icom
istituto per la competitività

MAKING EUROPE SAFER

A new cybersecurity strategy to build trust and resilience

Policy Brief
January 2021

AUTHORS

Silvia Compagnucci, Domenico Salerno

Abstract

Digitalisation is revolutionizing business models and the relationship between authorities and citizens and between enterprises and consumers creating new opportunities, but also raising some critical issues. Among these, one of the most important is IT security. The increase in online activities and devices connected to the network increases the points of vulnerability that could be exploited by cyber-criminals. The restrictions on the mobility of individuals imposed by governments to curb the Covid-19 pandemic have made this problem even more serious. For example, according to data collected by the Swiss Cybersecurity Institute, cyber-attacks in the country during the month of April 2020 tripled compared to the monthly average.

The growing importance of the problem has placed the issue of placing cybersecurity at the top of the European Commission's list of objectives. Since 2013, with the EU Cybersecurity Strategy, the EU authorities have tried to adopt measures to contain the problem. The enhancement of IT security is also a fundamental step to be taken in the implementation of 5G. The European Union must be able to define and implement effective security standards in order to make the development of 5G networks possible. This is a core target as these networks are a key element for the internal market to evolve, especially for the effective management of central economic and social services, such as energy, transport, financial services, health systems and industrial controls.

As a part of the Recovery Plan Communication “Europe's moment: Repair and Prepare for the Next Generation”, the Commission published a new Cybersecurity Strategy focused on three pillars and connected initiatives. These will increase the level of cyber resilience of critical public and private sectors, encourage the upskilling of the workforce, attract and retain the best cybersecurity talent, strengthen cooperation between EU bodies and Member State authorities responsible for preventing, deterring and responding to cyber-attacks and step up work with international partners to strengthen the rules-based global order, promoting international security and stability in cyberspace, and protecting human rights and fundamental freedoms online.

1. Cybersecurity in the EU. An overview

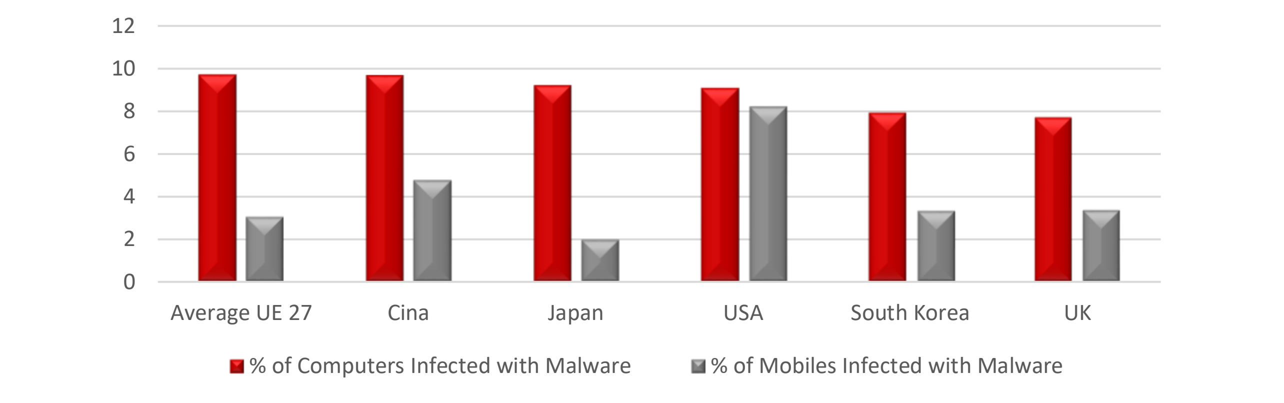
Over the last decade digitisation has transformed everyday life. Digital platforms in recent years, and overall during the Covid-19 pandemic, have represented the privileged space where individuals can carry out their work, social and leisure activities. According to the EU Commission, 40% of European workers have experienced forms of tele-working since the start of the pandemic, making home computers, which are generally less protected than office and company devices, the point of access to data and valuable digital activities. Along with the many advantages (always accessible, everywhere and at any moment), this relatively new way of living has brought to light many new problems in terms of security and, specifically, cybersecurity.

The digital environment is vast and, therefore, an ideal ground for cyberattacks that can be either indiscriminate or targeted, aimed at large and small organisations in both the public and private sectors. Therefore, Internet usage and its connected devices offer new opportunities for people and companies but, at the same time, create new risks. The range of potential attacks and attackers is wide and becoming more so by the day, up to the point that at the Davos World Economic Forum of 2021 cybersecurity was regarded as one of the greatest economic risks for the ongoing year. The new technologies, mobiles, smart devices connected to the Internet of Things and many artificial intelligence applications expose both private and public organisation to attackers, increasing the risks of, for example, shutdowns or subversion of industrial control systems. Furthermore, attacks are becoming worryingly more sophisticated and costly to detect.

