Represented Country: Czech Republic

Commission: Cybersecurity

What is the 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?

What are the threats and oppertunities:

The Government of the Czech Republic sees cybersecurity as a very important part of national security, economic stability, and democracy. As a country that is highly digitalized and has strong cybersecurity institutions, the Czech Republic has focused on protecting its digital systems while also respecting fundamental rights and national sovereignty.

However, we cannot ignore that digital threats are growing fast, especially those linked to artificial intelligence (AI). Even fake images seems to exist forever on the internet and unidentified drones are circling the airspace of our airports and military installations. Because of this, the European Union must find a way to improve cybersecurity without harming innovation, freedom, or the independence of its Member States.

As European societies rely more on digital technologies, they become more exposed to cyber threats affecting governments, healthcare systems, banks, energy networks, companies, and elections. Artificial intelligence has increased these risks by enabling deepfakes and disinformation campaigns. The Czech Republic has already faced cyber threats from foreign actors, proving that these dangers are real. Therefore, strong cybersecurity must be both a national responsibility and a shared responsibility within the European Union.

What is the solution?

To face those challenges, the Czech Republic supports the development of a European cybersecurity framework based on cooperation, information sharing, and common minimum standards. Instruments such as the EU Cybersecurity Act and the strengthened role of the European Union Agency for Cybersecurity help reduce weaknesses across the internal market and improve collective responses to cyber incidents.

To accommodate both threats and opportunities in this area the Czech Republic believes that EU rules should set a minimum level of protection and not limit countries that already have strong cybersecurity systems. Member States with advanced capabilities must be able to react quickly and effectively without being slowed down by too many regulations.

At the national level, the Czech Republic has established a strong cybersecurity system led by the National Cyber and Information Security Agency. Czech legislation already meets or exceeds many EU requirements, allowing effective prevention, rapid response to cyber incidents, and close cooperation with European partners. This demonstrates that European cooperation and national sovereignty can work together, and that the EU should strengthen national capabilities rather than take control away from Member States.

What is at stake?

Cybersecurity is also an important economic sector for the Czech Republic. It is supported by small and medium-sized enterprises, research centres, and skilled technology experts. European digital sovereignty should be developed in a decentralised way, ensuring fair access to funding, leadership roles, and research projects for all Member States. While supporting increased EU investment in cybersecurity technologies, the Czech Republic believes that regulations should be adapted to smaller companies and that projects should be distributed fairly across the Union.

The Czech Republic is an attractive country for technology and cybersecurity investments. Many international companies and successful Czech firms (Avast, GoodData, Y Soft, Seznam.cz, Socialbakers and STRV) work in the ICT sector, and this helps the country grow economically. There are also strong research centres and many students studying technology. Today, thousands of people work in ICT companies, which creates jobs, income, and more wealth for the Czech economy. However, introducing new restrictions or excessive regulation could weaken this positive trend. Stricter rules may discourage investment, slow innovation, and make it harder for companies to operate efficiently, ultimately reducing the sector's ability to grow and contribute to the national economy.

Protecting fundamental rights and privacy remains a key priority. Historical experience with authoritarian surveillance has created a strong national focus on transparency and data protection. Public trust is essential for effective cybersecurity policies, and measures that weaken privacy or allow mass surveillance could harm democracy and social stability. For this reason, the Czech Republic strongly supports the General Data Protection Regulation and believes that AI-based cybersecurity tools must be used transparently, fairly, and under clear legal control.

Looking ahead, the Czech Republic supports improved early warning systems, joint cyber exercises, stronger cooperation among EU Member States, and closer cooperation with NATO in cyber defence. However, national authorities must always retain control over critical infrastructure and security decisions. EU support should strengthen Member States, not replace national responsibility.

Conclusion:
The Czech Republic supports strong European cooperation in cybersecurity but is against excessive centralisation. A stable EU cybersecurity framework must protect citizens, support innovation, respect fundamental rights, and allow Member States to keep their sovereignty. As a committed and capable Member State, the Czech Republic is ready to contribute its experience and knowledge to help build a safer and more secure digital Europe.