MPR PARTNERS
MARAVELA, POPESCU & ASOCIAȚII

WE TRANSLATE LEGAL
TO BUSINESS

EUROPEAN UNION'S NEW CYBERSECURITY STRATEGY

1. Background

Cybersecurity is at the forefront of the European Union ("**EU**")'s efforts to build a resilient, green and digital Europe. In this respect, on December 16, 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented the European Union's new Cybersecurity Strategy for the Digital Decade[1] (the "**EU Cybersecurity Strategy**").

The EU Cybersecurity Strategy is an ambitious document aimed at ensuring secure and reliable digital tools and connectivity throughout Europe, being part of the broader EU digital strategy that aims to transform Europe in a global leader for digital economy.

We live in a world where vital sectors such as transport, energy and health, telecommunications, finance, security, democratic processes, space and defence rely more and more on increasingly interconnected network and information systems. In the near future, there will be an exponential increase in the number of interconnected devices throughout all the industries.

In order to help reduce the vulnerabilities presented by such interconnected devices, the EU started setting the stage, by creating the conditions for the integration of cybersecurity into all digital investments (particularly when it comes to technologies like Artificial Intelligence, encryption and quantum computing).

2. The structure of the Cybersecurity Strategy

The new EU Cybersecurity Strategy is divided into three parts: (i) resilience, technological sovereignty and leadership, (ii) building operational capacity to prevent, deter and respond and (iii) advancing a global and open cyberspace.

[1] More details can be found here: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

2.1. Resilience, technological sovereignty and leadership

This part of the Cybersecurity Strategy focuses on the EU's critical infrastructure and essential services. In the EU's view both the private and public sectors must be able to have a choice amongst the most secure infrastructures and services.

2.1.1. Reforming NIS Directive

According to the European Commission, the Directive on security of network and information systems ("**NIS Directive**") is at the core of the Single Market for cybersecurity. However, there is a need to increase the level of cyber resilience of all relevant sectors, including energy, transport, health and the financial sector, that are fundamental for the economy and society. Moreover, reviewing NIS Directive will help reduce the inconsistencies across the internal market, and it will provide specific rules for strategically important sectors, so that to become more cyber resilient.

2.1.2. The role of ISACs, CSIRTs and SOCs

In the race to become more cyber resilient, an important role will be played by the Information Sharing and Analysis Centres ("**ISACs**"), Computer Security Incident Response Teams ("**CSIRTs**") and Security Operations Centres ("**SOCs**"). These centres are set up by the public and private sector to tackle cybersecurity threats, by disseminating relevant information, identifying real-time anomalies or detecting the activity of malicious executables. Taking into account the importance of such centres, the European Commission is willing to spend over EUR 300 million to build a network of SOCs that would create collective knowledge and share best practices on fighting cyber threats.

2.1.3. Securing both the communication infrastructure and the next generation of broadband mobile networks

The Commission plans to work together with Member States to build a secure quantum communication infrastructure ("**QCI**") for Europe, that will ensure the security of communications of public authorities. The QCI will be composed both of fibre communications networks and of linked satellites covering the EU and EU overseas territories.

In March 2019, the Commission equally started working on 5G technology and the need to have secure next generation of broadband mobile networks, by publishing a Recommendation on the Cybersecurity of 5G networks ("**EU Recommendation**") In October 2019 this was followed by the EU coordinated risk assessment of the cybersecurity of 5G networks and in January 2020, by the Cybersecurity of 5G networks EU Toolbox of risk mitigating measures ("**EU 5G Toolbox**"), a common set of measures meant to mitigate the main cybersecurity risks of 5G networks.

In October 2020, the European Council called on the EU and the Member States "*to make full use of the 5G cybersecurity toolbox"* and "*to apply the relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessments, based on common objective criteria*".

In December 2020, the European Commission has published a report on the impact of the EU Recommendation, showing that Member States had made significant progress in implementing the EU 5G Toolbox, albeit with some variations and remaining gaps. However, the European Commission has encouraged Member States to continue implementing the main recommendations of the 5G Toolbox by the second quarter of 2021.

2.1.4. Keeping IoT and Internet secured

The European Commission will adopt the first Union Rolling Work Programme, as required by Article 47 of the Regulation 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) in the first quarter of 2021. The Rolling Work Programme has the role to identify strategic priorities for future European cybersecurity certification schemes.

The European Commission is also considering enacting new horizontal rules for bolstering connected product cybersecurity, such as a duty for software manufacturers to address software vulnerabilities (for example, by continuing to provide software updates and to erase personal and sensitive data at the end of the lifecycle of the software product). Cybersecurity will be strengthened also in motor vehicles and some wireless products.

