Cybersecurity for a stronger and more resilient digital Europe

An IEEE European Public Policy Committee Position Statement

Adopted 10 December 2020

Over the past few years, the European Union (EU) has proposed a wide range of measures to enhance the protection of its citizens and businesses against cyber attacks and to equip Europe with the tools necessary to deal with ever-changing cyber threats. In addition to the Directive concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) of July 2016[1], the European Commission adopted a cybersecurity package in September 2017 with proposals to further strengthen the EU's resilience and response to cyber attacks[2], along with the Cybersecurity Blueprint to respond effectively to large scale cybersecurity incidents[3]. These initiatives were more recently strengthened by the Cybersecurity Act[4], which has reformed the European Union Agency for Cybersecurity (ENISA) and enshrined in law EU cybersecurity certification frameworks; the NIS Toolkit[5] to implement the NIS Directive; and the proposed European Cybersecurity Industrial, Technology and Research and Competence Centre[6] to build and promote stronger cyber awareness and hygiene, skills base, and research and innovation actions. The European Commission's President von der Leyen has also proposed the establishment of a Joint Cyber Unit to promote a more centralized cybersecurity approach.

While these actions are commendable, the EU still needs more agile structures to coordinate and respond to cyber-attacks, more robust procedures to ensure stronger cyber protection and resilience, new standards and certification schemes for the cybersecurity of products, services and processes, and advanced skills and technologies to keep up with the evolving nature of cyber threats.

Recommendations

As the EU continues to implement the 2017 Cybersecurity Package and the recently-adopted EU Security Union Strategy for the period 2020 to 2025[7], and prepares for the new EU cybersecurity strategy and review of the NIS Directive, the IEEE European Public Policy Committee (EPPC), representing a large community of European engineering professionals, offers recommendations intended to support a stronger and more resilient digital Europe.

In particular, the IEEE EPPC recommends that the EU:

1. Strengthen cyber resilience and response to cyber attacks;
2. Rationalise the European cybersecurity regime into a common framework;
3. Support the development of effective cybersecurity certification schemes;
4. Facilitate regulatory compliance by stakeholders;
5. Promote cybersecurity education, awareness, and 'hygiene' habits;
6. Support research and innovation in cybersecurity.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017H1584&from=EN
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505297631636&uri=COM:2017:476:FIN
[6] https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018PC0630 and https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2018/0328(COD)&l=en
[7] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from=EN

These six main lines of action and the proposed measures included therein are described in greater detail in the following sections, together with the rationale, purpose and benefits associated with each proposed recommendation.

Rationale and discussion

1. Strengthen cyber resilience and response to cyber attacks

Cyber resilience is the ability to prepare for, respond to, and recover from cyber attacks. It helps protect electronic data and systems against cyber risks, limit the severity of incidents, and ensure the continuity, or quick resume, of operations during and after a successful attack. Strengthening resilience is part of the EU overarching objective to guarantee an open, stable and secure cyberspace[8] and is a way to increase the EU's capacity to deal with the negative consequences of cyber attacks and to reduce the risk of miscalculation and eventually overreaction. In recognizing the need to strengthen the cyber resilience of EU infrastructure as the foundation for economic and human development, as well as for proper functioning of states and societies, the EPPC encourages the EU to focus on internal resilience initiatives, especially those revolving around measures such as cybersecurity capacity building (e.g., cyber early warning systems, task forces and rapid response teams, and swift information-sharing, etc.).

In this regard, the EPPC specifically recommends that:

- The EU develop a cyber early warning system that, leveraging tools such as AI, collects data from Cyber Security Incident Response Teams (CSIRTs), public internet, dark web, industrial control systems in order to observe, anticipate and prepare for, or prevent, incoming attacks. To be effective, such an early warning system must collect data from different sources and in different formats; make real-time analysis to produce accurate and relevant information, while complying with all obligations related to privacy and personal data protection; be distributed amongst all EU Member States, yet allowing a central entity to calculate correlations, analyse big data, and send warnings to EU Member States that are likely to be under threat. The entire system could be built and modelled, to the greatest extent practicable, on the MeliCERTes, the facility used by the CSIRTs in the EU to cooperate and exchange information. Importantly, it shall be seen as one of the European digital capacities that contributes to establishing digital sovereignty and, as such, be included in the related forthcoming digital policy initiatives and possible regulatory actions.

