Author: Spain
Commission: Conseil de l'Union européenne sur la cybersécurité
Subject: 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 Kingdom of Spain is a parliamentary monarchy headed by His Majesty Felipe VI and governed by Prime Minister Pedro Sánchez of the Spanish Socialist Workers' Party, who leads a left-wing coalition government. Spain's political values and strategic interests are closely aligned with those of the European Union. In recent years, the country, like the rest of the European Union, has faced a significant rise in cyberattacks, many of which target artificial intelligence systems and compromise both private and public data, as well as essential government services. In this context, Spain strongly supports a coordinated European effort to establish a stable and coherent cybersecurity framework capable of addressing these threats without undermining fundamental rights, technological competitiveness, or state sovereignty.

Spain has observed a rapid increase in threats driven by artificial intelligence, including sophisticated phishing schemes and automated ransomware attacks that pose serious risks to both public institutions and private entities. These attacks have particularly affected the healthcare, financial, and governmental sectors, endangering the personal data of over 200,000 individuals. They have also targeted critical infrastructure such as energy networks, transportation systems, and telecommunications services, revealing structural vulnerabilities in systems that are often outdated or insufficiently protected against emerging forms of cyber aggression. This vulnerability is further aggravated by the expansion of connected technologies in everyday environments. The growing presence of smart homes, connected vehicles, and digitally integrated workplaces has broadened the attack surface, enabling malicious actors to exploit weaknesses in devices that were not originally designed with robust cybersecurity safeguards. Finally, geopolitical tensions—including debates surrounding Catalan independence and Spain's broader positioning within the European Union—have heightened exposure to disinformation campaigns, hacking operations, and data breaches aimed at influencing the political landscape.

Given the seriousness of these developments, Spain has adopted both defensive and strategic measures to counter the growing number of cyberattacks. The protection of fundamental rights, particularly the right to privacy, remains a central priority. Spain has therefore reinforced the security of its critical infrastructure and information systems in order to prevent data breaches and safeguard sensitive information. At the same time, national defense initiatives have been strengthened to address cyber interference that could threaten Spain's sovereignty or intensify geopolitical tensions. Spain is equally committed to reinforcing its technological sector in order to enhance competitiveness and secure greater strategic autonomy. Reducing dependence on technologies imported from outside the European Union is considered essential, particularly where such dependencies could create vulnerabilities in times of international conflict.

To address these challenges, Spain has developed and joined several major initiatives. In 2023, Spain established the Spanish Agency for the Supervision of Artificial Intelligence (AESIA), the first European public authority specifically dedicated to the oversight of artificial intelligence systems, with the objective of regulating high-risk technologies and limiting abuses such as automated ransomware attacks. As of early 2026, Spain has invested more than €1.157 billion in an offensive and preventive strategy known as "Unified Shield," led by the National Cybersecurity Institute (INCIBE) and the National Cryptologic Centre (CCN-CERT). This initiative strengthens threat detection mechanisms, facilitates rapid vulnerability patching, and improves coordination between sectors. Furthermore, Spain continues to work closely with the Digital Operational Resilience Act and the NIS2 Directive, both of which aim to reinforce digital resilience and harmonize cybersecurity standards across the European Union. Lastly, Spain has introduced training and awareness programs in schools, universities, and professional environments to foster a culture of digital responsibility. These efforts seek to ensure that citizens are better equipped to recognize and prevent cyber threats in their daily lives, particularly in increasingly connected environments.

Spain remains firmly committed to participating in and contributing to European cybersecurity initiatives in a manner that guarantees the protection of fundamental rights, strengthens technological competitiveness, and preserves state sovereignty. As a deeply pro-European nation, Spain advocates for a collective and coordinated approach at the level of the European Union. It stands ready not only to cooperate, but to play a leading role in shaping a balanced, forward-looking cybersecurity framework that extends beyond national borders and secures the Union as a whole.