The procedure outlined for requesting support from the EU Cybersecurity Reserve appears to be sluggish, lacking clear deadlines for response. The Committee underscores the necessity for a lightning-fast response in the event of a cyber incident.

1.12. The EESC calls for clarification by the European Commission regarding the definition of a 'significant amount of data' mentioned in Article 6(2), point (a) of this Regulation, as well as regarding the 'targets' referred to in point (c) of the same paragraph.

1.13. The Committee considers it crucial that the EU participate in global discussions regarding the establishment of an international cybersecurity strategy. Swiftly investigating cyber-attacks and holding the perpetrators accountable is paramount, including through diplomatic channels in non-EU cases.

1.14. The EESC is disappointed that the social partners and civil society organisations are not mentioned once in the document and emphasises that achieving enhanced cooperation between public and private entities requires the full involvement of EU organised civil society.

1.15. The Committee proposes that the report for the European Parliament and the Council should be presented two years after the Regulation takes effect (and not four as proposed by the Commission), along with the impact assessment which should accompany this Regulation. The EESC insists on the need to implement both precise performance measures that focus on attaining outcomes and Key Performance Indicators (KPIs) that evaluate the results.

2. **Introductory comments**

2.1. The constant change, anonymity and lack of boundaries in cyberspace present both opportunities and risks for the functioning of the information society at individual, state and transnational level.

2.2. With clear potential for rapid spill-over of cyber incidents from one Member State to another, the EU faces mounting cybersecurity risks and an intricate threat landscape. EU coordination is essential in order to overcome the existing fragmentation and to promote enhanced cooperation between Member States.

2.3. The EU single market needs a homogeneous interpretation and implementation of cybersecurity rules, even if different approaches should be provided for different sectors due to the way they function.

2.4. For a prompt and efficient response to any cybersecurity incident, it is crucial to have a rapid system for exchanging information among all significant stakeholders at national and EU level. This, in turn, necessitates a clear understanding of each party's roles and responsibilities.

2.5. The Committee acknowledges the European Commission's efforts in the field of cybersecurity and appreciates the large number of communications and proposals that focus on building a stronger EU framework, enhanced cooperation, resilience and deterrence-building. Europe requires leading-edge cyber technology, with a strong link between the defence and private sectors, in order to mobilise defence budgets and build cyber products for both military and civilian use. The Committee highlights that the response needed in the event of cyber incidents must cover not only capabilities and processes, but also hardware and software aspects.

2.6. This proposal for a Regulation also puts into effect the EU Cybersecurity Strategy, which was adopted in December 2020 and announced the establishment of a European Cyber Shield to strengthen cybersecurity threat detection and information-sharing capabilities across the EU.

2.7. As the European Cyber Shield is being developed, the European Commission proposes future gradual collaboration with networks and platforms responsible for information sharing in the cyber defence community, in close cooperation with the High Representative.

2.8. Russia's military aggression towards Ukraine has illustrated how offensive cyber operations can be executed as a crucial element of hybrid tactics that involve coercion, destabilisation and economic disruption.

3. **General comments**

3.1. The EESC welcomes the proposed Regulation, which intends to address the current market fragmentation and expedite collaboration among European stakeholders from the private and public sectors in order to better prevent, detect and respond to cyber threats. Once implemented, it has the potential to contribute to enhancing the resilience of European systems.

3.2. However, it should be pointed out that the same objectives set out in this proposal were highlighted in the Joint Cyber Unit proposal ([4]), namely increased cooperation, preparedness, and resilience of EU cyber systems. Although the Cyber Unit was expected to become operational by the end of 2022, it is not mentioned once in the Commission proposal.

3.3. No single technology or tool can provide complete protection against cyber threats; Member States should therefore agree on a holistic approach to security that involves skilled personnel, consistently applied processes, and suitable state-of-the-art technologies. Focus must be placed on better cooperation with the private sector.

3.4. The EESC expresses its disappointment that the social partners and civil society organisations are not mentioned once in the document. Enhanced cooperation between public and private organisations cannot be achieved without full involvement of EU organised civil society.

3.5. The EU should adopt a medium-term strategy towards achieving strategic autonomy in key technologies and critical sectors, and the EESC recommends that EU-based companies be supported in establishing research and production facilities to support an autonomous cyber ecosystem. The EESC has already suggested that 'the EU needs to reduce its dependency on non-EU tech giants by doubling its efforts to develop a secure, inclusive and values-based digital economy' ([5]).

([4]) Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents.

([5]) Opinion of the European Economic and Social Committee on Digital Sovereignty: a crucial pillar for EU's digitalisation and growth (own-initiative opinion) (OJ C 75, 28.2.2023, p. 8).