- The EU develop an harmonised approach to information sharing, notifications and reporting through the integration of existing EU Member States sharing platforms (e.g., Malware Information Sharing Platform (MISP)) covering products, services and processes. Sharing information about cyber threats is already beginning to take place in the context of the NIS Directive and the Cyber Security Act. A swift information exchange mechanism between all key players at the national and EU level is essential to effectively counter cyber attacks, since it allows for better understanding of cyber threats and future risks (such as the intentions and capabilities of attackers), as well as an increased likelihood of detecting or directly defending against attacks. In addition to strengthening cyber attack mitigation and response capabilities, a harmonized approach to information sharing has other important benefits including enhancing collective knowledge and effective collaborations and reducing cybersecurity investments.

European effectiveness in pushing forward cyber resilience can also be enhanced if resiliency measures, such as those described above, are publicly known, since their disclosure may convince threat actors that their malicious actions are unlikely to inflict the desired damage.

[8] See the 2013 EU Cybersecurity Strategy, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN

2. Rationalise the European cybersecurity regime into a common framework

The primary responsibilities for cybersecurity remain with Member States, but the EU has become a key framing actor. It acts as a policy maker, legislator, regulator, coordinator of Member States' actions, sponsor of funding initiatives, and customer. However, cybersecurity files and dossiers are split between a number Commissioners (e.g., Margrethe Vestager, Josep Borrell, Thierry Breton, Mariya Gabriel, Ylva Johansson), EC Directorates-General and Service Departments (e.g., CERT-EU, CONNECT, DEFIS, DEVCO, GROW, HOME, JRC, RTD), including the EEAS, and Agencies (e.g., EDA, ENISA, EUROPOL, REA), with roles, responsibilities and tasks of all parties concerned being not always clear[9]. Therefore, there is an urgent need for better coordination at all levels in order to minimise duplication, be able to respond effectively, and exploit synergies. The complex governance of European cybersecurity activities will not be easily streamlined into a common framework anytime soon. But with a common vision and good communication, drastic changes are not necessarily required in order to pursue effective action on cybersecurity. The IEEE EPPC recognises that overcoming national sovereignty worries over common EU policymaking requires building trust among all institutional actors and believes that this can be facilitated through making European cooperation central to each Member State's cybersecurity strategy.

For moving forward on this, the IEEE EPPC:

- Supports the Commission President's plan to establish a Joint Cyber Unit in order to guarantee a more centralized cybersecurity approach in the European Union, and recommends that this Joint Cyber Unit be responsible for all cyber security dossiers and includes the Commission, EEAS and other relevant parties in order to tackle the current fragmentation of the EU cybersecurity landscape.

- Suggests that the European Commission puts forward appropriate measures to prevent and reduce additional fragmentation at the national and regional level, with a view to also avoiding the creation of non-optimal collaborative strategies amongst regions and EU Member States. This can be achieved, whereas applicable, by aiming for and working towards regulations rather than directives, including through transforming the NIS Directive into a Regulation. These measures need to consider both the strategic level related to the technical elements involved in a sound continental approach to cybersecurity (e.g., network standards, speed to coordinated responses to attack), as well as the tactical level, stimulating local businesses (e.g., SMEs, start-ups) to develop European solutions that organically comply with EU requirements. The Israel National Cyber Directorate[10] and the US Department of Homeland Security[11] can serve as examples. Both actively support and strengthen their own cyber ecosystems, involving businesses and local authorities in order to develop innovative solutions that enhance their national cybersecurity.

3. Support the development of effective cybersecurity certification schemes

Cybersecurity certification is the formal attestation that ICT digital products, services and processes comply with specified requirements. In particular, cybersecurity certification schemes provide criteria to conduct conformity assessments that establish the degree of adherence of certain products, services and processed against a comprehensive set of rules, standards and procedures. As such, certification provides assurance to users about the level of conformity and plays an important role in establishing and maintaining an adequate level of trust and security in products, services and processes that help realize the Digital Single Market. There are currently different security certification schemes for ICT products in Europe. But without common EU-wide valid cybersecurity certificates, the risk of fragmentation and barriers remains high.

