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)

(2023/C 293/04)

Rapporteur: **Anastasis YIAPANIS**

Co-rapporteur: **Alberto MAZZOLA**

Plenary Assembly decision	20.9.2022
Legal basis	Rule 52(2) of the Rules of Procedure
	Own-initiative opinion
Section responsible	Consultative Commission on Industrial Change (CCMI)
Adopted in section	27.3.2023
Adopted at plenary	14.6.2023
Plenary session No	579
Outcome of vote	
(for/against/abstentions)	208/1/2

1. Conclusions and recommendations

1.1. The European Economic and Social Committee (EESC) supports the proposed EU policy on cyber defence, but would have expected organised civil society to be granted a more prominent role in developing these proposals. The Committee finds it difficult to assess at this point if the future initiatives outlined in the joint communication will be implemented and achieve their intended results. It urges the EU institutions and Member States to prioritise and swiftly advance the announced initiatives.

1.2. The EESC emphasises the need for additional measures to enhance the EU's ability to detect cyber threats and calls for R & D funding to be directed towards developing cutting-edge EU capabilities. Cooperation between private and public sectors is essential and must not be unidirectional. The EESC considers that EU coordination is necessary to address fragmentation and ensure cooperation and joint investment among Member States.

1.3. The EESC supports the creation of the EU Cyber Defence Coordination Centre and recommends that Member States commit to 24/7 rapid response, evaluate cyber-readiness and performance of EU cyber crisis response mechanisms, with focus on both military capabilities and critical sectors as identified by the Directive (EU) 2022/2555 of the European Parliament and of the Council1 (NIS2 Directive) ([1]). The Committee endorses the expansion of the mandate of the European Cybersecurity Competence Centre (ECCC) to assist the work of the EU Cyber Defence Coordination Centre.

1.4. To enhance the Union's cybersecurity strategic autonomy and sovereignty, the EESC believes that a dynamic, real-time testing and information sharing platform should be developed, or adopted, from the private sector, in order to identify current gaps in existing capabilities. It can also be used for sharing best practices, reporting cyber incidents and to create an EU list of all cyber criminals.

([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).

1.5. The EESC highlights the need for better preparation against cyberattacks such as the Russian ones in Ukraine, targeting critical infrastructure in particular. Cooperation between civilian and military ecosystems is crucial for efficient crisis management, interoperability and avoiding duplication of efforts and investments, including through simulated test cyberattacks.

1.6. The EESC believes that investments in cyber defence should prioritise the protection of EU citizens and critical infrastructure, including by using trusted hardware and software suppliers. It insists on having timely updates to priorities and investment, to be agreed upon by the EU and Member States, with the participation of relevant private stakeholders.

1.7. The EU must retain and develop the necessary capacities to secure its digital economy, society, democracy and critical technologies, and to provide key cybersecurity services. To ensure EU strategic autonomy, reducing dependencies on third countries is vital. The EESC considers it essential for the EU to adopt a medium-term approach towards autonomy as regards key technologies, and strongly advocates for research and production facilities to be established by EU-based companies, with an appropriate European industrial policy focused on an autonomous cyber ecosystem.

1.8. SMEs should receive targeted support and have access to financing programmes that increase their resilience to cyberattacks, as well as assistance, training and education opportunities on cyber risks and how to safeguard against them. The EU should provide an incentive mechanism that fosters progressive familiarisation for SMEs and development of innovative SMEs.

1.9. The EESC supports the plan to establish a Cyber Skills Academy, and asks the European Commission to coordinate and fund large-scale training and vocational education training programmes that involve all Member States and aim to create a skilled workforce for all agencies and organisations involved in cyber defence, as well as for private civilian networks.

1.10. The Committee considers raising citizens' awareness of cybersecurity crucial in reducing exposure to cyberattacks, and calls for cybersecurity education curricula and lifelong training programmes that will focus on improving cyber skills and knowledge. The EESC supports mainstreaming cybersecurity in all future EU public policies, and informing the public at large about cyber threats.

1.11. The EESC believes that strong cooperation with NATO allies in military areas must focus on full coordination and reciprocity, joint R & D&I projects, best practice sharing, large training programmes and simulations of cyberattacks, with the main objective being to extend the common response capacity.

