Opinion of the European Economic and Social Committee on the 'Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry'

(COM(2016) 410 final)

(2017/C 075/21)

Rapporteur: **Thomas McDONOGH**

Consultation	European Commission, 18.8.2016
Legal basis	Article 304 of the Treaty on the Functioning of the European Union
Section responsible	Section for Transport, Energy, Infrastructure and the Information Society
Adopted in section	15.11.2016
Adopted at plenary	14.12.2016
Plenary session No	521
Outcome of vote	148/0/1
(for/against/abstentions)	

1. **Conclusions and recommendations**

1.1 The Committee welcomes the communication from the Commission on Strengthening Europe's cyber resilience system and fostering a competitive and innovative cybersecurity industry. The Committee shares the concern of the Commission about the continuing vulnerability of Europe to cyberattacks, noting that at least 80 % of European companies have experienced at least one cybersecurity incident over the last year and the number of security incidents across all industries worldwide rose by 38 % in 2015 (The Global State of Information Security Survey 2016, PWC). We agree with the Commission that a range of measures are needed to strengthen Europe's cyber resilience system and to foster a competitive and innovative cybersecurity industry in Europe.

1.2 The Committee especially welcomes this proposal in the context of the recently adopted Network and Information Security Directive (NIS Directive) [1], which sets out to harmonise the approach to cybersecurity within the European Union, and the broader Cybersecurity Strategy [2], which outlines the current vision on how best to prevent and respond to cyber disruptions and attacks, to further European values of freedom and democracy, and to ensure that the digital economy can grow safely.

1.3 The EESC agrees that comprehensive measures are required to further protect Europe's vital digital infrastructure and services from security threats and we are pleased to see that the measures now proposed will go a long way towards implementing many of the Committee's recommendations in numerous previous opinions [3] on enhancing cybersecurity across the Union.

[1] OJ L 194, 19.7.2016, p. 1.

[2] JOIN(2013) 1.

[3] OJ C 97, 28.4.2007, p. 21;
OJ C 175, 28.7.2009, p. 92;
OJ C 255, 22.9.2010, p. 98;
OJ C 54, 19.2.2011, p. 58;
OJ C 107, 6.4.2011, p. 58;
OJ C 229, 31.7.2012, p. 90;
OJ C 218, 23.7.2011, p. 130;
OJ C 24, 28.1.2012, p. 40;
OJ C 229, 31.7.2012, p. 1;
OJ C 351, 15.11.2012, p. 73;
OJ C 76, 14.3.2013, p. 59;
OJ C 271, 19.9.2013, p. 127;
OJ C 271, 19.9.2013, p. 133;
OJ C 451, 16.12.2014, p. 31.

1.4 The EESC is pleased that the Commission has signed the contractual Public Private Partnership (cPPP) on cybersecurity that is expected to unlock EUR 1,8 bn investment in the EU cybersecurity industry to foster cooperation at early stages of the research and innovation process and to build cybersecurity solutions for various sectors, such as energy, health, transport and finance. We are particularly keen to see this cPPP used to support the development of early-stage cybersecurity companies across the Union.

1.5 The Committee welcomes the Commission's intention to evaluate the need to modify or extend the mandate of the European Network and Information Security Agency (ENISA) by the end of 2017 and we look forward to being consulted on this by the Commission. The EESC believes that any extension of ENISA's mandate should include a greater operational role for the agency to more effectively increase cyberattack threat awareness and response across the Union, as well as more direct responsibility for cybersecurity education and awareness programmes especially targeted at citizens and small and medium-sized enterprises (SMEs).

1.6 In order to provide the strength of leadership and integration required at EU-level to deal with the complexities of implementing an effective Europe-wide cybersecurity policy, the Committee asks the Commission to evaluate the possibility of changing the status of ENISA into an EU-level authority for cybersecurity, analogous to the central authority in the aviation industry, the European Aviation Safety Agency (EASA). If this change of mandate for ENISA is not feasible, then the EESC advocates the creation of such an authority from scratch.

1.7 The EESC calls on the Commission to consider creating a national cybersecurity development model and rating system, analogous to the Capability Maturity Model (CMM) in the IT industry, to objectively measure the status of cybersecurity resilience of each Member State.

1.8 The Committee notes that the Commission will consider the need to update the 2013 EU Cybersecurity Strategy in the near future and we look forward to being consulted on the Commission's thoughts in due course.