[9] See also https://www.enisa.europa.eu/news/enisa-news/do-you-know-who-is-who-in-eu-cybersecurity
[10] https://www.gov.il/en/departments/israel_national_cyber_directorate
[11] https://www.dhs.gov/topic/cybersecurity

In the wider framework of the EU Cybersecurity Act and of the legal basis it provides, the IEEE EPPC recommends that:

- Impact assessment of any new certification scheme be conducted in order to assess the pros and cons associated to the proposed certification scheme, as well as to clarify which products, services and processes are specifically covered by the proposed certification scheme. This will benefit businesses, industries and stakeholders alike, as they would avoid going through diverse certification processes.

- Certification be lightweight and cost effective, avoiding excessive burden so as to facilitate buy-in and widespread adoption. This can be achieved by establishing cybersecurity certification schemes based on existing standards, and where these are not available, through the development of new standards in the context of the existing standardisation system. Semi-automated procedures for cyber security (re)-certification can ensure the scalability of the process. Harmonized baseline requirements for cybersecurity certification schemes of lower assurance levels would significantly reduce the deployment of insecure items (e.g., products, services and processes) in the EU market.

- To facilitate the implementation of a Certification Framework (as called for the Cyber Security Act), appropriate consideration be given, inter alia, to the lifetime of a certification, procedures for suspension or revocation, certification authorities located outside of the EU, product software updates and patches, and burden placed upon all stakeholders (e.g., vendors, certification authorities, etc.).

- A harmonized approach to cybersecurity risks in 5G (including, but not limited to, exposure of critical infrastructure to advanced persistent threats) be developed to foster widespread 5G adoption. Consensus would be needed among industry (e.g., network and terminals vendors), operators and policy-makers in order to identify a common set of requirements to be considered towards cybersecurity certification of 5G systems in the EU.

- To systematically increase common understanding of all cybersecurity risks across the EU, the creation of a common European vulnerability database be fostered, especially in domains such as IoT, where cyber threats are continuously increasing. Benefits from such a database can be significant as the size of the actual sharing network becomes sufficiently large.

4. Facilitate regulatory compliance by stakeholders

Regulatory compliance describes the process and steps that organizations and individuals alike follow in order to adhere to national or regional laws, policies and regulations relevant to their operations. With the cybersecurity (and privacy) regulatory environment constantly evolving and growing, achieving compliance has become a difficult target. This issue is widely acknowledged especially by small businesses, which comprise most of the European industrial structure, for which compliance with the evolving cybersecurity regime has become all of the more difficult. To systematically facilitate regulatory compliance by stakeholders, effective guidance by EU institutions would be instrumental in helping navigate complexity, as resulting from the NIS Directive, GDPR and Cyber Security Act.

In this regard, the IEEE EPPC encourages the EU to:

- Develop a Maturity Assessment Framework[12] to help organizations conduct efficient gap analysis in terms of both compliance with specific regulations, and security controls and procedures. A semi-

[12] George Drivas, Argyro Chatzopoulou, Leandros Maglaras, Costas Lambrinoudakis, Allan Cook and Helge Janicke, "A NIS Directive compliant Cybersecurity Maturity Model", IEEE Computer Society Signature Conference on Computers, Software and Applications (COMPSAC 2020), 13-17 July 2020.

automated software that checks against all relevant cybersecurity regulations applicable to different sectors (e.g., energy, aviation, healthcare, public administrations, etc.) can be a valid supporting tool to the implementation of the Framework. Moreover, the Framework will help the EU prioritise cybersecurity mitigation plans that need to be implemented at the European level in terms of funding of specific actions and launching new security tools.

5. Promote cybersecurity education, awareness, and 'hygiene' habits

There are strong human and education dimensions to cyber security. For example, human error, be it intentional or not, continues to be the primary source of cybersecurity incidents. Moreover, despite the growing threat, the cybersecurity workforce gap is still very high. In 2019 alone, the cybersecurity skill gap[13] in Europe was 291,000, a value that almost doubled compared to 2018[14]. Cybersecurity is everyone's responsibility, and it is critical that all organizations and individuals understand cyber threats and behave accordingly. The European Commission is therefore encouraged to launch initiatives (e.g., ETEE platform[15]) intended to ensure that businesses and organisations adopt risk-based cybersecurity programmes; that an adequate number of highly-skilled cybersecurity specialists and professionals are educated and trained; and that individual citizens increase their awareness of cyber risks and develop cyber 'hygiene' habits.

