Opinion of the European Economic and Social Committee on 'Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres'

(COM(2018) 630 final — 2018/0328 (COD))

(2019/C 159/10)

Rapporteur: **Antonio LONGO**

Co-rapporteur: **Alberto MAZZOLA**

Consultation	European Council, 5.10.2018 European Parliament, 1.10.2018
Legal basis	Articles 173(3), 188 and 304 of the Treaty on the Functioning of the European Union
Section responsible	Transport, Energy, Infrastructure and the Information Society
Adopted in section	9.1.2019
Adopted at plenary	23.1.2019
Plenary session No	540
Outcome of vote (for/against/abstentions)	143/5/2

1. Conclusions and recommendations

1.1. The European Economic and Social Committee (EESC) welcomes the Commission's initiative, considering it an important step in developing an industrial strategy for cybersecurity and a strategic move to achieve robust and comprehensive digital autonomy. These aspects are essential for strengthening Europe's defence mechanisms against the ongoing cyberwarfare that threatens to undermine its political, economic and social systems.

1.2. The Committee points out that any strategy on cybersecurity must go hand in hand with widespread awareness and the adoption of safe practices by all users.

1.3. The EESC supports the general objectives of the proposal and is aware that specific aspects of how it will work will be dealt with at a later point. However, as this is a regulation, it considers that certain sensitive aspects related to governance, funding and achieving the objectives set should be outlined in advance. It is important that the future Network and the Centre should build as far as possible on the Member States' expertise and cyber skills, and that competences should not all be concentrated in the new Centre. It is also important to ensure that the activities of the future Network and the Centre do not overlap with existing cooperation mechanisms and bodies.

1.4. The EESC is in favour of extending the partnership to include the industry, on the basis of firm commitments on the scientific and investment fronts, and by including it in future in the Governing Board. In the event of a tripartite partnership between the European Commission, the Member States and the industry, the involvement of companies from non-EU countries should be limited to those that have long been established on European soil and are fully involved in the European technological and industrial base, and their involvement should be subject to proper screening and oversight mechanisms and to compliance with the principle of reciprocity and confidentiality obligations.

1.5. Cybersecurity requires a joint commitment from all Member States, which should therefore participate in the Governing Board on the basis of arrangements to be determined. Their financial contributions could draw on the allocation of EU funds to each Member State.

1.6. The proposal should explain more clearly how the Centre will be involved in coordinating the funding streams from the Digital Europe and Horizon Europe programmes, or, above all, what guidelines will be followed when framing and awarding contracts. This is of key importance in order to avoid duplications and overlaps. Furthermore, in order to increase the budget, it would be advisable to extend the synergies to other EU financial instruments (e.g. regional funds, structural funds, the CEF, the EDF, InvestEU, etc.).

1.7. The EESC considers it essential to set out the details of the cooperation arrangements and relations between the European Centre and the national centres. It is also important that the national centres be funded by the EU, at least when it comes to their administrative costs, thereby facilitating harmonisation in terms of administration and expertise, so as to reduce the gap between European countries.

1.8. The Committee reiterates the importance of human capital and hopes that – in cooperation with universities, research centres and higher education institutes – the Competence Centre can promote initiatives aimed at educating and training people to a standard of excellence, including through dedicated third-level and secondary-school courses. In the same vein, it is essential to provide for specific support for start-ups and SMEs.

1.9. The EESC considers it essential to further clarify the respective remits of and dividing lines between the Centre and the European Network and Information Security Agency (ENISA), and to clearly set out how they will work together and support each other and thereby avoid overlaps of responsibilities and duplication of efforts. Similar problems arise with other bodies dealing with cybersecurity such as the EDA, Europol and CERT-EU; it would be advisable to set up mechanisms for structured dialogue between each of the various bodies.

2. **Current framework for cybersecurity**

2.1. Cybersecurity is one of the issues at the top of the EU's agenda, given that it plays an essential part in protecting institutions, businesses and individuals, as well as in actually safeguarding democracies. Among the most worrying issues is the exponential increase in the incidence of malware disseminated online via automated systems, which has risen from 130 000 in 2007 to 8 million in 2017. Furthermore, the EU is a net importer of cybersecurity products and solutions, and this is problematic for economic competitiveness and civilian and military security.

2.2. Although the EU has considerable expertise and experience in the field of cybersecurity, the industry, universities and research centres are still fragmented, lacking alignment and a common development strategy. This is because the relevant cybersecurity sectors (e.g. energy, space, defence and transport) are not sufficiently supported, while synergies between civilian and defence cybersecurity are not harnessed.

