Euromad+ 2026 -EU Summit on Cybersecurity-

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?

Commissaires: Fabiola Cave, Carolina Gozalo et Juan Escribano

SUMMARY:

I) INTRODUCTION

The European Union is becoming more and more digital and technological. This brings a lot of benefits such as: faster communication, new ways to work, and better services for people. But it also brings new dangers that can threaten people's day to day lives. These problems are: Cyberattacks. Cyberattacks can now hit hospitals, banks, energy networks, or even elections. Not only can it be a small problem for someone, but it can ruin a whole business, a city, or even a country. These attacks are more advanced than before, and artificial intelligence (AI) is what is making them even stronger and faster.

Because of this, the European Union has to answer an important question: ***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?*** This is not an easy question, and certainly not a simple debate with an obvious solution**.** The European Union needs to find a solution to this problem by always keeping people, civil and military security, corporations, and public institutions safe without taking away any freedoms. In addition, it has to protect its economy and make sure all 27 Member States can work together, which is a condition for a strong collective defense strategy.

With all that being said, to help answer this question, our report focuses on four main themes:

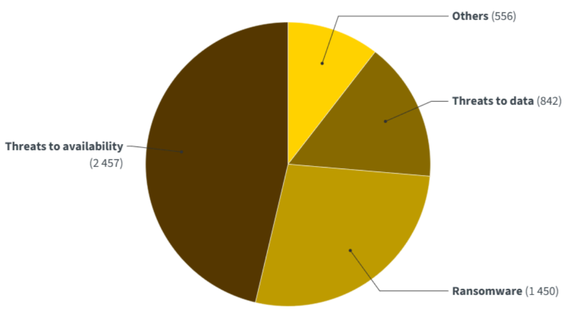
1- New Threats Linked to Artificial Intelligence:

Artificial Intelligence (AI) is becoming more and more powerful in everybody's life, and while it can be used to protect systems and help the public, it can also be a dangerous weapon. One of the biggest dangers is automated cyberattacks, where AI programs are set to attack networks or devices without any human control, often on a shockingly massive scale. Another danger is deepfakes. Deepfakes are videos, images, or voices created by AI that look and sound real but are completely fake. These can be used to trick people, spread lies, or damage someone's reputation because of how realistic it is.

Additionally, there is also intelligent hacking, where AI can learn how to break into systems, find their weaknesses faster than any human, and adapt to it not to get detected. This kind of technology can be misused by criminals to steal data or money, but it is also misused by states to spy on other countries or influence their politics. A clear example is disinformation and online manipulation: using AI to flood social media with false or misleading information, sometimes just to confuse

Threats to availability make up 47% of cyber threats

Threats to availability, ransomware and threats to data are the most prominent cyber threats in the EU.



people, and other times to influence elections or create political division. These threats are evolving quickly. For instance, in Spain, in 2025, at least five attacks were confirmed, including the municipality of Melilla, that included a ransom demand of $2.1 million and a three-week recovery period. The EU needs to be able to react just as fast to avoid them.

2- Developing a Strong European Legal Framework:

To protect against these new threats, the EU needs clear and strong laws that work in all Member States. Right now, some progress has been made such as the AI Act, which sets rules to explain how AI can be used, especially in high-risk situations. The situation could also improve thanks to the stronger role given to ENISA (European Union Agency for Cybersecurity), which supports EU countries in preventing and responding to any cyber incidents possible.The EU Cybersecurity Act (Regulation (EU) 2019/881) established EU-wide cybersecurity certification frameworks for ICT products, services, and processes; adapted structure: ENISA now serves as a central reference point for harmonizing technical cybersecurity standards across Member States, mitigating differences in national implementation of ICT security measures.

But this is not going to save us from cyberattacks, even though we can consider it a big help. There is still a big challenge, the national laws are different. This causes a difficulty for countries to work together and bond as a team, when a cyberattack happens across borders. Hackers do not stop at one country's border, so the European Union needs to align national laws to create a united and clear response. This would make it easier to share resources, react faster, and avoid situations where a weak legal system in one single country puts the whole European Union at risk. For example, concerning the GDPR, Member States retain national derogations for law enforcement, public sector exemptions, and age-related rules. Germany implemented additional national data breach reporting obligations for public authorities, while France allowed a longer reporting window in certain circumstances. Consequently, multinational companies must maintain differentiated cybersecurity reporting workflows tailored to each jurisdiction.

