Commission: Summit on Cybersecurity in the EU

Delegation represented: The Netherlands

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?

The Netherlands, strategically located at the heart of Western Europe and along maritime routes, is therefore deeply connected to the rest of the world. Composed of a constitutional monarchy and a parliamentary democracy, this state is often considered as one of the most wired countries in the world and the digital gateway of Europe. Although in the past, it was our geography that shaped our global influence, today, it is our digital infrastructure which makes us powerful. On that basis, security is no longer only about protecting territory, but also protecting cyberspace, which has become the foundation of our economy, infrastructures and democratic institutions. That is why the European Union needs to find a way to build a stable cybersecurity framework in response to intensifying digital threats, while ensuring the protection of fundamental rights, technological competitiveness, and state sovereignty.

The European Union is increasingly vulnerable to cyberthreats, particularly as artificial intelligence multiplies the scale and sophistication of attacks, putting critical infrastructures, the economy, and democratic institutions at risk. For the Netherlands, this is especially concerning because key infrastructures, such as the Port of Rotterdam — a major hub in the global economy — rely heavily on technology, and any disruption could threaten both national stability and European supply chains. Differences in cybersecurity regulations across EU Member States further weaken the Single Market, complicating cross-border operations and creating exploitable vulnerabilities. As one of the EU's most trade-dependent economies, the Netherlands sees cybersecurity as essential for both security and economic resilience. At the same time, Europe's reliance on non-European technology providers highlights the need to strengthen digital sovereignty, support domestic innovation, and protect strategic industries.

The Netherlands support a strong and coordinated European Cybersecurity framework. Indeed, our delegation presumes that having shared regulations between the countries of the EU will help make trade easier, faster, and less exposed to cyberattacks. Consequently, the Netherlands backs the NIS2 Directive, which strengthens the protection of essential systems and improves cross-border incident reporting. However, our delegation also emphasizes that EU members should remain in charge of their own national security, as reflected in the Netherlands' contributions to the EU discussions on the NIS2 Directive. In addition to that, our delegation supports a risk-based approach to artificial intelligence, meaning the EU should focus on high-risk uses of AI, such as infrastructure, finance, and elections, while permitting to the low-risk AI technologies to develop freely and keep ensuring innovation. But a key concern on cybersecurity for the Netherlands is digital sovereignty. Indeed, Europe's dependence on foreign companies for cloud services, telecommunications infrastructure, and cybersecurity tools underlines the importance of strengthening its own technological base. The Netherlands therefore prioritizes the protection of essential national assets, such as the Port of Rotterdam, its highly digitalized

water systems, and ASML's semiconductor leadership. Through measures like the Chips Act and targeted innovation investment, Europe can strengthen its strategic autonomy and long-term resilience. Finally, the most important point of this issue for the Netherlands is that all the cybersecurity measures that are about to be taken must respect fundamental rights and privacy. The General Data Protection Regulation sets the standard for data protection, and the Netherlands supports strict adherence to these principles while implementing cybersecurity policies. The Netherlands assures that keeping our citizens trust and freedom is essential for any European cybersecurity measure to be effective.

The Netherlands has already taken concrete measures to maintain an effective cybersecurity framework. Indeed, at national level first, with the implementation of the National Cyber Security Strategy (2022-2028), the Netherlands is trying to be more aware of cyber threats, to strengthen the cybersecurity workforce to ensure that adequate expertise is available to meet evolving digital challenges or also to review the national cybersecurity structure to improve the effectiveness of its cyber tools and resources. At a European level, the Netherlands has supported and committed to implementing key legal instruments such as the NIS2 Directive, the Cybersecurity Act of 2019, and the GDPR, reinforcing harmonized standards while maintaining national responsibility for security. In addition to that, our delegation has also approved the EU AI Act, made to regulate high-risk AI systems. During the debates, the Netherlands will push for a stronger European collaboration in cybersecurity, especially to work toward cyberattacks that are cross-border. Our delegation will also claim to have more support for European tech and innovation, but mostly, it will make sure that the freedom of its citizens is maintained.

All in all, the Netherlands believes that a strong European cybersecurity framework will be found with the balance of digital sovereignty, EU coordination, innovation and the protection of fundamental rights. Our delegation will keep trying to protect our critical infrastructures and to make cyberspace a safer area for trade and commerce. Overall, the Netherlands takes a **pragmatic, moderately pro-European stance**: it values EU cooperation to strengthen digital resilience, while carefully protecting national sovereignty and strategic industries.