Cyberspace and EU action to 2030

A report based on an expert webinar organised by the French Permanent Representation to the European Union on 9 July 2021 with the support of the EU Institute for Security Studies.

Report

INTRODUCTION

Cyberspace is today at the **core of prosperity and sovereignty**. Our societies are increasingly dependent on digital networks and services but are exposed to malicious cyber activities led by both State and non-State actors. The Covid-19 pandemic has revealed **deep cyber vulnerabilities** and spurred a sharp rise in cyber criminality, notably through ransomware attacks. The rise of malicious behaviour in cyberspace increasingly undermines and threatens the integrity, security and economic growth of our respective societies, and can lead to destabilising and cascading effects with enhanced risks of conflict. In addition, the **growing trend towards fragmentation of cyberspace and its exploitation** for political and ideological purposes directly challenges the EU's economic, security and democratic interests. It goes against the EU's position of advancing a global, free, stable, secure and open cyberspace.

The EU's recent push toward **digital and technological sovereignty** is vital for the EU's security and economic prosperity. The EU has already come some way in developing tools that reinforce cyber cooperation between the Member States across the four main cyber communities: digital security, cybercrime, cyber diplomacy and cyber defence. However, the EU cannot rest on its achievements. The **Strategic Compass and the first-ever threat analysis** conducted at the EU level has provided, regarding cyber, a clearer view over the wide range of pressing challenges and risks the Union faces. It is also a unique opportunity to strengthen, in the cyber realm, the EU's abilities and tools related to solidarity, resilience, technological edge and freedom of action. The **Strategic Compass** can give us a more complete picture of existing and future threats but, looking towards 2030, it can also **contribute to wider EU efforts to enhance its cyber resilience, especially through solidarity, and its strategic autonomy in cyberspace**.

AN ASSESSMENT OF THE CURRENT STATE OF PLAY, CHALLENGES AND THREATS

The EU has come some distance in developing its approach to cyber resilience over the past decade, especially as in the past the combinations of "cyber" and "defence" in the same sentence were treated as taboo. Such changes are needed because **cyber space is a battleground for geopolitical competition**. It is also the case that in the cyber realm there is a "grey area" that is being continuously exploited by malicious State and non-State actors. The EU needs to recognise that this **"grey area" is an arena where power is exercised** and it is a vital route for data gathering, active intelligence activities and espionage. In this respect, there is a need for the EU to recognise that

"there are no friends in cyberspace" and for it to truly develop its cyber defences it needs a **greater sense of European sovereignty and a strategic culture** to safeguard digital and technological critical infrastructure. However, today there is a trust deficit on cyber resilience.

Such a realisation has far reaching implications for the EU. First, it calls for **major investments in the cyber domain** and digital resilience to protect EU institutions and EU Member States. Second, the Union needs to invest in its **cyber crisis management capacities**. Third, cyber vulnerabilities raise questions with regard to the application of the **mutual assistance clause** (Article 42.7 TEU) and this requires a more ambitious level of solidarity among Member States. It also means considering how affected EU Member States could utilise EU-wide cybersecurity assets and frameworks in case of invocations of Article 42.7 TEU. Finally, there is a need to invest in collective EU cyber responses to **large-scale cyber-attacks** on EU critical infrastructures, even when they are below the threshold of Article 42.7 TEU.

However, it is necessary to recognise the steps that the Union has taken over the past years. Legislative mechanisms such as the Networks and Information Security (NIS) Directive and its forthcoming revision ("NIS 2" Directive) are positive developments. The EU Cyber Security Strategy also provides greater direction and the EU's Foreign Investment Screening Mechanism, the cybersecurity of 5G Networks toolbox and the cyber diplomacy toolbox are **valuable capacities**. The ongoing cyber-related Permanent Structured Cooperation (PESCO) projects will also enhance the EU's cyber resilience and security. The CERT-EU, ENISA and the European Commission play a decisive role in developing **monitoring, surveillance, early warning and response capacities to EU institutions**.

Despite these positive steps, there is more the EU can do to enhance its cyber resilience. First, the Union should treat cyber matters as a **cross-cutting issue** that intersects with various policy areas. While the EU has started to overcome the disjointedness of its cyber initiatives, more is required to ensure a **singularity of purpose** on cyber resilience across the EU's security, digital, economic and trade policies. If the EU wants to safeguard its **citizen-focused approach** it needs to develop its cyber resilience and technological sovereignty.