1.12. The Committee calls on the High Representative to examine the current bilateral cyber dialogues and engage in additional discussions with other countries and relevant international organisations to establish a worldwide framework for the adherence to international law in cyberspace, with a strong emphasis on reciprocity. The Committee considers that the EU is well-suited to take the lead in international discussions on the future of cybersecurity, particularly within the United Nations, as it has a strong foundation in fundamental democratic freedoms.

1.13. 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 and believes that responsible and efficient data management is essential to turn hyperconnectivity into a competitive advantage.

2. **Introduction and general comments**

2.1. The digital expansion of societies comes with a large number of cybersecurity threats generated by technological upgrades. Cyberattacks have grown significantly in number and sophistication in the past few years, undermining the security of both public and private entities. Whether we are talking about ransomware, malware, email attacks, data breaches, disinformation, distributed denial-of-service (DDoS) attacks or other forms of attacks, they all pose a consistent and continuous threat to EU security as a whole.

2.2. The EESC welcomes the Joint Communication on *EU Policy on Cyber Defence* ([2]) and considers that the time to act is now, with urgency and in a coordinated manner at EU level, involving both the civilian and military cyberspace ecosystems and ensuring the proper investment framework for cyber defence capabilities. However, the Committee notes that the communication is merely a statement of determination to act and a list of future EU initiatives that should deliver, and finds it impossible to assess whether these future commitments will actually be put in place, since future negotiations between the co-legislators will naturally influence the final outcome of the EU cybersecurity action plan.

2.3. The Russian attack on the KA-SAT satellite network, which disrupted communication between Ukrainian military forces and the recent scandal involving Éric Léandri being contracted by some defence companies to cyber-spy on their behalf, is putting cybersecurity at the top of the list of security threats in the EU. Although the GDPR is a solid piece of EU legislation and has been in force for several years, it is clear that the increasing amount of data available is vulnerable and the risk of third parties crossing the boundary of legality is getting higher each day.

2.4. Given the transnational nature of cyberattacks, EU coordination is necessary to reduce the current fragmentation and ensure that the Member States are prepared to cooperate and invest jointly. This is particularly important for future cases in which one Member State could be targeted and all others should have the opportunity to provide immediate support.

3. **Act together for stronger cyber defence**

3.1. The Committee takes note of the announced ambitious initiatives to establish an EU Cyber Defence Coordination Centre, to develop the CyDEf-X project, to create cyber rapid reaction teams, to develop an EU Cyber Solidarity Initiative and to explore the development of cybersecurity certification schemes for ICT products, services and processes. The EESC recommends that all Member States should commit to being ready to provide a 24/7 rapid response, with the EU Coordination Centre involved in assessing and developing regular reports on the cyber-readiness of Member States and the effectiveness of the European cyber crisis response mechanism, focusing both on military capabilities and on critical sectors identified by the NIS2 Directive. Each Member State should have specialists specifically trained to intervene in case of cyber incidents, and should regularly test their capability of intervention in other Member States.

3.2. While the communication provides a long list of step-by-step improvements, the EESC would have hoped to see an explicit roadmap on the implementation of these initiatives, with clear governance and deadlines for submission and adoption. Furthermore, the Committee would have expected organised civil society to be granted a more prominent role in developing these proposals.

3.3. The EESC considers that Member States need to strengthen their internal capacity to counteract cyber threats while engaging in cooperation projects and sharing information and best practices with their counterparts in other Member States. There is a need for rapid investment in cyber defence capabilities and for accelerated technology deployment ([3]) in all Member States and in common preparedness to detect, recover from and defend against cyberattacks. In order to support the cybersecurity autonomy of the Union, the Committee considers that a dynamic real-time testing and information sharing platform must be developed, or adopted from the private sector, focused on identifying current missing capabilities.

3.4. The EESC shares the view that, at this stage, military cyberspace operations should remain strictly the competence of Member States; the Committee supports the announced cooperation between EU military Computer Emergency Response Teams (milCERTs), the Computer Security Incident Response Teams (CSIRTs) and the Computer Emergency Response Team of the EUIBAs (CERT-EU).

3.5. The recently adopted NIS2 Directive and the Directive on the resilience of critical entities (CER) ([4]) already put in place specific national and sectoral obligations for the EU cyber defence framework. Further action is needed to improve the EU's collective detection capacity, and the EESC calls for R & D investment for developing cutting-edge EU capabilities.