1.9 Considering the importance of cybersecurity and the ever-growing threat of cybercrime, the EESC calls for the allocation of adequate funding and resources to the European Cybercrime Centre at Europol and the European Defence Agency.

1.10 Given the considerable importance of protecting the personal information of citizens that is stored by public administration institutions and agencies, the Committee calls for special training on information governance, data protection and cybersecurity for employees in public administration jobs.

1.11 Taking a comprehensive view of protecting the EU from cybercrime and cyberattacks, as well as growing a strong cybersecurity industry in Europe, the EESC considers that EU cybersecurity strategy and policy needs to deliver in particular on the following points: strong EU leadership; cybersecurity policies that enhance security while preserving privacy and other fundamental rights; awareness-raising among citizens and encouraging proactive protection approaches; comprehensive Member State governance; informed and responsible business action; deep partnership between governments, the private sector and citizens; adequate investment levels; good technical standards and sufficient R & D & I investments; and international engagement.

2. **Gist of the Commission Communication**

2.1 The Communication presents measures aiming to strengthen Europe's cyber resilience system and to foster a competitive and innovative cybersecurity industry in Europe, as announced in the EU Cybersecurity Strategy and in the Digital Single Market strategy.

2.2 To achieve this, the measures proposed by the Commission leverage the provisions in the NIS Directive to strengthen cybersecurity cooperation, information sharing, training and security organisation across the Union. The Commission will also complete an evaluation of ENISA by the end of 2017 and will consider the need to modify or extend the mandate of ENISA.

2.2.1 The Commission will work in close cooperation with Member States, ENISA, EEAS and other relevant EU bodies to establish a cybersecurity training platform.

2.2.2 There are a number of measures proposed to address inter-sectoral interdependencies and to enhance key public network infrastructure resilience, including the development of European Sectoral Information Sharing and Analysis Centres and their collaboration with CSIRTs. The Commission is also proposing that national authorities be allowed to request CSIRTs to conduct regular checks of key network infrastructures.

2.3 The measures proposed by the Commission will also address the need to increase support for the growth and development of a strong European cybersecurity industry with training, investment, single market requirements and the creation a new public-private partnership on cybersecurity that is expected to trigger EUR 1,8 billion of investment by 2020.

2.3.1 It is also proposed that a European ICT security certification framework proposal be developed, to be presented by the end of 2017, and to assess the feasibility and impact of a European lightweight cybersecurity labelling framework.

2.3.2 In order to scale-up cybersecurity investment in Europe and support SMEs the Commission will raise awareness about existing funding mechanisms among the cybersecurity community; step up the use of EU tools and instruments to support innovative SMEs in exploring synergies between civilian and defence cybersecurity markets (for example, the Enterprise Europe Network and the European Network of Defence-related Regions will provide new opportunities for regions to explore cross-border cooperation in the area of dual use, including cybersecurity, and for SMEs to engage in matchmaking activities); explore the feasibility of easing access to investment through a dedicated Cybersecurity Investment Platform or other tools; and develop a Cybersecurity Smart Specialisation Platform to help Member States and regions interested in investing in the cybersecurity sector (RIS3).

2.3.3 Furthermore, to stimulate and nurture the European cybersecurity industry through innovation the Commission will sign with industry a contractual Public Private Partnership (cPPP) on cybersecurity; launch Horizon 2020 calls for proposals related to the cybersecurity cPPP; and ensure coordination of the cybersecurity cPPP with relevant sectoral strategies, Horizon 2020 instruments and sectoral PPPs.

3. **General comments**

3.1 The digital economy generates over one fifth of GDP growth in the EU and most Europeans buy online each year. We depend on the internet and connected digital technology to support our vital energy, health, government and financial services. However, the critical digital infrastructure and services that play such an essential role in our economic and social lives are vulnerable to a growing risk of cybercrime and cyberattacks that threaten our prosperity and quality of life.

3.2 Much personal information on all citizens is now held electronically by governments and public institutions and agencies. Thus, good information governance, cybersecurity and data protection is of major importance to citizens across the Union, who need to be assured that their personal information and privacy is protected in accordance with EU directives and regulations. This is particularly the case with data concerning one's health, financial, legal and other matters that could be used to steal an identity or inappropriately disclosed to third parties. It is vitally important that all staff working in the public sector are well trained in information governance, cybersecurity and data protection.