The magnitude of the phenomenon becomes evident by observing the data on computer attacks that affect the electronic devices we use daily. According to a study carried out by Comparitech in the third quarter of 2019, 9.68% of computers and 3.04% of mobile devices in the EU were infected with **malware**[1]. Comparing the European data with that of the other major world economies, we can see how the European Union ranks first for the percentage of infected computers, ahead of China, Japan, the USA, South Korea and the UK. Instead, where mobile devices are concerned, the EU Member States are on average more protected than those of all the other geographical areas considered with the exception of Japan (Fig.1).

[1] Malware is any software intentionally designed to cause damage to a computer, server, client or computer network

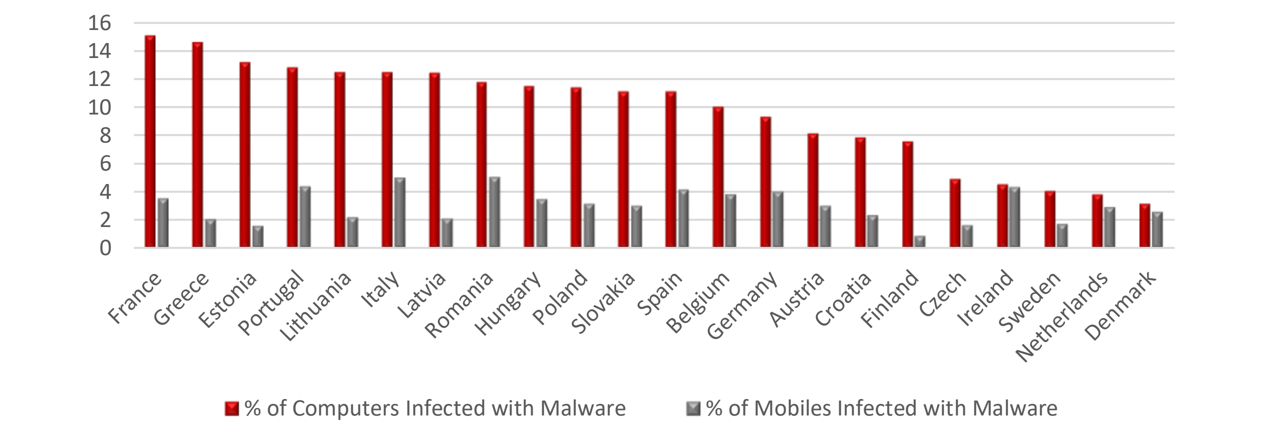
Fig.1: Cyber-attack target devices by geographic area (2019)



Source: Comparitech, 2020

By observing the individual EU MSs (Fig.2), we can see that those most targeted by cyber-attacks on computers are France (15.09%) and Greece (14.59%). Instead, those most vulnerable on mobile devices are Romania (5.04%) and Italy (5:01%).

Fig.2: Cyber-attack target devices in the EU (2019)

