GERMANY
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?

INTRODUCTION

Germany, officially the Federal Republic of Germany, is a country in Western and Central Europe. It borders 10 different countries and its capital is Berlin. Germany's government is nowadays a federal parliamentary democracy led by a federal chancellor (Bundeskanzler), Friedrich Merz since May 2025. Since the last elections, Germany has been governed by the coalition of CDU/CSU (Christian Democrat Union / Christian Social Union). Its basic values are catholic social teachings, conservatism, and the defense of a social economy with State laws and rules. Germany is ruled by the Fundamental Law of 1949.

Europe is facing numerous cyberattacks, threats and increasing their volume faster than never. Especially since Artificial Intelligence (AI) is developing at an enormous speed. The continent has to search solutions to this large issue agreeing with all 27 members of the European Union. We must debate about one vast question concerning EU security: **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?**

ISSUES AND CHALLENGES

This issue has two main difficulties, first, the new digital threads that our world has to face everyday, mainly because of AI rise. These two problems are: automated cyberattacks; AI set to attack devices by itself, and also what is called deepfakes; content created by AI (videos, audios, photos…) that seem totally real but aren' t, mostly used to spread lies and rumors, that can lead to damaging people's dignity and life. AI can cause automated cyberattacks on a huge scale, but it also can master getting into a system and not getting caught or even detected by the attacked system. The real issue is that these advanced hacking techniques are used by criminals and even states that try to spy or steal information. We recently have detected numerous attacks, our energy system is being targeted and we could link it to Russian interference, which preoccupies us, but we also care about our own citizens, they have been receiving messages which asked them for their security codes and passwords, and were actually a fraud.

The thing is, that social media, one of the most used media nowadays, is flooded with fake content, AI created, that most people believe are real, or just don't try to verify if it is. The European Union has to be capable of defending itself from these great problems. In parallel to the European Union, Germany alone is also being targeted by multiple cyberattacks on a massive scale. The last significant attack was in August 2024, where our aerial security was assaulted, probably by Russia's military. In addition, fake information about our chancelier was spreaded, damaging his political and personal reputation. Mostly before the elections, fake information was used to convince citizens to have a specific political opinion. In order to protect our country from these kinds of contemporary threats, we have set up some measures, and we can always continue to grow in terms of security. At the same time, our citizens must be protected, while still having privacy and not being clogged by strict laws that don't respect all of their fundamental rights. Germany has to find the solution with the other members of the European Union.

OUR POSITION

Our country is one of the most powerful countries in the EU, we have been members of it since its start. We maintain our position as one of the richest countries in the EU and also very stable and secure. We have adopted European legislation. The AI Act and the EU Cybersecurity Act, gives us rules to follow, and we have protection thanks to ENISA (European Union Agency for Cybersecurity). We must continue to grow as a team, because cyberattacks do not target just one country, and don't respect borders between countries. We also must align our rules to avoid weakness in case of attack and steer clear of putting the whole European Union at risk.Even though other countries don't set up the same regulations as us, we should align with each other in order to fight against these extremely dangerous assaults. Europe's legislation NIS 2 helps us since December 2025 feel more secure, because it elevates security systems all over our continent. In addition, the Cybercriminality convention organised by the NU (2024) has been signed by 193 countries, and that simplifies the difficulties set by frontiers and in parallel respects human rights.

In our country, we recently implemented new rules concerning information stealing for public authorities. Some attack-defense strategies have been set up with the aim of strengthening security in public and private spaces. All this is done thanks to BSI (Federal Office for Information Security), which helps us detect any form of spying or hacking. Recently, we reunited at the Summit on European sovereignty among 23 European countries, organised by ourselves and France cooperation. Our goal was to start taking our place in the digital environment and stop depending on other countries, especially the United States, who take the bigger spaces in terms of technology with companies (Apple, Google, Meta…) but also Asian companies (Samsung, TSMC, Sony…). We would like to have our own digital big multinationals in order to rely on our security inside the EU and that must be done as a team. At the same time, we want to guarantee that our citizens will conserve as much privacy as possible and will be safe from the possible following attacks.

IMPLEMENTED SOLUTIONS

As we said in the previous paragraph, Germany has started to commit more and more in issues concerning technology, it is now a key element in our daily lives that we can not remove but regulate. The economical expenses on cybersecurity are increasing by year with millions of euros (11.000 millions in 2024), and we expect to increase this outgo every year. These huge expenses are due to the elevated cost of cyberattacks, which forces us to enlarge our investments. Thanks to new rules and laws, we are creating a lot of employment opportunities, to cover up all the activities required by this sector. This year, 2026, we have many new rules to follow; the Data Act is planned to begin in September, which demands all the IoT fabricants to ensure a secure service, in order to stimulate innovation and competitiveness.

Another initiative is the Digital Omnibus, which consists in simplifying and organizing the digital rules by readjusting the pre existing laws. Since 2026's beginning, the Cyber Resilience Act is renewing its obligations to align with European Conformity. The Network and Information Security Directive 2 (NIS2) helps us detect the risks with strict standards and reinforced surveillance. We have to start implementing security measures such as a permanent EU platform where all our governments share information and strategies. We should be able to contact it all day, like a sort of "Cyber OTAN" that could provide help to multiple countries at the same time, coordinating itself at any time of the day. It could have strategies for different situations, and learn about the main hacker groups concerning Europe to manage crisis moments. The ideal is to be centralised in order to avoid misunderstandings between countries, but we could also function with an hybrid model, coordinating via ENISA, conserving every country's politics, because if we implement the same rules for all of Europe, it will take a long time, and meanwhile, we must follow what is currently in place. It should be financed by the Digital European Programme, with European funds, and at the same time, each participant country must contribute. As we said, if we want to avoid more attacks and less security, every European member should cooperate and play a part in this growing issue.

CONCLUSION

To conclude, we must repeat that we are consistent on cybersecurity growth with all European members as a team. We must stop depending on other continents and start creating a European network that protects us all and guarantees great and independent life to all of our citizens, because cybersecurity doesn't concern only technology, but also politics and citizens' safety. Reinforcing our position in the EU and taking advantage of the privileges of being a member of the EU.

Sofía López Ruiz

SITIOGRAPHY

https://www.deutschland.de/fr/topic/politique/desinformation-cyberattaques-allemagne

https://www.lemonde.fr/international/article/2025/12/12/l-allemagne-accuse-la-russie-d-une-cyberattaque-contre-la-securite-aerienne-et-d-ingerence-lors-des-dernieres-elections-legislatives_6657045_3210.html

https://www.touteleurope.eu/pays/allemagne/

https://allemagneenfrance.diplo.de/fr-fr/actualites-nouvelles-d-allemagne/02-europe/2744282-2744282

https://cybersecurity-centre.europa.eu/national-coordination-centre-cybersecurity-federal-office-information-security-bsi-germany_en

https://www.teamfrance-export.fr/infos-sectorielles/39758/39758-lallemagne-met-a-jour-sa-legislation-numerique-les-implications-pour-le-secteur-iot

https://www.deutschland.de/es/topic/politica/alemania-ciberseguridad-bsi-contrasena-y-seguridad

https://en.wikipedia.org/wiki/Federal_Office_for_Information_Security