Delegation: Belgium
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?"
Introduction

The Kingdom of Belgium is a federal parliamentary democracy and an active member of the European Union. Belgium strongly supports European cooperation, especially in areas such as digital policy and security.

Today, cybersecurity has become one of the most important challenges for Europe. Our daily lives, our economies and even our public institutions depend on the internet and digital systems. Because of this, the European Union has introduced several laws to protect citizens, companies and critical infrastructure from cyber threats.

However, while improving cybersecurity is necessary, the EU must also ensure that these measures respect the fundamental rights of citizens and the sovereignty of each Member State. Finding the right balance between strong security and the protection of individual freedoms remains a key challenge.

Belgium, like all Member States, recognises the need to strengthen resilience against cyberattacks, protect critical infrastructure and improve cooperation at the European level. For this reason, Belgium has welcomed recent European initiatives such as the NIS2 Directive and the work of the European Union Agency for Cybersecurity.

At the same time, Belgium understands that stronger European regulation can also create challenges for Member States. While there is general agreement on reducing Europe's dependence on external technology providers and strengthening the European digital sector, there are still different opinions about digital sovereignty and how to best protect the fundamental rights of European citizens.

Key Challenges and Relevance for Belgium

Cybersecurity threats rarely stop at national borders. A cyberattack against the infrastructure of one country can easily affect other countries in the European Union. This is why we need cooperation between Member States.

Each country must have strong national institutions responsible for cybersecurity, and these institutions must work together by sharing information and responses. This is especially important for sectors that are essential for our societies, such as energy, transport, healthcare and finance.

For Belgium, cybersecurity is especially important. Belgium hosts several key European institutions and has a very digitalised economy. Because of this, Belgium must ensure that its digital infrastructure is secure.

However, Belgium also believes that stronger cybersecurity rules at the European level must respect privacy and fundamental freedoms guaranteed under EU law, mainly the protection of personal data. Any new regulation must balance stronger security with respect for citizens' rights.

Belgium's Position on the Issue

Belgium has taken an active role in strengthening cybersecurity within the European Union. In fact, Belgium became the first Member State to fully implement the NIS2 Directive into national law in early 2024. The implementation of this law is supervised by the Centre for Cyber Security Belgium, also known as the CCB.

Our country also plays an important role in the European cybersecurity landscape because it hosts key international institutions such as NATO and the European Commission, which have both prioritised cyber defence in their security programes.

In addition, Belgium contributed to the development and adoption of the EU Cyber

Solidarity Act, published in January 2025. This regulation aims to help EU countries better detect, prepare for and respond to serious cyber incidents that may affect citizens and businesses. It also promotes solidarity between Member States during cyber crisis.

At the national level, Belgium has also adopted the National Cybersecurity Strategy 2.0, which provides a framework for addressing cyber threats and strengthening the country's digital security. The goal of this strategy is to make Belgium one of the least vulnerable countries to cyber threats in Europe.

Existing Measures and Proposed Solutions

Belgium supports these European legal frameworks because cyber threats are transnational and require coordinated action at the EU level.

At the same time, Belgium believes that cybersecurity policies must always respect democratic values, the rule of law and fundamental rights. In particular, Belgium strongly supports the General Data Protection Regulation, which protects the personal data and privacy of European citizens.

This means that even when cybersecurity measures are strengthened, they must remain lawful, transparent and proportionate. Any monitoring or surveillance must always respect the rules established under the GDPR.

Belgium has already taken several concrete steps:

First, Belgium has incorporated the NIS2 Directive into national law and has designated the Centre for Cyber Security Belgium as the authority responsible for cybersecurity and incident response.

Second, organisations in important sectors must adopt cybersecurity risk-management measures and report significant cyber incidents to the national authorities.

Third, Belgium promotes voluntary certification programmes such as CyberFundamentals, which help organisations improve their cybersecurity practices in a structured way.

Looking forward, Belgium would like to promote further cooperation within the European Union in three main areas.

First, improving the standardisation of incident reporting across the EU and strengthening information sharing between Member States.

Second, supporting national education and awareness programmes to teach citizens about cybersecurity and digital rights.

Third, continuing the development of European cybersecurity certification standards to ensure that digital products and services are secure by design.

Conclusion

In conclusion, Belgium strongly supports a balanced European approach to cybersecurity. Europe must strengthen its collective digital security while also protecting individual rights and national sovereignty.

Belgium therefore supports greater European cooperation and harmonisation in cybersecurity policies, while also ensuring that privacy, data protection and democratic freedoms are always respected.

Belgium firmly believes that a secure Europe must also be a Europe that protects the freedoms of its citizens. Cybersecurity policies should therefore reinforce these values, not weaken them.