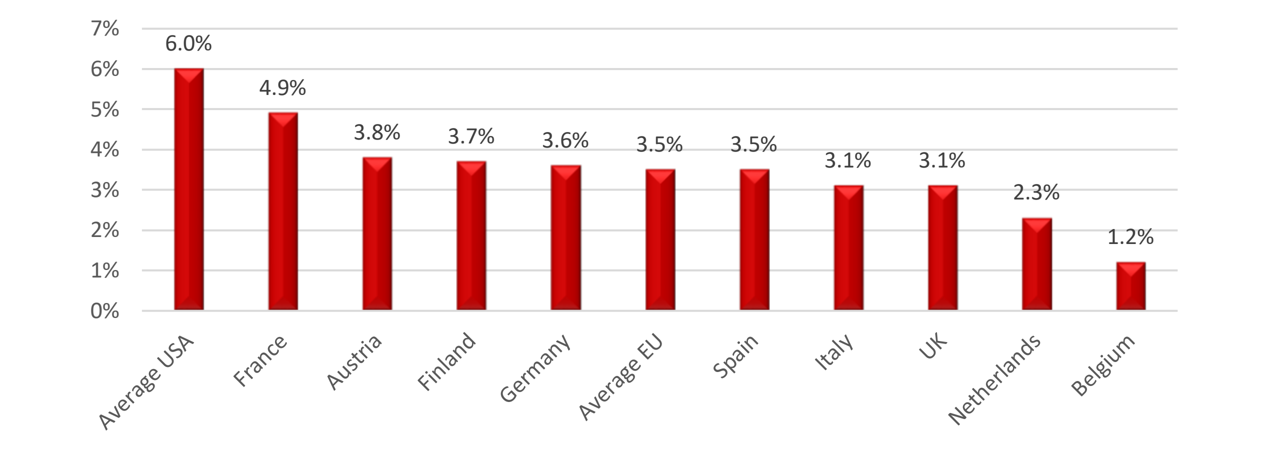


Source: Comparitech, 2020

The Covid-19 pandemic has created new opportunities for cybercriminals. For example, in April 2020, the Swiss National Cybersecurity Centre received 350 reports of cyber-attacks (phishing, fraudulent web sites, direct attacks on companies, etc.) compared to the usual 100-150. The pandemic and the increase in working from home were seen as a major cause of this, since individuals working at home do not enjoy the same level of protection as those in a working environment (e.g., internet security). This data highlights the need to increase investments in IT security. The "NIS Investments" report released by ENISA in December 2020 shows how the average

IT security spending of European organisations (in relation to the IT budget) is considerably lower than the average for US organisations. Looking at data released by ENISA (Fig.3), we can see that among European countries, the French organisations allocate the largest share of their IT budget to security.

Fig.3: IT security spending by organisations as a share of total IT budget by geography

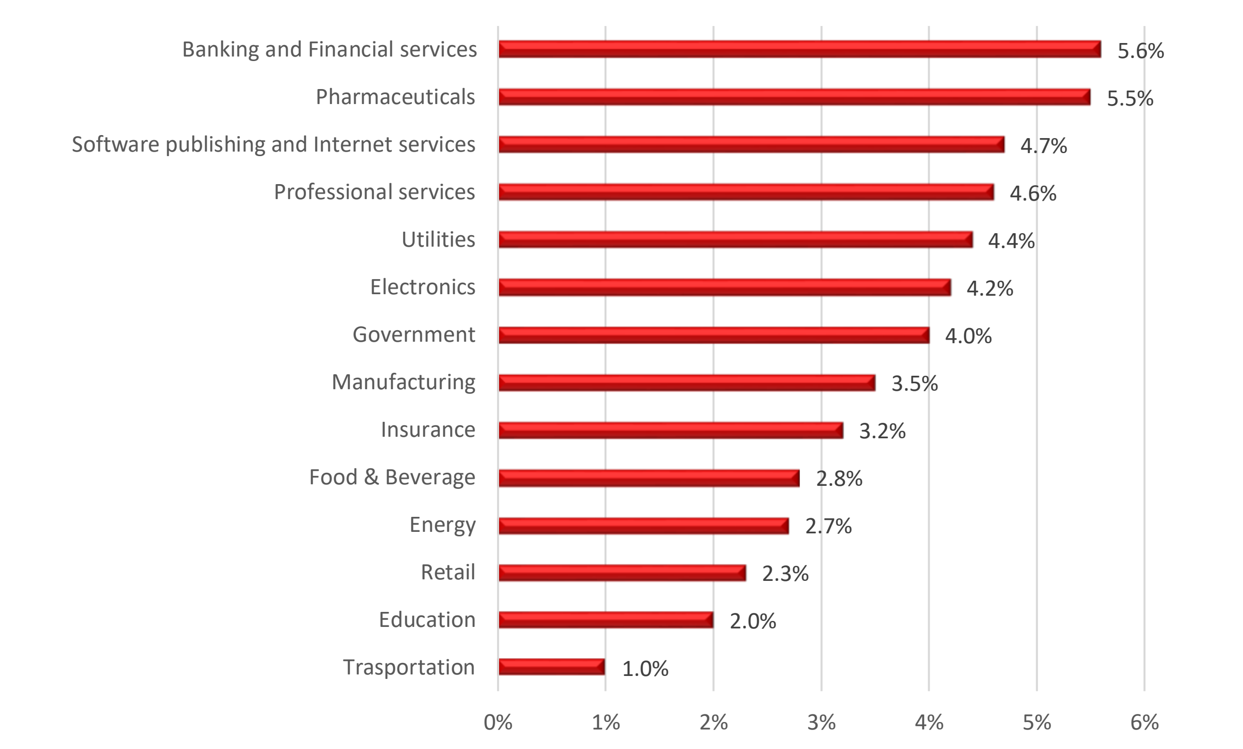


Source: ENISA, December 2020

The average **budget** invested by businesses for NIS Directive implementation projects is approximately €175,000, with 42.7% of affected organisations allocating between €100,000 and €250,000. The sectors in which the largest share of the IT security budget is invested (Fig.4) are in banking and financial services (5.6%), pharmaceuticals (5.5%) and software publishing and internet services (4.7%).