The European Commission will also be creating a contingency plan for extreme scenarios affecting the integrity and availability of the global DNS root system.

2.1.5. The importance of the technology supply chain

EU's ambitions are to propel its Industry Strategy[2] and leadership in digital technologies and cybersecurity across the digital supply chain (including data and cloud, next generation processor technologies, ultra-secure connectivity and 6G networks), in line with its values and priorities.

An important role will be played by the proposed Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres ("**CCCN**") that will be located in Bucharest, Romania. The CCCN, alongside the industry and the academic communities, will help developing the EU's technological sovereignty in cybersecurity, building capacity to secure sensitive infrastructures.

[2] More information can be found here https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy_en

2.1.6. Developing cyber skills

EU plans to massively invest in upgrading the digital skills of its workforce, especially by raising cybersecurity awareness among children, young people, and small and medium companies.

2.2. Building operational capacity to prevent, deter and respond to cyberthreats

A Joint Cyber Unit is envisioned as part of building the EU's operational capacity for fighting cybersecurity threats,. The European Commission will work with the Member States and relevant EU institutions and agencies to build the Joint Cyber Unit not as a standalone body, but as a virtual and physical platform coordinating the different cybersecurity communities (private and public) in the EU against major cross border incidents and threats.

The objectives of the Joint Cyber Unit would be to:

- prepare the cybersecurity communities to face threats;
- provide shared situational awareness;
- reinforce coordinated response and recovery.

The steps for defining, preparing, deploying and expanding the Joint Cyber Unit must be presented by the European Commission by February 2021.

However, building resilience capacity is not sufficient to remove cybersecurity threats. The European Commission also plans to strengthen the response capacity of enforcement authorities, by providing them with the necessary skills and tools. One of the stringent problems the European Commission will work on is providing access to electronic evidence for criminal investigations in different jurisdictions. In this regard, the European Commission has prepared a package of proposals regarding e-evidence, which it hopes will be adopted swiftly by the European Parliament and by the Council.

Cybersecurity resilience also entails diplomatic response. In May 2019, the EU introduced its legal framework for targeted restrictive measures against cyber-attacks. To date, eight individuals and four entities involved in or responsible for cyber-attacks were listed. The EU is committed to further increase its efforts to strengthen the cooperation with international partners in order to develop cooperative diplomatic responses.

Not only diplomatic, but strengthened military response is planned. The Cyber Defence Policy Framework ("**CDPF**") will be reviewed, and Member States together with the EU are encouraged to develop state-of-the-art cyber defence capabilities through different EU policies and instruments.

2.3. Advancing a global and open cyberspace

The overarching goal of the EU is promoting a model of cyberspace rooted in in the rule of law, human rights, fundamental freedoms and democratic values.

In order to promote these values, the EU will have to:

- increase its engagement in the standardisation process, including by increasing its representation in European and international standard development entities;
- to take a proactive role in advancing Member States' positions in international fora, as well as developing an EU position, on the application of international law in cyberspace;
- continue to promote and protect human rights and fundamental freedoms online;
- strengthen and expand its dialogue on cyberspace with third countries, enhance EU-NATO cooperation on cyber defence;
- defend the multi-stakeholder Internet governance;
- develop an EU External Cyber Capacity Building Agenda and an EU Cyber Capacity Building Board whose scope would be to support its partners to increase their cyber resilience and capacities to investigate and prosecute cybercrime.

3. Cybersecurity in European institutions

This part of the Cybersecurity Strategy takes stock of the current situation of cybersecurity in relation to EU institutions. Progress is reported on protection of EU classified information as well as sensitive non-classified information. However, there is still a limited interoperability of classified information systems, which prevents entities to seamlessly transfer information. Moreover, the level of awareness of cyber risks needs to be raised within EU institutions.

Therefore, a Regulation on Information Security in the EU institutions bodies and agencies and a Regulation on Common Cybersecurity Rules for EU institutions, bodies and agencies are proposed as strategic initiatives.

4. Conclusions

The EU Cybersecurity Strategy sets ambitious goals, both in terms of new regulations, as well as in terms of international cooperation. Nevertheless, as long as cybercrime remains extremely profitable for perpetrators (with an annual estimated cost of cybercrime to the global economy in 2020 of €5.5 trillion, double that of 2015), the safety of critical infrastructures and goods of ordinary citizens and companies will continue to be threatened. Thus, EU will need to step up efforts in order to be able to counteract the cyber-attacks of the future.

*****

This article contains general information and should not be considered as legal advice.

Flavia Ștefura

Senior Associate

flavia.stefura@mprpartners.com

Cristina Crețu

Senior Privacy & Technology Consultant

cristina.cretu@mprpartners.com