Position paper Lithuania Cybersecurity

Thematic: **“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 Republic of Lithuania recognises the ongoing and imminent cyber threats the member states are faced with, including state-sponsored attacks, hybrid warfare, misinformation campaigns or disruption of critical infrastructure. Due to our unique geographic location and history, Lithuania has been the target of persistent aggression at the hands of Russia and combined with smaller resource pools and geopolitical vulnerability, Lithuania relies on European integration in matters of cybersecurity to be able to effectively counter the existential nature of Russian aggression at our doorstep. Through NATO and the CSDP, Lithuania has always shown itself ready to cooperate and adapt to changing threats and stay loyal to Western partners in the battle to defend democracy and European values.

Firstly, the EU must agree upon a common Artificial Intelligence strategy and framework which balances the need for strategic autonomy in areas of critical infrastructure and reduces dependence on foreign technology while also maintaining healthy competition and strengthening local European tech firms to make Europe a valuable player on the global stage, and avoiding red tape and slamming the brakes on innovation.

Secondly, the EU must set a strong common cybersecurity policy, with possibility of integration into a wider Common European Defence Partnership, which emphasises cooperation to avoid member states being coerced or strong-armed by active enemies of our shared values, prosperity, and project of cooperation, peace, and development. We have seen wide-scale attacks such as hybrid warfare on critical infrastructure in the areas of communication, logistics, and healthcare, which cannot continue in this manner. At which point do we decide to combine forces and become ready to defend the European project with the geopolitical hard and soft power we have when we act as one.

Lithuania also recognises that the opportunity for digitalisation and development of cyber-defence capabilities can and should go hand-in-hand, realising that this is the moment in which Europe steps up and can negotiate on equal ground with the superpowers of the world. The benefits of digitalisation for efficiency in public procedure and business innovation are at a point beyond plausible denial, and we can see China and the US speeding ahead while the EU remains cautious, denying itself long-term growth and the economic strength that goes with it.

Therefore, Lithuania proposes a Common European Cybersecurity Policy (CECP) which will see the creation of a new wing at Frontex or the EDA, with the purpose of creating a Cybersecurity taskforce which operates at Union level with the goal of defending European digital systems and infrastructures and finally putting an end to the coercion by disproportionately powerful neighbours while operating within the European system.

To conclude, Lithuania is ready to negotiate and cooperate with fellow Member States, outlining our unique position of vulnerability while also sharing our experience, best practices, and lessons learned in cyber defence. We aim to contribute constructively to a common European framework that strengthens resilience, protects fundamental rights, and ensures the Union remains technologically competitive and sovereign in the digital domain.