The **sectors** registering the worst performance are also two of the most important - education (2%) and transport (1%). Transport, especially with the spread of self-driving vehicles, could become increasingly targeted by cybercriminal attacks. The Commission is very aware of the need for further investments in the sector. Where the detection and deterrence of cybercrimes is concerned, the Commission has launched the **Cybersecurity Competence Centre** in Bucharest. Further investment opportunities are now expected from the Member States thanks to the EU **Recovery Fund** plan.

Fig.4: IT security spending by organisation as a share of total IT budget by industry



Source: ENISA, 12-2020

2. The European regulatory framework on cybersecurity

The digital transformation of society and the economy has led to the rise of new security issues. Since 2013, the EU has worked on a wide legislation on cybersecurity to be able to adequately face the challenges of digitalisation. The EU Cybersecurity Strategy of 2013 was adopted to safeguard the online environment providing security and freedom. It outlines the EU's vision and proposes actions aimed at pursuing cyber resilience, reducing cybercrime, developing an EU Cyber Defence Policy and fostering the industrial and technological resources required to benefit from the Digital Single Market.

Nevertheless, a significant step forward in the EU legislation on cybersecurity was seen in the **Directive on Security of Network and Information System** (the **NIS Directive**), adopted by the European Parliament on **6 July 2016**, entering into force in August 2016. Member States had to transpose the directive into national law by May 2018, following Art. 7 of the Directive itself, that explicitly identifies the leading principle for national strategies. Moreover, the directive encourages cooperation and the exchange of information among MSs by setting up a cooperation group made up of MS representatives, the European Commission and ENISA. The group is involved in the planning, guidance, signaling and sharing of the strategies. In addition, the Directive creates a network of agents active on security issues and identifies the security and notification requirements needed by digital service providers. On **25 June 2020**, the Commission launched the **public consultation for the revision of Directive 2016/1148** on measures for an EU common level of network and information systems security ("NIS Directive").

The launch of the public consultation (closed on 2 October) was in line with the periodic review of the NIS Directive, provided for in Article 23, to verify its functioning and application in the individual MSs. In order to keep up with the dynamic developments of the digital and technological environment, the review had to take place, as announced by the Commission and in line with the political objective of making "Europe fit for the digital age", by the end of 2020 prior to the May 2021 deadline set by the afore-mentioned article. On **16 December 2020** a proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive) was published.

Three main objectives are at the core of the new Directive: **a) Protect** - the Commission highlights the need for a full and harmonised implementation of the NIS Directive. Using a step-by-step approach, MSs must increase cooperation, and major importance is also given to the protection of public administrations and government agencies. Thanks to the introduction of new protective caps, the Commission reinforces accountability, making risk assessments of the whole supply chain possible through a comprehensive approach; **b) Detect** – with a current average of 6 months needed to detect cyber-attacks, the Commission aims at reinforcing SOCs (Security Operation Centres) by providing them with the latest technologies and equipment in order to drastically reduce detecting time; **c) Deter –** by federating information and strategies, the Commission aims at intensifying cooperation among MSs. Emphasis is also placed on collaboration with private sector companies and all other stakeholders, who are regarded as key players both in directly countering attacks and in building consumer trust. The acceleration in the usage rate of new digital devices caused by the Covid-19 pandemic has also highlighted the need for greater intervention in the deterrence of cyber-attacks on all IoT technologies. The Commission is therefore assessing the need for possible regulatory intervention such as the imposition of horizontal requirements.

The new Directive, specifically: a) expands the scope of the current NIS Directive by adding **new sectors** based on their criticality for the economy and society, and by introducing a clear size cap – meaning that all medium and large companies in selected sectors will be included in the scope; b) leaves some flexibility for MSs to identify smaller entities with a high security risk profile and **eliminates the distinction between operators of essential services and digital service providers -** entities would be classified based on their importance and divided respectively in essential and important categories with the consequence of being subjected to different supervisory regimes; c) **strengthens security requirements for the companies**, by imposing a risk management approach providing a minimum list of basic security elements that have to be applied and introducing more precise provisions on the process for incident reporting, content of the reports and timelines; d) sets **more stringent supervisory measures for national authorities**, stricter enforcement requirements and aims at harmonising sanctions regimes across MSs; e) enhances the **role of the Cooperation Group** in shaping strategic policy decisions on emerging technologies and new trends; f) increases **information sharing and cooperation** between MS authorities and enhances operational cooperation including on cyber crisis management; g) establishes a **basic framework with responsible key actors** on coordinated vulnerability disclosure for newly discovered vulnerabilities across the EU, creating an EU registry on that operated by the European Union Agency for Cybersecurity (ENISA).

