January 2018

ETNO’s Position on the EU’s Cybersecurity Package

ETNO welcomes the proposals of the European Commission for a review of the EU’s Cybersecurity Strategy as a timely and important progress to address the threats to the European Digital Single Market. The 2013 European Cybersecurity Strategy was a fist attempt towards a comprehensive EU answer on cybersecurity, which remains primarily the responsibility of Member States.

The proposed Cybersecurity Package should be a major contribution to enhanced trust and confidence of consumers and businesses in the digital era. The digitization of the European and global economy is advancing rapidly, and the threat landscape for the digital environment is growing at an ever faster space. If the basic pillars of the 2013 Strategy still apply, they need to be reviewed in light of the technological, legislative and international developments including the fight against the cybercrime.

ETNO members support the Commission’s policy objectives to raise the cybersecurity competencies of the EU, in order to achieve a secure and performant Digital Single Market.

The EU Network and Information Security (NIS) Directive has been a significant step towards a more harmonized European answer to cyber threats. However, the NIS-directive was in proposed in 2013, adopted in 2016, and is due for national implementation in 2018. This legislation risks being outdated once transposed into national law, as it does not reflect the evolution of the digital economy and its value chain, especially the rapidly evolving Internet of Things (IoT) world. Therefore, the review of the implementation of the NIS-Directive should take into account contemporary challenges and the ever changing threat landscape in cyber security.

EU Cybersecurity Certification Framework

In today’s connected society, vulnerabilities can be found at every stage of the digital value chain. The use of connected devices is increasing exponentially, in particular the number of IoT devices, which could be used as attack vectors. Service and product manufacturers must also be required to minimize vulnerabilities and lower the risk of their products by applying minimum standards – obligations which have already been in place for infrastructure operators for a long time.

The initiative of an EU Cybersecurity Certification Framework is a positive step in the completion of a Digital Single Market in cybersecurity products and services. ETNO supports a risk-based approach that affords companies with enough flexibility to effectively identify and mitigate their own risks. When it comes to IoT devices, where the objective is to substantially raise the security standards, minimum levels of safeguards at EU level are needed to guarantee the required security levels and legal certainty for companies operating across the EU.

Therefore, it is important that any future EU Cybersecurity Certification Framework considers some basic criteria:

- Any certification schemes should build upon what already exists at national and international level, learning from current strong points and assessing and correcting weaknesses.
- EU cybersecurity certification schemes need to respect the role of the Member States in the certification process in particular with regards to article 4.2 of the TEU[1] and introduce areas of exemption such as national security and activity sectors of vital importance in the Member State. These areas of exemption should be under the sole responsibility of Member States and their concerned national security agencies.
- The EU Cybersecurity Certification Framework is conceived to start on a voluntary basis, as proposed by the Commission. Depending on the maturity of implementation in EU Member States, in the future we may evolve towards potentially mandatory schemes for ICT products and services in a phased approach. Such schemes should be accredited by national accreditation bodies by default. This should reinforce the grounds for trust. The criticality of a product or service should determine the potential evolution towards mandatory certification and labelling.
- Certification schemes involve considerable costs and it is important not to create market barriers for companies due to high entry costs. A level playing field with the same security rules applying to all stakeholders will provide legal certainty and imply cost benefits.
- Flexible cybersecurity solutions are necessary for industry to stay ahead of malicious attacks, therefore any certification scheme should avoid the risk to be quickly outdated, as the nature of products and services as well as the magnitude of the cybersecurity risks will vary significantly and will change even more rapidly.
- It is of the upmost importance to reinforce the involvement of governmental institutions in response to the strategic nature of the cybersecurity in terms of financial and operational support for the development of cybersecurity solutions. In addition, public authorities should set a good example by integrating appropriate security requirements into their public procurement practices.
- The lack of skills in cybersecurity is serious shortcoming in the EU; therefore a coordinated action at EU level focused on investment in professional and educational training programs in universities and research centers would help the development of a skilled work force and human development.

[1] Article 4(2) TEU states that:
"[t]he Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State."

- The certification schemes should include selection, reference and possible support of existing and well-established security certification and accreditation schemes at different levels, from the end user who has received an awareness training to the certification of qualified personnel in management of incidents or vulnerabilities.
- Raising the security awareness of the public (i.e. users) is essential as security remains a “people business”. Sustainable and regular awareness campaigns from the public sector and wide social dialogue would benefit the creation of a real culture of security.

In the long run, “security by design” should become the guiding principle and security standards must be integrated at all stages of the product lifecycle. We would also support the introduction of the principle of “robustness” of a product or service, i.e. their ability to cope with errors during execution, erroneous or forged input, or attempts of breach, while sustaining acceptable conditions of operation and security.

The established CE-label could serve as a model, as long as such a model relies on delivering robustness, as opposed to guaranteeing conformity to functional or quality specifications. Different product groups could be defined depending on the criticality of the application or processed data or on the sensitivity of their usage, as well as taking into consideration the lifespan of the product and its ability to be upgraded and/or patched with security measures.