2.3. In order to address the growing challenges, the EU established a Cybersecurity Strategy in 2013 to foster a reliable, safe, and open cyber ecosystem ([1]). Later, in 2016, the first specific measures were adopted on the security of network and information systems ([2]). This process led to the creation of a public-private partnership ('cPPP') on cybersecurity.

2.4. In 2017, the communication entitled *Resilience, deterrence and defence: Building strong cybersecurity for the EU* ([3]) pointed out the need to ensure that the EU retains and develops essential cybersecurity technological capacities to secure the digital single market, and, in particular, to protect critical networks and information systems and provide key cybersecurity services.

([1]) JOIN(2013) 1 final.
([2]) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).
([3]) JOIN(2017) 450 final.

2.5. Therefore, the EU must be in a position to secure its own digital assets and processes and to compete on the global cybersecurity market in order to achieve robust and comprehensive digital autonomy ([4]).

3. The Commission's proposals

3.1. The Competence Centre (or 'Centre') will aim to facilitate and coordinate the work of the Network of National Coordination Centres and act as a reference point for the cybersecurity competence community, driving the cybersecurity technological agenda and facilitating access to the expertise so gathered.

3.2. In particular, the Centre will do so by implementing relevant parts of the Digital Europe and Horizon Europe programmes by allocating grants and carrying out procurements. In view of the huge investments in cybersecurity made in other parts of the world and of the need to coordinate and pool relevant resources in Europe, the Competence Centre is proposed as a European Partnership with a double legal basis, thus facilitating joint investment by the EU, the Member States and/or industry.

3.3. The proposal requires the Member States to contribute a commensurate amount to the activities of the Competence Centre and Network. The budgetary allocation proposed by the EU is around EUR 2 billion from the Digital Europe programme; an amount to be determined from the Horizon Europe programme; and a total contribution from the Member States at least matching that from the EU.

3.4. The principal decision-making body is to be the Governing Board, in which all Member States will take part but only those that participate financially will have voting rights. Its voting mechanism is to follow a double majority principle requiring 75 % of the financial contribution and 75 % of the votes. The Commission is to hold 50 % of the voting rights. The Centre is to be assisted by an Industrial and Scientific Advisory Board to ensure dialogue with businesses, consumers and other relevant stakeholders.

3.5. Working closely with the Network of National Coordination Centres and the cybersecurity competence community, the Centre would be the main implementation body for EU financial resources dedicated to cybersecurity under the proposed Digital Europe and Horizon Europe programmes.

3.6. The national coordination centres are to be selected by the Member States. These centres must either possess or have direct access to technological expertise in cybersecurity, notably in domains such as cryptography, ICT security services, automatic intrusion detection, system security, network security, software and application security, and human and societal aspects of security and privacy. They must also have the capacity to effectively engage and coordinate with industry and the public sector, including authorities designated under Directive (EU) 2016/1148.

4. General comments

4.1. The EESC welcomes the Commission's initiative and considers it a strategic move for the development of cybersecurity, which gives effect to the decisions taken at the Tallinn summit in September 2017. At that occasion, the heads of state and government called on the EU to '*make Europe a leader in cybersecurity by 2025, in order to ensure the trust, confidence, and protection of our citizens, consumers and enterprises online and to enable a free and law-governed internet*'.

4.2. The EESC reiterates that we are currently in the midst of fully-fledged cyberwarfare, which threatens to undermine our political, economic and social systems, attacking institutions' IT systems, critical infrastructure (such as energy, transport, banking and financial institutions) and businesses, and affecting – partly through fake news – elections and democratic processes in general ([5]). A high level of awareness must therefore be promoted, combined with a robust and timely response. For these reasons, a clear and well-supported industrial strategy for cybersecurity is needed as a precondition to achieving digital autonomy. The EESC considers that the work programme should give priority to sectors identified in the Directive (EU) 2016/1148, which applies to companies providing services, be they public or private, that are essential because of their importance for society ([6]).

([4]) OJ C 227, 28.6.2018, p. 86 .

([5]) Information report on'How media is used to influence social and political processes in the EU and Eastern neighbouring countries', Ms Vareikytė, 2014.

([6]) OJ C 227, 28.6.2018, p. 86 .

4.3. The Committee points out that any strategy on cybersecurity must go hand in hand with widespread awareness and the adoption of safe practices by all users. For this reason, any technological initiative must be accompanied by appropriate information and awareness-raising campaigns in order to create a 'culture of digital safety' ([7]).

4.4. The EESC supports the general objectives of the proposal and is aware that specific aspects of how it will work will be dealt with at a later point. However, as this is a regulation, it considers that certain sensitive aspects related to governance, funding and achieving the objectives set should be outlined in advance. It is important that the future Network and the Centre should build as far as possible on the Member States' expertise and cyber skills, and that competences should not all be concentrated in the new Centre. It is also important to ensure that the activities of the future Network and the Centre do not overlap with existing cooperation mechanisms and bodies.