With **Regulation 2019/881**, known as the **Cybersecurity Act**, the EU reached a political agreement to strengthen the **ENISA** and established a wide certification framework on digital products, services and processes. The first part of the regulation, specifically the first 45 articles, disciplines the mandate, resources and new tasks of the ENISA, while from article 46 on, it describes the certification framework for cybersecurity with the aim of building up a Single Digital Market. The ENISA must propose implementation acts that the Commission can adopt and must also evaluate each certification system every 5 years.

The regulation identifies a set of security requirements for the European certification systems, dividing them into three groups – basic, substantial and high - and basing the evaluation on the expected risk level associated with the use of the product, service or process in terms of impact and probability of the occurrence of product inconvenience and liability. It specifies the evaluation activities and the remedies for each category. Furthermore, it prescribes at the organizational level the identification of a national authority in each Member State.

In addition, the Cybersecurity Act establishes the **European Cybersecurity Certification Group** (ECCG), made up of representatives from national cybersecurity certification authorities or other relevant national authorities, to assist the Commission in its work to ensure the implementation and application of the act, being an advisor in the relations between the Commission and the ENISA.

By 28 June 2024, and then every 5 years, the Commission will have to evaluate the impact and effectiveness of the ENISA and its work, with the possibility to modify its mandate and subsequent financial implications.

The continually evolving digital environment requires the European system to be able to define and implement effective security standards in order to make the development of 5G networks possible. This is a core target as these networks are a key element for the internal market to evolve, especially for the effective management of core economic and social services, such as energy, transport, financial services, health systems and industrial controls.

On 26 March 2019, the Commission adopted **Recommendation 2019/534** on the cybersecurity of 5G networks, highlighting the risks for these networks and suggesting risk-analysis and management methods at the national level to be implemented within a coherent European context. For 5G networks, it identifies a clear roadmap that the MSs must follow to evaluate risks, updating the requirements for firms that provide public communication networks or public communication services. In order to achieve an effective prevention of and fight against threats, the document points out the importance of a **European coordination of the evaluation systems** and encourages **information sharing between MSs and the European institutions**, in order to reach a common awareness of the cybersecurity risks connected to 5G networks. Moreover, each MS had to communicate its national evaluations to the ENISA by 15 July 2019, in order to complete a specific map of the 5G environment in Europe. Finally, the recommendation encouraged MSs to cooperate with the Commission in evaluating the effects of the document itself by 10 October 2020.

Hence, consistent with the recommendation, the **NIS Cooperation Group** published a **EU-wide coordinated risk assessment of 5G network security**. This is a report that, starting from the respective MS's evaluations, identifies the most important threats and most dangerous agents, the sensitive resources, the main vulnerabilities and the different strategic dangers. The report also focuses on the innovations brought about by these networks and, as well, the role of providers in setting up and using 5G networks, and the degree of dependence from the single provider. It also stresses the importance of the implementation of a new security paradigm through the analysis of the current strategic framework. Moreover, in its conclusion of 3 December 2019, the Council sustained the remarks of the Cooperation Group, once again underlining the importance of a coherent approach to avoid market fragmentation.

On 29 January 2020, the Commission published the **Communication "Secure 5G deployment in the EU - Implementing the EU toolbox"** which took note of the absolute importance of 5G for many essential services and, therefore, the strategic need for the Union to ensure 5G network cybersecurity at a time when cyberattacks are both on the rise, more sophisticated and affecting a wide range of stakeholders. Under the NIS cooperation and following the completion of MSs' 5G network infrastructure risk assessment procedures, the NIS Cooperation Group published a EU-wide report on the coordinated cybersecurity risk assessment of these networks, identifying the most important threats and their main perpetrators, the most sensitive resources and major vulnerabilities (technical and other) affecting 5G networks.

On the same date, the NIS Cooperation Group published the EU's **package of instruments**, including risk mitigation measures. It deals with all the risks identified in the coordinated risk assessment report, identifying and describing a range of strategic and technical measures, as well as corresponding support actions aimed at strengthening their effectiveness, which can be implemented to mitigate the identified risks. The document, in highlighting how Europe is one of the most advanced regions in the world regarding the commercial launch of 5G services (by the end of 2020, the first 5G services should have been available in 138 European cities), takes stock of some of the areas where 5G will operate as an enabling factor for a number of important applications and, more specifically, in e-health, intelligent energy networks, future factories, media and entertainment and mobility.

