Main

Delegation: Finland

Commission: EU Summit on Cybersecurity

Issue: How can the European Union build a stable cybersecurity framework in response to intensifying digital threats, while ensuring the protection of fundamental rights, technological competitiveness, and state sovereignty?

Finland, under the leadership of prime minister Petteri Orpo's coalition government, is truly dedicated to placing the country at the forefront of cybersecurity framework development within the European Union. Indeed, Europe has been increasingly exposed to cyberattacks, in addition, the rapid expansion of AI presents several new challenges to preserve our cyber-resilience. Therefore, we agree that the cybersecurity policy must be organized around four key dimensions: safeguarding individual liberties, strengthening Europe's strategic autonomy in the digital sphere, fostering innovation and industrial capacity, and ensuring an effective and coordinated reaction to evolving cyber risks.

As a matter of fact, Finland has been a victim of numerous attacks, like GPS jamming or disinformation campaigns on NATO membership. Likewise, the growing role of AI-enabled threats is alarming. These interrupt the continuity of both public and private services as well as our democratic integrity. Furthermore, inherent freedoms must be preserved; our policy must follow the GDPR and the EU charter of fundamental rights to prevent misuse of cybersecurity measures by states. Despite our reliance on external actors, new technological solutions are being released by European governments to balance. As a digital leader, Europe must be able to innovate, create, certify and deploy solutions at large scale. More importantly, the divergence of the EU countries regarding national rules on cybersecurity and reporting practices complicates cross-border responses. These divergences weaken links between multinational actors and limit EU-wide predictability.

Finland advocates for clear standards and harmonisation in the EU, for instance we actively supported the NIS2 directive and implemented it into national law with the Cyber Act 124/2025. Also we are closely involved in ENISA, as of 2025, we participated in the revision of the EU cybersecurity regulation. Regarding our position on fundamental rights and privacy, we strongly defend fundamental freedoms and do not support mass surveillance approaches, we believe that cybersecurity should not weaken the trust in democracy. Additionally, Finland is home to a strong technological startups ecosystem and leadership in 5G and 6G technologies, we encourage investment in European infrastructure and reducing high-risk suppliers. However we do not defend protectionism and our strategy must be compatible with open markets. Hence, we created a model cyber institution: the NCSC of Finland coordinates responses, raises awareness and cooperates with EU partner ENISA, all at a national level. Despite that, we recommend empowering ENISA while also not replacing national institutions.

Finland's proposed solutions will be organized around three strategic priorities : make harmonisation real, enhance our digital sovereignty and prevent surveillance approaches.

Firstly, we want to create real and strong coordination between states regarding incident reporting, threats prevention and resilience reinforcement. Our project consists of creating an EU-wide notification mechanism for cyber incidents that affect critical infrastructure with standardized reporting that will be coordinated by ENISA, which will serve as the central hub facilitating secure information sharing between national authorities.

Secondly, we should accelerate the process of EU cybersecurity certification adoption for ICT products and services in sensitive fields to reduce supply-chain risks. Furthermore we propose the creation of a European Secure Technology Certification that

would define supply chain transparency standards for ICT systems in essential sectors like energy, healthcare and public administration.

And last but not least, the use of artificial intelligence by governments must comply with the General Data Protection Regulation and remain exceptional when interfering with individual privacy, its use must be clearly justified and proportionate and subject to independent oversight mechanisms.

To conclude, the digital framework must promote harmony, coordination and innovation while ensuring the protection of individual freedoms. The Union must face the intensifying cyber threats with a common base, cooperation and prevent the hijacking of cybersecurity into surveillance tools. These elements justify our Europhile position, strengthening EU capabilities and sovereignty, and at the same time protecting our democracies in the digital era.

Sources

About the Industry - Teknologiateollisuus ry

Cybersecurity | Shaping Europe’s digital future

Ensuring Finland’s Cybersecurity – Policy Recommendations Against Russian Cyberattacks and Disinformation Campaigns – King's Think Tank

https://euromad.org/wp-content/uploads/2026/02/Methode_TPG_Conseils_Sommets_2026.pdf

https://euromad.org/wp-content/uploads/2025/03/IA_Espagne.pdf

https://euromad.org/wp-content/uploads/2026/01/Cybersecurite_Rapport.pdf