European Economic and Social Committee

INT/930
Cybersecurity strategy

OPINION

European Economic and Social Committee

Joint communication to the European Parliament and the Council

The EU's Cybersecurity Strategy for the Digital Decade
[JOIN(2020) 18 final]

Rapporteur: **Philip VON BROCKDORFF**

Referral	European Commission, 21/04/2021
Legal basis	Article 304 of the Treaty on the Functioning of the European Union
Section responsible	Single Market, Production and Consumption
Adopted in section	31/03/2021
Adopted at plenary	27/04/2021
Plenary session No	560
Outcome of vote (for/against/abstentions)	238/0/3

1. Conclusions and recommendations

1.1 The European Economic and Social Committee (EESC) considers the proposed strategy as a positive step towards protecting governments, citizens and businesses across the EU from global cyber threats, and safeguarding economic growth.

1.2 The EESC is of the view that additional funding resources need to be made accessible to state entities to enable investments in cybersecurity infrastructure to respond effectively to a crisis such as a pandemic.

1.3 The proposals to build a network of Security Operations Centres (SOCs) across the EU, and for the European Union Agency for CyberSecurity (ENISA) working with all stakeholders to limit risks posed by 5G, are welcomed by the EESC.

1.4 The EESC also welcomes the proposal to further develop Europol's role as the centre of expertise on cybercrime. Cooperation with the multi-stakeholder community as well as at international level are also deemed important.

1.5 The EESC cautions about the skills gap in cybersecurity, and recommends a EU-wide Cyber Security Career Pathways Tool that helps individuals identify, build and navigate a relevant career path.

1.6 The EESC highlights the issue of disinformation. Spreading disinformation could have serious consequences and preventing disinformation should form part of any strategy on cybersecurity.

1.7 The EESC recommends that any foreign investment in strategic sectors in the Union conforms with the EU’s security policy.

1.8 The EESC cautions about the advent of quantum computers and the risks they pose. Hence, the need for a transition to quantum-resistant or post-quantum cryptography.

1.9 The EESC recommends that the Commission's cybersecurity strategy be updated regularly but not less than every two years to respond effectively to future technologies and future risks.

1.10 Finally, the EESC highlights the importance of social dialogue in the design of cybersecurity policies that effectively protect individuals in the case of remote working and more general online activity.

2. European Commission's Communication

2.1 The objective of this Communication is to emphasise the EU's commitment to safeguarding an online environment providing the highest possible freedom and security, for the benefit of its citizens.

2.2 The Communication outlines the EU's vision in this domain, defining roles and responsibilities, and proposes specific activities at EU level aimed at providing robust and effective protection whilst safeguarding citizens' rights so as to make the online environment safe and secure.

2.3 The actions proposed aim to:

- achieve cyber resilience, by increasing capabilities, preparedness, cooperation, information exchange and awareness in the field of Network and Information Security, for public and private sectors and at national and EU level;
- standardise process sequences for cyber defence across the Union as well as building up a database containing relevant information to provide threat intelligence in support of the affected sector or economy;
- drastically reduce cybercrime by strengthening the expertise of those in charge of investigating and prosecuting it, by adopting a more coordinated approach between law enforcement agencies across the Union, and by enhancing cooperation with other actors;
- establish EU-wide education and certification for professionals that meet the requirements of qualified cybercrime experts evolving into a Union-wide coherent skill level;
- develop an EU cyber defence policy and capabilities in the framework of the Common Security and Defence Policy;
- foster the industrial and technological resources required to benefit from the Digital Single Market. This will help stimulate the emergence of a European industry and market for secure ICT; it will contribute to the growth and competitiveness of the EU economy; and it will increase public and private spending on cybersecurity Research and Development (R&D);
- enhance the EU's international cyberspace policy to promote EU core values, to define norms for responsible behaviour, to advocate for the application of existing international law in cyberspace and to assist countries outside the EU in building cybersecurity capacity; and
- develop and implement an EU security seal of approval for products, services and technologies that meet the standards and requirements for cyberproof solutions.

