Slovenia
Conseil de l'UE sur la Cybersécurité

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 Slovenia operates under a parliamentary system of government. The current Prime Minister is Robert Golob, while the President, who serves as Head of State, is Nataša Pirc Musar. Slovenia continues to be a prominent champion of a strong and unified European digital defense framework. As a Tier 1 "Role-modelling" country in the 2024 Global Cybersecurity Index (GCI), Slovenia demonstrates a maximum level of commitment across nearly all major cybersecurity pillars, particularly in legal and cooperation measures. The intensification of digital threats, including a global surge in ransomware and data breaches, requires a unified European response that does not compromise the individual rights of citizens or the sovereignty of Member States. This paper outlines Slovenia’s position on fostering a secure, competitive, and legally harmonized European cyberspace.

The European Union faces an evolving threat landscape where ransomware attacks against government services and breaches of critical infrastructure are becoming more frequent and intense. In 2023 alone, the global average cost of a data breach reached USD 4.45 million, highlighting the severe economic risk posed to technological competitiveness. Furthermore, large-scale technical outages have demonstrated a dangerous level of dependency on digital infrastructure, which can threaten national stability.

Even advanced nations face staffing and funding challenges, and the human element remains a primary vulnerability, requiring a user-centered approach that respects fundamental rights under frameworks like the GDPR.

The European Union has already taken steps to strengthen cybersecurity through the NIS2 Directive, which aims to improve risk management, incident reporting, and cooperation across Member States. However, further action is needed to address remaining gaps in awareness, training, and workforce capacity.

A stable EU cybersecurity framework relies on the five pillars of the Global Cybersecurity Agenda (legal measures, technical capabilities, organizational structures, capacity building, and international cooperation), with collective resilience preserving state sovereignty.

Slovenia strongly supports the harmonization of cybersecurity laws across the EU to ensure that legal measures are technology-neutral and applicable to both online and offline offenses. Slovenia’s perfect score of 20/20 in the Cooperation pillar reflects our belief that bilateral and multilateral agreements are the most effective tools for tracking transnational malicious actors.

Slovenia has already implemented several high-impact solutions that serve as models for the Union:

- Legal & Regulatory Frameworks: Slovenia has ratified and fully implemented comprehensive regulations on personal data protection and breach notification, ensuring alignment with the highest standards of the European Union.
- Technical Incident Response: Slovenia maintains a highly responsive National Computer Incident Response Team (CIRT) and participates in regional cyber drills to ensure readiness for large-scale attacks.
- Organizational Excellence: Our National Cybersecurity Strategy covers Critical Information Infrastructure (CII) and integrates stakeholder engagement throughout its entire lifecycle**.**

Proposed Solutions for the EU:

1. Unified Cyber-Awareness Campaigns:

Implementing coordinated cyber-awareness campaigns to focus on vulnerable groups with limited digital skills. Improving public awareness would help reduce cyberattacks supporting the goals of the NIS2 Directive.

Possible actions include EU-wide awareness weeks, cybersecurity education in schools and universities, free online training, and public media campaigns.

2. CII Training Standardization: Slovenia proposes an EU-wide incentive mechanism for sector-specific training to ensure professionals are prepared for localized infrastructure threats.

An EU-wide certification or training framework would: harmonize cybersecurity skills across Europe, enable faster and more effective responses to cyber incidents, improve cooperation between national security teams, and reduce vulnerabilities in essential services.

3. Incentivizing R&D: EU-level grants and scholarships for cybersecurity research and development to bridge the workforce gap and maintain technological competitiveness against global competitors.

Possible actions include EU grants for cybersecurity start-ups, partnerships between universities and industry, scholarships and specialized degrees in cybersecurity, and the development of advanced technologies such as AI-based threat detection.

Slovenia reaffirms its Tier 1 leadership in the European cybersecurity ecosystem. Firmly pro-European, Slovenia advocates for deeper integration of incident response teams and harmonized legal frameworks across Member States. By focusing on capacity building and international intelligence sharing, the EU can safeguard sovereignty and competitiveness while protecting citizens’ rights. Slovenia is ready to lead by example in making this vision a secure and trustworthy digital reality.