Represented Country: Austria

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 Republic of Austria recognises cybersecurity as a fundamental pillar of European stability, economic prosperity and democratic security. As digitalisation accelerates across all sectors of society, cyber threats have grown in scale, complexity and geopolitical significance. Attacks targeting hospitals, financial institutions, energy grids and electoral systems demonstrate that cybersecurity is no longer solely a technical issue, but a matter of strategic sovereignty and public trust. The central question raised by this Council, how the European Union can establish a stable cybersecurity framework while ensuring the protection of fundamental rights, technological competitiveness and Member State sovereignty, is therefore of vital importance

Austria, as a highly interconnected and export-oriented economy, is particularly aware of the vulnerabilities created by digital interdependence. Small and medium-sized enterprises, which form the backbone of the Austrian economy, are increasingly targeted by ransomware and phishing attacks. At the same time, the growing use of artificial intelligence in both civilian and military contexts creates new risks, including automated cyberattacks. These evolving threats require a coordinated and forward-looking European response.

Austria firmly supports the strengthening of the European legal framework, including the effective implementation of the NIS2 Directive and the EU Cybersecurity Act. Harmonised security standards, common certification schemes and enhanced cooperation through ENISA are essential to reduce fragmentation between national systems and ensure a rapid, unified response to cross-border incidents. However, Austria emphasises that such harmonisation must respect the principle of subsidiarity and preserve Member States' sovereign responsibilities in national security matters.

The protection of fundamental rights remains a core priority. Austria upholds the General Data Protection Regulation (GDPR) as a cornerstone of European digital governance and insists that cybersecurity policies must not compromise privacy, freedom of expression or democratic oversight. Security measures must remain proportionate, transparent and accountable in order to maintain citizens' trust.

At national level, Austria has implemented a comprehensive Cyber Security Strategy, reinforced cooperation between civil and military cyber defence structures, and invested in digital resilience programmes. Public-private partnerships, specialised cybersecurity training and awareness campaigns aim to strengthen prevention and response capacities. Austria also supports increased EU funding under programmes such as Digital Europe to promote innovation, research and the development of European cybersecurity technologies, thereby enhancing digital sovereignty.

Looking ahead, Austria proposes the expansion of EU rapid-response cyber teams, deeper intelligence-sharing mechanisms among Member States, and accelerated investment in European cloud infrastructure and encryption technologies. Reducing dependence on non-European technology providers will strengthen strategic autonomy while fostering economic competitiveness.

In conclusion, Austria advocates for a balanced, pragmatic and strongly coordinated European cybersecurity framework. As a pro-European Member State, Austria believes that unity, legal clarity and sustained investment are essential to ensure that the European Union remains secure, competitive and faithful to its fundamental values in the digital age.