3.6. The proposal to establish the European Cyber Shield, which will be composed of national and cross-border security operations centres (SOCs) and will be equipped with state-of-the-art technologies, is strongly welcomed. To ensure the resilience of the entire supply chain, SOC solutions must not only safeguard internal organisational resources, but also promote secure exchanges and wider cooperation within the ecosystem. The technical specifications of the future IT infrastructure must allow for full interoperability between national systems and the EU Cyber Shield.

3.7. The EESC emphasises the vital aspect of procuring only Europe-based technology for equipping the EU Cybers Shield members with state-of-the-art technologies. The EU cannot afford to risk acquiring critical cyber technologies from foreign companies and it is 'in the EU's strategic interest to ensure that the Union retains and develops the essential capacities to secure its digital economy, society and democracy, to achieve full digital sovereignty as the only way to protect critical technologies, and to provide effective key cybersecurity services' ([6]).

3.8. The Committee considers the proposed proportion for financing the procurement of equipment for national SOCs (50 % from national funding and 50 % from EU funding), involving an equal balance of national and EU funds, to be adequate. A joint effort is needed to ensure proper high-tech equipment and coordinated functioning of the SOC network.

3.9. The national SOCs must focus on establishing comprehensive security evaluation and testing protocols and should carry out periodic assessments. To evaluate and enhance resilience to potential cyber-attacks, they should also be prepared to conduct national stress tests on critical infrastructure. The results must be shared within the European Cyber Shield and joint efforts are needed to assess the existing problems, to update guidance on reporting issues, and to address issues effectively.

3.10. The EESC is concerned that no cybersecurity scheme has been adopted by the European Commission through implementing acts and no product has yet been cyber-certified four years after the adoption of the EU Cybersecurity Act. The EU's sectoral agencies should be involved in the process of developing the EU cybersecurity schemes and a minimum European standard should be adopted, in cooperation with CEN, Cenelec and ETSI, including for IoP devices and IoT.

3.11. Computer science and cybersecurity must be included on primary and secondary school curricula in all Member States. Since skill shortages in cybersecurity have increased in recent years, the Committee deems it necessary to consider potential incentives to support this initiative. The Committee welcomes the Cybersecurity Skills Academy initiative and considers that indicators that measure progress on reducing cybersecurity skills gaps are needed.

3.12. The worldwide digital economy faces a growing threat of cyber-attacks unless there is enhanced international cooperation among countries, industry and experts to establish common definitions and solutions for cybersecurity. International cooperation is vital in order to understand the cyber risks and the changing nature of global cyber-attacks, thus ensuring preparedness to address them. The EU must engage in global discussions on establishing an international cybersecurity strategy, with common international efforts and enhanced cooperation.

3.13. To establish effective deterrence, it is essential to enhance the EU's law enforcement response by concentrating on the detection, traceability and prosecution of cybercriminals. Investigating cyber-attacks promptly and bringing perpetrators to justice is crucial, including through diplomatic means in non-EU cases.

([6]) Opinion of the European Economic and Social Committee on the Joint Communication to the European Parliament and the Council: EU Policy on Cyber Defence (own initiative opinion) (OJ C 293, 18.8.2023, p. 21).

4. **Specific comments**

4.1. The EESC notes that there is a divergence of visions when it comes to more centralised action at EU level and the powers and jurisdiction of the Member States, and questions the final agreement on this proposal, especially since the Member States made it clear in the 2021 Council Conclusions ([7]) that the responsibility for responding to significant cybersecurity incidents and crises affecting their countries lies with them.

4.2. The EESC appreciates the strengthened role for ENISA and the proposed additional responsibilities after the Regulation is adopted. However, the Committee points out that any additional activities for ENISA need to have specific personnel designated for the tasks and to be accorded the appropriate budget. Unless this issue is solved, ENISA's key strategic role cannot be fulfilled in line with the EU's ambitions in the field of cybersecurity.

4.3. The EESC finds the Commission proposal unclear as to whether a national SOC can be part of more than one cross-border SOC. Furthermore, it is also unclear whether the grouping of national SOCs will be made according to geographical criteria or simply based on the free will of the Member States.

4.4. The EESC requests clarification of what 'significant amount of data' means in Article 6, paragraph 2, point (a) of this Regulation and what the 'targets' are that the Commission refers to in point (c) of the same paragraph.

4.5. Should the proposal for cross-border SOCs be embraced by Member States, and to ensure full involvement of national SOCs and shared management with the cross-border SOCs, the coordinating SOC of each consortium should have a mandate of one year, with all SOCs having the opportunity to coordinate the leadership in a rotation system.