Particularly in the area of IoT security, standards should be adopted and harmonised on a European level. Similarly to the CE-label, at a later stage the Commission could assess the need to oblige manufacturers to provide a mandatory declaration of conformity with standards depending on the criticality of the products and services. In that case, the declaration should be submitted to third-party, independent auditing.

Finally, there should be transparency and communication on the activities of the EU Cybersecurity Certification Group. There should be formal consultation processes with representative stakeholders in the preparation of EU Cyber Security certification schemes.

ENISA Mandate

The revaluation of the role the agency is highly welcome by industry. ETNO believes that stronger public-private cooperation in cybersecurity should be the top priority. ENISA could play a key role to enhance and promote the common understanding among the different public and private stakeholders with the objective to attain specific implementable agreements. ENISA should be the catalyst with the objective to successfully transform agreements between various public and private stakeholders into realities.

With an enhanced budget and staff, ENISA should support the implementation of the NIS Directive, assume the tasks of operational coordination, and become a focal point for the sharing of information, knowledge and tools to combat threats among the different stakeholders. Additionally these capacities should not only be available for Member States, but also for the private sector. This would help companies to detect security breaches in outdated hardware or software, or even backdoors.

ETNO welcomes the fact that in the proposed "Cybersecurity Act", ENISA's mandate is pre-eminently supporting in nature. As such, ENISA will assist the Commission in the preparation of certification schemes, provide a secretariat for the 'Group' (National certification supervisory authorities), maintain the inventory of approved schemes and liaise with standardization bodies.

Research

Quantum computing is developing at a high pace. With this technology, computers will be able to calculate at a much higher rate than any digital device with current technologies. Quantum technology will be able to breach most forms of currently used encryption in minutes. As the integrity of communications is crucial for any defence force or private and public enterprise, it is of vital importance that the efforts of Member States and the Commission focus on this crucial issue. European cyber security sovereignty and digital autonomy depends on this.

The Commission suggests that quantum cryptography research could benefit from the European Defence Funds of €90 million until the end of 2019 and €500 million a year from 2020. These budgets are allocated in 2018 by the Commission. The €1 billion quantum flagship funding does not provide any post quantum encryption research.

The EU defence research program should make post quantum cryptography its top priority. The funding should be invested in Europe's top research institutions in cooperation with Member States, universities and EU businesses. It is of outmost importance to avoid fragmentation and uncoordinated efforts in this field within the EU.

Towards a more comprehensive Review of the EU's Cyber Strategy

As mentioned before, ETNO members call for additional steps, following a review of the NIS Directive's transposition in Member States, highlighting the Directive's possible shortcomings, improving the level of harmonisation across the EU, and ultimately raising the security level of the European digital economy.

If cybersecurity is to be a shared responsibility amongst all actors throughout the entire value chain, everyone has a role to play, from service and network providers to hardware and software manufacturers as well as public administrations and consumers. The revision of the Directive should notably include the following elements:

- Extension of the scope, including hardware and software manufacturers.
- Obligations to disclose security incidents to the relevant authorities to be extended to hardware and software manufacturers.
- Obligation to remedy vulnerabilities and to apply the "security-by-design" principle. Security updates must be made available for the period of the expected product lifecycle.

- Suppliers should provide information about vulnerabilities to customers, with a reasonable delay and according to the bulletin delivered to Computer Emergency and Response Team contact or equivalent.
- Such obligations should be based on several qualifiers based on severity, risk assessment, risk of public disclosure, consideration of technical ability to mitigate the vulnerability and risk imposed on the user population by disclosure should be put in place.
- Government authorities should also be included in the regulation in order to avoid the exploitation of vulnerabilities as backdoors by security agencies.

Measures to ensure hardware and software liability are deeply needed. Large quantities of hardware and software contain bad code that make these ICT products vulnerable to malware and hacking due to low quality programming. Critical updates to fix security issues sometimes takes months before they are released, leaving customers vulnerable to cyber threats for an unacceptable amount of time. A liability regime for hardware and software would then improve the quality and accelerate the release of critical updates.

The Commission has proposed a duty of care initiative to be developed with the industry to promote security-by-design, announcing ‘next steps’ by June 2018. ETNO urges that progress should be made as soon as possible and should include serious steps towards a hardware and software liability regime. The EU-directive 85/374/EEC should be extended to IoT devices.

Concluding remarks

Cybersecurity is based on networks, hardware, software and processes across the entire value chain. None of these elements should take priority over the others. The best technical features in final products are useless if they are not complemented by appropriate use implementation and organizational measures. Therefore, minimum, common security requirements must be applied and cover the entire digital value chain.

Any comprehensive EU policy on cybersecurity should enhance skills, education, training and awareness raising exercises. Adequate skills and training, related to preventing cybersecurity incidents and mitigating their impacts, are key to achieving a strong cyber resilience.

The EU needs to prepare to represent a strong voice in meeting the global political challenges in the context of cybersecurity.

ETNO (European Telecommunications Network Operators' Association) represents Europe’s telecommunications network operators and is the principal policy group for European e-communications network operators. ETNO’s primary purpose is to promote a positive policy environment allowing the EU telecommunications sector to deliver best quality services to consumers and businesses.

For questions and clarifications regarding this position paper, please contact Paolo Grassia grassia@etno.eu