([2]) Commission Communication on EU Policy on Cyber Defence.
([3]) Such as NATO Defence Innovation Accelerator for the North Atlantic initiative (DIANA).
([4]) CER Directive.

4. **Secure the EU defence ecosystem**

4.1. The EESC believes that inherent complexities and fast-evolving technological challenges have transformed the defence ecosystem, and that cybersecurity has become a common subject for both military and civilian sectors, as well as for EU citizens. Cooperation between civilian and military ecosystems is now more important than ever and should bring benefits in terms of more effective crisis management, as well as continuous progress and interoperability, avoiding duplication or multiplication of the same efforts and investments. Member States should be ready to conduct national critical infrastructure stress tests in order to assess and increase resilience to future cyberattacks.

4.2. The EESC considers that investments in cyber defence must, as a priority, be targeted towards protecting EU citizens and critical infrastructure. Given the fast pace of digital transformation and the rapid evolution of the threat landscape, the Committee strongly urges that timely updates to priorities and investment should be agreed between the EU and Member States, with thorough consultation of relevant private stakeholders. Internet of Things (IoT) devices are often not as well protected as traditional devices, and the EESC calls for a minimum-security level to be ensured through IDAM platforms. Also, since certification is a key method of providing a higher level of security, the Committee calls for the new EU certification approach to place more emphasis on IoT security.

4.3. The EU must build resilience to cyberattacks and create effective cyber deterrence. Critical infrastructure must be protected against cyberattacks of all kind, including by EU defence systems. The Committee considers it to be 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. Reducing dependencies on third countries is also vital for the EU strategic autonomy. The EESC believes that sectoral EU agencies (ENISA, EASA, ERA, EMA, EBA, ESA, HADEA, etc.) should be involved in the process and provide guidance in developing cybersecurity schemes.

4.4. The COVID-19 pandemic has accelerated the digital transition and transformed traditional labour into hybrid and/or remote, creating new working relations and expectations as well as a new class of digital nomads, who are increasing in number. The EESC notes the rapid changes in the labour market, which have generated the adoption of 'Zero Trust' Architecture by companies, via IAM (Identity Access Management) and PAM (Privileged Access Management) solutions. The Committee considers that this type of management of companies' resources brings new solutions related to cyber threats and deems that the private sector must be supported in strengthening the security level of their innovative digital solutions.

4.5. The EESC is rather disappointed with the Commission's statement that 'an implementation plan could be established in cooperation with Member States' and considers such an implementation plan mandatory. It believes it should be drafted jointly with Member States and implemented as soon as possible. The Committee is concerned about the light-touch stance adopted by the Commission, and urges the EU institutions and Member States to facilitate rapid progress on the announced initiatives.

5. **Invest in cyber defence capabilities**

5.1. As the technological development is rapidly advancing, cyberspace has become the newest domain of warfare, after land, sea, air and space. It has also generated large crime opportunities for malicious cyber actors ranging from independent hackers to professional criminals and even state actors.

5.2. Investment in R & D is vital and the EESC welcomes the existing dedicated funds within the Digital Europe Programme, European Defence Fund, Horizon Europe and national recovery programmes. However, the Committee would appreciate more transnational projects that focus on cooperation and interoperability between cyber defence systems in all Member States, as well as more synergies between funding instruments, especially accompanying innovative SMEs.

5.3. As announced in the EU Cybersecurity Strategy back in 2020, the Committee notes that the deadline to create the Joint Cyber Unit is this year, and is awaiting news on the finalisation of the process and the EU's preparedness to respond to large-scale cyber incidents. The EESC expects it to improve the EU's situational awareness and the overall capacity to respond and recover.

5.4. The EESC supports the extension of the mandate of the ECCC to support the activity of the EU Cyber Defence Coordination Centre. In addition, this network could support European digital sovereignty by developing a competitive European industrial base for key technological capabilities, based in part on work developed by contractual public-private partnerships (PPP). PPPs have proven to be the most effective approach to improving the cybersecurity of the entire digital ecosystem, but it cannot be unidirectional: public institutions must also share their intelligence with the private sector.

5.5. The EESC notes that, in order to address future hacking attempts from quantum computers, the EU must immediately invest in cutting-edge technologies such as post-quantum cryptography. It believes that it is indispensable for Europe to take a medium-term approach to autonomy, and advocates strongly for research and production facilities to be developed by EU-based companies. The EESC considers it important to increase EU resources for digital R&I and to support operator and supplier investment in new technical security functionalities, also related to new trends such as augmented reality and the metaverse. In particular, it is essential to build up a European distributed cloud infrastructure based on European rules on topics such as data storage and processing ([5]).