2.4 The proposed strategy covers the security of essential services such as hospitals, energy grids and railways and the ever-increasing amount of connected equipment in our homes, offices and factories, building collective capabilities to respond to major cyberattacks and working with partners around the world to ensure international security and stability in cyberspace.

2.5 Since cybersecurity threats are almost always cross-border, and because a cyberattack in one country can affect either a group of Member States or the EU in its entirety, the Commission also proposes setting up a Joint Cyber Unit so as to provide the most effective response to cyber threats using the collective resources and expertise available to the EU and Member States.

2.6 The EUR 2 billion strategy will be funded under the EU's Digital Europe Programme and Horizon Europe, with investments from Member States and the private sector to be added.

3. General comments

3.1 Today, cybersecurity is universally accepted as an integral part of the functioning of the EU institutions and agencies, and of each Member State and its economy. Cybersecurity is crucial to support the Union's energy infrastructure and smart grid deployment[1], and the digitalisation and greening of EU economies. Equally as important is the protection and safeguarding of citizens' fundamental rights and freedoms guaranteed by cybersecurity. Safeguarding rights and freedoms is particularly relevant since cyberattacks could adversely affect citizens and households (as well as businesses, organisations and public services). The recent computer attack at a hospital centre in Tournai, Belgium, is an example of a threat posed not just to physical assets but human life too because of the postponement of surgical operations[2].

3.2 According to DIGITALEUROPE[3], cyber threats present a major obstacle to Europe's path to prosperity. Worldwide, the economic loss due to cybercrime was estimated to reach EUR 2.5 trillion by the end of 2020, and 74% of the world's businesses can expect to be hacked in 2021. Despite this, only 32% of European businesses have cybersecurity policies. Clearly and inevitably, cyber threats require a coordinated EU response and a cybersecurity strategy capable of both meeting current challenges and defending organisations and citizens from the next generation of cyber threats. This applies especially within public services where vast amounts of personal and sensitive data is managed and which need to be protected. Furthermore, the path to European data sovereignty and maintaining data confidentiality within the Union needs to be strengthened via cyber and digital resilience, which in turn will enhance prosperity within the EU.

3.3 The potential economic losses arising from cyberattacks are huge and include:

- the loss of intellectual property and confidential business information;
- online fraud and financial crimes, often the result of stolen personally identifiable information (PII);
- financial manipulation, using stolen sensitive business information on potential mergers or advance knowledge of performance reports for publicly traded companies;
- opportunity costs, including disruption in production or services, and reduced trust for online activities;
- the cost of securing networks, such as buying cyber insurance[4], and paying for recovery from cyberattacks; and
- reputational damage and liability risk for the hacked company and its brand, including temporary damage to stock value.

1 A cyberattack on a smart grid could impact energy supply to consumers and businesses.

2 https://www.databreaches.net/chwapi-hospital-hit-by-ransomware-operations-canceled-and-another-city-hit/

3 https://www.digitaleurope.org/.

4 Cyberinsurance of course is not in unlimited supply. COVID-19 has actually highlighted the fact that the accumulation of risks is a challenge to insurability. Recent work by AON support the claim that insurance is only a very minor (5%) part of expenses in cyberreadiness. Auditing and training were found to be the more important determinants of cost.

3.4 It is relevant to note that Europe suffers the highest economic impact of cybercrime, which is estimated at 0.84% of the EU's GDP, compared with 0.78% in North America, according to the latest report on the economic impact of cybercrime by the Center for Strategic and International Studies (CSIS).

3.5 Against this background, the proposed strategy, which follows a period of extensive consultations with stakeholders, could not have come at a better time with experts predicting that the number of connected devices around the world will rise to 25 billion by 2025. A quarter of these devices are expected to be in Europe.

