Commission : Conseil de l'UE sur la Cybersécurité
Subject: Building a stable cybersecurity framework in response to intensifying digital threats
Author: The Republic of Latvia

The Republic of Latvia, currently governed by the center-right New Unity party under Prime Minister Evika Siliņa, recognizes the rapid expansion of digital technologies and innovations in the European Union. While this evolution brings immense benefits across all sectors, it also exposes member states to significant digital threats, including attacks on critical infrastructures such as hospitals, banks, and energy networks as well as interference in electoral processes. Our country's extensive experience with a "100% digital" administration and e-signature systems makes us a primary target for these threats. Furthermore, the rise of Artificial Intelligence makes these attacks stronger, faster, and more complex.

The Baltic state of Latvia shares its borders with Lithuania, Estonia, Belarus, and Russia, giving it a strategic position with access to the Baltic Sea. However, this geography places our nation on the immediate frontline of the Union's eastern flank. For the Republic of Latvia, cybersecurity is an daily concern. We are heavily and routinely exposed to state-sponsored cyberattacks, hybrid threats, and disinformation campaigns linked to Russia purposefully designed to destabilize our democratic infrastructure. The proximity to hostile actors means that a breach in our network is not just a national failure, but a direct threat to the entire European Union.

The Republic of Latvia is an active member to both the European Union and NATO. To counter hybrid warfare, our country proudly hosts the NATO Strategic Communications Centre of Excellence (NATO StratCom COE) in Riga. This institution provides us with unmatched expertise in analyzing and neutralizing psychological operations and AI-driven interference. Our country strongly supports the mandate of the European Union Agency for Cybersecurity (ENISA) and the NIS2 Directive. However, given the severe security threats on our borders, we advocate for a flexible approach to the GDPR to ensure that intelligence agencies can effectively neutralize threats. We believe that European digital sovereignty must be achieved through total integration with NATO defense mechanisms.

To maintain our national security and internal stability in this hostile environment, the Republic of Latvia has been forced to take uncompromising, pragmatic measures. Recognizing the lethal nature of information warfare, we have had to aggressively block and censor Russian state media and implement stringent security policies regarding our Russian-speaking minority populations to neutralize internal hybrid threats and espionage. Furthermore, we must acknowledge an uncomfortable truth regarding our current infrastructure: Latvia, like much of Europe, remains dependent on American technological giants for our digital infrastructure and on NATO for our intelligence networks.

Latvia has actively ratified acts aligning national legislation with the NIS2 Directive and has committed to increasing defense spending, recently confirming the allocation of 5% of its GDP to defense to strengthen national and NATO capabilities. To address the commission's problematic, the Republic of Latvia proposes the following three pillars:

1. **The European Cyber Solidarity Fund:** As frontline states protect the entire Union, the EU must financially assist Member States in deploying advanced, sovereign European cybersecurity infrastructure. Europe is only as secure as its weakest border.
2. **EU-NATO Rapid Response Teams:** We propose the creation of joint elite units to counteract automated, AI-driven attacks, utilizing the data and research from the NATO StratCom COE in Riga.
3. **The "EU Digital Watchtower" Project:** Establishing a centralized European hub for hybrid threat detection in Riga. This center will serve as a real-time AI-driven analysis tower, protecting the Union's collective digital borders by detecting threats before they reach the heart of Europe.

In conclusion, the Republic of Latvia approaches this committee with a vision grounded in our harsh realities on the Eastern flank. While we maintain a strongly pro-Atlantic stance on cybersecurity, the current geopolitical volatility demands that the EU rapidly accelerate its own strategic autonomy. The technological competitiveness and sovereignty of the European Union can only be secured through harmonized laws, comitted financial solidarity toward frontline states, and unwavering cooperation with NATO.