Delegation : Romania

Commission : EU Summit on Cybersécurity

Issue: Strengthening a stable and coordinated cybersecurity framework within the European Union in response to escalating digital and AI-driven threats.

The Romanian government, led by an administration deeply committed to Europe and under the leadership of Prime Minister Nicolae Ciucă, aims to place Romania at the center of the European Union's digital defense. Romania understands that digital technology has become an essential element for national and European security. We therefore come to this summit as technical experts. Indeed, this role stems from the historic decision of the 27 member states to create the European Cybersecurity Competence Centre (ECCC) in Bucharest, the first EU structure established in our country. This center serves as a pillar of the EU's cybersecurity strategy and manages billions of euros from programs such as Digital Europe and Horizon Europe. In response to digital attacks, Romania proposes its vision: "Digital sovereignty through resilience," which means transforming our technical ability into protection for all European citizens.

The threats to the EU are no longer theoretical, they are daily realities, in Romania, the National Cybersecurity Directorate (DNSC) records between 25,000 and 50,000 cyberattacks every day, 14% more than last year due to the war in Ukraine. These attacks primarily target energy (31%), transport (22%), and public administration (19%), and nearly 40% occur in Bucharest. However, today European cybersecurity faces two major pressures. On one side, Russia conducts complex digital operations such as DDoS attacks, ransomware, and disinformation campaigns using artificial intelligence to destabilize Europe. It also looks to promote a vision of digital technology based on strong state control, which the EU rejects, favoring rules based on cooperation and state responsibility. On the other side, the EU remains heavily dependent on large American companies like Microsoft, Google, and Amazon Web Services for data storage and cybersecurity tool, but despite the importance of cooperation with the United States, Romania does not wish to be entirely dependent and aims to develop its own technologies with Europe to strengthen digital sovereignty.

Romania understands that a strong European defense requires bringing together the perspectives of all 27 EU member states. We want to act as a bridge between different countries and fully support the NIS2 Directive and the AI Act, while recognizing that each country has different needs, making a flexible approach necessary. Romania aligns with Eastern and Southern countries (such as Poland and the Baltic states) in asserting that national security must sometimes take precedence over full privacy protection. This differs from Northern and Western countries (such as Germany, the Netherlands, and Sweden), which insist on strict adherence to privacy and GDPR. However, we also support the Franco-German initiative to better integrate Europe, while national authorities are encouraged to retain control over their critical infrastructures. The ECCC in Bucharest aims to help reconcile these differences and enable wealthier countries to share resources with those needing assistance to catch up technologically. For us, network security is essential because it ensures that the privacy protections guaranteed by GDPR are truly effective.

At the European level, Romania proposes concrete solutions. Our country has nearly 200,000 developers and has helped companies like Bitdefender gain global recognition. Bitdefender is a

cybersecurity software company employing over 1,600 experts and has provided free tools to help Ukraine protect its energy network. This expertise stems from our history, and since the 1990s, Romania has transformed informal technical skills into internationally recognized know-how. In Romania, the 2022–2027 National Cybersecurity Strategy is a comprehensive roadmap, emphasizing prevention and public-private cooperation. One of our major successes is the election monitoring system, which prevents fraud and ensures security through digital verification. Thanks to the Special Telecommunications Service (STS) and the DNSC, Romania has created a model of "democratic digital resilience" that can be replicated across the EU. Currently, 39.3% of Romanian companies use advanced security solutions, and 38% use AI to automatically detect threats.

In response to increasing cyberattacks, disinformation campaigns, and foreign interference, Romania, to protect the EU's future, proposes three main actions led by the ECCC in Bucharest:

1. Establish a European Cybersecurity Solidarity Fund to help less advanced countries secure their energy and healthcare networks.
2. Create a European Hacking Academy to train cyber defenders in all 27 member states, ensuring the same level of expertise for everyone.
3. Develop an AI-based alert system to detect and block deepfakes and disinformation in real time.

Romania envisions a sovereign, united, and technologically strong European Union, and remains convinced that with the ECCC in Bucharest, the EU can combine regulation and innovation. While privacy protection is still important, faced with attacks from the East and technological dominance from the West, the 27 countries must choose collective strength to enhance the EU's technological autonomy. Romania is therefore ready to make this effort so that European digital space remains open and safe for all citizens.