Delegation: Estonia

Commission: 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?

The Government of Estonia is firmly committed to strengthening cybersecurity resilience at both national and European levels. Having experienced large-scale cyberattacks in 2007, Estonia recognizes cybersecurity as a cornerstone of national security, democratic stability, and economic growth. As digital threats intensify; ranging from ransomware and disinformation to state-sponsored cyber operations; the European Union must establish a coordinated and forward-looking cybersecurity framework that protects fundamental rights while reinforcing technological competitiveness and national sovereignty.

The rapid digitalization of European societies has increased exposure to sophisticated cyber threats targeting critical infrastructure, financial systems, healthcare, and democratic institutions. Estonia emphasizes that a comprehensive EU cybersecurity strategy must balance three essential principles: security, protection of fundamental rights, and innovation. Measures to counter cybercrime and hybrid threats must fully respect privacy, data protection, and freedom of expression, in line with the Charter of Fundamental Rights of the European Union. At the same time, cybersecurity regulation should enhance, not hinder, Europe's technological development and global competitiveness.

Estonia strongly supports the EU Cybersecurity Strategy and the NIS2 Directive, which reinforce resilience and cooperation among member states. As host of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia contributes actively to international cyber defense expertise. Nationally, Estonia has developed one of the most advanced digital governance systems in the world, including secure digital identity solutions, blockchain-based data integrity systems, and a robust e-governance infrastructure. The Estonian Cybersecurity Act and regular cyber defense exercises demonstrate the country's proactive approach to preparedness.

Estonia applies a whole-of-society cybersecurity model. The Estonian Information System Authority (RIA) oversees national cyber resilience, while strong public-private cooperation enhances threat detection and response. Investments in digital literacy and cybersecurity education further strengthen societal resilience. Estonia also promotes secure and decentralized data exchange through the X-Road platform, ensuring transparency while safeguarding data sovereignty.

Looking ahead, Estonia proposes deeper EU coordination through a strengthened European Cyber Rapid Response mechanism to assist member states during major cyber incidents. Enhanced intelligence-sharing frameworks and joint cyber exercises would improve collective preparedness. Estonia also supports harmonized cybersecurity certification under the EU Cybersecurity Act and increased investment in European cybersecurity research and innovation to reduce strategic dependencies.

At the same time, EU coordination must complement, not replace, national competencies. Member states should retain sovereignty over their national security structures while benefiting from collective European resilience.

Estonia remains committed to a secure, rights-based, and competitive digital Europe. By reinforcing cooperation, investing in innovation, and safeguarding democratic values, the European Union can build a stable cybersecurity framework capable of responding effectively to intensifying digital threats. Estonia stands ready to collaborate with fellow member states to strengthen the Union’s cyber resilience and strategic autonomy.