Background note

Session V: Towards strengthening the EU's collective effort to improve cyber-resilience and tackle disinformation

Introduction

Over the past few years, the development of digital technologies has reached a very high, even unprecedented pace, and has begun to affect virtually every aspect of daily life, global economy and policy. Therefore, the European Union was relatively quick to recognise that one of its objectives should be to increase technological capabilities and skills in the field of cybersecurity, alongside building a strong digital single market. The noticeable convergence of the military and civilian understanding of cyberspace along with the strengthening of the European Union Agency for Cybersecurity established in 2004 has become a significant element of the EU's approach to cybersecurity. The growing awareness of the importance of cybersecurity was also a consequence of the 2017 decisions of the European Commission, which adopted a three-pillar strategy for cybersecurity in the EU. The first pillar built the EU's resilience against cyberattacks, the second shaped effective cyber-prevention and the third strengthened international cooperation in the field of cybersecurity. In view of the above, the strategy is usually referred to as: resilience, prevention and defence, which became a staple of the EU's cybersecurity policy.

The key assumptions of this approach include: 1) development towards a single market for cybersecurity; 2) effective implementation and evaluation of the Directive on Network and Information Security; 3) enhancing resilience through rapid crisis response; 4) developing a strong EU cyber skills base; 5) promoting cyber hygiene and threat awareness; 6) identifying malicious actors; 7) fostering public-private cooperation in the fight against cybercrime; 8) improving political response in the cyberspace; 9) building cybersecurity capabilities, and 10) focussing on cybersecurity in external relations. The European Union outlined a detailed strategy for action in 2018, which involved the establishment of the European Digital Media Observatory to improve the detection of cyberattacks and disinformation, collaborate with online platforms and raise awareness, enabling citizens to respond to online disinformation.

The functioning of the European Digital Media Observatory proves that the increased awareness of the various types of online disinformation activities is linked to the protection of the EU cyberspace. The EU defines disinformation as false or misleading content that may cause public harm, disseminated with the intent to mislead or to secure economic or political advantage. The EU notes that disinformation also includes misleading content, which is made available without malicious intent, but which has harmful effects from the point of view of EU societies. The dissemination of both disinformation and unintentionally misleading information

(misinformation) may jeopardise European democracies and have many harmful consequences, such as promoting or even extending the influence of external enemies, exposing the health, security and environment of the EU to various threats with unforeseeable and immeasurable consequences. One should keep in mind that large-scale disinformation campaigns are a major challenge for Europe and require a coordinated response from EU states, EU institutions, online platforms, news media and EU citizens themselves.

In the new institutional cycle for the period 2024-2029, the European Commission promotes a democracy shield project, the priorities of which include combating disinformation. Therefore, the EU's latest objective is to develop a European Network of Fact-checkers and to ensure that this information is available in the official languages of all EU member states. The initiative to bolster the capacity of these institutions will build on the work of the European Digital Media Observatory. Another new action is the implementation of the Digital Europe 2025-2027 programme. It will focus on the deployment of artificial intelligence (AI) and its use by businesses and public administration, cloud computing and data, cyber resilience and digital literacy, and combating disinformation.

Current challenges

The scale of the cybersecurity challenges is best demonstrated by the latest European Union Agency for Cybersecurity report presented in March 2025. The report diagnoses the maturity and cyberthreat resilience of critical sectors, covered by the Directive on measures for a high common level of cybersecurity within the Union (NIS2). The important takeaway is that the analysis reveals significant disparities: while the energy, banking and telecommunications sectors are in the lead, others, such as public administration, healthcare and space sector, remain in the so-called risk zone. The report is the first comprehensive analysis to assess the maturity and resilience of the NIS2 sectors, providing both a comparative overview and a more in-depth analysis of each sector. The document is designed to help states and national authorities identify gaps and prioritise the effective use of resources to ensure a high level of cybersecurity across the Union. The survey is based on data from national authorities, companies and EU institutions such as Eurostat. The report not only identifies existing gaps and risks, but also offers a comprehensive set of policy recommendations aimed at states, supervisory authorities and the NIS2 sectors themselves. Sectors rated better in the study have benefited from significant regulatory oversight, global investment, policy direction and robust public-private partnerships, and their resilience is crucial for social and economic stability. Sectors with a sufficient level of maturity featured in the report included digital infrastructure, basic internet services, trust services, data centres and cloud services. Admittedly, there are still challenges in these sectors due to the inherent heterogeneity, cross-

border nature and the inclusion of previously unregulated entities within their scope, but the level of cyber resilience is relatively high.