The document's objective is to identify a possible common set of measures to **mitigate the main cybersecurity risks of 5G networks** (as identified in the EU-coordinated risk assessment report) and to provide **guidance in selecting the measures to be taken** so as to create a robust framework ensuring an adequate level of cybersecurity in the 5G networks across the EU and a coordinated MS approach.

The package's measures will contribute to achieving a number of important **safety objectives** necessary to address the risks identified in the risk assessment report and to protect the confidentiality, integrity and availability of 5G networks. These objectives are based on: a) strengthening security in the design, implementation and operation of networks; b) raising **basic safety standards** for product and service safety; c) minimising **exposure to the risks** arising from the risk profile of individual suppliers; d) avoiding or limiting the **main dependencies on a single provider** in 5G networks; and e) promoting a **diverse, competitive and sustainable market for 5G equipment**. The **package** identifies **8 strategic measures** and **11 technical measures** which are to be supported by a **number of actions** based on reviewing or developing network security guidelines and best practices, strengthening the testing and control capabilities at a national and European level, supporting standardisation, exchanging best practices on the implementation of strategic measures (especially, national disciplines for assessing the risk profile of suppliers), ensuring that public-funded 5G implementation projects take into account cybersecurity risks and ensuring the application of standard technical and organisational security measures through a specific European Certification Scheme. Paragraph 4.2 identifies **risk mitigation plans** for each of the nine risk areas identified in the EU-wide coordinated risk assessment report. These involve a combination of strategic and/or technical measures (along with appropriate support actions) that are classified into four levels, based on an assessment that considers risks to be faced and the persistent risks occurring after the application of the same measure. In conclusion, the toolbox calls on MSs to implement measures and obtain the necessary powers to mitigate risks, by strengthening security requirements for mobile network operators, assessing the risk profile of suppliers, and applying appropriate restrictions on suppliers considered to be high risk. The latter includes the necessary exclusions for critical assets, ensuring that each operator has an adequate multi-supplier strategy to avoid or limit any heavy dependence on a single supplier and avoid dependence on suppliers. The Commission expressed its willingness to continue to provide full support and take all relevant actions within its powers in order to support MS implementation of the package of tools and to strengthen its impact.

On **24 July 2020**, the NIS Cooperation Group, with the support of the Commission and the ENISA, published a **report on MSs' progress in implementing the 5G security toolbox**. It takes stock of the level of maturity reached by the various countries in the implementation of the measures contained in the toolbox and shows how, although all MSs have started to revise and strengthen their security measures in view of 5G, in some countries this work is still ongoing and, therefore, no final measures have yet been taken. At a general level, the report highlights that the three main risks identified are the incorrect configuration of networks, the lack of access control and state interference through the 5G supply chain. Regarding the latter, it highlights the belief, widespread among states, in the lack of adequate existing measures. Where the dependence on individual suppliers is concerned, the report highlights the need to understand the involvement of different suppliers in the individual elements of the network, the technical and operational difficulty of applying a multi-vendor strategy at certain points of the network, the limited number of 5G suppliers, the major critical issues for smaller countries, the possible effects on operators resulting from the formulation of diversified requests to suppliers and the need to identify specific regulatory bases that allow for imposing certain obligations on suppliers. Also interesting, are the considerations related to the implementation of measures to ensure the security of 5G networks. On this specific point, the document, after having defined the medium-low level of maturity reached in the implementation of such measures, describes a rather diversified panorama where, however, the request emerges from many MSs for a coordinated approach to EU standards. The deadline for MSs, in cooperation with the Commission, to determine whether further action is needed, expired on 1 October 2020.

On **16 December 2020**, the Commission launched several initiatives on security. Specifically, it adopted a proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive) already analysed above, a proposal of the directive on the resilience of critical entities (2020/0365 (COD), the new Cybersecurity Strategy and a report on the progress in implementing the EU 5G toolbox.

