Council of the European Union
General Secretariat

PUBLIC

Brussels, 14 September 2026

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (27.10.2026)

WK 13973/2026 INIT

LIMITE

CYBER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	Estonia, Finland, the Netherlands, Poland, Sweden
To:	Horizontal Working Party on cyber issues (attachés)
N° prev. doc.:	WK 10695/26
N° Cion doc.:	ST 5611/26 + ADD 1-4
Subject:	Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2): Title IV: Security of ICT Supply Chains: Guiding questions - Non-Paper by EE, FI, NL, PL and SE

Delegates will find in Annex a non-paper from Estonia, Finland, the Netherlands, Poland and Sweden on guiding principles to make the ICT supply chain mechanism work.

Non-Paper by Estonia, Finland, the Netherlands, Poland and Sweden on the Cyber Security Act 2

Guiding principles to make the ICT supply chain mechanism work

We welcome the Commission's proposal to mitigate cybersecurity risks at EU level. The Cybersecurity Act 2, more specifically the introduction of a new European framework for securing ICT supply chains, directly affects cybersecurity, strategic dependencies and the functioning of the internal market. Having a risk-based approach underpinned by thorough risk analyses is a strong foundation to enhance the EU's resilience. We would therefore like to underline our support for the objectives of this framework, as it is in our view the most pragmatic and coherent way to face the threats and manage those risks that affect the Union. We also support moving first with a phase out on mobile networks, building on the experience with the 5G Cyber Security Toolbox. However, further risk assessments are needed when it comes to the fixed and satellite networks.

We would therefore propose the following principles to guide the work to further strengthen the effectiveness and practical implementation of the CSA2 framework.

1. [redacted]
2. **We need stronger involvement of the Member States within the framework.** We believe that including Member States will help ensure that national expertise, sectoral insights and strategic interests are taken into account. Such involvement will also contribute to measures that are feasible and proportionate at national level. This could still be clarified further in the text in a balanced way to prevent slowing down the process or increasing the administrative burden for all involved.
3. [redacted]
4. [redacted]
5. The **future framework should remain coherent with existing European cybersecurity legislation**, including NIS2 and the Cyber Resilience Act, while ensuring legal certainty and avoiding unnecessary administrative burden. In this regard it is vital that we do not overlook the all-hazard approach of EU cyber regulation by focusing solely on antagonistic threats. To

ensure it is easily understood by all stakeholders and to support simplification, the framework should be constructed in a consistent and logical manner, and in line with previous legal definitions. The obligations set out in the framework should be without prejudice to national provisions transposing other relevant EU legislation as well as national measures transposing measures set out in the 5G toolbox, provided that such provisions are consistent with union law.

6. **We need a strategic prioritization mechanism to protect our infrastructure**. The framework needs to remain malleable, so that we have flexible instruments to use when needed. The framework should therefore not be unduly constrained from the outset, and flexible enough to allow for refinement. It could therefore benefit from a more focused strategic prioritization mechanism by concentrating efforts firstly on the sectors or ICT supply chains that are the most at risk or with the most significant dependencies on the EU level.

Overall, we support a framework that is risk-based, proportionate, focused, predictable and complementary to national measures. Strengthening the resilience of European ICT supply chains should go hand in hand with safeguarding competitiveness, investing in EU alternatives and innovation, maintaining open and diversified supply chains, and the proper functioning of the internal market. The framework should also ensure that risk mitigating measures remain feasible for entities to implement and do not negatively affect the continuity of essential services or the coherence with existing cybersecurity obligations.

PUBLIC