

Possible threats: Bulgaria must be particularly cautious of Russia as a direct cyber threat, China as a strategic and supply-chain risk, and other state-linked actors that use cyber operations to undermine EU and NATO members through espionage, disruption, and hybrid warfare.

**Pays : Bulgarie**

**Commission : Cybersecurity**

**Problématique : “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?”**

Building a Stable EU Cybersecurity Framework: Lessons from Bulgaria

Introduction

Bulgaria’s experience provides a useful case study for understanding the broader cybersecurity challenges facing the European Union. As an EU member state, Bulgaria has developed a formal cybersecurity framework through its Cybersecurity Act (2018) and a national strategy aligned with the EU’s Network and Information Security (NIS) Directive. This framework established national authorities, a CERT, and security obligations for operators of essential services.

Despite this progress, Bulgaria has been the target of significant cyberattacks. The 2019 breach of the National Revenue Agency, which exposed the personal data of millions of citizens, revealed serious weaknesses in cyber resilience and data protection. Additionally, DDoS attacks against government institutions, some attributed to foreign actors, demonstrated how cyber operations can threaten state sovereignty and public trust without using conventional force. These incidents show that legal frameworks alone are insufficient and that cybersecurity must balance security, fundamental rights, technological competitiveness, and sovereignty—a challenge shared across the EU.

Strengthening the EU Legal and Institutional Framework

At the European level, the NIS2 Directive represents a major step toward a more stable and coherent cybersecurity framework. By expanding its scope to more sectors, strengthening risk-management obligations, and improving incident-reporting requirements, NIS2 directly addresses vulnerabilities revealed by national experiences such as Bulgaria’s.

However, effectiveness depends on consistent implementation across all member states. Excessive fragmentation would weaken collective resilience, while over-centralisation could undermine national sovereignty. A stable EU framework must therefore reinforce national capabilities while ensuring strong coordination and shared standards.

Protecting Fundamental Rights

Cybersecurity and fundamental rights are closely linked. Weak security, as illustrated by Bulgaria’s 2019 data breach, can directly harm citizens’ rights to privacy and data protection. At the same time, overly intrusive security measures risk violating civil liberties.

The EU must ensure that cybersecurity policies:

- Respect privacy and data protection by design.
- Include judicial oversight and proportionality for intrusive measures.
- Remain aligned with the GDPR and the EU Charter of Fundamental Rights.

Public trust is essential: without it, cybersecurity policies risk losing legitimacy and effectiveness.

## Enhancing Technological Competitiveness

Cybersecurity is also a strategic economic issue. A strong EU framework can boost competitiveness by:

- Investing in cybersecurity research, innovation, and skills.
- Supporting European startups and SMEs to reduce dependence on non-EU technologies.
- Promoting secure-by-default products through initiatives such as the Cyber Resilience Act.

By strengthening its internal market for cybersecurity solutions, the EU can improve resilience while fostering innovation and growth.

## Safeguarding State Sovereignty and Strategic Autonomy

Cyber threats increasingly target critical infrastructure and public institutions, directly affecting state sovereignty. Bulgaria's experience with foreign-linked cyberattacks illustrates this risk. The EU must therefore pursue strategic digital autonomy, particularly in areas such as cloud services, telecommunications, and critical infrastructure protection.

This approach does not imply isolation, but rather reducing critical dependencies, strengthening EU-based infrastructure, and ensuring that member states retain control over key security decisions while benefiting from collective defense mechanisms.

## Conclusion:

Bulgaria's cybersecurity framework and the attacks it has suffered highlight the complexity of modern cyber threats and the limits of purely national responses. For the European Union, building a stable cybersecurity framework requires a balanced approach that combines harmonised legal standards, respect for fundamental rights, technological competitiveness, and state sovereignty.

By reinforcing national capabilities through coordinated EU action, investing in innovation and skills, and ensuring that cybersecurity measures remain democratically accountable, the EU can respond effectively to intensifying digital threats while preserving its core values and strategic autonomy.