As a part of the Recovery Plan Communication "*Europe's moment: Repair and Prepare for the Next Generation*", the Commission published a **new Cybersecurity Strategy**. Starting from the consideration that transport, energy and health, telecommunications, finance, security, democratic processes, space and defence are heavily reliant on the network, and information systems are increasingly interconnected and these cross-sector interdependences increase vulnerabilities to cyberattacks, the Commission has launched a strategy focused on three pillars and connected initiatives: **1) resilience, technological sovereignty and leadership:** to achieve these the Commission proposes: a) the reform of EU rules on the security of Network and Information Systems (launched on the same data of new Cybersecurity Strategy); b) the constitution of a **network of Security Operations Centres** across the EU and the support for improving existing centres and the establishment of new ones to create collective knowledge and share best practices also supporting the training and skill development of staff operating these centres: c) the deployment - in 2021-

2027 - of **a secure quantum communication infrastructure (QCI)** for Europe able to offer public authorities a brand new way to transmit confidential information using an ultra-secure form of encryption to shield against cyberattacks, built with European technology; d) the adoption, under the Cybersecurity Act, of the **first Union Rolling Work Programme** in the first quarter of 2021 (to be updated at least once every three years) to provide incentives for safe products and services without compromising on performance and allow industry, national authorities and standardisation bodies to prepare in advance for future European cybersecurity certification schemes. The Commission also announced its willingness to consider a comprehensive approach, including possible new horizontal rules to improve the cybersecurity of all connected products and associated services placed on the Internal Market; e) the development of a **contingency plan**, supported by EU funding, for dealing with extreme scenarios affecting the integrity and availability of the global DNS root system; f) the support for the adoption of a **DNS resolution diversification strategy**, the development of a **public European DNS resolver service** and **the uptake of key internet standards** including IPv664 and well-established internet security standards and good practices for DNS, routing, and email security; g) the development of a dedicated **cybersecurity Masters programme**, and the definition of a **common European Cybersecurity Research and Innovation Roadmap** beyond 2020; h) the upskilling of the workforce, the development, attraction and retention of the best cybersecurity talent and investments in world class research and innovation; **2) building operational capacity to prevent, deter and respond:** several strategic initiatives to be implemented have been identified and, specifically: a) complete the **European cybersecurity crisis management framework** and determine the process, milestones and timeline for establishing the Joint Cyber Unit; b) continue implementation of **cybercrime agenda** under the Security Union Strategy; c) encourage and facilitate the establishment of a MS **cyber intelligence working group** residing within the EU INTCEN; d) advance the EU's **cyber deterrence posture** to prevent, discourage, deter and respond to malicious cyber activities; e) review the **Cyber Defence Policy Framework**; f) facilitate the development of an EU "**Military Vision and Strategy on Cyberspace as a Domain of Operations"** for CSDP military missions and operations; g) support **synergies** between civil, defence and space industries; h) reinforce cybersecurity of critical space infrastructures under the Space Programme; **3) advancing a global and open cyberspace:** the Commission underlines that the EU should: a) define a set of **objectives in international standardisation processes**, and promote these at international level; b) advance international security and stability in cyberspace, notably through the proposal by the EU and its MSs for a **Programme of Action to Advance Responsible State Behaviour in Cyberspace (PoA)** in the United Nations; c) offer practical guidance on the application of **human rights and fundamental freedoms in cyberspace**; d) better **protect children** against child sexual abuse and exploitation, as well as a Strategy on the Rights of the Child; d) strengthen and promote the **Budapest Convention on Cybercrime**, including through the work on the Second Additional Protocol to the Budapest Convention; e) expand EU **cyber dialogue with third countries**, **regional and international organisations**, including through an informal EU Cyber Diplomacy

Network; f) reinforce the **exchanges with the multi-stakeholder community**, notably by regular and structured exchanges with the private sector, academia and civil society; g) propose an EU **External Cyber Capacity Building Agenda** and an **EU Cyber Capacity Building Board**.

The strategy also underlines the importance to improve the overall level of cybersecurity through consistent and homogeneous rules announcing proposals for common binding rules on information security and on cybersecurity for all EU institutions, bodies and agencies in 2021, based on ongoing EU inter-institutional discussions on cybersecurity.

On the same day, with the support of EU Member States, the ENISA and the EU Agency for Cybersecurity, the Commission published a **report analysing the impact of the Commission's Recommendation of 26 March 2019 on the Cybersecurity of 5G networks and the progress made in implementing the EU toolbox of mitigating measures since the progress report of July 2020**. As a result of its review of the Recommendation, the Commission found that most MSs are well on track to implement a significant part of the measures recommended in the toolbox in the near future. The Commission also called on MSs to complete the implementation of these measures by the second quarter of 2021 and to ensure that identified risks will have been mitigated adequately and in a coordinated way, particularly in minimising exposure to high-risk suppliers and avoiding dependency on these suppliers.