4.6. The Committee considers that the EU funding for the Hosting Consortium should be 100 % of the acquisition costs of the tools and infrastructure and 50 % of the operation costs (compared to the 75 %–50 % set out in the proposal), in order help set up the consortia more swiftly. Coordination on procurement should be guaranteed.

4.7. The Committee considers that the effectiveness of the EU Cyber Shield in helping Member States prepare for and respond to cyber incidents needs specific performance measures that focus on achieving tangible outcomes and KPIs that evaluate results. The EESC recommends that cybersecurity breaches be systematically recorded and that this information be made available to legitimate stakeholders. This will enable assessment, implementation of appropriate preventive measures, and protection against potential losses.

4.8. The EESC acknowledges and endorses the proposal to enable Member States to request coverage for costs associated with sending expert teams in the framework of mutual assistance. While the process of mutual assistance should be supported, the solidarity mechanism should be properly and gradually tested in order to prove its effectiveness before it is fully implemented.

4.9. The Committee is worried that more and more international AI tech gurus (Elon Musk, Geoffrey Hinton, etc.) are warning about the existential threat that developing AI in an unregulated environment poses. Regulation of AI must go into greater depth than the Artificial Intelligence Act ([8]), and the EESC calls for responsible use of AI technology in all projects in the EU, including cybersecurity. Further discussion and an enhanced regulatory framework are needed immediately.

4.10. The EESC has already mentioned that 'the EU should take a strong stance against any kind of social scoring system against citizens. The EESC makes it clear that true democracy cannot exist without effective personal data protection' ([9]). Protecting human rights and citizens' right to privacy must remain essential rules when developing enhanced cybersecurity systems across the EU.

([7]) Council Conclusions from 19 October 2021 on exploring the potential of the Joint Cyber Unit initiative.
([8]) EU Artificial Intelligence Act.
([9]) See footnote 6.

4.11. Europeans have an important role to play in signalling cyberthreats to the relevant authorities. The EESC considers that it is vital to guarantee proper communication channels with the public and civil society organisations, and calls for a designated platform for receiving relevant cyberthreat intelligence. In order to create tools for interaction with the public, the Committee calls for information and awareness-raising campaigns to promote the tools already available.

4.12. The EU and NATO should work together to harmonise cybersecurity and other technical standards in the defence sector in order to minimise bureaucratic hurdles and red tape. Furthermore, the EU and NATO should collaborate on procurement standards and should jointly establish an effective and transparent procurement framework that would enable companies, especially SMEs, to participate in public tenders and compete fairly.

4.13. The EESC considers the proposed available funding sources at EU level to be insufficient, and requests that additional sources be sought, including pooling private funding resources. It notes that the Commission has not offered a specific estimation of the costs for the necessary AI programmes, data analytics technologies and infrastructure development projects in all Member States and at EU level that will be necessary to implement the actions set out in this Regulation.

4.14. The Commission proposes that it be awarded implementing powers to establish uniform conditions for the implementation of this Regulation, including specifying the interoperability conditions between cross-border SOCs, setting procedural arrangements for information sharing during cybersecurity incidents, and defining technical requirements for the European Cyber Shield's security, etc. The EESC considers that all of these issues should have been clarified before and presented in this proposal for a Regulation, since cybersecurity remains a Member State prerogative, and placing too much power to exercise change in the hands of the Commission could generate unnecessary tensions by circumventing the EU democratic system.

4.15. The Cybersecurity Act includes an industrial component which aims to establish a unified market for cybersecurity solutions through the creation of the Cybersecurity Reserve. However, the procedure for requesting support from the EU Cybersecurity Reserve seems very slow, with no clear deadlines for providing a response. The Committee highlights that the response needed in the event of a cyber incident must be lightning-fast, which this long-list procedure will clearly not deliver.

4.16. The European Commission has explained that an impact assessment was not conducted due to the pressing nature of the proposal. It has also proposed to present a thorough report to the European Parliament and the Council four years after the Regulation enters into force. Given the fast-paced developments in the cybersecurity field, the EESC considers that the report should be presented two years after the Regulation enters into force, together with the impact assessment that is missing from this Regulation. Furthermore, it strongly recommends that the proposal pay greater attention to upholding the principles of subsidiarity and proportionality, in accordance with Article 4(2) of the TUE. This is important for preventing tension between centralised EU action and the powers and jurisdiction of the Member States.

4.17. Finally, the EESC emphasises the importance of integrating cybersecurity considerations into all EU policies.

Brussels, 13 July 2023.

The President
of the European Economic and Social Committee
Oliver RÖPKE