3.6 The announcement of the strategy coincided with computers at US federal government agencies being reportedly compromised by a cyberattack targeting a US company that develops software for businesses to help manage their networks and IT systems. Hundreds of US corporations were also vulnerable to the attack, in which malware was added by hackers to a software update that was downloaded by thousands of clients of the affected US company. This incident shows how public administrations, businesses across all sectors and society as a whole, could be at risk of cyberattack.

3.7 Not surprisingly, key sectors are coming under the scope of the strategy: they include data and cloud service providers, telecommunications, government IT systems, and manufacturing. Other relevant examples where cybersecurity threats could arise include contact tracing apps such as those being applied in response to COVID-19. Securing contact tracing apps obviously helps to increase public trust and confidence in the protection of private data with regard to COVID-19 measures deemed vital in response to the pandemic.

3.8 The COVID-19 pandemic has accelerated a change in working patterns with as many as 40% of EU workers having switched to remote locations in 2020[5]. However, an estimated 40% of EU users experienced security-related issues in 2020 with over 12% of businesses affected by cyberattacks.

4. Specific comments

4.1 The EESC considers the proposed strategy as a step in the right direction towards protecting governments, citizens and businesses across the EU from global cyber threats and providing leadership in cyberspace, while also ensuring that everybody can reap the benefits of the internet and the use of technologies.

4.2 The EESC considers cybersecurity to be essential to safeguard economic activity and enhance economic growth, as well as to ensure user confidence in online activities. It also agrees that bold steps are needed to ensure that Europeans can benefit securely from innovation, connectivity and automation.

4.3 The EESC acknowledges that, increasingly, the EU's economic sectors are becoming more digitally dependent and interdependent. There has also been a huge expansion in the use of

5 Eurofound (2020), Living, working and COVID-19, COVID-19 series, Publications Office of the European Union, Luxembourg.

Internet of Things (IoT) devices by consumers and businesses, as well as in industrial settings such as manufacturing, while FinTech and RegTech have also permeated into the mainstream. The rollout of 5G has picked up speed and, most recently, the COVID-19 crisis has accelerated the digital transformation of many companies and governments, forcing them to conduct business remotely almost overnight, largely leveraging cloud-based services. Such developments require an effective, speedy and inclusive cybersecurity response.

4.4 These changes have increased the level of critical risk to governments and industry. The EESC therefore supports the new cybersecurity strategy and its range of proposals to improve cyber resilience both in the EU and externally. Though public entities are eligible for EU funding under the various relevant programmes that support investments in this area such as Horizon 2020/Horizon Europe, the EESC is of the view that further funding opportunities may be required to publicly or partially publicly owned entities, to enable investments for an adequate cybersecurity infrastructure to ensure security of supply for citizens especially in a time of crisis such as during a pandemic.

4.5 The European Commission's proposal to build a network of Security Operations Centres (SOCs) across the EU that would leverage Artificial Intelligence (AI) and machine learning to improve threat and incident detection, analysis and response speeds is important and timely. The EESC recognises that preventing successful cyberattacks manually is becoming more difficult, due to the overwhelming number of daily alerts for security teams to deal with, coupled with the general shortage of specialised workers within the field. All this makes the automation of SOCs inevitable.

4.6 The EESC welcomes the objectives and actions on 5G security, which will be imperative to help mitigate new risks stemming from the growing attack surface that 5G network infrastructures will create. The EESC in particular supports the call for the European Union Agency for CyberSecurity (ENISA) and Member States to work with all stakeholders to better understand new 5G security technologies and capabilities as well as threats. It is evident that the strategy acknowledges that 5G's utilisation of new technologies like network virtualisation, network slicing and edge computing are particularly prone to specific vulnerabilities that require additional security measures.

4.7 The EESC also welcomes the proposal to further develop Europol's role as the centre of expertise on cybercrime to support national law enforcement authorities, as well as increased funding and a stronger mandate for CERT-EU. Both entities play critical roles in supporting cybersecurity efforts throughout the EU. These efforts will no doubt help improve the cybersecurity of EU institutions and agencies and beyond.