3- Innovation and Digital Sovereignty:

Cybersecurity is not only about defence, it is also about building strength for the future, for a better future. The European Union can't rely too much on technology from outside Europe, especially from countries that might not share the same values about privacy or security. This is why supporting European tech-companies and cybersecurity startups is so important.

If Europe puts money into its own companies, it can reduce dependence on non-European technologies and make sure it controls its own personal tools and data. This idea is called: digital sovereignty. It corresponds to having the ability to develop and protect Europe's digital and technological space without having to depend on others. Moreover, building a competitive digital Europe will also contribute to the creation of new jobs, encouraging innovation, and making sure Europe stays strong in the global technology race.

4-Protecting Fundamental Rights and Privacy:

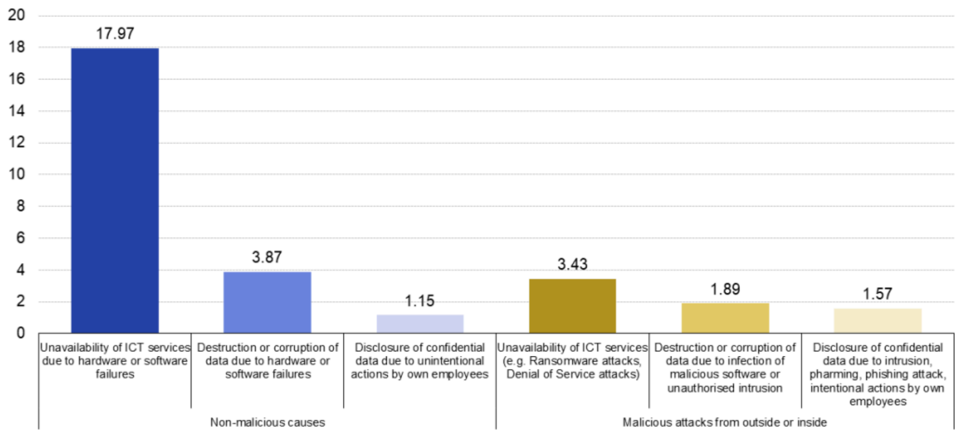
Cybersecurity is important, but it should never mean giving up on the basic rights and freedoms that people in the European Union enjoy in their day to day routine. We should not depend only on cybersecurity, because it could end up being dangerous. That is why, to understand this - the right way without any kind of misunderstanding and confusion - there is a law that incorporates all of this. The key law is the GDPR (General Data Protection Regulation), which is used to protect personal data and privacy. However, with AI becoming more advanced in our society, there's a risk it could be used for tracking which means watching people's activities online or in real life without them even knowing. Exactly like spying. So it could be in ways that could be considered not fair or legal.

Furthermore, there's also the risk of the misuse of AI by governments, companies or businesses to control the information, keep track of citizens, or even limit the freedom of speech. This is why the European Union must balance security needs with individual freedoms. It has to protect people, so the citizens, from cyber threats while making sure that the protection they are using does not turn into constantly keeping track of people or even censorship.

To sum up, respecting privacy and rights will guarantee citizens' trust and belief, which is essential for any cybersecurity policy to work correctly in every 27 member states of the European Union.

To conclude, these four themes will guide the rest of the report. They show that cybersecurity is not just about technology, it is also about laws, politics, rights, people's and citizens' safety, and Europe's place in the world. The goal of this introduction is to give a clear starting point so that everyone understands the main issues before the debates.