4.5. The EESC points out that, in its opinion TEN/646 on the Cybersecurity Act ([8]), it proposed tripartite PPP cooperation between the European Commission, the Member States and the industry, including SMEs, while the current structure, whose legal form needs to be fleshed out, essentially provides for a public-public partnership between the European Commission and the Member States.

4.6. The EESC is in favour of extending the partnership to include the industry, on the basis of firm commitments on the scientific and investment fronts, and by including it in future in the Governing Board. The establishment of an Industrial and Scientific Advisory Board may not ensure ongoing dialogue with businesses, consumers and other relevant stakeholders. Moreover, in the new landscape sketched out by the Commission, it is not clear what role the European Cyber Security Organisation (ECSO) will play. This body was established in June 2016 at the instigation of the Commission to act as the Commission's counterpart, and its capital in terms of networks and expertise should not be wasted.

4.6.1. In the event of a tripartite partnership, is important to give attention to the situation of companies from third countries. In particular, the EESC stresses that such a partnership should be underpinned by a robust mechanism to prevent the involvement of non-EU companies that might undermine the security and autonomy of the EU. The relevant clauses set out in the EDIDP ([9]) should also be applied in this context.

4.6.2. At the same time, the EESC recognises that certain companies that are from non-EU countries but have long been established on European soil and are fully involved in the European technological and industrial base could be very useful for EU projects, and should be able to access these projects provided that the Member States ensure proper screening and oversight mechanisms for these companies, and on condition that the principle of reciprocity and confidentiality obligations are respected.

4.7. Cybersecurity requires a joint commitment from all Member States, which should therefore participate in the Governing Board on the basis of arrangements to be determined. It is also important that all Member States make a sufficient financial contribution to the Commission's initiative. Their financial contributions could draw on the allocation of EU funds to each Member State.

4.8. The EESC agrees that each Member State should be free to appoint a representative to the Governing Board of the European Competence Centre. The EESC recommends that the profiles of the national representatives be clearly defined, combining strategic and technological expertise with management, administrative and budgetary skills.

4.9. The proposal should explain more clearly how the Centre will be involved in coordinating the funding streams from the Digital Europe and Horizon Europe programmes – currently still under negotiation – or, above all, what guidelines will be followed when framing and awarding contracts. This is of key importance in order to avoid duplications and overlaps. Furthermore, in order to increase the budget, it would be advisable to extend the synergies to other EU financial instruments (e.g. regional funds, structural funds, the CEF, the EDF, InvestEU). The Committee hopes that the Network of National Coordination Centres will be involved in managing and coordinating the funds.

([7]) OJ C 227, 28.6.2018, p. 86 .
([8]) OJ C 227, 28.6.2018, p. 86 .
([9]) COM(2017) 294.

4.10. The EESC notes that the Advisory Board is to comprise 16 members and that no detail is given as to how this body will draw on the worlds of business, universities, research and consumers. The Committee thinks it would be useful and appropriate to ensure that this board is made up of people with an outstanding level of knowledge of the subject who are representative in a balanced way of the different sectors involved.

4.11. The EESC considers it important to set out the details of the cooperation arrangements and relations between the European Centre and the national centres. It is also important that the national centres be funded by the EU, at least when it comes to their administrative costs, thereby facilitating harmonisation in terms of administration and expertise, so as to reduce the gap between European countries.

4.12. In line with its previous opinions ([10]), the EESC emphasises the importance of educating and training people to a standard of excellence in the field of cybersecurity, including through specific school curricula and undergraduate and postgraduate courses. Sufficient financial support should also be offered to SMEs and start-ups in the sector ([11]), which are essential to the development of cutting-edge research.

4.13. The EESC considers it essential to further clarify the respective remits of and dividing lines between the Centre and ENISA, and to clearly set out how they will work together and support each other and thereby avoid overlaps of responsibilities and duplication of efforts ([12]). The proposal for a regulation states that an ENISA representative is to be a permanent observer on the Governing Board; however, that does not guarantee structured dialogue between the two bodies. Similar problems arise with other bodies dealing with cybersecurity such as the EDA, Europol and CERT-EU. In this regard, it is interesting to note that a memorandum of understanding was signed in May 2018 between ENISA, the EDA, Europol and CERT-EU.

Brussels, 23 January 2019.

The President
of the European Economic and Social Committee
Luca JAHIER

([10]) OJ C 451, 16.12.2014, p. 25 .
([11]) OJ C 227, 28.6.2018, p. 86 .
([12]) OJ C 227, 28.6.2018, p. 86 .