5.6. SMEs should be given specific attention and have access to financing programmes that enhance their readiness against cyberattacks, as well as to assistance, training and education programmes that helps them understand the cyber risks and how to protect themselves. The EU should provide an incentive mechanism that fosters progressive familiarisation for SMEs.

5.7. The Commission estimates the existing skills shortage in cybersecurity at half a million people, and the EESC appreciates the proposal to create a Cyber Skills Academy. It is clear that efforts at Member State level are not enough to reduce the skills gap, so the Committee suggests that, together with launching the Academy, the Commission uses the momentum offered by the European Year of Skills and coordinates and finances large-scale training programmes and VET programmes at EU level that involve all the Member States and focus on delivering a skilled labour force for all the agencies and bodies involved in cyber defence, as well as for private civilian networks. Particular emphasis must be placed on training the workforce, in particular in the fields of science, technology, engineering, and mathematics (STEM).

5.8. Furthermore, the EESC considers that it is vital to raise citizens' awareness of cybersecurity in order to reduce exposure to cyberattacks, especially regarding basic cyber-crimes targeting the population at large. The Committee calls for cybersecurity education curricula and lifelong cybersecurity training programmes that will focus on improving cyber skills and make cybersecurity more familiar and attractive to citizens, especially the younger generation. The EESC favours mainstreaming cybersecurity reflections in all future EU public policies and informing the public at large about cyber threats, including through free training programmes for the population at large, free information cell-phone apps, or by communicating during prime-time TV times. Widespread cultural advancement at every level of society, towards a 'cybersecurity-oriented' approach, must be promoted in parallel with these actions.

5.9. The EESC believes that it is vital to assess the risk profile of suppliers and apply relevant restrictions to those considered to be high risk, including necessary bans on key assets and applications defined as critical and sensitive in the EU coordinated risk assessment, as well as certifying trusted hardware and software providers.

6. **Partner to address common challenges**

6.1. The level of preparedness for future cyberattacks differs widely from one Member State to another. The EESC considers that the immediate first step is to set up an intra-EU best practices communication platform, where the most cyber-advanced Member States can share their knowledge with and facilitate immediate uptake by the other countries. This would help improve mutual trust between national entities. Secondly, the Committee believes that stronger cooperation is needed between state and non-state actors across the EU in order to improve the cybersecurity of products and services within the internal market. The EESC also suggests the creation of a common EU platform for reporting cyber incidents, including an EU black list of all cyber-crime activists.

([5]) Such as Gaia-X, the Franco-German initiative.

6.2. The EESC is of the opinion that strong cooperation with our NATO allies in the military area must be focused not only on capacity building and early detection, but also on joint R & D&I projects, best practice sharing and exchanges between experts, large training programmes and simulations of cyberattacks. The main objective should be to extend the common response capacity and create synergies for countering future hybrid threats, following the 2016 Warsaw and 2018 Brussels Joint Declarations. The cooperation between the EU and NATO still has a number of avenues that can be exploited, and immediate progress can make a real difference in terms of ensuring security for our citizens and societies.

6.3. The Committee believes that discussions at global level and with our international partners should set the scene to promote a global and open cyberspace that protects human rights, fundamental freedoms and the rule of law, and focuses on developing binding international standards in sectors with fast digital development. The EESC advises the High Representative to review the existing bilateral cyber dialogues and engage in further negotiations with other countries and relevant international organisations in order to promote a global framework for the application of international law in cyberspace, based on a strict condition of reciprocity.

6.4. Finally, the Committee believes that the EU is best placed to lead the international debates on the future of cybersecurity, especially within UN discussions, due to its solid foundation on core democratic freedoms. The EU must also engage in combating totalitarian regimes that exercise citizen data monitoring and breach their rights and freedoms, and should position itself strongly against any kind of social scoring system against citizens. The EESC makes a clear statement that there cannot be a real democracy without effective personal data protection, and considers that responsible and efficient data management is vital to turn hyperconnectivity into an asset.

Brussels, 14 June 2023.

The President
of the European Economic and Social Committee
Oliver RÖPKE