3.3 The teaching of personal cybersecurity to citizens, including data security, should be a fundamental part of all digital literacy curricula. An education programme driven by the EU can support the efforts of less active Member States and also ensure that the strategy is properly understood, thus reducing privacy fears and increasing trust in the digital economy. Such a programme could be implemented with the involvement of consumer associations and civil society organisations across the Union, including education institutions serving the needs of older citizens.

3.4 Every Member State should empower its existing industrial development organisations to inform, educate and support the SME sector on issues regarding cyber security. The large firms can easily acquire the knowledge they need but SMEs need support.

3.5 It would be very useful to have an objective measure of the level of cybersecurity resilience of each Member State so that comparisons could be used to address weaknesses and drive improvements. Perhaps a national cybersecurity development model and rating system could be created, analogous to the Capability Maturity Model (CMM) in the IT industry, to measure the status of national cybersecurity protection and resilience.

3.6 A comprehensive cybersecurity strategy should include the following actions:

— strong EU leadership that puts in place the policies, laws and institutions to support high levels of cybersecurity across the Union,

— cybersecurity policies that enhance individual and collective security while preserving citizen rights to privacy and other fundamental values and freedoms,

— high awareness among all citizens of the risks of using the internet, and the encouragement of a proactive approach to protecting their digital devices, identities, privacy and online transactions,

— comprehensive governance by all Member States to ensure that critical information infrastructures are secure and resilient,

— informed and responsible action by all businesses to ensure that their ICT systems are secure and resilient, to protect their operations and the interests of their customers,

— a proactive approach by ISPs to the protection of their customers from cyberattacks,

— a deep partnership approach to cybersecurity across the EU between governments, the private sector and citizens, at strategic and operational levels,

— a design-led approach to build-in cybersecurity when developing internet technologies and services,

— adequate levels of investment in cybersecurity knowledge and skills development to grow a strong cybersecurity workforce,

— good technical cybersecurity standards and sufficient investment in R & D & I to support the development of a strong cybersecurity industry and world-class solutions,

— active international engagement with non-EU states to develop a coordinated global policy and response to cybersecurity threats.

4. **Specific comments**

4.1 Building on the cybersecurity governance framework outlined in the NIS Directive and the further measures now included in this Communication, the EU should consider addressing the fragmented approach to improving cybersecurity across the Union by creating a strong centralised cybersecurity authority, analogous to the European Aviation Safety Agency (EASA) or the Federal Chief Information Security Officer recently created in the USA (Cybersecurity National Action Plan, White House 9 February 2016), with responsibility for overseeing the implementation of cybersecurity policy at EU-level and integrating the efforts of the various agencies working in this domain.

4.2 The Committee is impressed by the competency that ENISA has developed over the years and we believe that it could contribute even more to Europe’s cybersecurity resilience and security. The operational mandate of ENISA should be strengthened to more effectively increase cyberattack threat awareness and response across the Union. A review of the mandate is timely, given how the cybersecurity environment has changed since ENISA was established. Building on the NIS Directive, perhaps the operational role of ENISA could be expanded to increase the value it can deliver to the EU, Member States, citizens and companies, by leveraging its competencies and synergies with the work of other EU and MS institutions, agencies and bodies, like CERT-EU, the European Cybercrime Centre and the European Defence Agency. ENISA should also be given more direct responsibility for cybersecurity education and awareness programmes specifically targeted at citizens and SMEs.

4.3 When the European Cybercrime Centre (EC3) was created in 2013, it only had an operational budget of EUR 7 million, less than 10 % of the total Europol budget (European Commission Memo/13/6 of 9 January 2012). In 2014, the Director of EC3 said that cutbacks had severely limited the resources allocated to his unit and that they were struggling to keep up with the rapidly evolving cybercrime threats (Security Magazine, 1 November 2014). The EESC believes that the resources allocated to Europol to fight cybercrime need to be significantly increased to keep-up with the evolving threat. The 2016 Europol budget is still only EUR 100 million [4].

4.4 The Committee welcomes the provisions in the NIS Directive and the actions proposed in the communication aimed at improving cybersecurity cooperation between MS. For the security of all citizens and to achieve strong cyber resilience across the EU, where critical infrastructure information systems are often interconnected, it is important that the cooperation measures address the growing divide between the countries with the most advanced cybersecurity competencies and those other MS with less developed competencies.

Brussels, 14 December 2016.

The President
of the European Economic and Social Committee
Georges DASSIS

[4] OJ C 113, 30.3.2016, p. 144.