More than this, the EU has to avoid treating digital technology, Artificial Intelligence (AI), 5G and quantum computing as separate technological domains because they are critical for cyber resilience - a common approach pulling together all of these areas is a necessity. The Union should also consider conducting **cyber threat mapping exercises** and undertaking more frequent cyber exercises. Such threat mapping exercises cannot only focus on the State level and they should allow EU Member States to undertake risk assessments of the regional and local levels, as well as to work with the private sector to ensure **effective public-private partnership** on cyber matters. To encourage cooperation at all of these political levels, the EU needs to enhance its strategic communication on cyber matters as EU citizens still do not fully comprehend the Union's actions in the cyber realm.

SETTING AN ADEQUATE LEVEL OF AMBITION FOR THE EU BY 2030

Cyber issues should become a fully-fledged plank of the EU's foreign and security policies, as this is a way to develop **greater strategic awareness for cyber issues** as well as to create a cyber risk culture among EU institutions and EU Member States. A core need at present is greater political awareness for the importance of cyber resilience. There is a need to generate **political awareness**, but the EU should not neglect a multistakeholder approach that engages the private sector and civil society. Such an approach would allow the EU to take a more **commanding role on cyber and technology** issues at the international level and allow it to push back against the normative and regulatory advances of third States. Integrating cyber issues in the Union's foreign and security policies would also allow the EU to develop **cyber partnerships** with vulnerable States and partners.

The revision of the NIS Directive ("NIS 2") offers the EU an opportunity to think intelligently through its weaknesses and to develop new tools. For example, the Union can aim to raise the costs of cyberattacks by **developing "cyber insurance" measures** that help protect businesses and individuals from sensitive data breaches. Regulation and norms are key to providing cyber resilience. New technologies and systems such as **cloud computing** require that EU data uses are regulated by EU rules and norms and not by standards and regulations imposed from outside the Union. The Union needs to invest in its **early warning capacities** for cyber resilience. Careful assessments of cyber-attacks and potential attribution will become more difficult in future, and this requires a more integrated situational awareness and intelligence framework.

The Union should recognise **that international norms and regulations** are important but they are **not enough** to ensure the EU's cyber resilience. Investment in technologies and services are required at a much faster pace in the EU. The reality today is that the EU lacks its own **ecosystem of technology providers** so as to supply the Europeans with trustworthy and secure systems and technologies for Europeans. This is important because of underappreciated trends in the digital sector: there is an overall **fragmentation of the Internet** as authoritarian States disconnect from the global system, but there is a **market concentration** around only a handful of increasingly powerful foreign firms. These two major trends should pose acute cybersecurity concerns for the EU, as well as raise questions about the Union's technological and digital sovereignty.

Digital powers are investing huge amounts of financial resources into new technology domains such as quantum, cloud and edge computing and AI. The EU needs to **prepare for a horizon to 2030** that includes wider and more **ambiguous digital** threats where the application of AI can be used by adversaries to undertake more sophisticated attacks on the EU's critical infrastructures and democratic societies. Enhanced geo-location technologies, deep fake videos, cyber vandalism, passive and active data routing technologies, biomedical tests and economic and financial data are likely to be used in the future to **maintain a technological edge and information superiority** over Europe.

The EU clearly needs to focus on future challenges in the cyber realm sooner rather than later. For example, the Union can enhance its strategic thinking on how to ensure secure and smart cities. **Urban environments are vital for the democratic and economic health** of EU Member States, but they are increasingly the locations for digital connectivity. This poses certain vulnerabilities that the EU needs to tackle, including through investments in secure networks and communications and ensuring that no digital "back doors" can be exploited by malicious State and non-State actors. Additionally, the EU needs to ensure that its **digital supply chains** are resilient.

The interface between critical digital and physical infrastructures should be increasingly factored in for the EU's approach to **critical infrastructure protection**. For example, there is a need to ensure the security of cloud services and to protect undersea telecommunications and fibre optic cables. Here, there is a need to consider a **"security by design"** approach to the development of digital infrastructure and technologies. Another factor that the EU should continue to focus on is the exportation of cyber surveillance technologies to regimes that may undermine human rights and the EU's values.