Within this set of initiatives, there is also the adoption of the **Next Generation EU** allowing the Commission to contract, on behalf of the Union, loans on capital markets of up to €750 billion at 2018 prices. The EU commitment will be to use these loans for the sole purpose of dealing with the consequences of the Covid-19 emergency, and where cybersecurity is identified as one of its top priorities, in accordance with the position expressed by the Council on 9 June 2020. This was especially linked to the increased number of cyberattacks occurring during the lockdown, revealing the current IT system's vulnerability. Over the last weeks, there has been an extraordinary increase in malicious attacks from multiple sources, attempting to capitalise on the sudden digital disruption caused by the pandemic (millions of digitally unskilled people obliged to carry out activities on the Internet were exposed to threats). Furthermore, the crisis has also shown the need for a stronger industrial and technological presence in strategic parts of the digital supply chain, since the security of technology is emerging as a critical and central key-topic.

As well as the reinforcements financed under Next Generation EU, other programmes are focusing on making the Union more resilient and addressing challenges that have been heightened by the pandemic and its consequences. These include boosting the Union's cyber-defences and supporting the digital transition by equipping the **Digital Europe Programme** with a total budget of €8.2 billion.

Conclusions

The massive use of smart working and distance learning and the greater use of digital services, accelerated by the Covid-19 pandemic, has increased exposure to possible attacks, underlining the urgency to strengthen the existing set of rules able to guarantee a secure digital ecosystem. Starting from the consideration that transport, energy, health, telecommunications, finance, security, democratic processes, space and defense are heavily reliant on the network, and information systems are increasingly interconnected and these cross-sector interdependences increase vulnerabilities to cyber-attacks, the Commission has launched a new security strategy focused on three pillars and connected initiatives. These will increase the level of cyber resilience of critical public and private sectors, encourage the upskilling of the workforce, attract and retain the best cybersecurity talent, strengthen cooperation between EU bodies and MS authorities responsible for preventing, deterring and responding to cyber-attacks and step up work with international partners to strengthen the rules-based global order, promoting international security and stability in cyberspace, and protecting human rights and fundamental freedoms online.

Although the individual initiatives that the Commission will adopt in the coming months to pursue the objectives set out in the strategy will be fundamental to its implementation, the initial assessment is certainly positive.

Indeed, the strategy aims, on the one hand, to encourage the acquisition - especially in small and medium-sized enterprises - of the skills necessary to prevent and counter possible attacks and criticalities and, on the other hand, to pursue the objective of strengthening the coordination and cooperation tools essential to create a unitary European ecosystem, harmonised and able to ensure a high standard of security.

The Commission has also presented a legislative proposal to update the NIS Directive (which could be identified as "NIS 2") to achieve a higher common level of cybersecurity across the Union and a new Critical Entity Resilience Directive covering a wide range of sectors. Both new directives aim to address current and future risks both online and offline - from cyber-attacks to crime or natural disasters - in a consistent and complementary manner. The proposed reform of the rules on the security of network and information systems pursues the objective of overcoming the existing regulatory fragmentation (in relation, for example, to the identification of the operators of essential services), extending the scope of application to include parties operating in sectors that are not currently covered by current regulations (such as aerospace, waste management, and food manufacturing) and increasing the level of cyber resilience of critical public and private sectors. These include hospitals, energy networks, railways, and also data centres, public administrations, research laboratories and the production of medical devices and critical medicines, as well as other critical infrastructures and services with the aim of increasing their security in an increasingly rapid and complex threat environment.

The new European Cybersecurity Strategy and the proposals described are an extremely important development to strengthen Europe's collective resilience against cyber threats, encourage the harmonisation of national regulatory frameworks and help reinforce the regulatory ecosystem in which all citizens and businesses can fully benefit from secure digital services and tools.

The strengthening of the IT security strategy of the Member States is also highly important in view of the development of 5G networks. As a key technology to enhance global cooperation and boost economic progress, 5G can be fundamental in helping reduce the digital divide, fostering innovation and allowing different actors to access markets. As 5G networks are becoming the backbone of many critical applications, their integrity and availability are per se a major security concern. The Commission's Recommendation on the cybersecurity of 5G networks (March 2019) highlighted the risks for these networks and suggested risk-analysis and management methods at the national level to be implemented within a coherent European context. Important findings from the EU coordinated risk assessment pointed out that 5G can cause an increase in the overall attack surface and, thus, the potential entry points for external attacks and, as well, certain pieces of equipment, such as key technical management functions, may also become more sensitive. For this reason, it is essential to adapt measures in order to create a solid framework that guarantees an adequate level of cybersecurity in 5G networks across the EU and a coordinated approach by Member States.