ETNO-GSMA Statement

Why filling the gap in supply chain management is a cybersecurity necessity

Following the current decision to not directly capture all relevant actors of the ICT sector with the Directive on measures for high common level of cybersecurity across the Union (NIS2 Directive), ETNO and the GSMA would like to re-emphasise how important it is for the resilience of European critical infrastructure to leave no gaps in the supply chain risk management.

As a starting point we would like to restate that the telecoms industry is strongly committed to delivering cybersecure networks and services. However, to achieve the overall NIS2 Directive's goal of increasing cybersecurity in the EU, the commitment of only one actor that sits at the very end of the supply chain will not be enough. Not filling this significant gap may well result in an increased risk for telecom operators for non-compliance, while the level of cybersecurity and the ability to effectively remedy a security incident would not be adequately increased.

Effective cybersecurity requires an end-to end commitment that covers all actors in the supply chain. The resilience of EU's critical infrastructure is at stake when there are regulatory gaps in the responsibility and liability cascading. As ICT supply chains become increasingly complex and more global with a multitude of parties involved, the actors that manage or assist network operators' critical functions are best placed to analyse and mitigate their own security risks.

Telecommunications operators simply cannot be fully in control of such elements. On the contrary, maintaining the *status quo*, whereby suppliers only have an indirect responsibility governed through their contractual relationships with the regulated entities as proposed in Art. 18 of the NIS2 Directive, will fail to speed up the response to incidents and to deliver effective solutions where the breach is due to vendor failures. Furthermore, Member States have adopted national security acts that govern the supply chain, typically putting the responsibility for certified and secure components and software on the infrastructure providers. This reinforces the fragmentation of the regulatory landscape in the digital single market, thereby entailing different levels of security and the risk of potential market distortions.

We recognise that it would be unreasonable to include all ICT providers in the scope of NIS2, as many ICT vendors are not critical to the functioning of critical infrastructure. However, the ICT providers that do play a critical role in the critical infrastructure supply chain should be held to the same regulatory standard as the essential entities under NIS2. Regulating these providers of critical ICT products and services in different pieces of legislation risks causing overlaps and confusion, including for national authorities that are called to implement and enforce the NIS2 Directive and other cybersecurity rules. Not regulating ICT suppliers at all would leave a large gap in securing EU critical infrastructure.

It remains therefore crucial to quickly close the persisting gap in supply chain security by including ICT suppliers of critical components in the scope of NIS2, which is the best tool to achieve this goal. It is not too late, as the Directive is still undergoing negotiations. There is still a chance to meaningfully increase the security and resilience of EU's critical infrastructure.