Enterprises experienced ICT related security incidents leading to consequences, EU, 2023
(% of enterprises)



Source: Eurostat (online data code: isoc_cisce_ic)

II) HISTORICAL CONTEXT & EU PROGRESS

1) Historical Overview of EU Cybersecurity Policy:

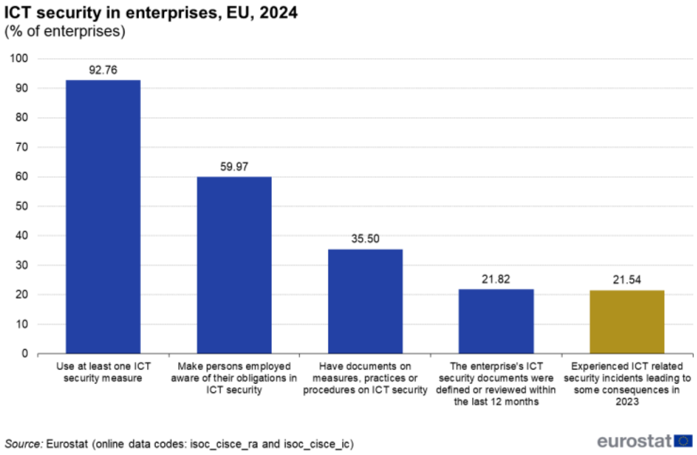
Over the past two decades, the European Union has developed a comprehensive approach to cybersecurity in response to the rapid growth of digital technologies and emerging threats. In 2007, large-scale cyberattacks against Estonia disrupted banks, media, and government services, showing how vulnerable EU countries could be to digital threats. This event, followed by attacks on German government networks in 2015 and the 2017 global WannaCry ransomware outbreak, pushed cybersecurity higher on the EU agenda.

Early efforts in the late 1990s and early 2000s focused mainly on improving network reliability and encouraging cooperation between Member States, leading to the creation of the European Network and Information Security Agency (ENISA) in 2004. By the mid-2010s, rising cyberattacks, political disinformation campaigns, and the emergence of artificial intelligence as both a security tool and a threat prompted the EU to introduce its first Cybersecurity Strategy in 2013 and the Network and Information Security (NIS) Directive in 2016. Subsequent years brought the General Data Protection Regulation (GDPR), the EU Cybersecurity Act in 2019, and the NIS2 Directive in 2022, while ongoing initiatives such as the proposed Artificial Intelligence Act aim to address new AI-related risks. Today, cybersecurity policy in the EU is shaped by four priorities: countering AI-enabled threats, strengthening the legal framework, boosting innovation and digital sovereignty, and safeguarding fundamental rights and privacy.

2) Progress:

The EU has made significant advances in each of these priority areas. It has integrated artificial intelligence into cybersecurity defence strategies while addressing disinformation through initiatives such as the Code of Practice on Disinformation (2018). This code was launched after evidence of foreign interference in EU and national elections, including the spread of false news through social media platforms like Facebook. Its legal framework has steadily expanded, from the initial NIS Directive to NIS2. The EU's main law on cybersecurity applies stricter security and reporting requirements across more sectors, including energy grids and water supply, in response to incidents like the 2021 ransomware attack on Ireland's Health Service Executive, which disrupted hospital operations nationwide.

The GDPR has established Europe as a global leader in data protection, and the Cybersecurity Act has created a EU-wide certification scheme for secure ICT products, referring to Information and Communication Technology products, like software, hardware, and online services. Innovation and digital sovereignty have been promoted through programmes like Horizon 2020, Digital Europe, and the establishment of the European Cybersecurity Competence Centre in Bucharest, while projects such as GAIA-X were designed to offer an alternative to US cloud service giants such as Amazon Web Services or Microsoft Azure. Throughout these developments, the EU has maintained a strong commitment to ensuring that cybersecurity measures respect the rights and freedoms guaranteed by the EU Charter of Fundamental Rights.



ICT security in enterprises, EU, 2024
(% of enterprises)

Source: Eurostat (online data codes: isoc_cisce_ra and isoc_cisce_ic)

3) Challenges:

Despite this progress, several challenges persist. AI technologies are evolving faster than regulatory frameworks, enabling malicious uses such as deepfakes, automated cyberattacks, and large-scale online manipulation. For instance, manipulated videos of politicians circulated during the 2022 French elections.

