Non-Paper by Estonia, Finland, the Netherlands, Poland, Sweden and Czechia 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. The framework should contribute **to reduce strategic dependencies and reliance on high-risk suppliers in critical ICT supply chains** and strengthening the resilience of the Union as a whole. Therefore, we do believe that the designation of high-risk suppliers should be based on objective criteria including relevant security risks arising from ownership structures and third-country influence. Measures should be evidence-based, proportionate, legally robust and non-discriminatory. This would ensure that the attention is concentrated on the areas where risks for security, resilience and strategic dependencies are the greatest.
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. All the Member States will, because of the dependencies within the supply chain, **benefit from harmonised risk mitigating measures elaborated at EU level**. This should be done through a thorough assessment of the cybersecurity, economic, operational, geopolitical and diplomatic consequences before implementing acts are adopted. Such assessments should involve Member States, sector experts and relevant stakeholders in order to ensure proportionate and feasible outcomes.
4. We **support a risk-based approach and welcome the work already carried out within the NIS Cooperation Group**. However, when formulating the risk mitigating measures, these analyses could benefit from an additional specific analysis that focuses on non-technical risks and consequences. This additional analysis could be supported by intelligence, open source threat intelligence and actor specific insights, in order to make sure that the final conclusions are supported by exhaustive and reliable (incident and/or threat) information. This is important to ensure a high quality risk assessment and to safeguard that the chosen mitigating measures are at the end proportional, and also adequate in relation to the (real) threat.
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.