Conseil de l'UE sur la Cybersécurité
"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?"
Hungary

Hungary is a central European member state of the European Union experiencing rapid numerization in both its economy and administration over the past few years, thus increasing opportunities and vulnerabilities in its cyberspace. Hungary's situation, at the junction between Central and Eastern Europe, integrated in EU energy, transport and financial networks, makes the protection of its infrastructure and digital services a strategic priority for the whole of Europe. Its privileged position in the Visegrad Group, along with Poland, the Czech Republic and Slovakia, is in fact at the heart of eastern European collaboration. Hungary's consent to EU measures will therefore be essential to be applied in such and cooperation.

The Hungarian republic has answered issues on this topic through the National Cybersecurity Strategy and dedicated authorities responsible for security and cyber-incident response, as shown below. In this context, Hungary believes that an EU cybersecurity framework must be brought together with a particular attention to common security, the maintenance of fundamental rights, including freedom of expression and media pluralism so dear to democracy, while not imposing ethics in the technological economy, all whilst maintaining the utmost principle that Hungary's national sovereignty is inviolable and inalienable. The measures taken must be fundamentally necessary for security, in alliance with Hungary's sovereign powers and be led with sufficient oversight and counter-actors to avoid surveillance and overly prescriptive legislation. All security measures need to stay precise and not vague, non-intrusive and carefully protect national interests.

Hungary supports efforts to strengthen the EU's cybersecurity plan through coherent and common legislation, including the implementation of the NIS2 Directive, the EU Cybersecurity Act, and the Cyber Resilience Act on secure products. When applied consistently, correctly and appropriately, which all states should ensure, these can improve resilience across the EU while maintaining opportunities for both public and private actors. The delegation of Hungary considers that any further growth of this framework must remain in accordance with the Charter of Fundamental Rights of the EU and find echoes with existing protection rules, especially the General Data Protection Regulation, in order to ensure rights, notably privacy. Nonetheless, Hungary strongly rebukes imposing a politically motivated message through these legal requirements, as these would lead to uncompetitiveness and would largely infringe national sovereignty in their interior and exterior affairs. Hungary will not tolerate any course of action designed to enforce a particular orientation, as these would open the way for censorship and ideological enforcement, silencing alternative views.

Furthermore, Hungary recognises the importance of international cooperation in cyberspace and supports the application of international law, in particular the UN charter, to state and other actors' behavior as is reflected by the republic's participation in the UN group of governmental experts and the Open-Ended Working Group. Nevertheless, the delegation would like to insist on the fact that the EU's cybersecurity framework must respect the division of competences agreed upon: while incident response and prevention may be prepared, the actual responsibility in terms of application, defense and national security reinforcement must remain solely in the hands of Member States, with the EU as an additional coordinating actor. National sovereignty should, in all regards, be superior to EU directives in this matter.

Considering Hungary's particular economy, the delegation of Hungary highlights the need for consideration of the this new dimension in cybersecurity. Excessive regulation may hinder innovation and affect growing enterprises, as well as limit the state's ability to choose which products and mainly which

investments are allowed on Hungarian soil. If over-reliance on dominant enterprises in the sector came to be proposed, regardless of nationality, Hungary strongly affirms that such measures impede sovereignty. Hungary defends a restricted approach to certification, assuring that no political interference may come from it, and no impositions are made in national matters under any circumstances. The delegation will strongly censure and decline any unilateral agreement from the economically strongest, struggling against one-sided economic development.

Hungary has developed and updated a National Cybersecurity Strategy, which reinforces the protection of critical information infrastructure such as government information systems and certain private actors. The model presented balances sovereignty and resilience, through mandatory risk assessment and reporting.The Hungarian government has even established institutions for this matter such as the National Cybersecurity and Computer Security Incident Response Team to identify and respond to incidents affecting any and all important actors. The latter has been key in managing incidents targeting governmental websites and other critical sectors in the past, such as the 2024 ransomware breach in Hungary's defense agency, drawing the conclusion that a pragmatic approach is essential, as well as coordination with other states by sharing information. The Republic has participated in EU and NATO cybersecurity exercises, showing trust and collective help between national authorities and supranational entities. The delegation of Hungary has noticed that best management of crises include the need for investment in education training and public awareness, and that this is a wise solution.

In conclusion, the delegation of Hungary supports the construction of a minimalist and restricted EU cybersecurity framework that strengthens security in the light of intensifying digital threats while safeguarding rights, economic competitiveness and most importantly, state sovereignty in national affairs. EU legislation may set common purely technical standards and common ground for cooperation, explicitly excluding geopolitical positions, mandatory threat attribution, promotion of values and supranational infringes on state sovereignty across all aspects. The delegation will contribute towards a realistic and regardful solution to defend EU cybersecurity as a useful tool, not consisting in itself the ultimate goal for the country.