May 2022

ETNO's response to the EC public consultation on cybersecurity of digital products and ancillary services – Cyber Resilience Act

ETNO welcomes the opportunity to provide complementary views to its response to the European Commission's (EC) public consultation on the cybersecurity of digital products and ancillary services.

Newer generations of connectivity and the maturing of 5G networks will enable the **rapid growth of the Internet of Things (IoT)**: the number of active IoT connections in Europe is expected to reach 352mn in 2023, up from 180mn in 2020, and is forecasted to exceed 850mn by 2029[1]. The surge in connected digital products will significantly increase the vulnerabilities and points of entry for cyberattacks, and the overall threat landscape for European citizens and most sectors of the economy.

In the telecommunication sector, the **shift to 5G** and to a virtualised, software-defined, and cloud-dependent infrastructure means that the networks and services of tomorrow will be delivered by an ecosystem of operators, vendors and providers, where important functions and control points will move closer to the end-user and will be outsourced from telecom providers to other actors in the value chain. Already today, a third of telecom security incidents in Europe are **third-party failures**, such as hardware malfunctions and software bugs[2]. The deeper interdependence of providers and third parties in the 5G architecture will expand the attack surface of the network.

For operators of critical infrastructure such as ETNO members, it is paramount to ensure network and service resilience through a **better allocation of responsibility for cybersecurity along their value chain**. Vendors of digital products that become an integral part of the critical services delivered to end-users are often best placed to manage their own vulnerabilities, and thus to address cyber threats related to their own products in the first place.

In the context of the review of the Network and Information Security (NIS) Directive, ETNO has advocated for the introduction of risk management obligations directly applicable to the key actors in the ICT supply chain. Nowadays, telecommunication providers are solely responsible of ensuring the security and resilience of their networks and services, and EU and national law telcos gives them full liability towards their customers and regulators. **Clear mandatory requirements for hardware manufacturers and software developers** to manage and mitigate cybersecurity risks through the product lifecycle would greatly enhance the level of security and robustness of digital products used in telecom networks and services.

[1] State of Digital Communications 2022 Report, ETNO.

[2] Telecom Security Incidents 2020 - Annual Report, ENISA.

Therefore, we look forward to **harmonised cybersecurity requirements for digital products in the announced Cyber Resilience Act (CRA)**, which could bridge the regulatory gaps in the cybersecurity responsibility and liability cascading in several sectors. It is critical that the CRA improve the cybersecurity of digital products in **business-to-business environments**, particularly of those products that are employed in the critical functions of users that operate in critical sectors.

ETNO would like to recommend to the EC some key principles that should guide and effective CRA:

- **Lifecycle approach**: The cybersecurity requirements imposed on vendors should cover the whole lifecycle of the digital product, particularly software. Rapid technological change and dynamic cybersecurity risks demand that vendors provide users **with regular, timely security updates and patches** throughout the period of the expected product lifecycle.

- **Risk-based approach**: The measures attesting compliance with the new cybersecurity requirements should be proportionate to the level of risk of a given digital product. For the sake of legal coherence, the risk profiles of digital products should be categorised into 'basic', 'substantial', and 'high risk' levels, in accordance with the assurance levels of the Cybersecurity Act (CSA). Digital products that support the **critical functions of business users in critical economic sectors** are an eminent example of 'high risk' products.

- **Full regulatory harmonisation**: The CRA should address the currently regulatory fragmentation for the cybersecurity of digital products in the EU. This is particularly important in the telecommunication sector, as Member States have adopted national legislation that govern supply chain security to implement the EU Toolbox for 5G security, typically putting the responsibility for certified and secure components and software on the infrastructure providers. This has further disjointed the regulatory landscape in the digital single market, thereby leading to different levels of security and the risk of potential market distortions. **Harmonisation of law is especially needed for 'high risk' digital products**, including through mandatory European cybersecurity certification schemes. On the contrary, the CRA should avoid creating an additional regulatory layer that conflicts with other pieces of law that address similar objectives, such as the CSA and the upcoming NIS2 Directive. The ongoing implementation of the CSA, the transposition of the NIS2 Directive by 2024, and the law-making process that will result in the final CRA must be synchronised with a holistic approach to provide for a **clear and coherent level of security for all digital products** in the EU market.

For questions and clarifications regarding this paper, please contact **Paolo Grassia**, Director of Public Policy (grassia@etno.eu).