European Telecommunications Network Operators' Association

Cyber-resilience of telecom networks:

ETNO calls for stronger European coordination at a delicate time

Brussels, 9 March 2022 – ETNO, the Association representing Europe's leading telecom operators, welcomes the ministerial debate on the cyber-resilience of European communications networks promoted by the French Presidency of the Council and applauds the joint call to reinforce the EU's cybersecurity capabilities signed in Nevers today.

As the military conflict in Ukraine and the mounting geopolitical tension may lead to the deployment of further aggressive cyberwarfare strategies, we must remain on high alert to prevent large-scale attacks to the European democratic institutions and the critical sectors of society.

European telecom network providers, which are responsible for critical digital infrastructure, have traditionally adopted a 'security first' mindset. The decades-long EU regulatory framework for electronic communications has entailed strict obligations regarding minimum network and service security requirements, risk management measures, data integrity, availability and confidentiality, and the mandatory reporting of security incidents to competent authorities.

Therefore, telecommunications operators, who today are also leading providers of cybersecurity services in Europe, are and will remain trusted partners to public institutions in countering cyber threats to digital infrastructure. While the current regulatory landscape provides numerous means for telcos to step up to the plate, the actions outlined in the joint ministerial call – and stronger coordination of cybersecurity agencies and competent authorities across Member States in particular – are necessary.

At the same time, we emphasise that critical IT infrastructures in other sectors like energy, finance, transport will be increasingly targeted by cyber-attacks. In light of the changing threat landscape, adequate regulatory precautions must be taken.

We also note Member States' concerns with emerging threats due to 5G as well as with the growing complexity of the global ICT supply chains. 5G is providing additional opportunities to secure communications, such as end-to-end encryption and stronger authentication. With the advent of 5G, operators are going to deploy a virtualised and software-defined infrastructure that will be delivered by an environment of operators, vendors, and managed service providers, where more functions will move closer to the user and will be outsourced to suppliers.

Supply chain risk management has therefore become a defining issue for the ICT industry and other sectors that are the top targets for cyber-attacks, like healthcare, energy, banking, education, and government. Member States have already taken a range of national measures to better protect their critical infrastructures. The rollout of 5G networks makes it all the more necessary to further harmonise the security regulatory framework across the EU's digital single market.

Since providers of ICT products and services that become an integral part of communication networks are best placed to manage their own vulnerabilities, their role in addressing cyber threats is paramount. We thus call for Council to consider the need for a better allocation of responsibility for risk management in digital infrastructures along the ICT supply chain.

The NIS 2 Directive would be the best instrument to close the persisting gap in supply chain security, if its scope included ICT suppliers of critical network components. It is not too late, as the Directive is still undergoing negotiations. This would bolster the overall resilience of critical networks and essential services, democratic institutions and processes, and economic security at large in Europe.