In this regard, the IEEE EPPC recommends that:

- ENISA gather a general overview of existing mechanisms of how cybersecurity and digital skills are acquired in EU Member States. On this basis, the European Commission should develop a Strategy and Action Plan containing specific supporting and coordinating measures to help Member States build a strong EU cyber skills base, including through addressing cybersecurity education and awareness at all levels, from industry stakeholders (especially SMEs) to educational establishments and individual citizens. Specific measures should be aimed at addressing the significant gender gap in this technical field and at fostering inclusive education and hiring policies.

- The European Commission propose an assessment framework for implementation by Member States with a view to recognising Academic Centres of Excellence in Cyber Security for both education and research. This framework may be similar to the ones developed by the UK National Cyber Security Centre (NCSC) for higher education institutions[16,17]. This assessment process can help identify universities that meet specific criteria and also create a pool of academic staff that is engaged in advanced cyber security teaching and research.

- The European Commission coordinate the efforts of Member States aimed at raising awareness of the cyber threats and risks faced by citizens when using digital tools and applications. Citizens need to be trained towards a cybersecurity hygiene culture, including through receiving the tools and skills necessary to detect and protect themselves against cyber attacks, to safeguard their digital devices, and to correctly follow best practices. This also requires introducing new specific cybersecurity curricula at schools to also make it natural for the professionals of tomorrow to design digital products that incorporate security standards from the outset.

[13] The cybersecurity skills gap is the difference between cybersecurity skills that employers want or need, and skills their workforce offer.

[14] https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482

[15] https://www.eda.europa.eu/info-hub/press-centre/latest-news/2018/11/20/cyber-education-training-exercise-and-evaluation-(etee)-platform-launched

[16] https://www.ncsc.gov.uk/information/academic-centres-excellence-cyber-security-research

[17] https://www.ncsc.gov.uk/blog-post/launch-of-the-academic-centres-of-excellence-in-cyber-security-education

6. Support research and innovation in cybersecurity

Developing and retaining the research and innovation capacity necessary to ensure an adequate level of technological and digital sovereignty needs to be a top priority for Europe. Institutions, industry players, innovative start-ups, research and development facilities, and universities play all a significant role in boosting the EU's ability to compete on the global market and reduce its dependence on non-European suppliers. Research and innovation is indeed a shared responsibility, with public sector organizations funding long-term and high-risk research and innovation actions, and private sector organizations focusing on short-term research and translating research results into technologies and practices. The IEEE EPPC therefore strongly endorses the creation of the European Cybersecurity Industrial, Technology and Research Centre and of the Network of National Coordination Centres in order to drive cybersecurity research and innovation.

To further stimulate research, development, innovation and deployment of cybersecurity technologies, and increase EU's autonomy, competitiveness and cybersecurity resilience, the EPPC welcomes the European Commission's initiatives to:

- Increase the number of innovation programmes, encourage the creation of research and development centres and facilities, and increase the number and size of funding opportunities, including through appropriately increasing funding in the context of the Horizon Europe and Digital Europe programmes. There would be great value if interdisciplinary research would continue to be promoted, with EU calls encouraging the submission of multidisciplinary proposals. Today's cybersecurity landscape goes beyond the purely science and technology domains, and includes social, psychological and economic factors that need to be appropriately integrated.

and recommends that the European Commission:

- Accelerate the transition from cybersecurity research into cybersecurity technologies and products. This can also be facilitated through fostering the development of an ecosystem of innovative start-ups in the cybersecurity sector. All of this should become a policy priority in order to face the competitive pressure from other regions of the world.

This statement was developed by the IEEE European Public Policy Committee (EPPC) Working Group on ICT and represents the considered judgment of a broad group of European IEEE members with expertise in the subject field. IEEE has nearly 60,000 members in Europe. The positions taken in this statement do not necessarily reflect the views of IEEE or its other organizational units.

Contact Information

Should you want to get in touch with the IEEE European Public Policy Committee or find out more about its activities, please go to http://www.ieee.org/about/ieee_europe/index.html

About IEEE

IEEE, with more than 419,000 members in over 160 countries, is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity. It publishes 150 prestigious journals, organizes more than 1,800 conferences in 95 countries annually, has led the development of over 1,200 consensus-based global standards, and supports science and engineering education at all levels. IEEE has members in every European country, and over 200 European organizational units. The IEEE European Public Policy Committee provides opportunities for engineers and scientists from across the continent to share their expertise in the development of sound technology policies.