Delegation: France
Commission: Conseil de l'Union européenne – Cybersécurité
Issue: 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?

Cybersecurity has become one of the greatest challenges to the European Union. Under the leadership of President Emmanuel Macron, France places cybersecurity at the center of its national and European priorities. As a strongly pro-European country, it believes that only a coordinated European response can effectively address digital threats. Cyber technologies have become indispensable to public services, commercial activities, and the democratic process. At the same time, cyber threats are on the increase, becoming more complex, and include cross-border attacks. Hospitals, energy networks, transport systems, public administrations, and electoral processes may be targeted by these cyberattacks. These threats do not recognise national borders, and therefore, the issue cannot be solved by Member States acting independently. The European Union has already developed a significant cybersecurity framework in the form of common laws, agencies, and cooperation mechanisms. However, recent cyberattacks demonstrate that this framework needs to be reinforced to ensure adequate responses to escalating digital risks. For example, ransomware attacks against European hospitals in 2023 and 2024 disrupted medical services and exposed sensitive patient data, showing that critical infrastructure remains vulnerable to increasingly sophisticated digital threats. France believes that cybersecurity is not only a technical issue, but also a matter of fundamental rights, technological competitiveness, state sovereignty, and trust in the European project. As a country with advanced digital infrastructure and major public institutions, France is directly exposed to these risks and therefore considers cybersecurity a national priority.

The EU has adopted several key legal instruments to improve cybersecurity, such as the General Data Protection Regulation to protect personal data, the NIS2 Directive and DORA to secure critical infrastructure, and the Cyber Resilience Act and the Cybersecurity Act to strengthen the security of digital products and services. This is a good foundation, showing that the European Union is committed to protecting its citizens and institutions in the digital space. However, France considers that this framework needs further strengthening. One of the main weaknesses is the varying implementation of the EU cybersecurity laws in the Member States. Sometimes the same rules are applied differently, with varying deadlines, sanctions, and procedures. For example, while Germany and France implemented the NIS2 Directive quickly, countries such as Belgium and Poland experienced delays in adopting national measures. This legal fragmentation weakens the overall security of the Union and creates gaps that can be exploited by cybercriminals and hostile actors. Furthermore, cooperation in cybersecurity is still too slow and poorly coordinated. Information on cyber incidents is not always provided promptly, which allows for the spread of attacks from one country to another. Finally, the European Union is still highly dependent on non-European digital providers, mainly in cloud services and critical technologies. This situation limits the strategic autonomy of Europe and raises concerns about the control of sensitive data and infrastructures.

France fully supports the objectives of the European Union's cybersecurity framework, including the protection of critical infrastructure, public services, and personal data of citizens. France also agrees with the strengthening of common rules, as well as with the role of European agencies to coordinate cybersecurity. At the national level, France has strengthened its cybersecurity system by transposing the NIS2 Directive, reinforcing its National Cybersecurity Agency (ANSSI), and investing in critical infrastructure protection

and crisis management. However, France argues that the European Union must go beyond having an approach that is mainly regulatory to create an approach that is more operational and enforceable. Laws alone are not enough if they are not supported by effective cooperation tools such as shared threat-intelligence platforms and coordinated EU crisis response mechanisms. Cybersecurity must respect the fundamental rights, including the rights to privacy, data protection, and freedom of expression. At the same time, France considers cybersecurity to be closely linked to state sovereignty and technological competitiveness. Europe must be able to protect itself and not be overly dependent on external actors, such as China and the United States, especially in the public administration, defence, and health sectors, while maintaining an ability to promote innovation and economic growth.

First, France proposes reducing legal fragmentation across Member States by introducing common EU cybersecurity rules to be applied with the same deadlines, sanctions, and procedures throughout the Union. This will guarantee equal protection and enhance European cyber resilience overall. Second, France supports the introduction of mandatory EU-wide cybersecurity certification for critical digital services, specifically cloud services used by public authorities. No provider hosting sensitive public data should be allowed to operate without complying with strict EU-level security standards. Third, France proposes the creation of a permanent EU-level real-time threat intelligence platform allowing Member States to immediately share information on cyber incidents, vulnerabilities, and emerging digital threats. France also supports the creation of an EU rapid cyber alert system that would notify Member States within hours in the event of a major cyberattack affecting critical infrastructure. Finally, France supports the idea of strengthening the European cybersecurity agencies through better coordination, increased funding, and enhanced cooperation with national authorities and law enforcement agencies in countering cybercrimes.

France sees that the European Union has built a solid cybersecurity framework, but that it must now become more coherent, more operational, and more sovereign. A stable cybersecurity framework must be able to respond to intensifying digital threats while protecting fundamental rights, supporting technological competitiveness, and reinforcing state sovereignty. As a strongly pro-European country, France firmly believes that only a united European approach can ensure long-term digital security and resilience. By strengthening common rules, enhancing cooperation, and preventing strategic dependencies, the European Union will be ready to protect its citizens, its infrastructure, and its democratic values in the digital age.