In addition, the report identifies four sectors and two sub-sectors, which are in the 'risk zone'. They include: 1) ICT service management; 2) space sector, 3) public administration; 4) maritime sector; 5) healthcare and 6) gas sector. These sectors require particular attention to ensure that the identified maturity gaps are addressed in a way that enables their constituent entities to effectively tackle additional challenges. The report demonstrates that all sectors face challenges in building their own maturity and meeting the requirements of the NIS2 directive. To better support these sectors, closer cooperation within and between sectors is recommended, as well as the issuing of sector-specific guidelines for the implementation of risk management measures.

The recommendations identified the need to develop national cybersecurity capabilities, with a particular focus on sectors in the so-called 'risk zone'. One possibility is to create specific technical and knowledge support programmes for regulators and public sector organisations. It is also important to increase the availability of specialised training, cybersecurity exercises and tools to support risk analysis and incident response. In addition, the European Union Agency for Cybersecurity places a strong emphasis on the need to promote information sharing and cross-sector cooperation. It is suggested to expand the role of structures such as ISACs *(Information Sharing and Analysis Centres*), which should exist not only at national level, but also at European level. The report notes that joint exercises, sharing threat scenarios and the development of information-sharing platforms are key to increasing awareness and preparedness. Finally, the integration of sectoral risk analyses with decision-making processes at public policy level is key to ensuring cybersecurity. Some sectors - including energy and banking - are already using such approaches, but there is a need to extend this practice to more industries, especially in sensitive sectors such as healthcare, public administration, and ICT services. This should lead to better resource planning, investment and more effective implementation of digital security strategies. The report also includes a recommendation to further develop cybersecurity exercises on a European level. Cyber Europe exercises, which include cross-sector failure scenarios, should be expanded to include components of operational technology, supply chains and critical cross-sector dependencies. This includes in particular the integration of sectors that have so far rarely taken part in such events, such as space, district heating and hydrogen sectors.

In the area of disinformation, the challenges stem from the complexity of the phenomenon. In principle, it has three forms: 1) disinformation disseminated by external actors (such as states or organisations); 2) local disinformation, which in many cases replicates the former, but this is by no means necessarily the rule; and 3) misinformation, which includes the dissemination of manipulative or false content by individuals, often unknowingly, through

a variety of communications (TikTok, X, Facebook). In order to effectively combat disinformation and misinformation, a number of actions and measures are required, which include: 1) funding and supporting entities that identify and record specific instances of disinformation, including fake news (*fact-checking*); 2) developing human resources, mainly by acquiring qualified personnel; 3) effective communication, including the creation of truthful, interesting narratives and effective delivery of messages that reach their audience; 4) building relationships and trust, as actors fighting against disinformation need to constantly strengthen their credibility and undertake positive campaigns to build trust and commitment among citizens, while understanding their needs and the delicate balance in a pluralistic democratic society with different opinions and views (the fight against disinformation cannot be a means of imposing a single vision of the world: if it is perceived in this way, it will turn into disinformation); 5) digital transformation, which will provide access to effective digital tools for data acquisition and visualisation, graphic design and video editing, which will allow content verification and thus ensure critical thinking skills.

The importance of security was highlighted in the 'Warsaw Call' - a joint statement adopted by EU cybersecurity ministers on 5 March 2025 during an informal meeting organised by the Ministry of Digital Affairs. The Warsaw Call is an important reference point for future European Union action on the protection of digital space at a time of growing geopolitical challenges. It draws attention to specific EU actions in the following areas: 1) strengthening crisis management through the seamless adoption of the Cybersecurity Blueprint; 2) strengthening civil-military cooperation in the area of cybersecurity, including EU-NATO partnership; 3) adopting a roadmap for new technologies and strategic foresight in the area of cybersecurity; 4) increasing efforts to combat the shortage of cybersecurity experts in the EU.

A particular challenge in the area of cybersecurity and disinformation concerns building the resilience of democratic societies to crisis situations. Particular protection should be given to all democratic procedures, such as elections or referendums, which are targeted by attacks and manipulation. Experience shows that these moments coincide with particular interest from external actors in influencing the political scene of the EU member states. The institutions upholding democracy must operate in a particularly careful and measured manner so that public trust is not damaged and the institutions themselves do not start to be seen as participants in a broad and complex process of disinformation.

Questions for discussion

1. What is the role of the European Union and its institutions in building EU resilience to threats concerning cyber-infrastructure and disinformation?

2. How to strengthen the cyber resilience of sectors in the so-called risk area, namely ICT service management, administration and healthcare?
3. What should be the role of digital platforms in ensuring cybersecurity for EU societies?
4. How to strengthen civil society organisations in the effective fight against disinformation?
5. How to modify tools to combat disinformation when it changes and adapts to socio-political contexts?
6. How to build effective communication channels aimed at raising trust in information to increase the audience's awareness of the potential for disinformation or misinformation?
7. What are the possibilities of using artificial intelligence (AI) to ensure adequate levels of cybersecurity and effectively combat disinformation?