The Republic of Poland is located between Germany and Belarus and is a parliamentary democratic EU member state. The current government supports cooperation within the EU all while emphasizing national security, stability for the country, as well as the protection of critical infrastructure, democratic institutions, and citizens from facing threats that could put at risk their lives. As digitalization evolves, particularly with the enhancement of artificial intelligence, cyber threats have increasingly affected Europe and have become a fundamental concern for the stability of the EU. In this context, the EU is obliged to strengthen cybersecurity to prevent further threats, including cyberattacks, cybercrime, disinformation campaigns, and hybrid warfare. However, this task is challenging, as it requires balancing the protection of citizens' rights with technological innovation, and maintaining national sovereignty in all of the European countries. 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 nature of these cyber threats includes attacks on hospitals, energy systems, elections, and banks, as well as disinformation campaigns and hybrid warfare, all aimed at destabilizing the European Union. These threats are cross-border, and no single country can effectively defend against them alone. For Poland, these threats are particularly challenging due to its geographical position in Eastern Europe and its exposure to aggressive and hostile cyber activities and disinformation campaigns, making it more vulnerable to attacks from nearby countries such as Belarus and Russia. Poland faced thousands of cyberattacks in early 2026, about 3 200 attempted attacks every seven days, many targeting official polish networks and infrastructure. Poland also recognizes that, while cybersecurity needs collective European action, it is also closely linked to national security and defense. Therefore, the country feels the necessity to balance European cooperation with national duty and responsibility.

Poland supports EU cooperation but seeks to preserve its sovereignty. It agrees with EU-level coordination and considers information sharing between member states of EU, as well as the development of common cybersecurity standards, essential for ensuring collective security within the Union. Poland recognizes EU mechanisms and institutions such as the European Union Agency for Cybersecurity (ENISA) as key tools for this cooperation. The Republic of Poland emphasizes that cybersecurity is closely linked to national security, intelligence services, and defense capabilities, all of which must, according to Poland, remain under national authority. At the same time, cybersecurity measures must respect individual privacy, protect personal data, and comply with EU legal standards such as the General Data Protection Regulation (GDPR). While achieving these goals is challenging, security measures must remain democratic and must not lead to violations of human rights.

Poland has taken steps to improve national cybersecurity. The Cybersecurity Strategy 2019–2024 focuses on protecting critical infrastructure, sharing information, and working with private companies. The Polish Cybersecurity Act updates national law to match EU rules like NIS2. Poland also takes part in EU projects, such as the European Cybersecurity Competence Centre, and supports the national CSIRT to respond to cyberattacks. Poland could suggest more EU funding for cybersecurity research and innovation that lets each country stay in control, as well as practice exercises where EU countries work together to respond to

cyberattack so that they are more prepared for incoming attacks. Poland also supports cooperation between the EU and NATO (North Atlantic Treaty Organization, a military alliance of countries from Europe and North America) in hopes of making a more resilient stable cyber security.

In conclusion, Poland supports assistance from EU all while recognizing that effective cybersecurity requires cooperation and solidarity among all member states to face these threats. At the same time, it is essential to ensure that fundamental rights are always protected, regardless of the circumstances or the severity of the threats, to preserve the country's democratic values. Furthermore, the national sovereignty of Poland, even in the context of security, must continue to be respected and carefully balanced with EU-level cooperation.