

DELEGATION : Denmark

COMMISSION : Conseil de l'UE sur la 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?”*

As one of the most digitized nations in the world, Denmark is firmly committed to cybersecurity and sees it as a strong pillar of stability. The Danish government, led by Prime Minister Mette Frederiksen from the Social Democrats political leftwing party, continues to strengthen our country's institutions to face cyberattacks which intensify day after day. These threats are a direct attack to citizens' daily life and Denmark wants to make sure we can assure a safe future, protecting fundamental rights and its state sovereignty, but with European support. Our country is so dependent on digital systems that any breach of security directly threatens the high level of public trust that is the foundation of Danish society.

With the uncontrollable rise of AI, cybersecurity is deeply threatened, with algorithms with no human control who find weaknesses faster and can more accurately open security breaches on an individual level and national level. These new technologies can also lead to massive misinformation by generating fake news and images that can be problematic for our democratic countries. Denmark is particularly exposed due to its leadership in sectors like green energy and maritime shipping which have already been attacked in the last few years.

As a result of different threats and disruptions in our country like waterworks sabotage in 2024, national and european election interferences in 2024-2025, and the attack of twenty-two energy companies in 2023, which is considered the largest cyber attack until today, the government is extremely committed to developing the cyber protection, with the idea that we must be able to protect ourselves sufficiently. A high level of cyber security will continue to matter to the growth of Denmark and the safety and trust in the public authorities in a digitized age. Our country wants to be able to count on the UE's cooperation. Following the 2022 referendum, Denmark has ended its defense opt-out, signaling a historic shift towards full integration in the EU's security and defense programs. Our country has transitioned from a specialized observer to an active leader in the EU's Common Security and Defence Policy. No nation can resist global hybrid threats in isolation. Therefore, Denmark supports a robust and unified EU framework, including the strict implementation of the NIS2 Directive and the Cyber Resilience Act (CRA). However, while Denmark is a dedicated partner in the Union's collective defense, it insists that this collaboration must strictly respect Article 4(2) of the Treaty on European Union (TEU). This article ensures that national security remains the sole responsibility of each Member State. For our country, the EU should act as a force multiplier by sharing intelligence and setting high standards, but the operational management of critical infrastructure and intelligence services must stay under national sovereign control to ensure democratic accountability.

Denmark has already started several successful solutions to protect our country. Our country was one of the first in Europe to apply the NIS2 Directive, which forces over 1,000 essential companies to follow strict security rules. The Center for Cybersecurity (CFCS) works 24/7 to monitor threats and help the government react quickly to hacks. The National Strategy for Cyber and Information Security (2022) provides significant funding to improve national cyber-defense and military protection. Finally, the government launched Sikkerdigital.dk, a

special website that gives free tools and advice to citizens and small businesses to help them stay safe online. During the debates, Denmark may propose three new projects to the European Union: first, a European fund to give money to small businesses so they can buy better security tools. Second, our country might ask for an emergency security clause that would allow every nation to act fast in case of an emergency. If Denmark finds a dangerous piece of technology from a high-risk country in our essential domains, we shouldn't have to wait months for the EU's authorisation to ban it. And finally, to prevent massive data leak in very digitized countries Denmark could propose a certificate for all government workers to teach them how to protect private data.

As a conclusion, Denmark is a dedicated and active member of the European Union. Our country believes that a strong and united Europe is the best way to stop global cyber threats and protect our digital society. However, the Danish government will always defend its national sovereignty and its right to protect its own citizens and infrastructure. By working together on practical projects, like helping small businesses and training government workers, the Union can build a safer future for everyone.