Country: Luxembourg

Key problem : 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?

Commison : EU Council on Cybersecurity

Introduction

Luxembourg has been governed since November 2023 by a tripartite coalition led by Prime Minister Luc Frieden, reflecting the country's tradition of political consensus and democratic stability. As a founding member of the European Union, Luxembourg positions itself as a committed pro-European actor, deeply attached to European integration and the rule of law.

As a major financial and technological hub, the country is particularly vulnerable to the growing wave of cyberattacks targeting critical infrastructure. Luxembourg therefore strongly advocates for a coordinated European approach to cybersecurity, firmly believing that no single state can effectively address these threats alone.

Problem Statement

The committee turns its attention to the following question: *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?"*

This issue raises three major challenges: strengthening European cooperation in the face of cross-border cyberattacks, protecting critical infrastructure without infringing on fundamental rights, and reducing technological dependence on non-European powers to ensure the EU's digital sovereignty.

Key Issues and Problem Statement

These issues directly concern Luxembourg on several levels. As a European financial center home to nearly 120 banks and numerous investment funds, the country is a significant target for cybercriminals and economic espionage. Its small size limits its individual defense capabilities, making European cooperation essential. Furthermore, Luxembourg hosts major data infrastructure (data centers) whose security is critical to the European economy. Finally, deeply committed to fundamental freedoms, the country seeks to ensure that cybersecurity measures respect the rule of law and do not drift toward mass surveillance.

Luxembourg's Stance on Cybersecurity

Luxembourg advocates a coordinated European approach to cybersecurity, built on three pillars: enhanced cooperation between member states, protection of fundamental rights, and European digital sovereignty. As a small but economically significant state, Luxembourg considers that its security depends on European solidarity.

The country has actively supported key legislative milestones, including the NIS2 Directive (2022), which sets strict standards for critical infrastructure, and the Cyber Resilience Act

(2023), aimed at reducing technological dependence. At the operational level, Luxembourg cooperates with ENISA through its national incident response center, CIRCL.

Domestically, Luxembourg relies on its National Cybersecurity Strategy and the Budapest Convention on Cybercrime. Firmly committed to the rule of law, it ensures full compliance with the GDPR and the EU Charter of Fundamental Rights, rejecting any drift toward mass surveillance. The country also supports the Digital Europe Program and hosts initiatives such as GAIA-X, advancing European digital sovereignty.

Solutions Already in Place

Luxembourg has established CIRCL (2008) to coordinate incident responses and collaborate with European CSIRTs, alongside the Luxembourg House of Cybersecurity, bridging the public, private, and academic sectors. As a financial hub, the country consistently applies cybersecurity standards that exceed European minimum requirements

New Proposals

1. European Cyber Rapid Response Team Luxembourg advocates for a response team capable of acting within 24 hours in the event of a major cyberattack against a member state, pooling expertise and resources for a coordinated and swift response.

2. Mandatory European Certification for Critical Infrastructure Imposing a European cybersecurity certification for all equipment used in critical infrastructure (energy, healthcare, finance, telecommunications) in order to reduce risks and dependence on non-European technologies.

3. European Cyber Resilience Fund for SMEs Creating a dedicated fund to help small and medium-sized enterprises strengthen their cybersecurity by financing audits, training, and protective tools, as SMEs often represent the weakest link in the security chain.

Conclusion

To conclude, the European Union can build a stable cybersecurity framework by harmonizing legislation through the NIS2 Directive and the Cyber Resilience Act, while strengthening institutions such as ENISA for a coordinated response. Fundamental rights and GDPR compliance must remain central, ruling out any drift toward mass surveillance. Initiatives like GAIA-X will help preserve European technological competitiveness and reduce dependence on non-European powers, while a subsidiarity-based approach ensures that European cooperation complements rather than replaces national sovereignty.