4.8 The EESC commends the emphasis within the strategy on the EU's international cooperation, such as via cyber diplomacy in international relations, increased bilateral dialogues on cybersecurity, and cyber capacity-building in third countries. Cybersecurity threats are global and not just regional, and effective policies to counter them must also be global.

4.9 The EESC also notes that the importance of dialogue and cooperation within the multi-stakeholder community, notably by regular exchanges with the private and public sectors, the

social partners and academics, is emphasised in the strategy. This approach is welcome and will be essential to further developing the proposals contained in the strategy and to addressing important developments such as the security challenges posed by remote working. The input of all relevant stakeholders should be ongoing as the level of technology used in cybercrime becomes more sophisticated.

4.10 The EESC welcomes the emphasis placed on developing relevant skills protecting against cyber threats generally. However, for the majority of European companies and especially SMEs, the growing skills gap remains a huge problem against cybersecurity threats. The EESC believes that this skill gap can only be addressed through an EU-wide Cyber Security Career Pathways Tool that helps individuals identify, build and navigate a potential career path in cybersecurity by increasing understanding of the knowledge, skills and abilities needed to begin, transition or advance a cybersecurity career. This tool should also include specific programmes which address accessibility and diversity in the cybersecurity space. The role of Vocational Education and Training (VET) institutions is deemed critical to support an EU-wide Cyber Security Career Pathways Tool. Moreover, the EU should increasingly be looking to joint research initiatives (within the EU and beyond) to produce skilled and qualified cybersecurity professionals in an inclusive manner, given the evolving role technology plays in creating a more inclusive workplace and society. Finally, encouraging students to enter cybersecurity degree studies by providing scholarships for bachelors, masters and graduate degrees focusing on cybersecurity, in return for service in EU institutions and agencies as well public services across the EU upon graduation, should be actively considered.

4.11 The EESC notes that one aspect that has not been addressed in the Cybersecurity Strategy is the connection between cybersecurity and disinformation. Specifically, the EESC refers to the study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs[6]. In the era of internet cyberspace, spreading disinformation could have serious consequences. Cross-border attacks can target information centres, governmental or European institutions to spread disinformation and such attacks could also reduce trust in public authorities. Hence, the need to place emphasis on preventing disinformation in any strategy on cybersecurity.

4.12 The EESC also notes that foreign investment in strategic sectors, acquisition of critical assets, technologies and infrastructure in the Union and supply of critical equipment may also pose risks to the EU's security. In this regard and in accordance with existing rules on public procurement, the EESC recommends that security considerations be given more weighting when awarding contracts.

4.13 The EESC also notes that the security of current cryptographic software and systems is undermined by the advent of quantum computers, which are expected to be publicly available in a decade or less. This motivates the need for a transition to quantum-resistant or post-quantum cryptography. This is witnessed by worldwide initiatives for the standardisation of post-quantum cryptographic schemes, such as the US NIST Post-Quantum Cryptography Standardisation Process, the European Telecommunications Standards Institute (ETSI) working

6 https://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf.

group on Quantum-Safe Cryptography and the Chinese Association for Cryptologic Research Post-Quantum Cryptography Competition.

4.14 The EESC recommends that national cybersecurity strategies be revised to ensure consistency with the Commission's strategy and to ensure that decisions taken at Member State level converge with the proposals contained in the Commission's strategy. The EU-wide strategy as well as national strategies should converge to deal with cyber threats effectively today and in the future.

4.15 Because future risks are largely unpredictable and with reference to 4.13 above, the EESC recommends that the Commission's cybersecurity strategy be updated regularly but not less than every two years to respond effectively to future technologies and future risks. As stated earlier, stakeholders' involvement and high-level research will also be critical in updating cybersecurity strategies.

Brussels, 27 April 2021.

Christa SCHWENG
The president of the European Economic and Social Committee