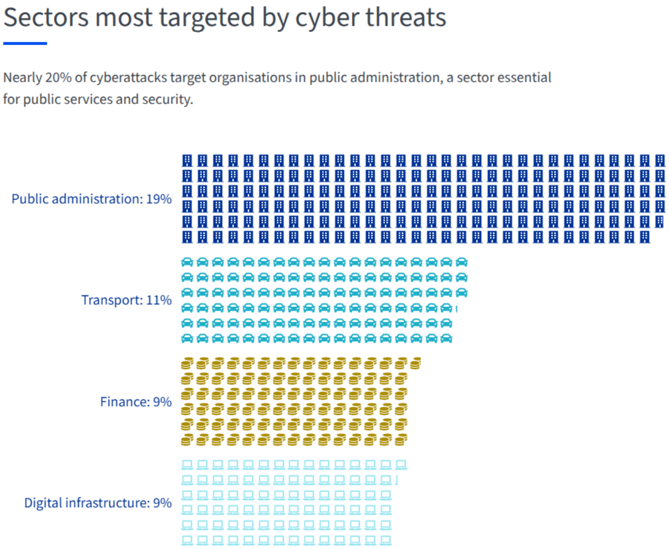
Legal harmonisation remains incomplete, with significant differences in cybersecurity maturity and national laws across Member States, as well as political sensitivities about ceding too much security control to EU institutions. Europe remains heavily dependent on non-European technology providers such as Microsoft, Google, Huawei, and Cisco for cloud computing, telecom infrastructure, and security software; creating vulnerabilities if geopolitical tensions rise. Balancing security needs with the protection of privacy and individual freedoms continues to be a sensitive issue, as advanced monitoring and surveillance capabilities risk weakening public trust. Addressing these issues will require coordinated policy, sustained investment, and legal frameworks that adapt quickly to new threats.

III) POLITICAL LANDSCAPE: MEMBER STATES' DIVERGENCES

All Member States recognise the need to strengthen resilience against cyberattacks, protect critical infrastructure, and improve cooperation at the EU level. Instruments such as the NIS2 Directive and the role of ENISA enjoy general political support. There is also consensus on the importance of reducing dependence on external technology providers and building a more competitive European digital sector.

Despite these common goals, positions diverge in some areas. First, on sovereignty versus integration: large Member States such as France and Germany want to strengthen EU-level regulation and digital sovereignty, whereas some smaller or newer Member States prefer to retain greater national control over security matters. Second, concerning privacy, Northern and Western countries, including Germany, the Netherlands, and the Nordic States, emphasise the protection of fundamental rights and strict limits on state surveillance. By contrast, some Southern and Eastern States, facing severe security threats, favour more flexible approaches that prioritise national security over individual privacy. Third, in terms of investment capacity, wealthier Member States are able to fund advanced cybersecurity strategies, while others rely heavily on EU funding instruments to close the gap.

Geopolitics also strongly influence national positions. Eastern Member States such as Poland and the Baltic States, exposed to recurrent cyberattacks and disinformation campaigns linked to Russia, consistently call for stronger defence measures and closer cooperation with NATO. Western Member States, while also concerned with security, place greater emphasis on regulating the influence of large non-European technology companies, particularly those based in the United States, and on developing European alternatives. Meanwhile, growing concerns about Chinese technology providers have pushed many Member States to align with EU-level initiatives aimed at securing supply chains.



Sectors most targeted by cyber threats

Nearly 20% of cyberattacks target organisations in public administration, a sector essential for public services and security.

IV) SITOGRAPHY

https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises#Highlights

https://www.enisa.europa.eu/

https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

https://www.nbu.gov.sk/national-cyber-security-strategy/

https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/

https://www.itpro.com/business/policy-and-legislation/nis2-why-are-firms-struggling-to-comply

https://www.ft.com/content/853f0ba0-c6f8-4dd4-a599-6fc5a142e879

https://www.thetimes.com/world/europe/article/poland-deputy-pm-krzysztof-gawkowski-interview-255rzbpqq

https://www.orrick.com/en/Insights/2024/10/NIS2-Where-do-European-Countries-Stand-on-Implementing-Cybersecurity-Strategies